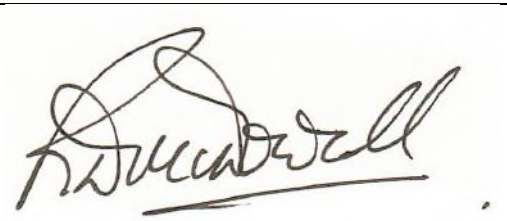
Assessment of SG Systems V5-Traceability Version 5.9

For Compliance with the Requirements of

FDA 21 CFR 11 (Electronic Records and Electronic Signatures Final Rule) and

21 CFR 211 Regulations, the Applicable FDA Predicate Rule for Pharma Manufacturing

Report Prepared By: R.D.McDowall, BSc, PhD, CSci, CChem, FRSC Director R D McDowall Limited 73 Murray Avenue, Bromley, Kent, BR1 3DJ, UK	**Report Prepared For**: Stuart Hunt Chief Executive Officer SG Systems LLC 4101 McEwen #240, Dallas TX 75244, USA
 Signature	Date 3rd December 2025

Document Information

General Information

Project Name	SG Systems Part 11 and 21 CFR 211 Software Assessment
Document Identity (file name)	SG_Systems_V5_Version 5.9_Part 11_ Compliance_Assessment_Final Signed.docx

Document Revision History

Version	Date	Reason for Change	Status
V 0.01	07 Feb 2021	Core document for SG Systems	Draft
V 1.0	09 Apr 2021	Incorporation of final review comments and approve the document	Approved
V 1.1	24 Mar 2025	First draft for Version 5.9	Draft
V 1.2	25 Apr 2025	Incorporation of review comments and addition of new V5 features	Draft
V 1.3	03 Jun 2025	Addition of new V5 features	Draft
V 1.4	28 Sep 2025	Update of the document	Draft
V 1.5	14 Oct 2025	Update of the document	Draft
V 1.6	02 Nov 2025	Final draft	Draft
V 2.0	03 Dec 2025	Final comments incorporated and released	Approved

Table of Contents

1. Executive Summary

1. SG Systems V5 Traceability version 5.9 software has been assessed remotely for compliance with the technical requirements of FDA's 21 CFR 11 and the GMP predicate rule (21 CFR 211) by Dr Bob McDowall, Director, R D McDowall Limited, UK between February and September 2025.

2. The assessment of V5 Traceability was conducted as follows:
   - Operator and supervisor roles with typical access privileges for using the application
   - System administrator with all access privileges

3. It is important to recognize that compliance with both 21 CFR 11 and the applicable predicate rule regulations requires technical controls that are the responsibility of the supplier (SG Systems) as well as the procedural and administrative controls that are the responsibility of the customer. This assessment discusses all applicable controls and highlights the responsibilities of both the supplier and a customer for compliance with these regulations.

   To be compliant with the US GMP regulations all appropriate technical, administrative and procedural controls need to be in place for any system. Therefore, both the supplier and the customer have roles and responsibilities in the regulatory compliance of any computerised system and this is reflected in this report.

4. V5 Traceability version 5.9 technical controls for both 21 CFR 11 are compliant with this regulation such as:
   - Security and Access Controls (both via a PIN code and via Active Directory with single sign on)
   - Device Checks (e.g. the balance or scale connected to the system for dispensing ingredients is the correct one and it is functioning correctly)
   - Operational System Checks (the software works in the correct sequence or workflow and cannot be overridden)
   - Integrity of Data / Electronic Records
   - Detection of Altered Records (this is a requirement to trigger an audit trail entry)
   - Audit Trail to monitor the creation and modification of GMP-relevant records) including a configurable approval workflow function to document and record electronically a supervisor audit trail review
   - Module that can enforce that a user is trained before they can execute a recipe or review a batch record
   - Electronic Signatures
   - Record and Signature Linking

5. There is no delete function in the system as the electronic records contained within it are required for serialisation and traceability of an ingredient from warehouse lot to use in manufacture of batch(es) of a product. This feature also permits a faster review as the person does not need to check if a performer has deleted records.

6. V5 Traceability is designed to work electronically and eliminate paper batch records. The system cannot operate in hybrid mode (electronic records with signed paper printouts). The business benefit of this is the elimination of the high administrative overhead of controlling master templates and blank forms used in pharmaceutical production as well as manual data input and checks for transcription errors.

2. Purpose

The purpose of this document is to report the 21 CFR 11 and 21 CFR 211 compliance assessment of the SG Systems V5 Traceability version application software performed by Dr Bob McDowall, Director of R D McDowall Limited, UK.

The assessment was carried out remotely between February and October 2025.

2.1 Software Version Assessed

The application assessed was SG Systems V5-Traceability version 5.9 installed on a laptop running Windows 11.

The system consists of three main components:

1. **V5 Control Centre** allows setup and control of key daily production and inventory control requirements to provide full forward and backward traceability from materials to manufactured product.

2. **V5 Terminal**: a tablet or terminal is used to receive instructions, follow recipes or input information
    a. **V5 Formula Control Scale System** ensures recipe ingredients are measured and traced accurately and consistently; a recipe is input into the system with acceptable tolerances that is enforced by the system. hen an ingredient in correct sequence is due to be weighed, the system scans and validates lot numbers, providing real time inventory usage and eliminating costly traceability paperwork.
    b. **V5 Product Labelling System** ensures finished products are identified accurately and consistently, with a direct link to the manufactured batches for serialisation.
    c. **V5 Statistical Process Control System**: enables sample check weighing of work in progress and finished products, providing trending and statistical monitoring of material weights used in recipes
    d. **Sampling** allows the instructions for sampling in the warehouse using a configurable checklist that links with the type of container to be used and sample amounts to be taken to for QC analysis and reserve samples as well as the storage conditions prior to analysis. Labels for the containers are generated with information on material, lot number, lot received and sampled dates/times and the individual who took the sample
    e. **Electronic signatures** can be configured by customers in workflows according to their own requirements e.g. checklists, documents, formulae, batch sign-off etc.

3. **V5 Warehouse Management System** covering the main functions of inventory management, goods receipt allowing comments on the packaging, storage locations, order picking, movement of materials and adjustment of inventory. There is also the facility for label printing.

All components operate using the same database which can be either Microsoft SQLServer..

Production instructions such as weighing ingredients for recipes were assessed using simulated rather than actual equipment attached to the application.

2.2 System Architecture

An on-premise network installation of V5 Traceability is shown in Figure 1. It consists of the application and data base installed on a network server with resilient storage to ensure one method of protecting electronic records generated and stored in the system. Access to the system can be via terminals each with a scanner attached to a

balance for weighing ingredients according to a predefined recipe. If required, bar code labels can be printed to be affixed to the container with all ingredients. Access to the system can be from fixed terminals and workstations or via mobile tablets in the warehouse or production areas.

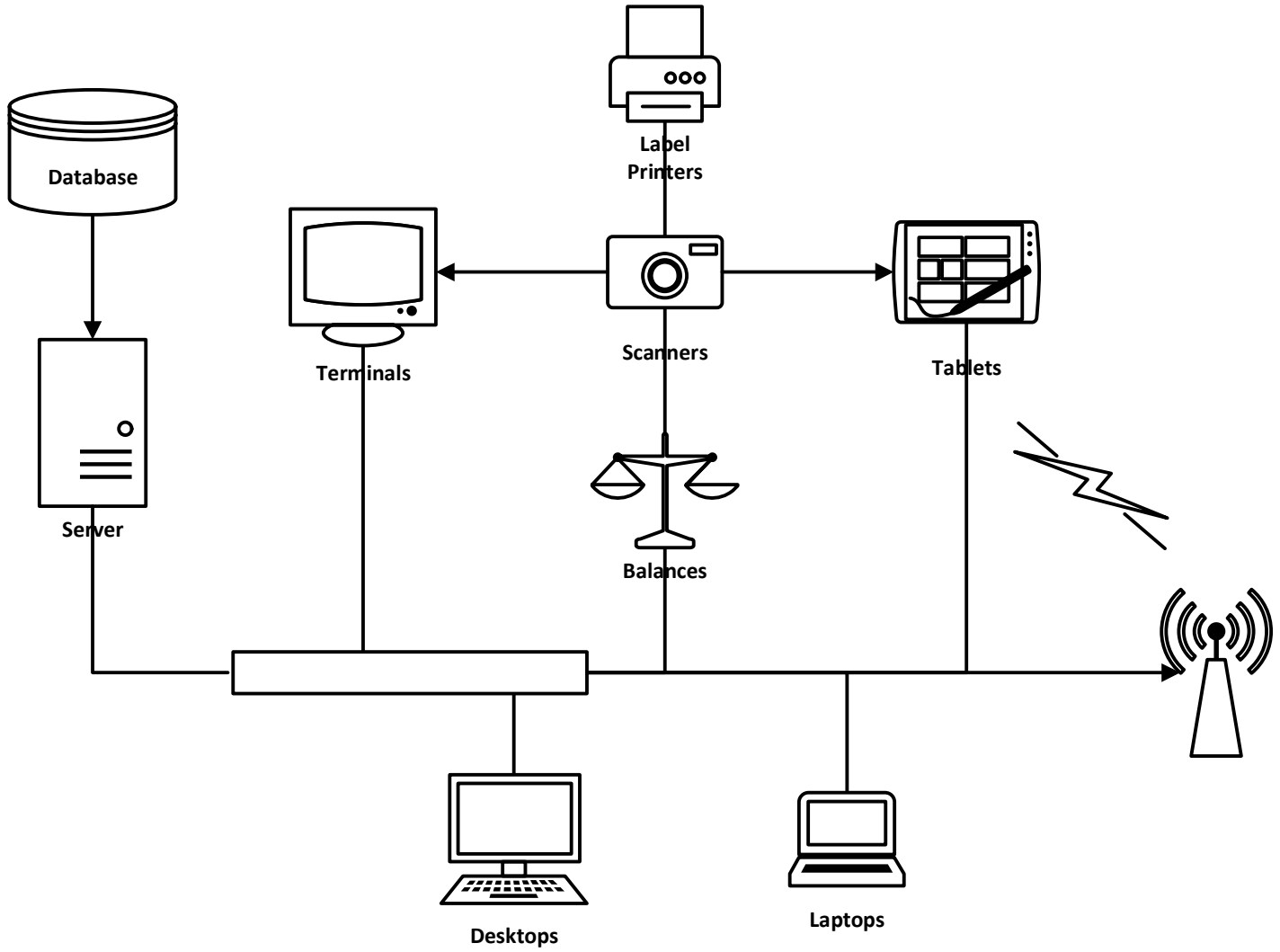


FIGURE 1: V5 TRACEABILITY SYSTEM ARCHITECTURE

2.3 Data Integrity Issues in the Pharmaceutical Industry

One of the major topics in the pharmaceutical industry is data integrity. This can vary from poor data management practices, with a focus on paper not electronic records as the GMP record to falsification and fraud. As a result, FDA published a data integrity guidance (2018) and updated the Compliance Policy Guide 7346.832 (Pre-Approval Inspections) three times (2010, 2019 and 2022). In addition, the GAMP Forum has published data integrity guidance documents. The key aspects are presented below which are complimentary and, in some cases overlap, with 21 CFR 11 requirements.

2.3.1 Key Messages from the Data Integrity Guidance Documents

The three key messages from these data integrity guidance documents are:

- **Control of Blank Paper Forms**
  Blank paper forms used in manufacturing and the master templates that generate them must be controlled. A master template must be approved and version controlled and each copy used in regulated manufacturing must be uniquely numbered and reconciled. Damaged forms must be retained and accounted for with a justification for reissue. The rationale is that unless this happens there is no way of knowing how many times a task has been performed.
- **Hybrid Systems are not Encouraged**
  Computerised systems with electronic records that have signed paper printouts are the worst situation to have as the two record sets (electronic records and paper printouts) must be synchronized and reviewed.
- **Work Electronically and Use Technical Controls to Enforce Data Integrity**
  Eliminating paper from a process and working electronically with electronic signatures is the best option as the technical controls within the computerised system can enforce ways of working. Validate the technical controls once and use many times results in easier execution and review of work.

The bottom line is that organisations need to automate their processes and eliminate hybrid systems to reduce regulatory scrutiny with respect to data integrity.

The advantage of V5 Traceability is that it only works electronically thus obviating the need to manage and reconcile blank paper forms.

2.3.2 ALCOA++ Criteria for Data Integrity

There are five criteria used for data integrity by inspectors and auditors based on the acronym ALCOA that was developed in the 1980s by an FDA inspector for his colleagues. This was expanded in 2010 by the European Medicines Agency (EMA) into nine criteria and a 10th criterion was added in 2023 by EMA and this is known as the ALCOA++ criteria. These are listed below:

- **Attributable:** Identification of the individual or system that performed an activity and the date that they performed it. Time is also applicable with a computerised system and time zone if a system spans time zones.
- **Legible:** Can you read and understand the electronic data together with any associated metadata or all written entries on paper?
  Legible should also extend to any original data that has been changed or modified by an authorised individual so that the original entry is not obscured.
- **Contemporaneous:** Documented as an official record on controlled paper or electronically in a validated computerised system at the time of an activity.
- **Original:** A written observation or printout, or a certified or verified copy thereof, or an electronic record including all metadata of an activity.
- **Accurate:** No errors in the original observation(s) and no editing without documented amendments / audit trail entries by authorised personnel. Any instrumentation used is qualified and calibrated within acceptance criteria.

- **Complete:** All data from an activity including any data generated before a problem is observed, data generated after repeating part or all of the work or reanalysis performed with a documented justification. For hybrid systems, the handwritten signed paper output must be linked to the underlying electronic records used to produce it.
- **Consistent:** All elements of the GMP record such as the sequence of events are consistent and do not contradict each other. Entries are dated (all processes) and time (sometimes paper records and all using a hybrid or electronic systems) stamped in the expected order of work.
- **Enduring:** Recorded on authorised media e.g. numbered worksheets for which there is accountability or electronic media that can last throughout the record retention period.
- **Available:** The complete collection of GMP records can be accessed or retrieved for review and audit or inspection over the lifetime of the record.
- **Traceable:** Data should be traceable throughout the data life cycle. Any changes to the data, to the context/metadata should be traceable, should not obscure the original information and should be explained. Changes should be documented as part of the metadata (e.g. audit trail).

2.3.3 Data Integrity Guidance Documents Overview: Designing and Implementing Systems to Assure Data Integrity

Collectively the various data integrity guidance documents encourage system suppliers to design software in a way that encourages compliance with the principles of data integrity. The table below takes the relevant criteria from various regulatory guidance documents and discusses how V5 Traceability meets them.

Data Integrity Criterion	How V5 Traceability Meets ALCOA+++ Criteria
Data owner	• This role should be allocated to the process owner of the application in production and who takes legal responsibility for the system and the data acquired and stored on it. • The data / process owner should ensure that each user has a unique user identity so that actions within V5 Traceability are attributed to a specific individual.
Access to clocks for recording timed events	• The system clock is on the server that the application software is installed upon and this should be synchronised to the network time server. It is assumed that the customer's IT infrastructure has a time server that checks with a trusted time source for accuracy on a predefined frequency (typically between 5 minutes to daily). • Access to the system clock must be restricted to IT personnel only to prevent time travelling by users.
Accessibility of records at locations where activities take place so that ad hoc data recording and later transcription to official records is not necessary	• Verified electronic recipes within the application ensure that all records required are collected automatically at the time work is performed, the operator does not have to record any information outside of the application. • All data associated with a recipe are in the V5 Traceability database so collation of data and the associated metadata are in a single and secure location.
Control over blank paper templates for data recording	• Using V5 Traceability with electronic signatures means that issue of controlled blank master templates and reconciling individually numbered blank forms for recording work is not required. • Manual entries into a production record are eliminated.
User access rights which prevent (or audit trail) data amendments	• The data / process owner should define user roles and appropriate access privileges to each role. These can be configured at time of system set up • Avoiding conflicts of interest between administrators and laboratory users is key. User access rights should be controlled by an IT administrator who does not have any conflicts of interest.

Data Integrity Criterion	How V5 Traceability Meets Data Integrity and Some Part 11 Criteria
Automated data capture or printers attached to equipment such as balances	• Automated data capture is performed via scales connected to V5 Traceability or bar code scanners. • There are options either to print a record if required or electronic data can be exported from the system in various file formats
Access to electronic records for staff performing data checking activities	• All measurements acquired during execution of a recipe are available in the database for review by a second person or during an audit or inspection.
Avoiding time travelling	• The application is installed on a network that should have time synchronisation from the network time server to a trusted time source such as a network time protocol (NTP) server or national observatory. • Access to the server clock should be restricted to IT personnel only
Hybrid systems are not encouraged	• Hybrid systems (signed paper printouts with electronic records) are not encouraged by regulators. • There needs to be a move to electronic records with minimal paper printouts for better compliance with regulations and better business efficiency. • V5 Traceability operates fully electronically when electronic signatures are enabled.
Enforce sequence / recipe	• There is an enforced workflow for any recipe: ingredients are weighed in strict order according to the recipe. • Enforced tolerance check of the balance used to weigh ingredients • Enforced acceptance criteria for each weighed ingredient: a recipe cannot continue until an ingredient is within limits
Complete data / information	• All records are stored in the V5 Traceability database. • All ingredients and batches are available from each recipe executed
Audit trail functions	• The audit trail can help second person review and audits by providing searches of application configuration set up and changes, user account management, input, update and execution of recipes etc.

2.4 Referenced Documents

The following documents are referenced in this assessment report:

2.4.1 Regulations

- 21 CFR 11: Electronic Records; Electronic Signatures Final Rule, 1997
- 21 CFR 211: Current Good Manufacturing Practice Regulations for Finished Pharmaceuticals, 2008

2.4.2 Regulatory Guidance

- FDA Compliance Program Guide (CPG) 7346.832, Pre-Approval Inspections, Published in May 2010 but effective from May 2012 with three objectives:
  1. Readiness for Commercial Manufacture
  2. Conformance to the Application
  3. Data Integrity Audit

  Updated in 2019 with the same format and with more details of ways to hide data integrity manipulation
  Updated again in 2022 with a new objective:
  4. Quality in Pharmaceutical Development

- FDA Guidance for Industry, Data Integrity and cGMP Compliance, December 2018
- EMA Guideline on computerised systems and electronic data in clinical trials, 2023
- FDA Guidance for Industry, Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations: Questions and Answers, October 2024
  Ignore the clinical and digital health technologies, as this is the first final guidance on 21 CFR 11 issued by the FDA since 2003.

2.4.3 Industry Guidance

- GAMP Guide, Version 5 Second Edition, ISPE, Tampa FL, 2022
- GAMP Good Practice Guide on Risk Based Validation of Laboratory Computerised Systems, Second Edition, ISPE, Tampa, FL, 2012
- GAMP Good Practice Guide IT Infrastructure Compliance and Control, ISPE, Tampa FL, Second Edition, 2017
- GAMP Guide Records and Data Integrity, ISPE, Tampa FL, 2017
- GAMP Good Practice Guide Data Integrity – Key Concepts, ISPE, Tampa FL, 2018
- GAMP Good Practice Guide Data Integrity by Design, ISPE, Tampa FL, 2020

3. 21 CFR 11: Electronic Records and Electronic Signatures

Published in March 1997 and effective on 20th August 1997, the Electronic Records; Electronic Signature final rule (21 CFR 11) has had the greatest impact on computerized systems than any other regulation. The basic requirement is to ensure that computerized systems produce electronic records that have integrity and reliability and electronic signatures are trustworthy and equivalent to handwritten signatures executed on paper records.

3.1 21 CFR 11 Compliance Assessment Checklist

The following 21 CFR 11 compliance assessment has been developed and compiled from many compliance assessments performed for clients since 1999. The FDA's Guidance for Industry on Part 11 Scope and Application has narrowed the scope of Part 11 and has modified the compliance requirements for a number of Part 11 requirements notably validation, device and operational system checks, audit trail, copies of records and retention of records.

3.2 Interpretation of 21 CFR 11 Regulations

3.2.1 Interpretation of 21 CFR 11 Requirements

The interpretation of sections of 21 CFR 11 requirements is based on Bob McDowall's experience since 1998 in interpreting these regulations for clients. This work has included the writing or review of Corporate Part 11 Policies and corporate procedures, training staff in 21 CFR 11 assessments and performing Part 11 assessments on behalf of clients. In addition, he has published many articles, book chapters and books as well as run training courses on this subject.

It is important that readers refer to their corporate interpretation of 21 CFR 11 and check that the technical controls in V5 Traceability meet your requirements. From experience, most customer assessments will meet the majority of interpretations of Part 11 but individual organisations have their own interpretations where the regulation and / or the preamble are vague.

3.2.2 Role of the GMP Predicate Rule

Part 11 states what needs to be done to ensure that electronic records and electronic signatures are trustworthy and reliable. However, the regulation does not state what records and signatures are required and this is the role of the applicable predicate (pre-existing) rule e.g. 21 CFR 211 or current Good Manufacturing Practice for Finished Pharmaceutical Products.

As V5 Traceability captures all ingredient, recipe and finished product data either from a balance or label scan the issue of predicate rule interpretation is covered. However, it is the interpretation of the predicate rule for signing that is important. It is essential to differentiate between:

- Attribution of action within the system: individual stages that are executed by named individuals
- Signing of a record at the end of an activity e.g. completion of a recipe execution

This is down to an individual regulated company's interpretation of 21 CFR 11 and 21 CFR 211 regulations. Regardless of the selection of attribution or electronic signature, V5 Traceability can meet either requirement in a compliant manner.

3.3 Format of the Compliance Assessment Tables

The tables for the assessment of the Part 11 compliance of V5 Traceability have the following structure:

- Column 1: 21 CFR 11 reference number.
- Column 2: presents the specific section from the Part 11 regulation and is typically quoted verbatim – underneath are the questions for assessment derived from the requirement.
- Column 3: defines the type of control required. For ease of presentation, administrative and procedural controls are summarised under the topic “Proc” and technical controls are listed under “Tech”.
- Column 4: this defines the responsibility for the control item – the customer for procedural controls and the supplier (SG Systems) for technical controls.
- Column 5: Assessment of the software and / or any supporting comments.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
	§ 11.10 Controls for Closed Systems			
System Validation [11.10(a)] ***Validation of the systems to ensure accuracy, reliability, consistent intended performance and the ability to discern altered and invalid records.***				

3.4 Technical, Administrative and Procedural Controls

Part 11 requires a regulated healthcare organisation to have in place three levels of control:

- **Administrative controls**: Verification of an individual’s identity and policies for Part 11 and the use of electronic signatures
- **Procedural controls**: SOPs for using the system coupled with effective user training
- **Technical controls**: functions built into software that ensure the reliability and integrity of the function e.g. security, audit trails

Please note that you cannot purchase a 21 CFR 11 compliant application.

There are applications that can be designed to be compliant with 21 CFR 11 technical controls, but it is the user that is responsible for providing policies and procedures to ensure the systems are fully compliant with the regulations and the predicate rule applicable. This is shown in Figure 2 below and illustrates the importance of an integrated approach to 21 CFR 11 compliance and why you cannot purchase a 21 CFR 11 compliant application.

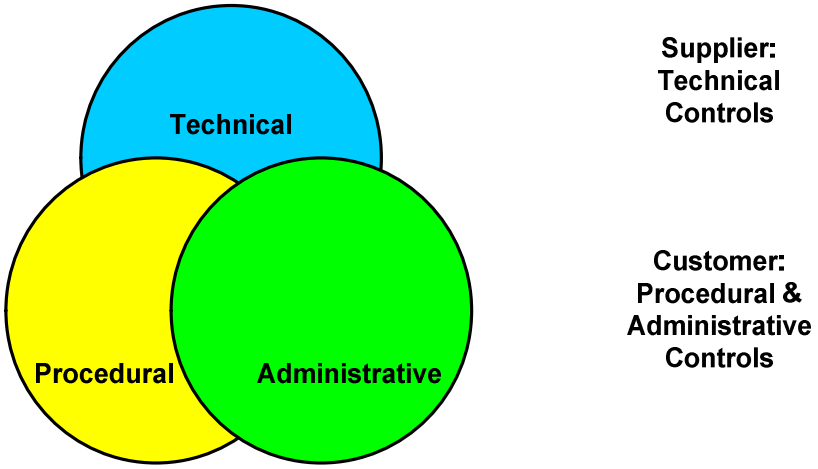


FIGURE 2: A 21 CFR 11 COMPLIANT SYSTEM REQUIRES 3 ELEMENTS: ONE FROM THE SUPPLIER AND TWO FROM THE CUSTOMER

4. 21 CFR 11: Controls Required for Electronic Records

Abbreviations for 21 CFR 11 Control Type: Proc = Procedural & Administrative (Customer responsibility); Tech = Technical (Supplier responsibility)

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
	§ 11.10 Controls for Closed Systems			
System Validation [11.10(a)] ***Validation of the systems to ensure accuracy, reliability, consistent intended performance and the ability to discern altered and invalid records.***				
11.10(a) / 1	Is the system validated to the Company standards?	Proc Proc	Customer Supplier	The end user is responsible for validation following established company policies and procedures. Software development is triggered via a change request that is outlined in the company's QMS change management policy. A summary of the SG Dev Process can be found on the company web site.
11.10(a) / 2	Did validation include tests and checks that demonstrate compliance with all applicable parts of 21 CFR 11 (e.g. audit trail, backup/restore, archive, security controls, device/terminal checks, e-signatures)? If No, determine omissions as part of the Action Plan. .	Proc Proc	Customer Customer	The end user is responsible for validation of these features following established company policies. This will include altering a record to trigger an audit trail entry under 11.10(e) and input of wrong data (invalid record). Policies within the software enable a customer to configure the security and access controls such as password expiry. Authentication and authorisation information can be found on line: Log On Process. The settings of these policies will need to be documented by each regulated customer following their computerised system validation policy and procedures.
Record Inspection [11.10(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*.**				
11.10(b) / 3	Can the system generate accurate and complete copies of records in both human readable and electronic form for inspection by the FDA?	Tech Proc	Supplier Customer	Yes, copies of electronic records can be produced by users with appropriate security access. Records can be exported in a number of formats such as PDF, CSV, Docx, txt, xml files, selectable from Jaspersoft Web Reports Suite An SOP for the handing of electronic records during an inspection is strongly recommended.
11.10(b) / 4	Does the Computer System generate copies of which user has access to a particular resource e.g. file accesses, grants, permissions, etc.?	Tech	Supplier	Yes, application configuration settings can be printed.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
Records Protection [11.10(c)] ***Protection of records to enable their accurate and ready retrieval throughout the records retention period.***				
11.10(c) / 5	Are all electronic records saved to a secure area, preferably on the site network?	Tech Proc	Supplier Customer	Electronic records are stored in a database installed on a network server. A networked system is always the preferred solution as the backup of the electronic records generated are backed up by the IT organization rather than the users.
11.10(c) / 6	Do SOPs cover who is responsible for backup and recovery and how this shall be done?	Proc	Customer	A user procedure is essential to meet this requirement. Checks that the backups have worked must be implemented. Regular test restores must also be conducted to ensure backup works. No backup: no disaster recovery.
11.10(c) / 7	Do SOPs cover who is responsible for long term archiving and retrieval and how this shall be done?	Proc	Customer	The users should comply with their corporate standards or guidelines for archival and retrieval of electronic records.
11.10(c) / 8	Are all electronic records included in system backups?	Proc	Customer	The customer is responsible for ensuring that all electronic records are backed up.
11.10(c) / 9	Can data generated from earlier software versions be retrieved from archive and viewed in its entirety?	Tech Proc	Supplier Customer	When a new application version is released the release notes for the version state what is required in terms of any data migration. If the database version is updated or there are changes in the current data base structure, then existing data are migrated from the old version to the new one. The customer must validate any database upgrade as part of the system revalidation according to current change control or validation SOPs.
11.10(c) / 10	If records can be copied outside the application, is user access to the copy read-only? • If no, does the software prohibit the overwriting of the original record by the copy?	Tech Proc	Supplier Customer	Yes, records can be copied outside of the application in a variety of formats such as CSV, PDF, txt, Docx. etc.. PDF is considered the most secure of the two formats. The customer needs to have procedures for handling the data copied or exported from the system.
11.10(c) / 11	Are Critical Records stored in one location only? • If No, do validated automatic functions exist to maintain data integrity?	Tech	Customer	Yes, the database is installed on a network server, this server should incorporate fault tolerant features to mitigate the impact of any hardware failure. Consideration of duplicate facilities is recommended.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
11.10(c) / 12	Is concurrent write access by multiple users prohibited?	Tech	Supplier	. Only a single user can create and update a record at at time. It is possible for other users can open multiple records on the newer version of the Jasper Reports, but they are always read only, with the data drawn from the database itself.
11.10(c) / 13	Can data be recreated after computer system failures?	Proc	Customer	Providing that the system backup is complete and successful, the system and data can be recreated after a failure up to the last backup. Periodic restores should be undertaken to verify that the backup works.
11.10(c) / 14	Are the records protected from hazards such as fire, heat and water by environmental controls (e.g. ventilation)?	Proc	Customer	The server should be in an environmentally controlled computer room / data centre with redundant utilities such as power, network access, and fire suppression.
11.10(c) / 15	Have retention periods for the electronic records retained in the system been specified?	Proc	Customer	Minimum requirements for GMP record retention is batch expiry plus one year for US regulations or 5 years after certification of the batch by the Qualified Person in the EU. The customer should refer to their company policy to determine the length of time that GMP records should be held.
Security [11.10(d)]: ***Limiting system access to authorized individuals.***				
11.10(d) / 16	Are devices for storage of electronic records (e.g. file/database servers, backup and archive durable media) located in a controlled area or physically secured?	Proc	Customer	The customer is responsible for purchase and installation of a suitable server and locating it in a secure location with appropriate access and environmental controls.
11.10(d) / 17	Does the system limit system access to authorised individuals?	Tech Proc	Supplier Customer	Yes, the system enforces that user identities are unique. The same user identity cannot be created in the system. There must be a user account management procedure that allocates all users a unique user identity. The customer must maintain a list of current and historical users of the system along with their role in the system.
11.10(d) / 18	Does the system prevent deletion of users from the system, to ensure uniqueness of user identities? The user identity should be “deactivated” but retained.	Tech Proc	Supplier Customer	User identities are disabled but not deleted in the database. The user account management procedure must disable a user when they move department and no longer require access or leave the company.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
11.10(d) / 19	Does the system have a password-protected inactivity lock enabled?	Tech Proc	Supplier Customer	Yes, there is a configurable option available This needs to be specified and documented in the configuration specifications and set in the application.
11.10(d) / 20	Is user access to the Operating System restricted to the System Administrator, or equivalent authorised user?	Proc	Customer Supplier	The application is installed on a network server and the IT department can limit access to the directories on the server. Terminal and the Warehouse Management System software can be configured to start with Windows & shut down upon being closed, preventing users accessing the local OS at any time. This is not applicable for Control Center, as users here will require access to the remainder of their system to perform their other duties.
11.10(d) / 21	If the computer system can be accessed remotely, are additional security measures, such as “call back” or SecurID included?	Proc	Customer	Remote access to the system can be configured following a request from a customer.
11.10(d) / 22	Do remote access sessions automatically log-off when a disconnect is detected?	Tech	Supplier	Yes
11.10(d) / 23	Are safeguards in place to detect attempts at unauthorised use, and to lock the account after several consecutive unsuccessful attempts to enter a password?	Tech Proc	Supplier Customer	If using the username/password style login, 3 unsuccessful login attempt will result in the user account being locked, requiring unlocking by an administrator. When using Active Directory, if the user cannot log into the Windows OS, they cannot log into the software. Part of the system administration SOP should include how to unlock disabled accounts.
11.10(d) / 24	Is there an approved procedure that describes the administration of user and administrator security and access control (system security)?	Proc	Customer	The customer must write an SOP to control system access and the establishment and maintenance of logical security.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
Audit Trail [11.10(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.***				
11.10(e) / 25	Are there computer-generated (automatic audit trails) of all user actions?	Tech	Supplier	Yes, there is a single audit trail covering all relevant human and system actions within the application. The audit trail is searchable and information is displayed in a split screen. At the top of the screen the individual audit trail entries are shown. For a single selected entry, the details of the transaction and the changes made to the record are shown in two screens underneath the main audit trail screen. There is 'Mark As Viewed' event when a supervisor is reviewing a batch record or document etc. is recorded in the audit trail. This can be seen using a 'view.log' table in the database. The preferred reporting method is to use Jaspersoft Web Reporting as this is more user friendly. The same data can be viewed within the Control Centre of the application Account lock is present once Active Directory configuration is enabled with Single Sign On Double space. The choice of reporting mode is left to each customer's preference. Yes, the audit trail is turned on at installation and cannot be turned off.
11.10(e) / 26	Are audit trail entries date stamped DD-MMM-YYYY?	Tech	Customer	Yes, the audit trail date format uses the Windows settings from the database server. The date format is selected by each customer.
11.10(e) / 27	Are audit trails time stamped HH-MM-SS in local time?	Tech	Customer	Yes, the audit trail time format uses the Windows settings from the database server. This is selected by each customer.
11.10(e) / 28	Are there controls to ensure that the system clock date and time stamps are accurate and secure from tampering?	Tech	Customer	If networked, the system clock can be synchronised with a trusted third party e.g. internet time source linked to a national laboratory or a network time protocol (NTP) server.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
11.10(e) / 29	Do all audit trail entries include operator identity, using full name or the Customer-defined user ID of an individual?	Tech	Supplier	The system references the database user identity which in turn references the users name as entered by the customer.
11.10(e) / 30	Is there an audit trail entry for system activity, including all user logon and failed access attempts?	Tech	Supplier	If using the username/password login option, unsuccessful login attempts are recorded in the audit trail, along with the device they were attempting to log in to. Failed AD login attempts will simply not allow the user to log into Windows, and hence the software
11.10(e) / 31	Is an audit trail entry generated during creation of data?	Tech	Supplier	Yes. Entries are made in the audit trail when users enter or modify data.
11.10(e) / 32	Is an audit trail entry generated during modification of data by a user?	Tech	Supplier	Yes.
11.10(e) / 33	Is an audit trail generated during “deletion” or “inactivation” of data?	Tech	Supplier	As the system is used for serialisation and traceability of ingredients and products, there is no possibility of deletion from the database.
11.10(e) / 34	If the record is changed does the system retain/display the old and new values?	Tech	Supplier	Yes, the old and the new values are displayed in the audit trail.
11.10(e) / 35	Does each audit trail entry describe the action performed?	Tech	Supplier	Yes
11.10(e) / 36	Does the audit trail contain sufficient information to allow a reviewer to trace all changes to a record from its current state back to the original values?	Tech	Supplier	Yes, the system is designed for traceability and serialisations and therefore it can trace from warehouse receipt to use in an individual recipe for a specific product lot.
11.10(e) / 37	Is the audit trail directly associated with the record, but located separately?	Tech	Supplier	Yes, the audit trail is a separate and secure table in the database.
11.10(e) / 38	Are audit trail records being maintained for at least as long as the retention of the underlying records? (Are they backed up with the records and can they be retrieved?)	Tech Proc	Supplier Customer	Audit trails are maintained within the system while it is operational. Backup of the database is an essential regulatory and business requirement. Backup must be coupled with regular test restores to ensure that backup works.
11.10(e) / 39	Is a read-only display or report available for viewing the audit history?	Tech	Supplier	Yes, this can be achieved within the Control Centre or using Jaspersoft Web Reports
11.10(e) / 40	Are audit trails available for review and copying by regulatory authority?	Tech Proc	Supplier Customer	Yes, audit trail entries can be exported in a variety of formats. PDF is recommended as a more secure format.. A procedure is recommended for copying records for regulatory inspection.
11.10(e) / 41	Are all users, (including the Administrator) unable to modify audit trail details?	Tech	Supplier	Yes, there are no delete privileges or options in the whole system
11.10(e) / 42	Are changes to user authority levels and permissions audit trailed?	Tech	Supplier	Yes.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
Operational Checks [11.10(f)] ***Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.***				
11.10(f) / 43	If the sequence of system steps or events is important in a process, is this enforced by the system (as appropriate)?	Tech	Supplier	Yes, each recipe step must be completed in order. If a recipe requires a fixed sequence of steps the system enforces this. At the dispensing stage, there is a check to ensure that all labels on the ingredients are clear, not smudged or if a label is missing. The system enforces a user to take a photograph that can be emailed to supervisors or managers for assessment.
	If the sequence of system steps or events is important in a process, is this enforced by the system (as appropriate)?	Tech / Proc	Customer	Yes, the recipe must be executed as defined and configured by the customer and described in the question above. A user can find out further information about a label by clicking the specification tab. There is an electronic signature sign-off by the operator and user from the approval workflow. There is a visual check of weight tolerance: a green or red light that is defined for each ingredient in a specific recipe to indicate when the weight of material is in the acceptable range. If acceptance criteria for an ingredient are not met, the step or task cannot be completed. When a recipe is executed it is assigned to a specific terminal with an associated weighing device. An SMS/email message can be sent to a supervisor in case of a deviation or non-conformance. The system will also force an operator to input contemporaneous notes of the deviation. A supervisor logging on can be notified if any batches are pending for review or sign-off.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
Authority Checks [11.10(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.***				
11.10(g) / 44	Does the software require entry of a separate user ID and password, in addition to that required by the operating system?	Tech	Supplier	Yes, the application has its own security and access control if not using Active Directory
11.10(g) / 45	Does each user have an individual account?	Tech Proc	Supplier Customer	Yes, a check is made to ensure that all new user accounts are unique within the system Customers need to have a user management SOP.
11.10(g) / 46	Has the system various user-defined access control levels?	Tech Proc	Supplier Customer	Yes, two levels predefined within the application: operator and supervisor with access levels that are provided as default by the supplier. Additional operator privileges can be assigned to either role to allow/prevent various actions within the system. The customer should allocate users to either operator or supervisor role
11.10(g) / 47	If the system has various user levels, are there SOP(s) in place to describe how a user's access shall be defined?	Proc	Customer	The customer should have an SOP that defines the user types with the associated access privileges for each type. Users and their access privileges need to be reviewed on a regular basis
11.10(g) / 48	Are modifications/deletions to data always performed through the application control (E.g. data are not changed through SQL or other data access tools)?	Tech Proc	Supplier Customer	Only the supplier can access the database Access to the administration functions of the application is an IT function and outside of the users of the application.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
Device and Terminal Checks [11.10(h)] ***Use of device (e.g. terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction***				
11.10(h) / 49	Are device checks to determine validity of the source of input or operation designed and implemented in the system (as appropriate*)? [E.g. an application indicating that data input is derived from a particular device, such as a balance, should identify the device or only allow data entry from that device, and not from a terminal].*	Tech	Supplier	Yes, a recipe is downloaded to a specific terminal attached to a specific scale. Before beginning a recipe, the system requests a user confirm if specified equipment is available. The system checks if an asset such as a scale is within its calibration window. If not and there is a suitable alternative available, the system will allow a substitute asset to be used. A recipe can include a check that a scale is measuring within acceptable limits before the recipe instructions are executed.
11.10(h) / 50	Are terminal checks to determine validity of the source of input implemented?	Tech Proc	Supplier Customer	Yes, this can be included in the instructions for a recipe. The scale or balance can be checked against acceptance limits using a calibrated mass or check weight.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
Personnel Qualifications [11.10(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***				
11.10(i) / 51	Has it been documented that the following persons have the education, training, and experience to perform their assigned tasks: Developers of the computerised system? Users of the computerised system? .	Proc Proc Tech	Supplier Customer Supplier	SG Systems staff have 21 CFR 11 awareness training applicable to their roles. *Note: Following the preamble, this requirement only goes as far as internal developers. (Comment 87). In order to answer Yes to this question, the vendor must maintain training records and be aware of the 21 CFR 11 implications. Documentation should be available for review during audits.* There is a training module within V5 that a customer can configure and use to document user training on the system. A learner can be provided with reading material prior to the training. Material for training modules can be generated by the customer or by accessing the SG Systems resources. Questions for checking understanding can be written by a customer or generated by AI based on SG System's training material. An untrained user can be locked out from various areas of the software, such as executing a recipe. Following the completion of a training module, understanding can be assessed by a multiple-choice questionnaire with a minimum pass mark before allowing a user to access the desired areas of the software, such as recipe execution. Results can be reviewed by a second person if required. Assessment failure will result in a discussion with a supervisor and repeating the training. There is a recurring interval function which is customer configurable up to 365 days before refresher training is scheduled and due. 15 days before training is due the system will check if training is scheduled, and if not the system will automatically schedule it and email the user. Failure to retrain by the due date will result in a user being locked out of a recipe. Training modules are under change control and have an owner who is informed of any changes by email.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
11.10(i) / 52	External maintainers of the computerised system?	Proc	Supplier	SG Systems staff have 21 CFR 11 and GMP awareness training applicable to their roles.
11.10(i) / 53	Internal maintainers of computerised system?	Proc	Customer	Training of the maintainers of the system needs to be documented by the customer.
11.10(i) / 54	Users of the computerised system?	Proc	Customer	Training of user's needs to be documented by the customer.
Accountability and Responsibility for Actions [11.10(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***				
11.10(j) / 55	Have policies and/or procedures holding individuals accountable and responsible for actions initiated under their electronic signatures been established and followed?	Proc	Customer	The customer needs to have an SOP coupled with effective training for the use and accountability for the user of electronic signatures.
Systems Documentation Controls [11.10(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.*** *Note: This covers vendor supplied manuals/documentation as well as logs for the system (backup, errors etc.)*				
11.10(k) / 56	Are there adequate controls over the distribution of documentation for system operation and maintenance?	Proc	Customer	Controlled copies of SOPs should be issued by the Quality Assurance Department.
11.10(k) / 57	Are there adequate controls over access to documentation for system operation and maintenance?	Proc	Customer	The procedures and other documentation for system operation and maintenance must be controlled.
11.10(k) / 58	Are there adequate controls over the use of documentation for system operation and maintenance?	Proc	Customer	The procedures and other documentation for system operation and maintenance must be controlled.
11.10(k) / 59	Are revision and change control procedures in place to maintain an audit trail that documents the time-sequenced development and modification of the systems documentation? *(Only applies to documentation that can be changed by individuals within the Customer).*	Proc Proc	Supplier Customer	Yes, there is a an online help file available for each version of software that is updated with each major and minor release of the application. The customer is responsible for ensuring only the correct version of the online help is available especially if copies or pages have printed have been made from old versions. Old SOPs for using the system must be withdrawn and replaced by new versions.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
§11.50 Signature Manifestations.				
Signing Requirements [11.50(a)] ***(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.***				
11.50(a) / 1	Do electronically signed electronic records contain information associated with the signing that clearly indicates: The full printed name of the signer? [11.50 (a)(1)]	Tech	Supplier	Yes
11.50(a) / 2	The date and time when the signature was executed? [11.50(a)(2)] *N.B. Handwritten signatures on paper records require date only.*	Tech	Supplier	Yes
11.50(a) / 3	The meaning of the signature? [11.50(a)(3)]	Tech Proc	Supplier Customer	Yes The meaning of the signature needs to be defined by the user according to their working practices.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
Controls for Electronic Signatures [11.50(b)] ***(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).***				
11.50(b) / 4	Are all items in the signature manifestation subject to the same controls as for electronic records? [11.50(b)].	Tech Proc	Supplier Customer	Electronic signatures are configurable. The default setting is for two signatures by two separate individuals as operator performer and supervisor reviewer. There is a configurable function to ensure that a supervisor cannot approve their own work. This is essential in a GMP environment. If required, and configured, there is an option for all performers to sign for the work they executed for a batch. Where appropriate, batches can be collated and signed together, subject to adequate second person review of each batch. Signature release policy defines which roles can sign for work performed or reviewed. The customer needs to define which user roles that have electronic signature powers for performing and reviewing work.
11.50(b) / 5	Are all items in the signature manifestation included as part of any human readable form of the electronic record (such as electronic display and/or printout or report)? [11.50 (b)]	Tech	Supplier	Yes, the signature information is available as part of the electronic record on the report of the recipe executed, completed checklist or approved document.
§11.70 Signature/Record Linking.				
Linking Signatures to Electronic Records [11.70] ***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.***				
11.70 / 1	Are all *electronic* signatures on electronic records 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? [11.70]	Tech	Supplier	Yes, the database ensures that electronic signatures are linked to the appropriate electronic records.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
11.70 / 2	Are *hand written* signatures on electronic records linked to their respective electronic records? *Note: Minimum requirement is initials of signer, print date/time unique sample identifier, and, if appropriate, file name and location / file size.*	Proc	Customer	This is not applicable A) If attribution of action is selected for performing and approving work, or B) If electronic signatures are implemented and the system is used electronically.

5. 21 CFR 11: Controls Required for Electronic Signatures

Abbreviations for 21 CFR 11 Control Type: Proc = Procedural & Administrative (Customer responsibility); Tech = Technical (Supplier responsibility)

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
§11.100 General Requirements.				
Uniqueness of Signature [11.100(a)] ***(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.***				
11.100 (a) / 1	Are electronic signatures unique to an individual? [11.100 (a)]	Proc Tech	Customer Supplier	The customer needs to implement procedural controls to ensure that electronic signatures are unique to an individual. Typically, this means that user identities are unique throughout an organisation and are never reused. Yes, the application has a technical control that ensures that user identities are unique and prevents the same user identity being reused. If the application is integrated with Active Directory the user identity is also unique.
11.100 (a) / 2	Does the system prohibit use of shared/group accounts as components of electronic signatures?	Tech Proc	Supplier Customer	Yes, if configured, each user role can have electronic signature privileges. The customer also needs to ensure that user identities and passwords are not shared through a procedural control and training.
Verification of Identities [11.100(b)] ***(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.***				
11.100 (b) / 3	Electronic signatures cannot be reused by, or reassigned to, anyone else [11.100 (b)]	Proc	Customer	The customer must ensure that the same user identity must never be allocated to another individual.
Certification to the FDA [11.100(c)] **(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.*** ***(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.***				
11.100 (c) / 4	Is the identity of an individual verified before an electronic signature is allocated? [11.100 (c)]	Proc	Customer	The procedure for verifying the identity of users need to be determined and implemented, records of the user identity verification need to be maintained.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
11.100 (c) / 5	Has the customer organisation sent a letter to the FDA, stating their intent to use electronic signatures?	Proc	Customer	The organisation must send a single letter to the FDA stating that electronic signatures are the legal equivalent of handwritten signatures. The letter covers the whole organisation and should be done before electronic signatures are used.
§11.200 Electronic Signature Components and Controls.				
Components and Sessions [11.200(a)] ***(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.*** ***(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.*** ***(1) Be used only by their genuine owners; and*** ***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.***			
11.200 (a) / 1	Is the signature made up of at least two components, such as an identification code and password [11.200 (a)(1)]	Tech	Supplier	Yes, the two components used are user identity and password.
11.200 (a) / 2	When several signings are made during a continuous session, is the secret part of the signature executed at each signing? Both components must be executed at the first signing of a session. [11.200 (a)(1)(i)]	Tech	Supplier	All electronic signatures require the input of both components.
11.200 (a) / 3	If signings are not done in a continuous session, are both components of the electronic signature executed with each signing? [11.200 (a)(1)(ii)]	Tech	Supplier	There is no continuous session within the system, therefore both signature components are required for each signing.
11.200 (a) / 4	Are signatures designed to ensure that they can only be used by their genuine owners? [11.200 (a)(2)]	Proc	Customer	The customer must ensure that user identities and passwords are never shared.
11.200 (a) / 5	Would an attempt to falsify an electronic signature require the collaboration of at least two individuals? [11.200 (a)(3)]	Proc	Customer	Yes, falsification would require two individuals to collaborate.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Comments
Biometric Electronic Signatures [11.200(b)] ***(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.***				
11.200 (b) / 6	Have biometric electronic signatures been validated including attempted use by other users? [11.200(b)]	Tech	Supplier	Not applicable
§11.300 Controls for Identification Codes/Passwords.				
Uniqueness of Electronic Signature [11.300(a)] ***(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.***				
11.300 (a) / 1	Does the system keep all password details confidential, so that they are not available to any system user, including the Administrator?	Tech	Supplier	Yes, local user passwords are encrypted and kept confidential from all users including the system administrator.
11.300 (a) / 2	Are controls in place to maintain the uniqueness of each combined identification code and password, such that no two individuals can have the same combination of identification code and password? [11.300 (b)]	Proc Tech	Customer Supplier	The customer needs to ensure that identities are allocated to a single individual and never reused and passwords must never be divulged. Yes, there is a technical control to ensure that user identities cannot be duplicated.
Checking of IDs and Passwords [11.300(b)] ***(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g. to cover such events as password ageing).***				
11.300 (b) / 3	Are procedures in place to ensure that the validity of identification codes is periodically checked? [11.300 (b)]	Proc	Customer	The customer needs to have a procedure in place for a regular check of the users defined in the system and making any corrective actions.
11.300 (b) / 4	Do passwords periodically expire and need to be revised? [11.300(b)]	Tech Proc	Supplier When integrated with Active Directory additional controls such as preventing reuse of old passwords. Customer	Yes, there is a user defined password expiry. The customer needs to implement the password aging time that is consistent with their organisation's corporate policies.
11.300 (b) / 5	Are passwords obscured when entered?	Tech	Supplier	Yes, the characters used in the password are obscured.
Loss of Passwords and Tokens [11.300(c)] ***(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.***				
11.300 (c) / 6	Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred? [11.300(c)]	Proc	Customer	The customer needs a procedure for a system administrator to set an account to inactive when a user moves, changes position or leaves the company.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Comments
11.300 (c) / 7	Is there a procedure for temporary or permanent replacements using suitable rigorous controls? [11.300(c)]	Proc	Customer	The customer procedure needs to ensure that resetting of account passwords is secure and that only the appropriate account is reset.
Unauthorised Use [11.300(d)] ***(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.***				
11.300 (d) / 9	Is there a technical feature to detect attempts at unauthorised use and for informing security? [11.300(d)]	Tech	Supplier	Failed user log-on attempts are recorded in the audit trail when using the system's username and password login option. When the application is integrated with Active Directory this is possible via the customer's Active Directory controller.
11.300 (d) / 10	Is there a procedure for immediate and urgent reporting to security/management any attempt at unauthorised use of identification codes and passwords? [11.300(d)]	Tech Proc	Supplier Customer	Account locking is possible when using the system's username and password login option. If using Active Directory an alert can be generated from the customer's Active Directory controller. A customer SOP for handling security alerts is required.
Checking Devices [11.300(e)] ***(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.***				
11.300 (e) / 11	Are tokens or devices regularly checked or replaced?	N/A	N/A	Tokens and devices are not supported by the system.

6. Outline Biography of R.D.McDowall

- 15 years' experience in the pharmaceutical industry with Smith Kline and French and Wellcome Research Laboratories plus six years' experience in forensic toxicology

- Over thirty years' experience as a consultant and nearly forty years' experience in computer validation.
    - Principal of McDowall Consulting (1993 – 2015) specialising in LIMS, chromatography data systems, computer validation, corporate validation and Part 11 policies, electronic signatures and electronic records, process redesign, laboratory automation strategies and projects.
    - Director of R.D.McDowall Limited (1998 – date) specialising in corporate computer validation and Part 11 policies, data integrity, analytical equipment qualification and validation of GMP, GLP and GCP computerised systems. Audits of laboratories, computerised systems and software suppliers.
    - Advisor to the Pharmaceutical Industry Group of PricewaterhouseCoopers and Coopers&Lybrand 1993 – 2017

- PhD degree from University of London, Chartered Scientist, Chartered Chemist and Fellow of the Royal Society of Chemistry

- Co-chair of a session the FDA and AAPS meeting on Validation of Bioanalytical Methods held in Crystal City, December 1990 and co-author of the published proceedings in 1992

- ISO 17025 (UKAS) assessor for chromatography and computer validation 1994 - 2000.

- Visiting Senior Fellow, Department of Chemistry, University of Surrey 1991 - 2001.

- Internationally recognised expert in validation of bioanalytical methods, LIMS, chromatography data systems, laboratory informatics, laboratory automation, validation of computerised systems, 21 CFR 11 and data integrity

- Member of the Editorial Boards of LC-GC North America, LC-GC Europe, Spectroscopy, Quality Assurance Journal (2001 – 2011) and Journal of the Association of Laboratory Automation (2004 – 2009)

- Editor of Laboratory Information Management and Laboratory Automation and Information Management 1991 - 1998.

- Editor of the Pharma IT Journal 2007 – 2008.

- Published over 600 peer reviewed papers, scientific magazine articles and book chapters, given over 2,000 presentations and workshops at symposia, meetings and training courses.
    - Writer of the Questions of Quality column in LC-GC Europe since 1993 and the Focus on Quality column in Spectroscopy since 1999
    - Writer of the Validation and Verification Column and member of the Editorial Board of Scientific Data Management 1997 – 1999
    - Author of Validation of Chromatography Data Systems: Meeting Business and Regulatory Requirements (first edition) published by the Royal Society of Chemistry, 2005 and the second edition Validation of Chromatography Data Systems: Ensuring Data Integrity, Meeting Business and Regulatory Requirements 2017
    - Author of Data Integrity and Data Governance: Practical Implementation for Regulated Laboratories, Royal Society of Chemistry, 2019

- Presenter at many training courses on regulatory compliance including analytical instrument qualification, computerised system validation, 21 CFR 11, EU GMP Annex 11. EU GMP Chapter 4 and data integrity

- Presented with the 1997 LIMS Award for contributions and advancement to the subject and teaching
    - Long service teaching awards from the Association of Laboratory Automation and the Society for Laboratory Automation and Screening

- Co-author of a stimulus to the revision process for USP <1058> on Analytical Instrument Qualification published in Pharmacopoeial Forum January – February 2012
  Co-author of the redrafted version of USP <1058> submitted to the USP Council of Experts in August 2013. Issued as in-process revisions in May-June 2015 and May - June 2016 issues of Pharmacopoeial Forum.
  New version of USP <1058> effective 1st August 2017 in USP 40, second supplement.

- Appointed as an Expert Advisor to the USP Sub-Committee for the revision of USP <1058> on Analytical Instrument and System Qualification, March 2021

- Contributor to the GAMP Good Practice Guide on IT Infrastructure Compliance and Control, 2005

- Contributor to second edition of the GAMP Good Practice Guide for Risk-Based Approach to GXP Compliant Laboratory Computerized Systems published October 2012.

- Core industry expert of the GAMP Data Integrity SIG from 2014 – 2022.

- Subject matter expert input and review to the GAMP Guide on Records and Data Integrity (RDI), April 2017. Input and review of the GAMP RDI Good Practice Guide on Data Integrity – Key Concepts 2018 and Core Team Member of RDI Good Practice Guide: Data Integrity by Design 2020.