WHITE PAPER

What you should know to assure laboratory data integrity with LabSolutions

In order to assure data integrity in life sciences industry laboratories it is necessary to address procedural, behavioural and technical controls. While it is regulated companies who are accountable for data integrity within their organisations, both regulated companies and laboratory instruments and their data management suppliers must be responsible for ensuring that all aspects of compliance are addressed.

In this white paper, Shimadzu outline the controls that are needed to address data integrity in the laboratory, provide an overview of the procedural and behavioural issues that must be addressed and explain how Shimadzu fulfil their responsibilities for technical compliance with regulatory requirements for data integrity through the use of their LabSolutions CS analysis data management system

Current regulatory position (regulatory concerns, inspections, common findings and enforcement actions)

Although there is currently a significant industry focus on data integrity within the pharmaceutical and wider life sciences industry, this is not a new issue. In order to appropriately respond to recent regulatory guidance[1] on data integrity it is important that regulated companies place more recent enforcement actions in an appropriate context and do not over-react to the fear, uncertainty and doubt which is being generated in some quarters.

In the 1980s and 1990s, data integrity was already an issue of concern for regulatory authorities. However, the focus was very much on the integrity of data within automated process and equipment control systems, many of which were custom developed or customized. During the mid to late 1990s the focus shifted to the use of electronic signatures within the industry, leading the US FDA to promulgate US 21CFR Part 11, Electronic Records, Electronic Signatures.

Confusion over the scope and enforcement of 21CFR Part 11 shifted the focus away from a broader consideration of data integrity concerns and it can be argued that the focus should never have shifted away from a broader consideration of data integrity.

Publish Date:
26 March 2019

Authors:
Hiroomi Nishimura

IT Solution Business Unit,
Analytical & measuring Instrument Division,
Shimadzu Corporation

[1] UK "'GXP' Data Integrity Guidance and Definitions", March 2018
US FDA "Data Integrity and Compliance with Drug CGMP" Data Integrity and Compliance with Drug CGMP, December 2018
WHO "Guidance on good data and record management practices", Part of Technical Report 996, May 2016
PIC/S DRAFT "GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED GMP/GDP ENVIRONMENTS", November 2018

More recently, with greater focus on so-called 'overseas' inspections (specifically in India and China, with the establishment of FDA offices in those countries), regulatory agencies have become aware of a number of data integrity issues. These have included many examples where genuine mistakes have been made, where data has certainly been falsified and examples of where some regulated companies have almost certainly attempted to commit fraud. These have been so significant that the quality of products and the safety of patients could not be reasonably assured by regulatory authorities.

This issue for those regulated companies who consider themselves to be above such malpractice is that until appropriate data integrity is convincingly established, it is difficult to tell companies apart based upon evidential inspections. This means that all regulated companies must take data integrity seriously, regardless of current practices or previous inspection history.

A number of these inspections and findings have focused in Good Manufacturing Practice (GMP) Quality Assurance (QA) laboratories, with a focus on associated instruments and Laboratory Information Management Systems (LIMS). Examples of these inspection findings are provided, and enforcement actions have included FDA Warning Letters and import restrictions, but it should be noted that:

- These findings have not been limited to Asia – other routine inspections in Europe and the USA have also uncovered similar data integrity issues.
- It is not just the USA FDA who are focusing on data integrity – European regulatory agencies, other national regulatory agencies and also the World Health Organisation have been focusing on these topics.
- Data integrity is not just an issue within the QA laboratory or the wider GMP domain, but is a wider topic that applies in all areas of a regulated business.

Note that in some cases, regulators have established clear deadlines for establishing specific data integrity controls (e.g. UK MHRA) and this white paper does not seek to address specific regulatory topics or individual deadlines for compliance.

As often happens when regulatory authorities focus on a specific topic, there has been a good deal of immediate response from within the industry, with many new books being published and conferences being organised. This has led to 'fear, uncertainty and doubt' on the part of some regulated companies, who need to exhibit a mature and considered approach to addressing data integrity.

Behind the scenes organisations such as ISPE and their GAMP Community of Practice have been developing a more considered risk based approach to data integrity, including data integrity associated with the use of laboratory instruments and systems.

While regulated companies do need to address any concerns with respect to the use of laboratory instruments and systems, this needs to be part of an organisation wide approach to data integrity outlined in the recent ISPE GAMP Records and Data Integrity Guide[2].

The remainder of this white paper looks at this broader context and provides specific guidance on assuring data integrity in the use of laboratory instruments and systems, including how the features and functions of Shimadzu's instruments and LabSolutions CS software support data integrity and electronic records compliance in the laboratory.

[2] GAMP Guide: Records & Data Integrity, March 2017, available from www.ispe.org

Cultural and Organisation Aspects in Assuring Data Integrity

In many recent regulatory inspections, there have been two key factors that have undermined data integrity. These are:

- Lack of technical controls, which allow:
  - Data integrity to be compromised,
  - Data integrity breaches to go undetected,
- Lack of procedural controls and a poor data integrity culture, leading to falsification and fraud.

The provision and implementation of technical controls at the instrument and software level are covered in detail below. This includes an overview of how LabSolutions CS analysis data management software meets the regulatory requirements for electronic record/electronic signature and data integrity controls.

However, the lack of procedural controls and a lack of data integrity culture within an organisation is a key factor which cannot be overlooked. These are probably more important issues across the broader organisation as they impact on data integrity across the whole organisation and not just within the laboratory.

In many recent inspections a common theme is that individuals have falsified data and this has not been detected by senior management. While poor technical controls mean that data falsification is possible and is harder to detect, it is important to realise that senior management will only detect data falsification (or accidental alteration or deletion) if they actively look for such falsification (or errors).

While the technical controls available in LabSolutions CS can significantly reduce the extent of data falsification and make such falsification easier to detect, even the best software cannot prevent this entirely. It is for instance impossible to prevent laboratory technicians or system operators from entering falsified data into an instrument or system which is within an expected and allowable range – the software has no way of knowing whether a single item of data is falsified or not. It is therefore essential that senior management put in place a data governance programme to address the cultural and organisational issues that can lead to data falsification.

In some cases, falsification has taken place because senior management place undue pressure on staff to complete analyses in impossible timescales. In other cases senior management have turned a ‘blind eye’ to such issues when it allows batches of product to be shipped on time.

In some cases, there is a high likelihood that senior management have been complicit in the falsification of data and have either encouraged such falsification or have instructed that it should take place. These fraudulent acts have in some cases been so widespread that the quality of product and safety of patients cannot be assured.

The majority of inspections relating to data integrity have related to issues in the QA laboratory. In many cases instruments have been used to conduct duplicate or trial analytical runs prior to an ‘official’ run being performed. In many cases these trial runs have been used to adjust the analytical method (e.g. by changing and falsifying the weight of the sample being analysed, or by manually changing integration parameters or missing or adding steps to the analytical sequence) and in one case a ‘shadow’ QA lab was discovered to perform such ‘trial runs’ before the official QA laboratory performed the initial analysis.

In other cases, data providing out of specification results has been deliberately deleted, data from an analytical run which is within specification has been copied over data from another batch which was out of specification or operators have deliberately interrupted an analytical run once they see that the results will be out of specification e.g. by disconnecting data cables or adjusting parameters partway through the run, to provide a ‘reason’ for the analytical results being discounted.

While many of these issues have occurred in the QA laboratory, data integrity is a much wider organisational issue and the fact that such practices could routinely take place in large laboratories demonstrates that these issues go beyond simple data falsification by individuals, and at least suggests systematic fraudulent practices and collusion by senior management.

While many responsible managers would claim that these issues could never happen in their own organisation, the relatively widespread abuse of established principles now means that it not sufficient to state that it has not happened in the past and would not happen in the future. All responsible organisations now need to establish a data governance and data integrity programme to provide a high degree of assurance that the falsification or fraudulent manipulation of data cannot happen, and if it did happen, it would be detected and addressed.

Key to this is establishing the right culture in which data falsification cannot take place. This means that:

- Investments are made in technical and procedural controls, to make data falsification almost impossible and easily detectable
- Staff (including data stewards and data owners) feel free to voice concerns over data integrity, without fear of punishment or reprisal
- Senior management are truly accountable for data integrity
- Competence is built up within the organisation that makes the need for data falsification redundant

Unless these organisational and cultural issues are addressed, and unless regulated companies can demonstrate that the integrity of data is built upon the solid foundations of a well thought out approach to assuring data integrity, technical controls and even the best software controls will be insufficient to meet regulatory expectations.

The GAMP Records and Data Integrity Guide provides regulated companies with guidance on how to address organisational compliance issues associated with both electronic records & signatures as well as broader data integrity. This includes:

- Data Governance frameworks
- The data life cycle
- Quality risk management in the context of data and records
- Establishing a Corporate Data Integrity Programme
- Use of Data Integrity Maturity Models
- Human factors
- Data Auditing and Periodic Review
- Inspection Readiness
- Integrating data integrity to existing records management processes

The content of this recent ISPE/GAMP guide will form the basis for the data governance and data integrity assurance processes for many regulated companies and will become increasing recognised by various regulatory authorities.

It is therefore recommended that these issues are addressed at the same time as technical issues are reviewed and addressed, and for laboratory instruments and systems the following key organisation issues need to be considered.

Training of Users

All users of laboratory instruments and systems must be appropriately trained on how to adhere to applicable standard operating procedures (SOPs). This training should not only address everyday laboratory and data processing operations, but should also address general regulatory and organisation expectations and specific data integrity and information security controls.

Users should be expected to verify the effectiveness of this training after a period of supervision as ‘read and understood’ confirmation of having simply read an SOP is generally insufficient to confirm that a user really knows what they are doing.

Training of System Administrators and Segregation of Duties

In a similar manner, those responsible for supporting, maintaining and calibrating instruments and for administering data management systems should also be trained with respect to their specific responsibilities. Because such ‘system administrators’ often have elevated privileges there is a higher likelihood of data being accidentally or deliberately being deleted or modified and the importance of effective information security and data integrity training is even greater.

Historically, a ‘super user’ in the laboratory has been made responsible for such maintenance and support, but this can introduce a conflict of interest where the same person is responsible for analytical or data processing operations, but through administrator privileges also has the ability to turn off audit trails and delete data.

In most cases, a segregation of duties through a careful analysis of roles and privileges should ensure that no individual has the permissions to use and administer an instrument or system. Only where other controls are known and have been verified to be fully effective in detecting such data falsification should combine these roles be allowed.

Data lifecycle modelling

In order to identify electronic record and data integrity risks, data lifecycles should be modelled. This should initially be at a high level, using the laboratory business processes and analytical sequences to identify the lifecycle of the data (and meta data). Such modelling should identify the operations performed on the data, who performs such operations, the associated risks to data integrity and controls required including the possibility of not utilising the option to delete data although the system might permit it.

In most cases, this modelling can be restricted to a high level overview of the data lifecycle and can leverage any such data life cycle modelling performed by the instrument or data management vendor in the establishment of their in-built electronic record and data integrity controls.

However, where regulated companies are performing non-standard activities (such as validating a new analytical method, integrating instruments and data management software from different vendors or using general IT infrastructure to manage data), it may be useful to perform a more detailed data lifecycle

modelling activity, identifying each detailed step in the lifecycle to be able to identify and mitigate specific or unusual risks.

Key principles of Data Integrity with respect to Laboratory Systems

While organisational and cultural issues must be addressed, customers must also ensure that appropriate technical controls are established to assure data integrity and comply with electronic record and signature requirements.

Within the laboratory this requires the use of instruments and systems that are capable of complying with current data integrity expectations and more importantly, that are configured in such a manner to enforce data integrity controls. As described below, Shimadzu's LabSolutions CS analysis data management software provides comprehensive functionality for assuring data integrity and for complying with electronic record and electronic signature controls.

There are also additional, broader aspects of technical compliance that also need to be addressed and these are summarised below.

- **Instrument Qualification**

Laboratory instruments should be qualified before use. This is usually achieved through a process of Installation Qualification (IQ – to ensure that the instrument is installed and set up correctly) and Operational Qualification (OQ – to ensure that the instrument can perform in accordance with the vendors published specifications).

This is usually achieved by executing IQ and OQ scripts or protocols which are usually provided by the vendor. These may either be executed by the regulated company or a qualified third-party, or using professional services provided by the vendor or their agents.

With respect to data integrity it is essential that these scripts verify that the instrument can be configured in such a manner as to leverage the built-in data integrity features and controls, and that these controls cannot be disabled in everyday use. This is because many instruments are used across a broad set of industries, many of which do not require such extensive data integrity controls to be in place. For this reason, such controls are optional and it is essential to ensure that the controls are applied correctly and securely.

- **IT Infrastructure qualification, including system backup and data archiving**

Laboratory instruments must obviously be qualified, but in addition to this any supporting IT infrastructure should be qualified. This will include the IT infrastructure used to host any data management systems or LIMS, including servers (physical or virtual), network storage, and any active or passive network components such as bridges and switches and structured cabling that make up the local area network (physical or virtual LAN). Where wide area networks (WANs) are used to connect remote locations to central systems, these should also be qualified.

Any suppliers used to provision such infrastructure (including Infrastructure as a Service [IaaS] cloud service providers) should also be appropriately assessed/audited to ensure that an equivalent level of infrastructure controls are in place.

This should also be extended to the infrastructure and services used to perform system backup and restore and any data archiving processes and such qualification should include suitable risk based functional and performance testing.

- **General Information Security Controls**

A good deal of electronic records and data integrity compliance is based upon effective information security controls. While simply implementing information security controls will not be sufficient to address regulatory expectations, they do form a sound base upon which other electronic records and data integrity compliance can be built.

While formal registration to a standard such as ISO 27001[3] is not essential, implementing applicable controls from this standard (and the more than a dozen related standards) can help regulated companies to ensure that they have established appropriate risk based controls that can assure the basic security of records and data. While this will not prevent the fraudulent entry of data, the implementation of basic information security controls does help address data integrity issues such as accidental deletion, lack of availability, corruption etc.

[3] ISO/IEC 27001:2013Information technology -- Security techniques -- Information security management systems -- Requirements

Compliant Laboratory Data Management

While general IT controls need to be established, LabSolutions CS provide comprehensive functionality to assure data integrity. The broad nature of these controls allow a compliant data management environment to be quickly and easily established whether working with a small number of instruments within a single laboratory or whether working with multiple instruments across a large number of laboratories.

This also includes the ability to:

- Manage additional, non-analytical instruments in a compliant manner (e.g. balances / weigh scales)
- Capture additional laboratory data in a compliant and integrated manner
- Integrate common third-party instruments from multiple vendors into a single compliant data management environment.

LabSolutions CS provides multiple features and functions which support such data integrity and electronic records/electronic signatures compliance. These general features are described below, and specific features are mapped against 21CFR Part 11 (Electronic Records, Electronic Signatures), EU Eudralex 4 Annex 11 / PIC/S PI001-3 Computerised Systems and data integrity ALCOA+ requirements in the tables below.

Software and Analytical Methods Validation

In addition to instrument and IT infrastructure qualification, instrument or data management system software should be appropriately validated. Risk-based validation can leverage the activities and documentation of the vendor to reduce the scope of such validation, but regulated companies are accountable for ensuring that software is capable of meeting their specific requirements in a reliable and repeatable manner.

While the basic operation of an instrument may be verified as part of OQ, user specific requirements are usually validated as part of Performance Qualification (PQ), which verifies that the software is capable of meeting the specific requirements of the regulated company when using a validated analytical method in the context of a defined set of laboratory processes (sequence).

In most cases, IQ and OQ will be performed and the software associated with a specific instrument and data management system will be validated in detail. Once the initial instrument is qualified and the broad functionality of the software validated, analytical methods will then be validated to demonstrate that a qualified instrument and validated software is capable of repeatably producing expected results following a defined sequence of events and analytical techniques. Such validation records can be recorded in the LabSolutions CS database, providing clear evidence of analytical methods being appropriately validated.

Once an analytical method has been validated, it can then be used on identical (or similar) instruments through the transfer of the analytical method, as long as each instrument is qualified (IQ and OQ) and the base software and configuration is identical.

Good data integrity controls require that once an analytical method is validated, it should not be possible for users to change the method (e.g. the sequence of activities, controlled variables or data processing steps) in normal operation. LabSolutions CS ensures that it is either not possible to make changes to validated analytical methods in e.g. GMP QA laboratories, or that where it may be necessary to adjust measurement or processing parameters during QA analysis, all changes are audit trailed with reasons required for making any such adjustments.

Every regulated company should define the processes by which the qualification of instruments, validation of software and validation of analytical methods are performed, and how those processes are interrelated with respect to dependencies and pre-requisites.

Key Data Integrity Features

In order to ensure data integrity, it is important that laboratory instruments and data processing systems have the features and functions to support data integrity expectations. While many of these appear obvious and basic, these are not always available on instruments and in software from vendors who do not specialise in the life sciences market.

In other cases, it is only later versions of equipment and software that support these features and it may be necessary for regulated companies to replace instruments and/or upgrade software in order to assure compliance with data integrity expectations.

It is however worth noting that based upon a well-documented data life cycle model and risk assessment, it may be possible to establish effective procedural controls on an interim basis, allowing investment in replacements or upgrades to be planned and prioritised on the basis of risk.

In additional to basic information security controls, the following are key features which need to be understood and effectively established. Where such features and controls are available it is essential that

they are configured and verified following an effective IQ process.

User access permissions

As described above, it is important that the rights and permissions of users and system administrators should be segregated to ensure that there is no conflict of interest with respect to what any single individual is allowed to do.

This requires that instruments and systems are able to define and enforce permissions for specific groups of users i.e. Users, Supervisors, Quality Assurance etc.

Individuals should be assigned to user groups with predefined permissions and checks will be implemented to ensure that no single person has a conflict of interest e.g. is not a User and a System Administrator, or is not a Supervisor and a QA user.

Where possible, it is useful if instruments and systems can leverage organisation level groups through integration with e.g. Microsoft Active Directory (whose integration with LabSolutions CS is supported). In these cases, User IDs (and passwords) and business process based user groups can be managed at the organisational level, thereby reducing the overhead of separately managing users and groups within the data management system. However, even where this is possible, the system specific permissions associated with each user group still need to be defined and managed within the data management software.

Where it is not possible to leverage organisational authentication services, individual users and appropriate user groups will need to be established and setup within the database management software.

Ideally such conflicts of interest can be pre-defined and the software would be able to identify any such breach in segregated duties. However, in most cases this requires checking whenever permissions are changed and should be subject to risk-based periodic review.

For older or simpler instruments such group based permissions may not be available and procedural controls will need to be established. These are likely to be expensive to maintain and likely to break down over time and the use of such procedural controls should only be seen as a temporary control.

LabSolutions CS provides comprehensive features for defining and managing user groups and associated permissions and for assigning individuals to such groups. Changes to user permissions are retained in the software audit trail and there are extensive, configurable password and account management rules which allow regulated companies user access controls to be reflected in the laboratory.

Laboratory Data Management and Standalone Instruments

Modern laboratory data management systems no longer maintain data in separate unrelated files, but tie associated datasets together as part of a related database, often using the capabilities of relational databases to link and index data. This makes it much more difficult to manipulate individual datasets without either leaving evidence in an audit trail or breaking the referential integrity of the relational database, and this is the approach taken by LabSolutions CS where all applicable data is collated in a defined, secure record set e.g. related to a batch analysis.

While this could be defeated by careful falsification of linking data values, related meta data values (e.g, timestamps) and database indexes, this is beyond the ability of most laboratory operators (even if they have permissions to do so). Even a database administrator is unlikely to sufficiently understand the complexity and consistency of the vendor's relational database model and also understand the context of the analytical data to flawlessly attempt such comprehensive falsification.

However, in many cases standalone instruments do exist and do not have the ability to store and link such comprehensive information and the use of standalone instruments outside the context of a laboratory data management system is increasingly seen as a data integrity risk.

This is because even where standalone instruments have a computer system attached (e.g. a desktop PC), in many cases the relatively simple file storage system used is easier to manipulate. In other cases, the limited storage capacity (when compared to regulatory data retention periods which can extend to decades) forces users to delete older data to continue analytical operations.

For many standalone instruments there is also the issue that it is not possible to prevent the operator from making changes to the analytical method – it is not possible (certainly on many older instruments, or instruments with older versions of software) to lock out the control panel to prevent such unauthorised changes being made. It is also the case that many standalone instruments have little or no audit trail capability nor practical organisational hierarchy controls to detect when such changes have been made.

Regulators are increasing seeing and reporting standalone instruments as a risk to data integrity and a relatively easy target during regulatory inspections. The use of comprehensive laboratory data management solutions as seen as the 'gold standard' with the ability to:

- Manage interfaces to multiple instruments (including relatively simple instruments such as laboratory balances),
- Remotely operate analytical instruments in accordance with a defined and controlled analytical method, locking out the ability to make changes via the instrument front panel
- Define, manage and audit trail all data (raw data, analytical methods, metadata, results, reports etc) from multiple instruments as part of single analytical dataset, including the ability to capture manually entered data in a defined, structured manner which is capable of minimising data entry errors.

Such systems, when correctly configured, provide a significantly higher assurance of data integrity when compared to the use of standalone instruments. The use of LabSolutions CS means that all associated data (raw data, results, reports, audit trails, validation of the analytical method, allowable changes to measurement or processing parameters etc) is tied to the analysis and is available for human readable review through various event viewers.

Audit trails

While mandatory for electronic records, audit trails should be established for all important data and metadata. This should include instrument raw data which usually needs to be retained to allow subsequent reprocessing, but should also be extended to critical datasets and files such as

- Analytical methods and sequences (both changes to validated analytical methods and changes made to methods or sequences during an analytical run, where permitted)
- Report templates
- User Groups and permissions.
- Results data

Audit trails should capture:

- What data / meta data has been created, changed or deleted, including the old value(s) and new value(s)
- When the data / meta data was created, changed or deleted
- Who created, changed or deleted the data / metadata (traceable to a uniquely and legally identifiable person)
- Why the data / metadata was changed. This may be implicit because of the nature of the operation (i.e. a specific step in an analytical method) or may require the user to enter a reason.

Such audit trails need to be automatically generated and it should not be possible for users to turn off such audit trails. Preferably, even system administrators should not be able to disable audit trails, especially for GMP related activities.

Audit trails associated with records subject to routine review (e.g. batch records) should be easily available to be reviewed as part of the record. This is to identify any authorised or unauthorised changes to the data as part of the record review. Such audit trails must be easily human readable and should be retained for as long as the record to which they relate. All of these comprehensive audit trail features are available in LabSolutions CS, ensuring full traceability of every analytical run. It has been recently suggested that such review of audit trails be made mandatory by departments such as QA before accepting results. The practicality of such requirements remains a subject of debate within the industry.

Other audit trails should be reviewed on a periodic or risk-based basis, to identify any data integrity issues and to support any quality or data integrity investigations. These audit trails should be retained at a minimum as determined by risk assessment and should be human readable. Where this is not the case, controlled methods (data base queries or reports) should be developed to facilitate the review of such audit trails.

Where instruments and systems do not have such audit trail capability, procedural controls may be established. These are likely to require extensive and time-consuming change control processes and such controls should again be used only as a temporary measure. The use and acceptability of such strategies will be dependent on the risk assessment and criticality of the tests and operations being carried out and can only be a used as an interim measure.

Record / file locking and signatures

Not all data is considered a record (as defined by US 21CFR Part 11 Scope and Application guidance[4]), but where data is considered an electronic record (or is part of such a record), additional and specific controls are required to comply with US 21CFR Part 11[5].

Based upon a documented data life cycle model and risk assessment, it may also be applicable to apply such controls to data which is not strictly considered as an electronic record.

[4] US FDA Guidance for Industry: Part 11, Electronic Records; Electronic Signatures — Scope and Application, August 2003
[5] US Code of Federal Regulations, Chapter 21, Part 11—Electronic Records; Electronic Signatures

All such records and files should be secured using good information security practices and should have audit trails applied.

Where such records (or datasets) are signed, applicable electronic/digital signature controls should be applied. Where there is any doubt as to the scope or security of audit trails, digital signatures should be used to allow any unauthorised changes to the record (or dataset) to be detected.

- **Forensic data analysis**

Regulators are increasing requesting access to databases to be able to analyse datasets. This is in order to identify any data integrity issues. Forensic data analysis techniques can be employed to detect likely falsified data (human beings find it extremely difficult to generate truly random datasets which match the data patterns which occur as a result of a truly random or pseudo random analytical processes, and these differences can be detected) or to identify cases where data from one analysis may have simply have been copied to another record.

While good data integrity controls should effectively prevent such measures, vendors are increasing developing software to allow users to proactively search for, or to allow the software to automatically highlight and suspect data. While this is not yet a common feature on laboratory instruments it is something that should be employed in data management systems where available.

It is also possible to perform orthogonal data review, which looks for data anomalies across multiple data sets. Examples might be checking the date and time stamps on data from different laboratory instruments, to confirm that the time stamps reflect the analytical sequence and timing associated with the approved analytical method. This can easily be achieved using the data from most mature laboratory data management systems

This concept can be extended to include data from other systems e.g. do the time stamps from the manufacturing systems and the ERP system which releases the batch align with data from the laboratory and does the time and attendance system confirm that a laboratory supervisor who approved results was actually on-shift at the time the results were approved.

While these techniques cannot be applied for the review and approval of every set of results and every batch, such techniques can be used as part of periodic data integrity audits.

Shimadzu Regulatory Compliance Analysis

Supplier Responsibilities

As a responsible supplier to the life sciences industry, Shimadzu understand and fulfil our responsibilities for developing, supplying and supporting products to assure technical compliance with data integrity, electronic record & signature and other regulatory requirements. At an organisational level Shimadzu:

- Develop, supply and support mature products with appropriate technical controls to address all aspects of regulatory compliance
- Assure, as far as is practically possible, backward and forward compatibility across different software versions, for the availability and readability of complete laboratory data throughout regulatory retention periods
- Provide flexibility around instrument and data management software architecture and hardware support, to support a wide range of solutions including on-premises installations, the use of dedicated physical servers and virtualization and the use of off-premise Infrastructure as a Service installation
- Are open and transparent with customers regarding potential regulatory issues with respect to legacy instruments and software and support customers to implement appropriate procedural and behavioural controls as well as upgrades
- Are committed to maintain a detailed understanding of the regulatory environment within which our life sciences customers operate
- Are commitment to providing product support and upgrades to keep pace with the evolving regulatory expectations, including data integrity

US FDA Warning Letter Excerpts (2012 – 2017)

“Your firm has failed to exercise appropriate controls over computer or related systems to assure that changes in master production and control records, or other records, are instituted only by authorized personnel.”

“Your firm did not put in place requirements for appropriate usernames and passwords to allow appropriate control over data collected by your firm's computerized systems including UV, IR, HPLC, and GC instruments. All employees in your firm used the same username and password. In addition, you did not document the changes made to the software or data stored by the instrument”

“Your firm had no system in place to ensure appropriate backup of electronic raw data and no standard procedure for naming and saving data for retrieval at a later date“

“You have not implemented security control of laboratory electronic data. All laboratory analysts share the same password for the HPLCs in the QC analytical chemistry lab and Omnilog in the microbiology lab. In addition, analysts have access to the HPLCs which allow them to create and/or modify validated methods”

“Your firm’s “Jasco LC-Net II” HPLC instruments do not have restrictions in place to prevent any change or deletion of analytical raw data. Additionally, there is no audit trail in place to determine any previous deletion of raw data”

“The inspection documented that all of your QC laboratory computerized instruments (HPLCs) were found to be stand-alone, and laboratory personnel demonstrated that they can delete electronic raw data files from the local hard drive.”

“Your firm deleted multiple HPLC data files acquired in 2013 allegedly to clear up hard drive space without creating back-ups. Your QC management confirmed that there is no audit trail or other traceability in the operating system to document the deletion activity. Furthermore, your analysts do not have unique user names and passwords for the computer and laboratory information systems; your QC analysts use a single shared user identifier and password to access and manipulate multiple stand-alone systems”

“While reviewing gas chromatography data on instrument QA/G07, our investigator found unreported results, including an out-of-specification (OOS) test result for raw materials. You did not investigate this OOS result or explain why you excluded the failing result from the official record”

““The inspection of your facility documented multiple incidents of performing "trial" testing of samples, disregarding test results, and reporting only those results from additional tests conducted.”

“Your firm failed to have adequate procedures for the use of computerized systems in the quality control (QC) laboratory. Our inspection team found that current computer users in the laboratory were able to delete data from analyses. Notably, we also found that the audit trail function for the gas chromatograph (GC) and the X-Ray Diffraction (XRD) systems was disabled at the time of the inspection. Therefore, your firm lacks records for the acquisition, or modification, of laboratory data”

“Multiple analysts, testing multiple drugs, deleted unknown peaks without justification. These manipulations made the drugs appear to meet their specifications. Of concern, one of these unknown peaks was for a residual solvent known to be a genotoxic impurity.”

Part 11 Subparts

The following table shows how regulated companies, supported by Shimadzu, can comply with the requirements of US 21CFR Part 11 (Electronic Records, Electronic Signatures)

Subpart A—General Provisions	
§11.1 Scope.	The scope of 21CFR Part 11 is as stated in subpart 11.1 (not reproduced here). Laboratory results (including raw data) are generally considered to be in the scope of 21CFR Part 11. Other data not considered to be within the scope of 21CFR Part 11 (e.g. analytical method records, user access records) should nevertheless exhibit appropriate risk-based data integrity (see below)
§11.2 Implementation.	
(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.	Paper laboratory records are not generally considered to exhibit sufficient data integrity with respect to consistency completeness, security and electronic records are the preferred solution to assure data integrity.
(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that: (1) The requirements of this part are met; and (2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.	Not generally applicable to laboratory results / records, unless submitted to the agency as part of e.g. a New Drug Application.

§11.3 Definitions.	Notes:
(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part. (b) The following definitions of terms also apply to this part: (1) *Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)). (2) *Agency* means the Food and Drug Administration. (3) *Biometrics* means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable. (4) *Closed system* means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system. (5) *Digital signature* means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified. (6) *Electronic record* means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system. (7) *Electronic signature* means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature. (8) *Handwritten signature* means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark. (9) *Open system* means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.	Biometrics are not usually employed within the laboratory Most laboratory systems would be considered a closed system when networked within the laboratory or on a local area network over which the data owner has full control. Different laboratories may be connected on a fully controlled wide area network (e.g. using dedicated links on an MPLS cloud) and may still be considered a closed system. When laboratories are connected via the Internet, this is considered an open system (because the data owner does not control data routing over the Internet) and appropriate controls must be applied (see below).

Subpart B—Electronic Records	
§11.10 Controls for closed systems. Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	Applicable in a single laboratory or laboratories connected on a local area network or fully controlled wide area network. These controls should include behavioural, procedural and technical controls as discussed above and as defined below. Note that these controls should also be applied to open systems (see below).
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Regulated companies are accountable for the validation of any instruments and data management systems which manage electronic records. Responsibility for such validation can be delegated (in full or in part) to Shimadzu, but regulated companies remain accountable for ensuring that any such validation is appropriate. Practically, regulated companies will usually retain overall responsibility for validating again specific user requirements (via Performance Qualification) and will often delegate other validation tasks to instrument / database suppliers such as Shimadzu.
(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	Regulated companies are accountable for providing such copies to the agency, using the features and facilities of database systems such as LabSolutionsCS. All such data available in LabSolutionsCS is available in human readable format.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	LabSolutionsCS provides extensive security features to protect the integrity of all such records and to make them readily retrievable during lengthy record protection periods.
(d) Limiting system access to authorized individuals.	LabSolutionsCS provides extensive user management features (including audit trails of changes to user accounts) to restrict the permissions applied to defined user groups. This includes the ability to lock out access to the instrument front panel of Shimadzu instruments.

(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	LabSolutionsCS provides comprehensive computer generated, time-stamped audit trails, which record the time/date of any changes, retain the previous value and the new value Regulated companies are responsible for ensuring that the time zone of operating systems under which LabSolutionsCS runs are synchronised to an accurate time source (e.g. Internet time source or network based time synchronisation server) on a regular basis. Audit trail data is retained as long as the applicable record set and is available for review in human readable format.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	LabsolutionsCS records any changes to the analytical method, sequence or parameters and change may be audit trailed (see above). Where required, analytical methods and sequences are enforced (i.e. cannot be changed without requiring an audit trailed change record, or may be locked completely)
(g) Use of 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.	LabSolutionsCS provides extensive user management features (including audit trails of changes to user accounts) to restrict the permissions applied to defined user groups. This includes the ability to lock out access to the instrument front panel of Shimadzu instruments. This limits the ability to perform such operations to defined user groups.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	
(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Regulated companies are responsible for ensuring the appropriate education, training, and experience of all staff, consultants and contractors. All Shimadzu staff and agents are appropriately educated, trained and experienced and details can be provided for any Shimadzu staff on request.

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	Regulated companies are responsible for ensuring that all such policies and SOPs are in place and that training against such policies and SOPs is complete and effective.
(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Regulated companies are responsible for the distribution, access to, use of and change control of all such documentation. All such Shimadzu documentation is subject to appropriate revision and change control. Regulated companies are responsible for ensuring that staff have access to applicable Shimadzu documentation for purposes of use, calibration, maintenance etc.

§11.30 Controls for open systems. Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ 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. Such procedures and controls shall include those identified in §11.10, as appropriate, and 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.	Applicable when instruments and database systems are connected via a wide area network over which the data owner does not have complete control e.g. use of the public Internet, or when hosted in a third party data center. Additional controls include: • The use of encrypted network connections (e.g. https protocol, use of encrypted virtual private network for connections) • Security of of data at rest is ensured through limited access, audit trails and locking when necessary, for sensitive information by database encryption. Additionally regulated companies can utilise hard disc or disc storage array encryption. • Since LabSolutionsCS has an e-signature capability, if this is configured as required, that would constitute a further check and elaboration for any change made to a record.
§11.50 Signature manifestations.	
(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	The time and date of every signature event is recorded with reference to a common time which is also used to time stamp all audit trail entries (ensuring consistency with respect to data integrity). LabSolutionsCS allows users to define and select predefined meanings for actions requiring signature (where these are associated with common steps in the analytical sequence) or to enter the reason for unusual signature events.
(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	This information is available in the LabSolutionsCSapplication as and where required

§11.70 Signature/record linking. Electronic signatures and handwritten signatures executed to electronic records shall be 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.	LabSolutionsCS provides such signature and record linking.
Subpart C—Electronic Signatures	
§11.100 General requirements.	
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Regulated companies are responsible for establishing procedural controls to confirm the legal identify of all systems users and ensuring that signature components (User ID, tokens etc) are uniquely traceable to a legally identified individual.
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	
(c) Persons using electronic signatures shall, prior to or at the time of such use, certify 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. (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.	This requirement predates the general acceptability of legally binding electronic signatures under the US E-Commerce Act (US CFR 15 Part 96), but remains in effect. Regulated companies are responsible for complying with these requirements. If not already done, this can be achieved by sending a single letter providing such certification, to be signed by an authorised member of the senior management or a legal officer of the company.
(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	Such agency request is extremely rare, but regulated companies such ensure that all such staff, contractors etc are willing to provide such additional certification.

§11.200 Electronic signature components and controls. (a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password.	LabSolutionsCS uses a combination of User ID and Password
(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	LabSolutionsCS has a configurable solution that can comply with either requirement based on the organisations policies and practices.
(2) Be used only by their genuine owners; and	Regulated companies should establish effective behavioural and procedural controls to ensure that User IDs and passwords are not shared and that System Administrators do not know user passwords.
(3) Be 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.	
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	LabSolutionsCS does not use biometric identification as standard. If Regulated companies use computer hardware that does allow for biometric identification, this should be qualified and validated to ensure security, data integrity and availability of access using the organizations framework controls.
§11.300 Controls for identification codes/passwords.	
Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: (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.	Regulated companies are responsible for establishing procedural controls ensure that all User IDs are uniquely traceable to a legally identified individual (there can be no guarantee that two users will not have the same self-selected ‘secret’ password)
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Regulated companies are responsible for configuring LabsolutionsCS password management aging in accordance with established procedures and for establishing a process to periodically review user accounts, permissions and password use.

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised 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.	Regulated companies are responsible for establishing behavioural and procedural controls to report lost, stolen, missing or compromised passwords and procedures for issuing new passwords.
(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	Regulated companies are responsible for configuring LabsolutionsCS password management to report repeated login attempts and disable accounts according to established procedural controls, which should include the escalation of repeated attempts to data owners.
(e) 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.	Not applicable for standard LabSolutionsCS systems, unless modified to use such tokens or cards by the regulated company through the use of their own authentication systems.

Annex 11 Applicable Clauses

The following table shows how regulated companies, supported by Shimadzu, can comply with the requirements of EudraLex (The Rules Governing Medicinal Products in the European Union), Volume 4 9Good Manufacturing Practice, Medicinal Products for Human and Veterinary Use) Annex 11: Computerised Systems

Note that regulated companies are accountable for complying with the broader aspects of Eudralex Volume 4 Annex 11

1. Risk Management Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.	Regulated companies are responsible for taking a risk-based approach to the qualification of laboratory instruments and validation of laboratory systems. Where Shimadzu's professional services are supporting the specification, installation, qualification and validation it is important that regulated companies clearly define how our instruments and systems will be used and the risk criticality attached to the use of an instrument or system i.e. whether used in a research laboratory or manufacturing QC laboratory
2. Personnel There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	Staff and subcontractors supplied by Shimadzu (including our network of approved agents) are all suitable qualified, educated and trained to perform their respective their specification, installation, qualification and validation tasks
3. Suppliers and Service Providers 3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous. 3.2 The competence and reliability of a supplier are key factors when selecting a productor service provider. The need for an audit should be based on a risk assessment. 3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled. 3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.	3.1 Shimadzu expect formal agreements to be established with all regulated companies 3.2 Shimadzu are a mature and well-established supplier, adhering to defined quality management systems e.g. ISO 9001. Most regulated companies leverage this status allows regulated companies to perform an assessment of Shimadzu rather than a full on-site audit. 3.2 Shimadzu provide comprehensive documentation which can be fully leveraged in the implementation and validation of our instruments and systems. 3.4 Shimadzu are able to provide copies of our quality system certifications on request

4. Validation 4.1 The validation documentation and reports should cover the relevant steps of the lifecycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment. 4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process. 4.3 An up to date listing of all relevant systems and their GMP functionality (inventory)should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available. 4.4 User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle. 4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately. 4.6 For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system. 4.7 Evidence of appropriate test methods and test scenarios should be demonstrated Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy. 4.8 If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.	4. Regulated companies are accountable for fulfilling these requirements 4.1 Regulated companies may leverage Shimadzu's standard instrument / system documentation or project specific documentation prepared by our qualified staff 4.2 This is the responsibility of the regulated company. Shimadzu's staff will only make changes to production instruments / systems under the scope of the regulated companies change control system 4.3 Regulated companies are accountable for fulfilling this requirement 4.4. Regulated companies User Requirements may leverage Shimadzu's standard instrument / system specifications, but should be specific to the intended use of instrument / system. 4.5 See section 3 above 4.6 Regulated companies are accountable for fulfilling these requirements. Shimadzu's instruments and systems are not intended to be customised. 4.7 Shimadzu's standard IQ and OQ Protocols may be leveraged (executed by the regulated companies or our own staff) as part of the test activities 4.8 Verification checks are standard when integrating Shimadzu's instruments and systems
5. Data Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.	This is a standard function when integrating Shimadzu's instruments and systems, or certified third party instruments.

6. Accuracy Checks For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.	Such checks can be configured in applicable Shimadzu instruments and systems
7. Data Storage 7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. 7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.	7.1 All data stored in Shimadzu systems are logically secured by a comprehensive set of security controls, including role based access permissions and user authentication 7.2 Regulated companies are accountable for fulfilling this requirement and making use of the backup and archiving features provided in LabSolutionsCS
8. Printouts 8.1 It should be possible to obtain clear printed copies of electronically stored data. 8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.	8.1. Human readable copies (including hard copies) can be provided for all relevant data 8.2 This data can be viewed and printed by the LabSolutionsCS audit trail viewer.
9. Audit Trails Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.	This is a standard feature in the LabSolutuionsCS audit trail viewer, which applies to a wide range of data and records e.g. changes to user roles and permissions, analytical methods, results, reports etc.
10. Change and Configuration Management Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.	Regulated companies are accountable for fulfilling these requirements. Shimadzu's staff will usually only make changes to production instruments and systems in co-ordination with the regulated company and under a regulated companies change control system.
11. Periodic evaluation Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.	Regulated companies are accountable for fulfilling these requirements. Shimadzu are able to conduct periodic evaluations of our instruments and systems on behalf of regulated companies, to confirm that they remain in a valid state and are compliant with GMP requirements, including data integrity.

12. Security 12.1 Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. 12.2 The extent of security controls depends on the criticality of the computerised system. 12.3 Creation, change, and cancellation of access authorisations should be recorded. 12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.	12.1 Shimadzu's instruments and systems provide comprehensive logical security controls, including extensive configurable user authentication and role based permissions. 12.2 The rigor of Shimadzu's instrument and system access controls and user authentication rules may be configured based upon risk 12.3 Regulated companies are accountable for fulfilling these requirements. 12.4 Shimadzu's standard audit trails meet these requirement (see Section on 21 CFR Part 11)
13. Incident Management All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.	Regulated companies are accountable for fulfilling these requirements.
14. Electronic Signature Electronic records may be signed electronically. Electronic signatures are expected to: a. have the same impact as hand-written signatures within the boundaries of the company, b. be permanently linked to their respective record, c. include the time and date that they were applied.	Shimadzu's standard electronic signatures feature meet these requirement (see 21 CFR Part 11 below)
15. Batch release When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.	Regulated companies are accountable for fulfilling these requirements. Use of appropriate user role and permissions can be used to restrict this to defined individuals.

16. Business Continuity For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.	Regulated companies are accountable for fulfilling these requirements. Although Shimadzu's instruments and systems are highly reliable, a suitable number of instruments should be installed to ensure appropriate business continuity.
17. Archiving Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.	Regulated companies are accountable for fulfilling these requirements.

Data Integrity Controls

The following table shows how regulated companies, supported by Shimadzu, can comply with the requirements for data integrity.

As described above, regulated customers are responsible for ensuring behavioural and procedural controls.

Shimadzu's laboratory instruments and database systems include multiple features and functions which, once correctly configured and verified, ensure that the ALCOA+ principles of data integrity are assured. Some of the latest functions and features of our LabSolutionsCS software are described below to provide an indication of how our instruments and software implement enhanced technical controls and help customers prevent some of the data integrity risks that can result from poor procedural compliance and poor data integrity behaviours.

ALCOA+ Attribute		Control description	Example Features and Functions											
			Requiring reasons for data editing to be entered in audit trails	Human readable audit trails viewable via the log browser	Manageable change history for changes to measurement methods	Ability to review and print our measurement method used	Ability to review and print our measurement parameters used	Registration of validation data in secure database	Transfer of results file into external LIMS system	Data processing results (Spectrum/ time data) is available in data information view	Complete integrated and complete report set on selected data files	Management of reports and measurement parameters with secure database	Ability to sign/approve confirmation results in results files	Ability to predefine and select reasons for audit trails changes to data / rules
A	**Attributable**	Who did it, when did they do it, why did they do it?	☑	☑	☑			☑	☑	☑	☑		☑	☑
L	**Legible**	Can it be understood, is it permanent?	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

C	**Contemporaneous**	Was it captured / recorded as it happened?	☑	☑	☑								☑	☑
O	**Original**	Is it original or a verified copy?						☑	☑	☑				☑
A	**Accurate**	Are there no undocumented errors or changes?				☑	☑							
+	**Complete**	Is all the data included, including metadata and audit trails?	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑		
	Consistent	Are all data and time stamps consistent	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑		
	Enduring	Is it recorded on controlled media (hard copy or electronic)?	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
	Available	Is it available to authorised users throughout the life cycle?	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Shimadzu Corporation
www.shimadzu.com/an/