Assessment of SG Systems V5-Traceability Version 5.8

For Compliance with the Requirements of

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

EU GMP Annex 11 (Computerised Systems) with Chapter 4 (Documentation) Regulations,

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
RDMcDowall Signature	Date 17th October 2023

Document Information

General Information

Project Name	SG Systems Part 11 and Annex 11 Software Assessment
Document Identity (file name)	SG_Systems_V5_Version 5.8_Part 11_Annex 11_ Assessment_V1.6_Draft_20231013.docx

Document Revision History

Version	Date	Reason for Change	Status
V 1.0	09 Apr 2021	Incorporation of final review comments and approve the document	Approved
V 1.1	05 Apr 2023	First draft of V5 Version 5.8 assessment for review	Draft
V 1.2	21 Apr 2023	Minor amendments made and questions returned for comments	Draft
V 1.3	22 May 2023	Incorporate review comments	Draft
V 1.4	06 Oct 2023	Update of report incorporating updated reports and comments plus proposed Annex 11 updates	Draft
V 1.5	13 Oct 2023	Incorporation of feedback	Draft
V 2.0	17 Oct 2023	Final changes and approval of the report	Approved

Table of Contents

1 Executive Summary

1. SG Systems V5 Traceability Version 5.8 software has been assessed remotely for compliance with the technical requirements of FDA's 21 CFR 11 plus EU GMP Annex 11 (Computerised Systems) and Chapter 4 (Documentation) by Dr Bob McDowall, Director, R D McDowall Limited, UK during March – October 2023.

2. The assessment of V5 Traceability was conducted at three levels:
   - Operator and supervisor roles with typical access privileges for using the application
   - System administrator with all access privileges
   - Access outside of the application via the operating system

3. It is important to recognize that compliance with both 21 CFR 11 and EU GMP Annex 11 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 and EU 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 5.8 technical controls for both 21 CFR 11 and Annex 11 are compliant with these regulations such as:
   - Security and Access Controls (both via user identity and password or via Active Directory with single sign on)
   - Device Checks (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)
   - Electronic Signatures
   - Record and Signature Linking

   The system is designed to work electronically and not be a hybrid solution, the latter is not recommended by regulatory data integrity guidances from the World Health Organisation (WHO) and Pharmaceutical Inspection Co-operation Scheme (PIC/S) as well as the proposed update of Annex 11 by European Medicines Agency (EMA) and PIC/S.

   Similar to the majority of applications, the Annex 11 requirement for review of audit trail entries does not currently have a technical control within the application to demonstrate that a reviewer has checked the entries. This must be performed procedurally now.

5. All records are maintained within the database. There is a soft delete available to authorised users only but the impacted records are still available in the database and can be searched with an appropriate report. The rationale for this approach is that all records are required for serialisation and traceability of an ingredient from warehouse lot to use in manufacture of batch(es) of a product.

6. V5 Traceability is designed to work electronically and eliminate paper batch records. 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 V5 already has the capability of paperless working, the system is in advance of the proposed EU GMP Annex 11 update due in 2026 to include *regulatory expectations for digital transformation*.
   The individual requirements of the proposed Annex 11 update and how the current system meets these potential requirements are presented in Appendix 1 of this report.

2 Purpose

The purpose of this document is to report the 21 CFR 11 and EU GMP Annex 11 (computerised systems) in combination with Chapter 4 (Documentation) compliance assessment of the SG Systems V5 Traceability version 5.8 application software performed by Dr Bob McDowall, Director of R D McDowall Limited, UK.

The assessment was carried out remotely between 28th March and 16nd October 2023.

2.1 Software Version Assessed

The application assessed was SG Systems V5-Traceability version 5.8 installed on a laptop running Windows 10.

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. When 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

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 (the preferred option) or MySQL.

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 database 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 or scale 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.

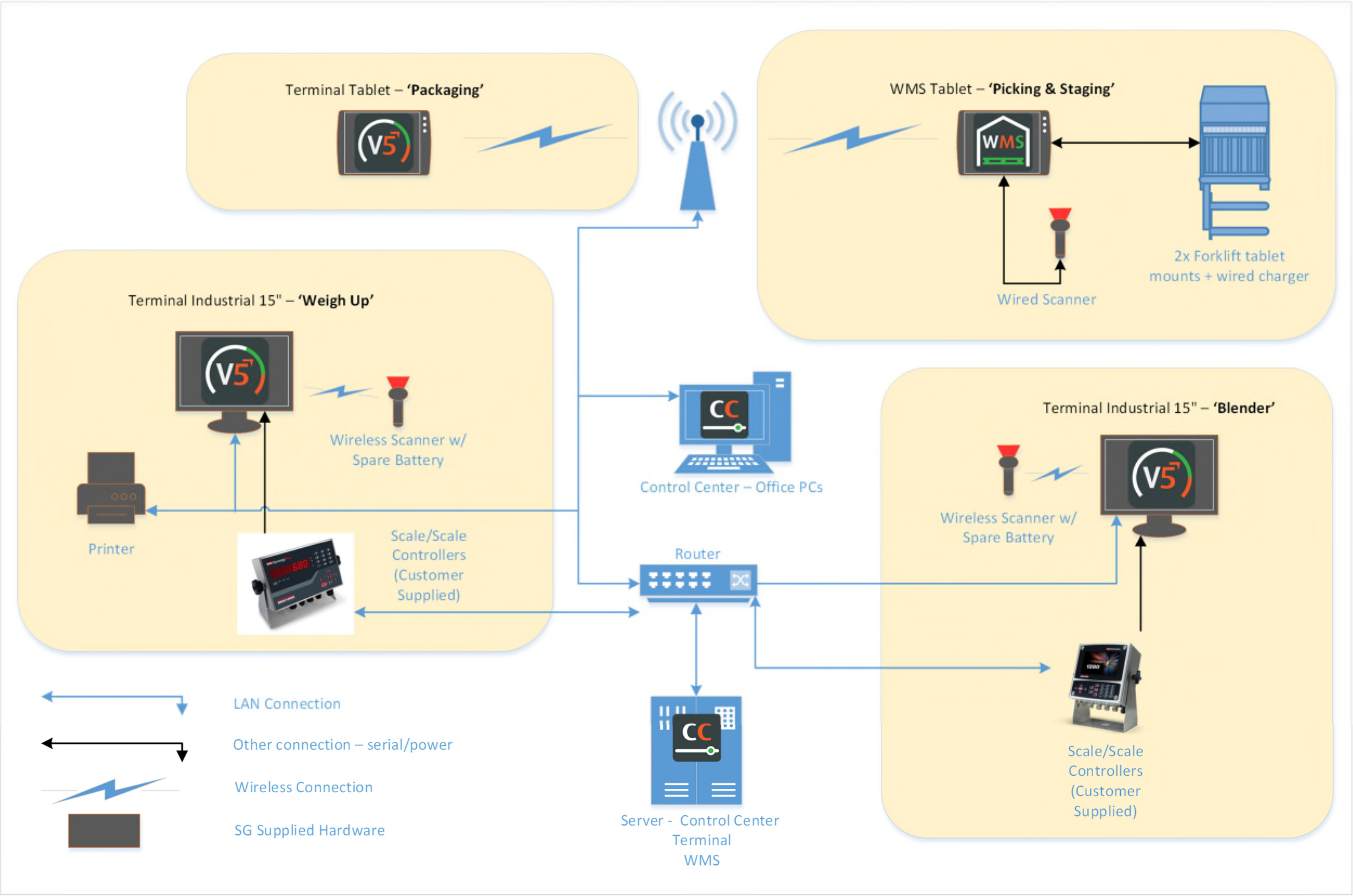

Terminal Tablet – 'Packaging'
WMS Tablet – 'Picking & Staging'
2x Forklift tablet mounts + wired charger
Wired Scanner
Terminal Industrial 15" – 'Weigh Up'
Wireless Scanner w/ Spare Battery
Printer
Scale/Scale Controllers (Customer Supplied)
Control Center – Office PCs
Router
Terminal Industrial 15" – 'Blender'
Wireless Scanner w/ Spare Battery
Scale/Scale Controllers (Customer Supplied)
LAN Connection
Other connection – serial/power
Wireless Connection
SG Supplied Hardware
Server - Control Center Terminal WMS

FIGURE 1: V5 TRACEABILITY SYSTEM ARCHITECTURE

Supervisors and managers can access the system via the V5 Control Center to perform tasks such as formulation and production scheduling.

2.3 Prototyping V5 Functionality using a Virtual Factory

Some customers prototype functionality of the V5 system in a virtual factory environment running on Amazon Web Services (AWS) and operated by SG Systems. In this environment a customer can assess the software and configure it to meet their needs. This approach helps a customer to understand and refine their requirements from which they can update their User Requirements Specifications.

The configured application can then be transferred by SG Systems support staff to the customers installation. Note this if this occurs, the dates of installation in the system will be the date of installation in the cloud not the date of transfer to the customer site and the subsequent IQ/OQ.

2.4 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, regulatory authorities from MHRA (UK), FDA (US), WHO, Pharmaceutical Inspection Cooperation Scheme (PIC/S) regulatory authorities from 54 countries as well as the International Society for Pharmaceutical Engineering (ISPE) through the GAMP Forum, have published data integrity guidance documents. The key aspects for ensuring data integrity and avoiding regulatory citations are presented below which are complimentary and, in some cases overlap, with 21 CFR 11 requirements.

2.4.1 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. The WHO (2016) and PIC/S data integrity guidances both do not recommend hybrid systems and strongly suggest that they should be replaced as soon as possible
- **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 third item in the proposed update of EU GMP Annex 11, discussed in Section 9, *regulatory expectations to 'digital transformation'*.
As V5 already has the capability of paperless working, the system is ahead of the proposed regulatory change.

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

2.4.2 ALCOA, ALCOA+ and ALCOA++ Criteria for Data Integrity

There are five criteria used for data integrity 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) guidelines on computerised systems in clinical trials into nine criteria, now known as the ALCOA+ criteria that are listed below:

- **Attributable:** Identification of the individual who performed an activity and the date that they performed. 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 (on paper or electronically) 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 equipment interfaced should be qualified and calibrated within pre-defined acceptance criteria.
- **Complete:** All data from a production batch including any data generated before a problem is observed, data generated after repeating part or all of the work performed. For hybrid systems, the 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 date (all processes) and time (sometimes paper records and all using a hybrid or electronic systems) time and date stamped in the expected order.
- **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 records can be accessed or retrieved for review and audit or inspection over the lifetime of the record.

In 2023, the EMA Clinical Guideline was updated and introduced a tenth criterion to make ALCOA++:

- **Traceability**: Data should be traceable throughout the data life cycle. Any changes to the data, to the context or metadata should be traceable, should not obscure the original information and should be explained, if necessary. Changes should be documented as part of the metadata (e.g. audit trail). Traceability exists in some of the other ALCOA+ criteria e.g. consistent and accurate but it is implicit. Traceability is the glue that links the data and metadata of other nine ALOCOA+ criteria together for each production batch.

2.4.3 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 (Process owner)	• This role should be allocated to the process owner of the system 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 V5 system clock must be restricted to IT personnel only to prevent time travelling.
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 templates 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.
Automated data capture	• Automated data capture is performed via scales and bar code scanners connected to V5 Traceability. • There are options either to print a record if required or electronic data can be exported from the system in various different file formats
Access to all electronic records for staff performing data review 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.
Using Electronic Signatures	• For paperless operation V5 Traceability uses two electronic signatures. One for the operator performing the batch instructions and operations and one for the individual who reviews the data and audit trail.
Avoid 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

Data Integrity Criterion	How V5 Traceability Meets ALCOA+ Criteria
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. • Enforced tolerance check of the balance used to weigh ingredients • Enforced acceptance criteria for each weighed ingredient: the recipe cannot continue until an ingredient is within limits
Complete data / information	• All records are stored in the V5 Traceability database and can be accessed via Jasper Reports. • 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 changes, user account management, input and execution of recipes etc.
Traceability	• All records and data from the start of the batch to the end of production must be traceable including time and date stamps of all activities and any changes etc.

2.5 User Roles

There are four user roles within the system:

- Operator: person responsible for performing recipe instructions when making a batch
- Supervisor: individual responsible for recipe management and review of data and records before release of a batch
- IT Administrator: In-house individual responsible for user account management as well as support of the IT platform and infrastructure where V5 is installed
- Supplier: individual responsible for application and database maintenance

Within each role there are a number of access privileges that can be tailored to an individual's training and capabilities.

2.6 Standard Reports

There are several standard reports available within the system e.g.:

- List of users and roles
- List of users and access privileges
- List of user logins and failed user attempts
- Application configuration settings

- Audit trail entries for a batch
- The recommendation is that reports are printed to PDF especially for the configuration settings and user roles as this would enable a later printout to be compared with the one generated at initial validation using Adobe Acrobat Pro to identify if there are any changes. If so these can be checked with change requests to see that the system is under control and remains validated.

2.7 Referenced Documents

The following documents are referenced in this assessment report:

2.7.1 Regulations

- 21 CFR 11: Electronic Records; Electronic Signatures Final Rule, 1997
- 21 CFR 211: Current Good Manufacturing Practice Regulations for Finished Pharmaceuticals, 2008
- EU GMP Annex 11 Computerised Systems, 2011
- EU GMP Chapter 4 Documentation, 2011
- EU GMP Annex 15 Qualification and Validation, 2015
- EMA and PIC/S Concept Paper on the revision of Annex 11 of the guidelines on Good Manufacturing Practice for medicinal products – Computerised Systems
  In November 2022 EMA and PIC/S proposed an update to Annex 11 with a new version of the regulation due in late 2026. The proposed changes for technical controls only are presented in Appendix 1.

2.7.2 Regulatory Guidance

- FDA Compliance Program Guide (CPG) 7346.832, Pre-Approval Inspections, Updated in May 2010 but effective from May 2012 contains three objectives:
  Readiness for commercial manufacturing
  Conformance to the application
  Data integrity audit
  Updated again in September 2019 with the same format and with more details of ways to conceal data manipulation
  Updated again in December 2022 with an added 4th Objective of assessing quality in Pharmaceutical Development
- FDA Guidance for Industry, Data Integrity and cGMP Compliance, December 2018
- MHRA Guidance for Industry, GMP Data Integrity, March 2015
- MHRA 'GXP' Data Integrity Guidance and Definitions, March 2018
- World Health Organisation, Good Data and Record Management Practices, TRS 996, Annex 5, June 2016
  This guidance was replaced in 2021, the replacement document is inferior to the 2016 document. The latter contains the best description of ALCOA criteria in any regulatory guidance document
- PIC/S PI-041 Good Practices for Data Management and Integrity In Regulated GMP/GDP Environments, July 2021

2.7.3 Industry Guidance

- Good Automated Manufacturing Practice (GAMP) Guide, Version 5 Second Edition, ISPE, Tampa FL, 2022
- Good Automated Manufacturing Practice (GAMP) Good Practice Guide IT Infrastructure Compliance and Control, Second Edition, ISPE, Tampa FL, , 2017
- Good Automated Manufacturing Practice (GAMP) Guide Records and Data Integrity, ISPE, Tampa FL, 2017
- Good Automated Manufacturing Practice (GAMP) Good Practice Guide Data Integrity – Key Concepts, ISPE, Tampa FL, 2018
- Good Automated Manufacturing Practice (GAMP) Good Practice Guide Data Integrity by Design, ISPE, Tampa FL, 2020
- Good Automated Manufacturing Practice (GAMP) Good Practice Guide on Manufacturing Records, ISPE, Tampa FL, 2019
- Good Automated Manufacturing Practice (GAMP) Good Practice Guide on Enabling Innovation, ISPE, Tampa FL, 2021

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 records that have the 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 the regulations for a number of clients, *whether* pharmaceutical companies or instrument/equipment or software supplier's. 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 training courses on this subject. It has also included advice to suppliers for interpretation of regulations, implementation of compliance features in software or compliance assessment of applications.

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 shown in Figure 2.

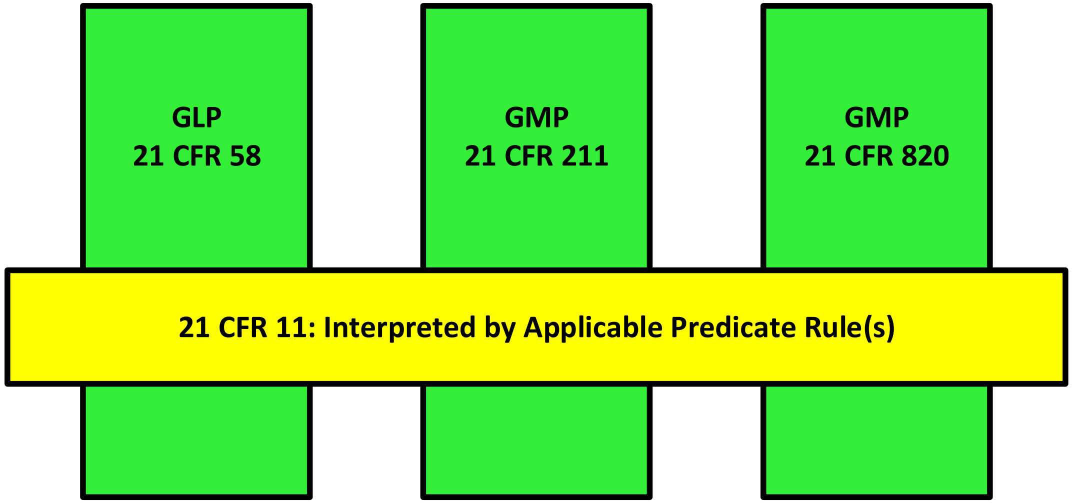


FIGURE 2: INTERPRETATION OF 21 CFR 11 BY THE APPLICABLE REGULATION (PREDICATE RULE)

As V5 Traceability captures all ingredient, recipe and finished product data either from a scale 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 with unique user identities
- Signing of a record at the end of an activity e.g. completion of a recipe execution or the review of a batch record

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 / Annex 11 compliance of V5 Traceability have the following structure:

- Column 1: 21 CFR 11 or Annex 11 reference number.

- Column 2: presents the specific section from the Part 11 / Annex 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:

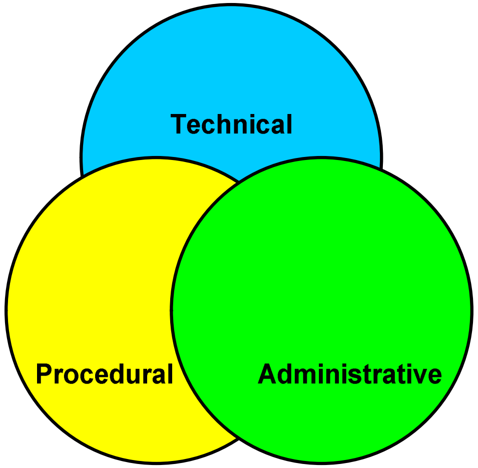
- Administrative controls: e.g. policies for Part 11 and the use of electronic signatures

- Procedural controls: SOPs for using the system

- 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 3 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. Note that for EU GMP Annex 11, there are only procedural and technical controls.



Supplier:
Technical
Controls

Customer:
Procedural &
Administrative
Controls

Figure 3: 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. 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: https://support.sgsystemsglobal.com/v5/modules/users/ The settings of these policies will need to be documented by each regulated customer following their computerised system validation policy and procedures.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
	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. Printing to PDF is advised as this can be used as a basis for future data integrity and periodic review checks as discussed in Section 2.5
PDF	**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.
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.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
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 available, release notes outlining all changes and their impact can be requested by customers. The release notes 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.
11.10(c) / 12	Is concurrent write access by multiple users prohibited?	Tech	Supplier	There is only one record open for a single user at a time.
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 to verify that the backup works should be undertaken as required by Annex 11, 7.2.
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.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
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 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. When the system is installed, the system asks for the name of the engineer who is installing it. Also, when the application is upgraded the system will also prompt for the name of the engineer upgrading the module. 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.
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.
11.10(d) / 19	Does the system have a password-protected inactivity lock enabled?	Proc Tech	Customer Supplier	This needs to be specified and documented in the configuration specifications and set in the application. Yes, there is a configurable option available.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
11.10(d) / 20	Is user access to the Operating System restricted to the System Administrator, or equivalent authorised user?	Proc	Customer	The application is installed on a network server and the IT department can limit access to the directories on the server. .
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 Proc	Supplier Customer Customer	There is a configurable lockout after a pre-defined number of failed attempts. Account lock is also available with Active Directory (Single Sign On). IT administrators can also lock user accounts if required. Part of the system administration SOP should include how to lock user accounts and 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. The IT Administrator role has no access to commodities, batch records, recipes, purchases or sales data and records. As noted in Section 2.5, SG Systems are typically responsible peripherals, equipment and application maintenance.

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. The preferred reporting method is to use Jaspersoft Web Reporting as this is more user friendly. However, 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.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
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 which should be documented as part of their validation of the system.
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.
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	When the system is integrated with Active Directory unsuccessful user attempts are recorded. Account locking is configured and monitored via Active Directory. User log-ons are recorded in the audit trail and can be searched by a report template.
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 lot of product. If permitted there is only an option to vary the batch size, no recipe changes or ingredient substitutions are permitted.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
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 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	No. There are no delete privileges or options in the whole system. There is a soft delete for items such as user identity which remains in the database and can be recovered.
11.10(e) / 42	Are changes to user authority levels and permissions audit trailed?	Tech	Supplier	Yes, there is a report that lists the changes to user privileges

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: the right materials at the right time. There is also an option to prevent an operator bulk producing products (i.e. adding all ingredients at the same time). When a recipe is executed it is assigned to a specific terminal with associated weighing device. There is a visual check of weight tolerance: green or red light that is defined for each ingredient in a specific recipe. If acceptance criteria for an ingredient are not met, the step or task cannot be completed. There is an option prior to production that several lots of the same commodity can be added to the run, and then stock is automatically deducted from these lots according to FEFO/FIFO protocols until the job is complete or lots are exhausted There are messages for operators who scan the wrong item for batch production e.g. • The Commodity For This Step Was Not Found On This Pallet, • Items on this pallet however are required for other steps in this batch A configurable function is Pallet Manager, where a pallet can be given a hold status and it is excluded from production.
	If the sequence of system steps or events is important in a process, is this enforced by the system (as appropriate)?	Proc	Customer	Yes, the recipe must be executed as defined by the customer and described in the question above. Non changes are permitted.

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	No, the application has its own security and access control.
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 The customer should allocate users to either operator or supervisor role

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
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 – see the EU GMP section on Annex 11.
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 under terms of the service agreement Access to the administration functions of the application is an IT function or supplier role and outside of the users of the application.
	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 A recipe can include a check that the 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? *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.*	Proc	Supplier	SG Systems staff have 21 CFR 11 and Annex 11 awareness training applicable to their roles.
11.10(i) / 52	External maintainers of the computerised system?	Proc	Supplier	SG Systems staff have 21 CFR 11 and Annex 11 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.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
	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.
.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.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
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. SG Systems maintain basic training documents on their support website (https://support.sgsystemsglobal.com/v5/) that can help inform customers on the major areas of the system and these are updated as new features are added/old ones retired. Customer specific needs can be catered for with training sessions that are recorded or bespoke documentation if required. 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.
	§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

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
11.50(a) / 3	The meaning of the signature? [11.50(a)(3)]	Tech Proc	Supplier Customer	Yes. There are two roles in the system for performer of the work by an operator and review by a supervisor. The meaning of the signature needs to be defined by the user according to their working practices.
	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	There are two electronic signatures in the system for two separate individuals as operator (performer) and supervisor (reviewer). There is a function to ensure that a supervisor cannot approve their own work. Signature release policy defines which roles can sign for work performed or reviewed. The customer needs to define which users have electronic signatory 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.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
	§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 associated with a specific batch
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. The system is designed to work electronically and customers should not use the system as a hybrid.

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 computer user identity must never be allocated to another individual.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
	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.
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.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Comments
	§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*** (2) ***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.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Comments
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.
	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 within the system to ensure that user identities cannot be duplicated.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Comments
	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 for users that no longer require system access. This could be during a QA audit, data integrity audit or periodic review of the system.
11.300 (b) / 4	Do passwords periodically expire and need to be revised? [11.300(b)]	Tech Proc	Supplier Customer	Yes, there is a user defined password expiry. Passwords expiry can be configured to expire between 1 and 180 days with 90 days as a default Logging onto a new account for the first time, a user must change their default password by entering the new one twice. If a user logs into their account after the password has expired, they are told to select a new password and enter this twice. When integrated with Active Directory additional controls such as preventing reuse of old passwords. 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.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Comments
	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.
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 but allocated to an individual. However, when the application is integrated with Active Directory this is possible.
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 only possible when integrated with Active Directory. An alert can be generated from Active Directory to comply with this requirement. A customer SOP for handling security alerts is required.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Comments
	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 EU GMP Annex 11 and Chapter 4

6.1 European Union GMP Annex 11 and Chapter 4 Updates

In April 2008, the EU issued a proposed update of Annex 11 on computerised systems used in GMP environments, the update was approximately four times the size of the current version that had been in force since 1992. In the draft there was the ability to use electronic signatures for the first time in EU GMP regulations. There were approximately 1400 comments received by the EU and these were used to revise the draft regulation. The new version of Annex 11 was issued in January 2011 and became effective on 30th June 2011. There are some significant changes in the regulations for computerised systems including the requirement to qualify IT infrastructure.

EU GMP Chapter 4 on Documentation was also updated and released at the same time. Although it states that these are “consequential” changes as a result of the update of Annex 11, the current version of Chapter 4 contains major revisions that impact computerised systems that are included in this assessment for completeness. To understand Annex 11 properly you need to read it in conjunction with Chapter 4 especially the sections on Good Documentation Practice (4.7 – 4.9) and Record Retention (4.10 – 4.12).

It is important to realise that when EU GMP mentions documentation there are two main requirements for GMP compliance: instructions (e.g. SOPs and analytical procedures) and records (evidence that instructions were followed).

In November 2022, the European Medicines Agency (EMA) published proposals to update Annex 11, the possible technical controls applicable to V5 are listed and discussed in Appendix 1.

6.2 Annex 11 and Chapter 4 are Equivalent to Part 11

Taken in combination, the regulations for computerised systems in Annex 11 and the new sections in Chapter 4 on the need to define raw data and new records retention requirements can be seen as equivalent to the 21 CFR 11 regulations.

6.3 Annex 11: Applications Validated and IT Infrastructure Qualified

The key requirement in the principle is for software applications to be validated, there is no change here as it has been the situation since 1992 when Annex 11 was first introduced to EU GMP. However, the major change is that for the first time in a regulation is the requirement for IT infrastructure to be qualified, as this is outside the topic of this document. Readers can find further information in the GAMP Good Practice Guide on IT Infrastructure Compliance and Control second edition.

7 EU GMP Annex 11 Regulations for Computerised Systems

Many of the controls required by the new Annex 11 regulations are the same as those for 21 CFR 11. Therefore in this section, where there is direct correlation between the Annex 11 and Part 11 controls the assessment will refer to the Part 11 assessment in the previous section of this document.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	Principle **This annex applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together fulfil certain functionalities.** **The application should be validated;** **IT infrastructure should be qualified.** **Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance.** **There should be no increase in the overall risk of the process.**			
A11/ P/ 01	Has the customer SOPs for computerised system validation?	Proc	Customer	The customer needs to have a procedure for the risk-based validation of computer applications.
A11/ P/ 02	Is the customer's IT infrastructure qualified?	Proc	Customer	The customer needs to have a procedure for the qualification of IT infrastructure including associated software applications. This is important as an unqualified IT infrastructure can nullify the application validation efforts.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	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.**			
A11/ 1/ 01	Has the supplier used risk management during the software development process for the application?	Proc	Supplier	The aim of risk management is to focus development and testing effort on the most critical parts of the application to ensure data integrity and overall quality. When a change request is raised the impact of it is assessed on the system and this determines the extent of specification and testing.
A11/ 1/ 02	Is risk management incorporated in the computer validation SOP and associated procedures?	Proc	Customer	Customers should also incorporate risk management throughout their computer validation procedures: e.g. system level risk assessment to determine if validation is required, risk assessment at the requirements level, risk assessment during change control, etc.
A11/ 1/ 03	Risk can also be managed by selecting commercial products rather than developing custom or bespoke software to automate a process.	Proc	Customer	Customers should select software that is in GAMP Categories 3 and 4 rather than develop custom solutions to minimise the impact of the system on data integrity, patient safety or product quality.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	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**			
A11/ 2/ 01	Have the supplier's development staff been trained in GMP awareness?	Proc	Supplier	SG Systems development and support staff have been trained in Part 11 and Annex 11 awareness.
A11/ 2/ 02	Has the customer established processes for co-operation?	Proc	Customer Supplier	This is achieved through a support agreement that defines the support scope and roles and responsibilities of both parties as per EU GMP Chapter 7 (Outsourcing).
A11/ 2/ 03	Are training records available to demonstrate the appropriate levels of education training and experience to perform assigned tasks?	Proc	Customer	Training records should demonstrate the appropriate level of education, training and experience to perform assigned tasks versus a position description.
	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**.			
A11 / 3 / 01	Has the customer established an agreement with their IT supplier for services and support?	Proc	Customer	A customer needs to establish through a contract or service level agreement the computing services from a supplier or an IT department.
A11 / 3 / 02	Is the agreement with IT service provider in accordance with the requirements of EU GMP Chapter 7 (Outsourcing)?	Proc	Customer	IT Departments are considered as service providers and there needs to be an agreement between production and IT

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
A11 / 3 / 03	Are agreements in place to cover services supplied by SG Systems to the customer?	Proc	Customer & Supplier	Agreements between SG Systems and a customer need to outline the services provided and the responsibilities of both parties.
	3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.			
A11/ 3/ 04	Each customer needs a risk-based procedure for determining if a supplier audit is required or not.	Proc	Customer	The customer's system risk assessment of SG Systems should determine the need for an audit or not.
A11/ 3/ 05	Does the supplier have a quality management system?	Proc	Supplier	SG Systems have a Quality Management System, some of the procedures are available on the web site.
	3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.			
A11/ 3 / 06	Does the customer have a procedure to review supplier documentation?	Proc	Customer	Documentation provided by SG Systems needs to be reviewed to assess if any user requirements have been fulfilled, this needs to be documented e.g. in the customer's validation of the system.
	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.			
A11/ 3 / 07	In the customer's regulatory inspection SOP is there facility to allow inspectors to read supplier audit reports?	Proc	Customer	Customers need to ensure that suppliers know that audit reports can be read by inspectors and that any non-disclosure agreements signed need to include this fact.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	4. Validation **4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.**			
A11/ 4/ 01	Is there a risk-based computerised system validation SOP available?	Proc	Customer	Each customer needs to have a risk-based computer validation procedure that is flexible and fits the work done to the overall risk posed by the system and the data it contains.
	4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process			
A11/ 4/ 02	Is there a means of recording changes to validation documents?	Proc	Customer	This should be part of a customer’s validation and document control procedures.
A11/ 4/ 03	Is there a means of documenting deviations observed during the validation?	Proc	Customer	This should be part of a customer’s validation procedures.
	4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available.			
A11/ 4/ 04	Is there an inventory of all GMP and Non-GMP systems (including spreadsheets) for the organisation?	Proc	Customer	A system level risk assessment should determine the GMP impact of an application and if it needs to be validated or not. Then the application should be listed in the inventory of all computerised systems within the company.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	4.3 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.			
A11/ 4/ 05	Does the customer have a risk assessment process that categorises systems according to risk?	Proc	Customer	Risk management must be applied throughout the computer life cycle as per Annex 11 clause 1. Categories of system risk are important as they define the amount of validation that needs to be performed on each type and extent of the controls that need to be applied to each system.
A11/ 4/ 06	Is there a procedure for writing a system description for critical systems only?	Proc	Customer	Only critical systems need a system description that needs to be kept current. The customer's risk assessment methodology should determine if V5 Traceability is a critical system or not. Some required information for a system description listed in Annex 11 may be found in other documents so the system description should cross-reference these documents rather than repeat the same information.
	4.4 User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact			
A11/ 4/ 07	Does a URS exist that covers the functions that the system must perform (intended use)?	Proc	Customer	A user requirements specification is essential to define the intended use of any computerised system. A computerised system cannot be validated without a current URS (see FDA Guidance for Industry entitled General Principles of Software Validation, section 5.2).
A11/ 4/ 08	Are user requirements traceable throughout the life-cycle?	Proc	Customer	Requirements need to be traceable to the place in the life cycle where they are verified or tested. Therefore they should be uniquely numbered to enable effective traceability.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	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.			
A11/ 4/ 09	Does the computer validation SOP have provision for risk based assessment to determine if a supplier should be audited or not?	Proc	Customer	This links with clause 3.3. The need to audit a supplier and obtain information about the quality system and product development should be based on a risk assessment.
A11/ 4/ 10	There should be a specific assessment to determine if SG Systems should be audited, a remote questionnaire sent or no action required.	Proc	Customer	This requirement links with clause 3.3. The need to audit a supplier and how to obtain quality system and application development information should be based on a risk assessment. This should be stated in the validation documentation.
	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.			
A11/ 4/ 11	Is there any bespoke software in the application?	N/A	N/A	This clause is not applicable to V5 Traceability as it is a commercial product. The software is configured by a customer and there is no bespoke software supplied for the application.
A11/ 4/ 12	How is bespoke software managed?	N/A	N/A	N/A.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	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.**			
A11/ 4/ 13	How are recipes managed?	Tech Proc	Supplier Customer	Once input recipes are version controlled. The differences between two versions can be identified. Input of recipes and versioning need to be validated and under a procedural control
A11/ 4/ 14	How are validation test scenarios linked to the user requirements?	Proc	Customer	Testing scenarios need to be based on the user requirements specification and linked via a traceability matrix. The testing needs to be based on the way the system is used as defined in the URS.
A11/ 4/ 15	How are test cases designed?	Proc	Customer	Test cases should be designed to include testing to pass as well as testing to fail. In addition, testing should include stress testing of limits and error handling especially at critical points of an analysis e.g. where a result is in specification or out of specification.
A11/ 4/ 16	How is testing evidenced?	Proc	Customer	Test evidence can be based on a combination of paper printouts, screen shots (where appropriate), and electronic records within the application such as test reports and audit trail entries.
A11/ 4/ 17	How will automated test tools be assessed for their adequacy?	Proc	Customer	If automated test tools are used in a validation, they need to be qualified to demonstrate that they are fit for purpose.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	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.			
A11/ 4/ 18	Is this a new installation of the application?	N/A	N/A	This clause would not apply for a new installation of V5 Traceability.
A11/ 4/ 19	What happens if this is a new version of V5 Traceability is being implemented?	Tech	Supplier	If the installation is an upgrade to a new version of the system, then SG Systems will provide software utilities for the migration of data. Old data is available in a new version of the application.
A11/ 4/ 20	How will the migration be validated?	Proc	Customer	The customer needs to ensure that the original database is backed up and then migrate the data to the new data base using the software utilities provided. Checks to ensure the completeness and accuracy of the data migration need to be carried out.
	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.**			
A11/ 5/ 01	What controls and checks are there for data acquired from scales interfaced to the system?	Tech	Supplier	A recipe is downloaded to a specific terminal and this is attached to a weighing device, up to 4 scales can be connected via serial interface to the terminal, which in turn links to the database

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
A11/ 5/ 02	How are data acquired from instruments checked for accuracy?	Tech	Supplier	Development of the system ensures that data generated at the balance are correctly transferred to the application database.
		Proc	Customer	Calibration of the balance or scale before connection to the system is the responsibility of the customer.
		Proc	Supplier	Qualification by SG Systems ensures that the instrument and the software are correctly installed and communicate together at a system level in a customer’s facility.
		Proc	Customer	Validation of the installation to demonstrate that the scale / software combination work under actual conditions of use.
A11/ 5/ 03	If V5 Traceability is interfaced to another software package what controls are there to ensure that data are correctly transferred?	Tech	Supplier	There is a flexible approach to data integration via file sharing, SQL injections or by developing middleware to connect via an API. See also the SG Systems web site: https://support.sgsystemsglobal.com/v5/api/
		Proc	Supplier	Testing of the interface is essential and may also include capacity (i.e. stress test) and error handling between the two applications.
		Proc	Customer	Validation of the interface between the two systems is a critical part of the overall system validation that must be specified and tested.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	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.**			
A11/ 6/ 01	What checks are there on the accuracy of data entered manually into the system?	Proc	Customer	If data are entered manually, procedures should be developed to check that these data are correct.
	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.**			
A11/ 7/ 01	How is physical access to the computer room and communication cabinets controlled?	Proc	Customer	Physical access to the computer room / data centre and communication cabinets needs to be restricted to authorised individuals only.
A11/ 7/ 02	How is access controlled to data stored in the system?	Proc	Customer	If required, logical controls can hide the server from all but IT staff so that it cannot be seen on the network. User account management needs to be implemented so that only authorised individuals can access the system.
A11/ 7/ 03	How are stored data checked for accessibility, readability and accuracy?	Proc	Customer	A risk based determination needs to be made to determine the frequency of and extent of checks to be made to ensure that data are readable and have not changed. See the section on Chapter 4 for the record retention period.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	7.2 Regular backups 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.			
A11/ 7/ 04	Has the backup software application been qualified as part of the infrastructure qualification?	Proc	Customer	This is a requirement under the Principle of Annex 11.
A11/ 7/ 05	Is there a backup SOP?	Proc	Customer	There needs to be a backup and recovery SOP within IT that includes media management and provision of evidence that backup has been done.
A11/ 7/ 06	Has the backup and restore of the database been validated?	Proc	Customer	Backup and restore needs to be validated before the system is released for use in an operational environment. Alternatively, the backup application could be validated for a whole facility.
A11/ 7/ 07	Is there a procedure for checking that backups can be periodically restored?	Proc	Customer	Periodic checks that data can be restored from backup media need to take place and be documented.
	8. Printouts **8.1 It should be possible to obtain clear printed copies of electronically stored data.**			
A11/ 8/ 01	Can electronic records within V5 Traceability be printed?	Proc	Customer	Yes, Reports are available of work performed. This function should be included in the validation of the system: a requirement should specify this function and it should be tested as part of the user acceptance tests or PQ phase of the life cycle.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
	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.			
A11/ 8/ 02	Are printouts available to demonstrate if data used for batch release have been changed since the original entry?	Tech	Supplier	When editing formulas, a user would be be prompted for a reason for the change (custom entry or predefined list or both), and then a new formula version would be created. Can be accessed by the version history report to identify the changes between two versions.
A11/ 8/ 03	As the application is involved in generating data for batch release, has this feature been validated?	Proc	Customer	Validation using changed data will demonstrate that this function works acceptably.
	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.**			
A11/ 9/ 01	Is an audit trail needed?	Proc	Customer	Risk assessment of each system is necessary to determine if an audit trail is required or not. However, regulatory changes mean an audit trail in a GMP environment is becoming mandatory – see Appendix 1 for proposed changes to Annex 11. Further, working electronically will require that an audit trail is essential to ensure data integrity.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
A11/ 9/ 02	Is there an audit trail in V5 Traceability?	Tech	Supplier	Yes, V5 Traceability has an effective and secure audit trail to meet GMP requirements. The V5 Traceability audit trail is turned on when the application is installed and cannot be disabled or turned off. See also the detailed comments in the Part 11 section under §11.10(e).
A11/ 9/ 03	Is there a field for a user to add a reason when data are changed?	Tech	Supplier	Yes, there is a field for a user to add the reason for change or there is an option for context sensitive reasons for change.
A11/ 9/ 04	Is the audit trail searchable and can the searches be printed?	Tech	Supplier	V5 Traceability has the ability for users to search the audit trail and the output can be printed to paper or converted to a PDF file.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
A11/ 9/ 05	Is there a means of showing that the audit trail has been reviewed?	Tech	Supplier	V5 Traceability is involved in generating data used for batch release, the audit trail should be reviewed before batch release as part of the second person check of the data. The audit trail does not have a function indicating that a supervisor has reviewed the audit trail that is stored within the system. Currently, this must be conducted procedurally by customer.
		Proc	Customer	A procedure is needed for reviewing the V5 Traceability audit trail, the frequency of this review and how to document the review is required. As the operation of a recipe is fixed and there is positive identification of each ingredient as well as acceptance criteria for the amount added, there is scope for review by exception of the audit trail. This would be subject to a risk assessment. The SOP for this should state that the meaning of the second person review signature means that the applicable electronic records including audit trail entries have been reviewed.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	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.**			
A11/ 10/ 01	Is there a change control SOP for computerised systems?	Proc	Customer	Change control is a customer procedure that needs to incorporate risk assessment to determine the level of revalidation required.
A11/ 10/ 02	Does the change control SOP cover configuration management?	Proc	Customer	The configuration of a computerised system is an input to the change process to help determine the extent and impact of a change. At the end of a change, the system configuration should be updated to reflect the change.
A11/ 10/ 03	How can the release notes from SG Systems help with the change control process for V5 Traceability?	Proc	Supplier	Release notes from a supplier are an input into the change management process to help determine the impact and risk of each change. This will enable the extent of any revalidation to be determined.
	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.**			
A11/ 11/ 01	Is there a process for identifying high, medium and low risk systems?	Proc	Customer	The risk posed by a computerised system determines the frequency of periodic review.
A11/ 11/ 02	Is there a formal schedule for periodic review of all computerised systems?	Proc	Customer	There should be a time table for periodic review of computerised systems within a laboratory where each system is identified with the date of next review.
A11/ 11/ 03	Is there a procedure for periodic reviews?	Proc	Customer	This is an independent and formal audit of all regulated computerised systems on a defined schedule.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	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.**			
A11/ 12/ 01	How is access to the system controlled?	Tech	Supplier	Initial access is via user identity and password. The user identity is linked to further access control mechanisms that define user groups and user types each with configurable access privileges.
A11/ 12/ 02	How is access to V5 Traceability controlled?	Proc	Customer	User account management by the IT Administrator is required to only allow access to a computerised system to authorised individuals. If a user identity is deleted or restored, the SOP should include details of how the system administrator should carry out these operations. Recovery of a user identity should also be included in this procedure.
	12.2 The extent of security controls depends on the criticality of the computerised system.			
A11/ 12/ 03	How is the criticality of security controls determined?	Proc	Customer	A risk assessment will determine the extent of the controls to be deployed: physical, logical or procedural. The controls available in V5 Traceability are technical but need to be configured and implemented by the customer; see also the answers to questions A11/ 12/ 01 and A11/ 12/ 02 above.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	12.3 Creation, change, and cancellation of access authorisations should be recorded.			
A11/ 12/ 04	How are user accounts created, changed and disabled?	Tech	Supplier	The software creates unique user identities within the database. A second account with the same name cannot be created.
		Proc	Customer	User account management should be authorised by the process owner and executed either by a system administrator or the system owner.
		Proc	Customer	Records of current and historical users will need to be maintained similar to Part 11 earlier in this document.
	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.			
A11/ 12/ 05	How are the identities of users working on the system captured by the system?	Tech	Supplier	All actions of individual users are identified in the audit trail and in the records of each recipe. Please see further comments under 21 CFR 11 and clause 9 of Annex 11.
		Proc	Customer	The server must be synchronized with a network time server.
		Proc	Customer	Customers should ensure that user identities or accounts are not shared between two or more users.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	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.**			
A11/ 13/ 01	How are incidents with computerised systems handled?	Proc	Customer	A procedure is required to record all incidents that have occurred with a computerised system, then to classify and analyse each one. A CAPA is required for critical incidents to resolve the issue and prevent it from occurring again.
	14. Electronic Signature **Electronic records may be signed electronically. Electronic signatures are expected to:** **a. have the same impact as handwritten 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.**			
A11/ 14/ 01	How are electronic signatures implemented in V5 Traceability?	Tech	Supplier	V5 Traceability has the technical controls to apply electronic signatures (via user identity and password) to electronic records (i.e. completed recipes) as discussed in the sections on 21 CFR 11.10(e) earlier in this document. Reasons for signing are either performer or reviewer and should be documented in the validation documentation and operational procedures for the system.
A11/ 14/ 02	How are users trained to use electronic signatures?	Proc	Customer	Customers need procedural controls and training to use electronic signatures correctly and effectively as discussed in the section on 21 CFR 11.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	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.**			
A11/ 15/ 01	If a computerised system is used for batch release, how does it restrict the process to Qualified Persons only?	N/A	N/A	This requirement is not applicable as V5 Traceability does not provide the functionality for certification and release of batches by a Qualified Person or Authorised Person.
	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.**			
A11/ 16/ 01	Is there a business continuity plan that has been tested?	Proc	Customer	Customers need to have in place a business continuity plan that covers all computerised systems and the order in which they need to be restored including V5 Traceability. Recovery is dependent on an effective system of backup, therefore the latest backup needs to be available and accessible. The plan must be tested regularly to demonstrate that it works.
A11/ 16/ 02	Is the business continuity plan kept up to date?	Proc	Customer	This plan needs to be revised regularly to keep pace with technical developments and the revision tested to demonstrate that it works.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	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.**			
A11/ 17/ 01	Is there an archiving procedure in place?	Proc	Customer	Archiving is a user driven process that is performed periodically that needs to be controlled by a procedure.
A11/ 17/ 02	Does the system provide the ability to archive data?	Tech	Supplier	Records can be archived within the system and available online as read only.

8 EU GMP Chapter 4 Regulations for Documentation

The current EU GMP Chapter 4 notes in the Principle of the regulation that:

- Good documentation constitutes an essential part of the quality assurance system and is key to operating in compliance with GMP requirements. The various types of documents and media used should be fully defined in the manufacturer's Quality Management System.
- Documentation may exist in a variety of forms, including paper-based, electronic or photographic media.
- The term ‘written’ means recorded or documented on media from which data may be rendered in a human readable form.
- Suitable controls should be implemented to ensure the accuracy, integrity, availability and legibility of documents.
- There are two primary types of documentation used to manage and record GMP compliance: instructions (directions, requirements) and records/reports.
- Records provide evidence of various actions taken to demonstrate compliance with instructions, e.g. activities, events, investigations, and in the case of manufactured batches, a history of each batch of product, including its distribution.

The above is a summary of the Principle from Chapter 4 and readers of this document are encouraged to read the actual regulation to gain a full understanding to the full scope of documents required under this section of EU GMP.

NOTE: That under the scope of Chapter 4, “documents” can include electronic records referred to by the US regulation 21 CFR 11. Therefore to get a full understanding of Annex 11, the relevant sections of Chapter 4 must be included. EU GMP Annex 11 and Chapter 4 taken together are equivalent to 21 CFR 11 regulations, albeit written in a more concise and less legalistic way.

Ref No.	Chapter 4 Requirement and Reference	Control	Responsible	Assessment
	Principle (a portion only) **Records include the raw data which is used to generate other records. For electronic records regulated users should define which data are to be used as raw data. At least, all data on which quality decisions are based should be defined as raw data.**			
C4 / P/ 01	Is there a procedure for defining raw data in computerised systems used to make quality decisions?	Proc	Customer	A procedure is required to define and document raw data used to make quality decisions i.e. successful execution of a recipe. This is similar to the FDA Part 11 Scope and Application guidance that recommends documenting the electronic records within a computerised system.

Ref No.	Chapter 4 Requirement and Reference	Control	Responsible	Assessment
	Generation and Control of Documentation **4.1 All types of document should be defined and adhered to. The requirements apply equally to all forms of document media types. Complex systems need to be understood, well documented, validated, and adequate controls should be in place. Many documents (instructions and/or records) may exist in hybrid forms, i.e. some elements as electronic and others as paper based.** **Relationships and control measures for master documents, official copies, data handling and records need to be stated for both hybrid and homogenous systems.** **Appropriate controls for electronic documents such as templates, forms, and master documents should be implemented.** **Appropriate controls should be in place to ensure the integrity of the record throughout the retention period.**			
C4 / P/ 01	Is there a procedure for ensuring the integrity of electronic records if a system is used electronically?	Tech Proc	Supplier Customer	Controls for ensuring data integrity include quality system development by the supplier, SG Systems. There is no ability to delete data within the system. The database should be located on a networked drive and only accessible by the IT staff responsible for support. Validation of the configured V5 Traceability system by the customer plus training of staff with the availability of procedures.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
C4 / P/ 02	Are controls in place to ensure the integrity of records if the system is used as a hybrid?	Proc	Customer	If V5 Traceability is used as a heterogeneous (hybrid) system the controls needs to be applied to both the signed paper printouts as well as the V5 Traceability database. There must be checks to ensure the two sets of records are the same and consistent. Hybrid systems are not recommended in the PIC/S and WHO data integrity guidance documents. **This not a recommended option**.
	Retention of Documents **4.10 It should be clearly defined which record is related to each manufacturing activity and where this record is located. Secure controls must be in place to ensure the integrity of the record throughout the retention period and validated where appropriate.**			
C4 / 10/ 01	Is there a procedure for defining the records produced by the use of the system (e.g. raw data)?	Proc	Customer	This is similar to the definition of electronic records under 21 CFR 11 and the same document can be used to meet both regulations.
C4/ 10/ 02	Is the location of the records documented?	Proc	Customer	This requirement can be met easily if V5 Traceability is used electronically as this will be the database of the system or any archived database. Otherwise the location of both the electronic records and the signed paper printouts will need to be defined.

Ref No.	Chapter 4 Requirement and Reference	Control	Responsible	Assessment
	4.11 Specific requirements apply to batch documentation which must be kept for one year after expiry of the batch to which it relates or at least five years after certification of the batch by the Qualified Person, whichever is the longer. For investigational medicinal products, the batch documentation must be kept for at least five years after the completion or formal discontinuation of the last clinical trial in which the batch was used. Other requirements for retention of documentation may be described in legislation in relation to specific types of product (e.g. Advanced Therapy Medicinal Products) and specify that longer retention periods be applied to certain documents.			
C4/ 11/ 01	Are records for production batches retained for at least five years after certification by the QP?	Proc	Customer	If records are to be destroyed at the end of the retention period there also needs to be a procedure with evidence that following management approval, the records were destroyed.
C4/ 11/ 02	Are records for investigational medicinal products retained for at least five years after completion or discontinuation of the last clinical trial the batch was used in?	Proc	Customer	If records are to be destroyed at the end of the retention period there also needs to be a procedure with evidence that following management approval, the records were destroyed.
C4/ 11/ 03	Is there a mechanism for archiving records with V5 Traceability?	Tech	Supplier	Using 'SQL Backup Master' the V5 database can be periodically backed up to a specified local or networked location, based on customer preference.. Methods and products are not archived as these are needed in V5 Traceability for subsequent analyses after data has been archived. The archive process is one way and data cannot be retrieved but the database is still able to be read throughout the record retention period.

Ref No.	Chapter 4 Requirement and Reference	Control	Responsible	Assessment
	4.12 For other types of documentation, the retention period will depend on the business activity which the documentation supports. Critical documentation, including raw data (for example relating to validation or stability), which supports information in the Marketing Authorisation should be retained whilst the authorization remains in force. It may be considered acceptable to retire certain documentation (e.g. raw data supporting validation reports or stability reports) where the data has been superseded by a full set of new data. Justification for this should be documented and should take into account the requirements for retention of batch documentation; for example, in the case of process validation data, the accompanying raw data should be retained for a period at least as long as the records for all batches whose release has been supported on the basis of that validation exercise.			
C4 / 12/ 01	Are the data held in a computerised system supporting a Marketing Authorisation?	Proc	Customer	The customer needs to determine if any data held by V5 Traceability constitutes critical data that supports a marketing authorisation for one or more drug products. If a system contains critical data that supports a Marketing Authorisation then the data need to be identified and determined if it needs to be archived for the length of time that a marketing authorisation is in force or it falls into the category where justified retirement and replacement is acceptable.

9 Appendix 1: Proposed Update of Annex 11 Technical Controls

In November 2022, a joint publication from the European Medicines Agency (EMA) and the Pharmaceutical Inspection Co-operation Scheme (PIC/S) gave notice of their intention to update Annex 11 on computerised systems. Although the updated regulation is not intended to be issued until September 2026, there are several areas where the regulation would be enhanced to ensure that:

> *Configuration hardening and integrated controls are expected to support and safeguard data integrity;* ***technical solutions and automation are preferable instead of manual controls****.*

The emphasis is for automated technical controls to replace manual and error-prone procedural controls.

The table below lists the proposed updates to Annex 11:

- No refers to the number in the EMA notification of changes to Annex 11
- A11 Ref is the clause of Annex to be modified
- Proposed Change is the verbatim text from the EMA notification
- Potential Impact analyses the changes on the Supplier or Customer if the regulation is updated according to the proposed change

No	A11 Ref	Proposed Change	Potential Impact
4	Principle	The scope should not only cover where a computerised system “replaces of a manual operation”, but rather, where it replaces ‘another system or a manual process’.	**Customer**: This proposed update should have minimal impact if a V5 system is designed correctly
5	A11 1	References should be made to ICH Q9 (Note added Now ICH Q9(R1) on Quality Risk Management)	**Customer**: Read and apply ICH Q9(R1) principles, if applicable
6	A11 3.1	The list of services should include to ‘operate’ a computerised system, e.g. ‘cloud’ services.	**No impact**: V5 is an on-premises installation
7	A11 3.1	For critical systems validated and/or operated by service providers (e.g. ‘cloud’ services), expectations should go beyond that “formal agreements must exist”. Regulated users should have access to the complete documentation for validation and safe operation of a system and be able to present this during regulatory inspections, e.g. with the help of the service provider.	**No impact**: V5 is an on-premises installation

No	A11 Ref	Proposed Change	Potential Impact
8	A11 3.3	Despite being mentioned in the Glossary, the term “commercial off-the-shelf products” (COTS) is not adequately defined and may easily be understood too broadly. Critical COTS products, even those used by “a broad spectrum of users” should be qualified by the vendor or by the regulated user, and the documentation for this should be available for inspection. The use of the term and the expectation for qualification, validation and safe operation of such (e.g. ‘cloud’) systems should be clarified.	**Not applicable**: to either a SG Systems or a Customer. The system will be validated following risk-based principles.
9	A11 4.1	The meaning of the term ‘validation’ (and ‘qualification’), needs to be clarified. It should be emphasised that both activities consist of a verification of required and specified functionality as described in user requirements specifications (URS) or similar.	**No Impact**: The PIC/S and EMA GMP Glossary defines both terms.
10	A11 4.1	Following a risk-based approach, system qualification and validation should especially challenge critical parts of systems which are used to make GMP decisions, parts which ensure product quality and data integrity and parts, which have been specifically designed or customised.	**Supplier**: controls are already built into V5 modules to ensure recipe components are added in the correct order and amounts. **Customer**: verify that the integrated system meets intended use requirements and that recipes work.
11	A11 4.4	It is not sufficiently clear what is implied by the sentence saying “User requirements should be traceable throughout the life-cycle”. A user requirements specification, or similar, describing all the implemented and required GMP critical functionality which has been automated, and which the regulated user is relying on, should be the very basis for any qualification or validation of the system, whether performed by the regulated user or by the vendor. User requirements specifications should be kept updated and aligned with the implemented system throughout the system life-cycle and there should be a documented traceability between user requirements, any underlying functional specifications and test cases.	**Customer**: A URS is a living document that must be updated as the application is ungraded or new functions are used. Traceability of requirements can be achieved through validation tools or Office products.
12	A11 4.5	It should be acknowledged and addressed that software development today very often follows agile development processes, and criteria for accepting such products and corresponding documentation, which may not consist of traditional documents, should be clarified.	**Supplier:** GAMP 5 Second Edition already has supports Agile Development in Appendices D8 and D9. SG Systems uses Agile development.
13	A 11 6	Guidelines should be included for classification of critical data and critical systems	**Customer**: Data supporting product quality, data integrity and ensuring patient safety should already be defined as critical regardless of the upgrade to Annex 11.

No	A11 Ref	Proposed Change	Potential Impact
14	A11 7.1	Systems, networks and infrastructure should protect the integrity of GMP processes and data. Examples should be included of measures, both physical and electronic, required to protect data against both intentional and unintentional loss of data integrity.	**Customer**: is responsible for ensuring resilient infrastructure, firewalls and cybersecurity measures are available. These measures should already be in place.
15	A11 7.2	Testing of the ability to restore system data (and if not otherwise easily recreated, the system itself) from backup is critically important, but the required periodic check of this ability, even if no changes have been made to the backup or restore processes, is not regarded necessary. Long-term backup (or archival) to volatile media should be based on a validated procedure (e.g. through 'accelerated testing'). In this case, testing should not focus on whether a backup is still readable, but rather, validating that it will be readable for a given period.	**Customer**: Backup and restore are key to ensuring no data loss and disaster recovery measures can work. Both are regulatory requirements now.
16	A11 7.2	Important expectations to backup processes are missing, e.g. to what is covered by a backup (e.g. data only or data and application), what types of backups are made (e.g. incremental or complete), how often backups are made (all types), how long backups are retained, which media is used for backups, and where backups are kept (e.g. physical separation).	**Customer:** These measures should already be in place to protect data as well as the business. Recovery Point Objective (RPO) and Recovery Time Objective (RTO) should be defined and tested.
17	A11 8	The section should include an expectation to be able to obtain data in electronic format including the complete audit trail. The requirement to be able to print data may be reconsidered.	**Supplier:** Audit trail entries are already capable of being exported electronically as PDF
18	A11 9	An audit trail functionality which automatically logs all manual interactions on GMP critical systems, where users, data or settings can be manually changed, should be regarded as mandatory; not just 'considered based on a risk assessment'. Controlling processes or capturing, holding or transferring electronic data in such systems without audit trail functionality is not acceptable; any grace period within this area has long expired.	**Supplier**: V5 already has an audit trail that monitors manual changes

No	A11 Ref	Proposed Change	Potential Impact
19	A11 9	The audit trail should positively identify the user who made a change, it should give a full account of what was changed, i.e. both the new and all old values should be clearly visible, it should include the full time and date when the change was made, and for all other changes except where a value is entered in an empty field or where this is completely obvious, the user should be prompted for the reason or rationale for why the change was made.	**Supplier**: V5 already meets these proposed criteria.
20	A11 9	It should not be possible to edit audit trail data or to deactivate the audit trail functionality for normal or privileged users working on the system. If these functionalities are available, they should only be accessible for system administrators who should not be involved in GMP production or in day-to-day work on the system (see 'segregation of duties').	**Supplier**: Already compliant with this proposed change. The V5 audit trail is active from installation and cannot be turned off.
21	A11 9	The concept and purpose of audit trail review is inadequately described. The process should focus on a review of the integrity of manual changes made on a system, e.g. a verification of the reason for changes and whether changes have been made on unusual dates, hours and by unusual users.	**Supplier**: Searches of audit trail Jasper reports will highlight manual changes. **Customer**: The audit trail for each batch should be reviewed before release.
22	A11 9	Guidelines for acceptable frequency of audit trail review should be provided. For audit trails on critical parameters, e.g. setting of alarms in a BMS systems giving alarms on differential pressure in connection with aseptic filling, audit trail reviews should be part of batch release, following a risk-based approach.	**Customer:** PIC/S and FDA data integrity guidance documents already make it clear that an audit trail for a batch must be reviewed before release
23	A11 9	Audit trail functionalities should capture data entries with sufficient detail and in true time, in order to give a full and accurate picture of events. If e.g. a system notifies a regulated user of inconsistencies in a data input, by writing an error message, and the user subsequently changes the input, which makes the notification disappear; the full set of events should be captured	**Supplier**: The system already complies with this requirement
24	A11 9	It should be addressed that many systems generate a vast amount of alarms and event data and that these are often mixed up with audit trail entries. While alarms and events may require their own logs, acknowledgements and reviews, this should not be confused with an audit trail review of manual system interactions. Hence, as a minimum, it should be possible to be able to sort these.	**Supplier:** Not applicable as these are not generated by the system.

No	A11 Ref	Proposed Change	Potential Impact
25	A11 11	The concept of configuration review should be added. Instead of taking onset in the number of known changes on a system (upgrade history), it should be based on a comparison of hardware and software baselines over time. This should include an account for any differences and an evaluation of the need for re-qualification/validation	**Customer:** This is linked closely with change control and a CMDB is the bast way to document baseline and changed configurations.
26	A11.12.1	The current section has only focus on restricting system access to authorised individuals; however, there are other important topics. In line with ISO 27001, a section on IT security should include a focus on system and data confidentiality, integrity and availability.	**Customer**: IT security should be already implemented to protect the system and the data it contains.
27	A11 12.1	The current version says that “Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons”. However, it is necessary to be more specific and to name some of the expected controls, e.g. multi-factor authentication, firewalls, platform management, security patching, virus scanning and intrusion detection/prevention.	**Customer & Supplier**: this proposed change is too prescriptive and may not be practicable on a manufacturing floor.
28	A11 12.1	It should be specified that authentication on critical systems should identify the regulated user with a high degree of certainty. Therefore, authentication only by means of a ‘pass card’ might not be sufficient, as it could have been dropped and later found by anyone.	**Supplier**: Pass cards are not implemented in the V5 system.
29	A11 12.1	Two important expectations for allocation of system accesses should be added either here or elsewhere; i.e. ‘segregation of duties’, that day-to-day users of a system do not have admin rights, and the ‘least privilege principle’, that users of a system do not have higher access rights than what is necessary for their job function.	**Supplier**: Segregation of duties is already implemented in the system.
30	A11 12.3	The current version says that “Creation, change, and cancellation of access authorisations should be recorded”. However, it is necessary to go further than just recording who has access to a system. Systems accesses and roles should be continually managed as people assume and leave positions. System accesses and roles should be subject to recurrent reviews in order to ensure that forgotten and undesired accesses are removed.	**Customer**: This is good IT practice and should be part of either a data integrity audit or periodic review of GMP systems.

No	A11 Ref	Proposed Change	Potential Impact
31	A11 17	As previously mentioned (see 7.2), it is not sufficient to re-actively check archived data for accessibility, readability and integrity (it would be too late to find out if these parameters were not maintained). Instead, archival should rely on a validated process. Depending on the storage media used, it might be necessary to validate that the media can be read after a certain period.	**Supplier:** See C4/ 11/
32	NEW	There is an urgent need for regulatory guidance and expectations to the use of artificial intelligence (AI) and machine learning (ML) models in critical GMP applications as industry is already implementing this technology. The primary focus should be on the relevance, adequacy and integrity of the data used to test these models with, and on the results (metrics) from such testing, rather that on the process of selecting, training and optimising the models	**Supplier:** There are no plans to implement AI or ML in V5. It may be that data are exported into third party applications for this.
33	NEW	After this concept paper has been drafted and prepared for approval of the EMA GMP/GDP Inspectors Working Group and the PIC/S Sub-committee on GMDP Harmonisation, the FDA has released a draft guidance on Computer Software Assurance for Production and Quality System Software (CSA). This guidance and any implication will be considered with regards to aspects of potential regulatory relevance for GMP Annex 11.	**Supplier and Customer**: The FDA's draft CSA guidance adds little to the body of knowledge for risk-based computerised system validation.

10 Appendix 2: 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

- Thirty years' consulting experience and thirty seven 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 in the FDA and AAPS meeting on Validation of Bioanalytical Methods held in Crystal City, December 1990 and only European co-author of the published proceedings in 1992

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

- Visiting Senior Lecturer / Senior Research Follow, 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 450 peer reviewed papers, scientific articles and book chapters, given over 1,000 presentations and workshops at symposia and meetings.

- 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, February 2005 (ISBN 0-85404-969-X)
  Second edition Validation of Chromatography Data Systems: Ensuring Data Integrity, Meeting Business and Regulatory Requirements (ISBN 978-1-84973-662-6)

- Presenter at many training courses on regulatory compliance including EU GMP Annex 11 and 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.

- 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 – 2020.

- 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
  Core Team Member of RDI Good Practice Guide: Data Integrity by Design 2020.

- Author of Data Integrity and Data Governance: Practical Implementation for Regulated Laboratories, Royal Society of Chemistry, 2019