How to get your SCFN system GAMP5 ready

Document:	**RAC-2612**
Released:	**19-02-2016**
Updated:	
Rel. Software:	**2.0 or later**

Summary

1 Document's Aim

To briefly explain the ISPE GAMP5 Guidelines. To describe the procedures and actions to take along with helpful advice to make the applied project, based on the SCFN software SCADA platform, perform in conformance with these regulations.

This document has been written by SCFN to inform about its concepts and the best way to apply it with digital data recording functions and in the guidelines recommended by the ISPE regulations. This document has no legal value and is not liable in any way to SCFN: it is the client's responsibility to verify that they have developed the application in compliance with the above mentioned regulations along with any updates that may have been made.

1.1 Introduction

The GAMP guidelines relate to the Regulated company and their good manufacturing practices, the responsibility for full compliance of relevant standards ultimately stops there. In GAMP 5 however greater importance has been placed on Supplier Leverage, that is the supplier of a product or service should be aware of the guidelines and adhere to them, this has the effect that Regulated companies can use the suppliers documentation, testing, verification, and quality plan, to prove compliance to regulation authorities. This puts more responsibility to the supplier, and reduces the amount of duplication the Regulated company needs to carry in order to have a compliant system to the required standards.
The key driver behind the evolution of the GAMP guidelines from GAMP 4 to GAMP 5 is to focus attention on patient safety, product quality and data integrity, through categorizing computer systems by risk, novelty & complexity. There is a need to avoid duplication by integrating engineering activities with computer system activities, and to leverage supplier activities whilst ensuring fitness for intended use. The aim is not to restrict but to aid innovation..

1.2 About ISPE

Founded in 1980, the International Society for Pharmaceutical Engineering (ISPE) is a global not-for-profit industry trade group for pharmaceutical science and manufacturing professionals, and has 25,000 members in more than 90 countries.
ISPE aims to be the catalyst for pharmaceutical innovation by providing pharmaceutical industry professionals with opportunities to develop technical knowledge, exchange practical experience, and collaborate with global regulatory agencies and industry leaders. ISPE has worldwide headquarters in Tampa, Florida, USA; its European office in Brussels, Belgium; and its Asia Pacific office in Singapore.
ISPE offers access to industry-standard technical documents, peer-reviewed publications, industry and regulatory resources, relevant continuing education and training, and the first competency-based international certification for pharmaceutical professionals. And is the drive behind the GAMP guides.

GAMP applies to Healthcare industries who produce pharmaceutical, biotechnology & medical devices fall under the embrace of the GAMP guidelines.
The ISPE is an international organization, the GAMP documents are a guide to progress good manufacturing practices world wide. Because the GAMP guidelines are not a standard a company cannot be Certified, Compliant or Approved

Activity to gain more understanding of healthcare automated manufacturing started in the late 80's and early 90's, when greater validation of the pharmaceutical industries was becoming necessary as automated systems played a greater role in healthcare production. The first GAMP guidelines were put into action in March 1994. January 2008 being the latest release of the GAMP 5 guidelines.

The GAMP guide has been updated to keep up with concepts and regulatory & industry developments.

- Avoid duplication of activities, fully integrate engineering and computer system activities so that they are only performed once.
- Leverage supplier activities to the maximum possible extent, while still ensuring fitness for intended use.
- Scale all life cycle activities and associated documentation according to risk, complexity, and novelty; e.g. If the system uses non-configured off the shelf software, complexity, novelty and risk is therefore low. If the system uses programmed software designed specifically for the application, the novelty, complexity and risk is high.

1.3 A comparison between FDA and GAMP guidelines

GAMP focuses on the whole system and the end product, where as the FDA focuses on each process and stage of production that contributes to the end product. FDA guidances are incorporated into the GAMP guidelines.
As the GAMP 5 guidelines have "Automated" built into the name and their philosophy—they envision process and system (computer) validation as integrated entities. An automated process is tested as an installation, operational, and performance qualification to be certain that the automated procedure has been properly installed, tested, and used. By contrast, the FDA's GMP document assumes a manual process with reference to the reality of automated process systems through the separate document 21 CFR Part 11, which defines system validation and provides guidelines for it. The GAMP stresses bottom-line performance, while the FDA stresses the process itself (procedurally and with automation). Under GAMP 5, an investigator would validate the results of an automated analysis system as a functioning analytical unit. Under GMP, an investigator would validate the analytical process of each step of the process.

Similarly, the GAMP focuses on quality assurance (QA). While still emphasizing QA, the FDA approach puts equal weight on the quality control (QC) process, including all aspects of production and operation as well as the final QA overview.
The result is, the FDA has a greater reliance on analysis at all phases, where GAMP has reliance on the final result rather than the interim steps that lead to that result. In short, process understanding (FDA) versus process outcome (GAMP).

2 GAMP Appendices

The following paragraphs contain experts from the GAMP 5 Appendices, and summarizes their content. For further concise information please reference the GAMP 5 guidelines.

2.1 Backup & Restore -appendix O9

The backup and restore should be a well define company procedure. Procedures should exist for regular testing of Backup & Restore operations, which should be documented.

The backup and restore procedure must: ensure the backup operation is to a secure location, ensure integrity of the storage facility, ensure correct recovery to the on-line equipment, and ensure that all activities are logged. Full and incremental backup operations are possible.

The procedure should include: user authorization, full and incremental backup and restore operations, frequency of the backup, location of the stored data, test procedure, which software to backup or restore. Backup & Restore instructions should be securely stored with the backup data.

The latest operating system or software should be able to be restored. All software components required for operation should be included in the backup i.e. operating system, layered software, application software, configuration data; to ensure the full system can be restored.

Once the system is in operation is should be backed up after software modification, and at regular intervals. At least two generations should be kept.

A full backup operation should be performed before a restore operation is carried out. The restore operation must include a procedure to resynchronize with interdependent systems.

2.2 Security Management – appendix O11

The system must ensure against wilful or accidental loss, damage or unauthorized change; and maintain confidentiality, integrity, viability of regulated systems, records, and processes.

Ensure a list of authorized persons is established and maintained, and that appropriate levels of security are managed.

Persons should be made aware that their activities are monitored, and education is supplied to ensure security is maintained.

The security system policy ensures physical security of the system and stored data, access is by user ID & password, with all access activity being recorded.

2.3 Archiving & Retrieval – appendix O13

It must be possible to take records off-line and move them to a different location, to protect against further changes and deletion, and secure against wilful or accidental damage by physical or electronic means.

The application(s) that support the archived data should also be archived. Consider also the operating system and hardware needed to access the records.

Stored records should be checked initially after archiving, and periodically for accessibility, durability, accuracy and completeness. Human readable copies of data must be made available, and electronic signatures must be preserved.

All activity is logged and user authorization is required.

2.4 Electronic Production Records – appendix S2

Electronic records must provide a high level of assurance that the product has been produced according to its specification. Common type of record include, Electronic Device History Record (EDHR), Electronic Batch record (EBR).

Review by exception (RBE) records data to report on critical process exception, and filter production data for limit violations. Communication errors that prevent a critical process being reported must be included in the RBE. When no critical errors occur, the RBE indicates the operation completed without error.

Exception reports should include sufficient contextual information to allow for retrieval of associated data.

The GAMP approach is: processes are maintained within defined tolerances, data & events are recorded; process data is monitored at appropriate intervals, alerts and alarms are generated when tolerances are exceeded. Electronic records are trustworthy, accurate and secure.

2.5 Patch & Update management – appendix S4

Regulated companies should provide criteria for determining threat levels (security & critical process defects), and thus the urgency for applying patches.

First determine what effect applying or not applying the patch or upgrade will have on the compliant system. Configuration records must be kept that show the version and patch level for the system. With change records describing what level of testing was completed.

2.6 Performance monitoring – appendix O3

Performance monitoring is a part of overall preventive maintenance, and uses performance data in diagnosing problems. Trends that indicate performance problems are used as a part of corrective and preventive actions (CAPA) to reduce down time.

Example parameters include:

Servers / workstations / Control systems: CPU utilization, Cache utilization, response time, disk capacity, hardware status, alarms.

Network: Availability of components, network load, broadcasts.

Applications: Error messages, response times, availability to users.

Notification: Console message, Audible & Visual, Email to system operator, SMS or Pager alerts, logging of alerts.

This list is a broad example of the conditions that could be monitored. Please refer to the guidelines for further information.

2.7 Supplier quality and Project planning – appendix M6

The Quality and Project Plan defines how the supplier will fulfil the quality requirements of the project, and how the Quality Management System (QMS) will be applied.

Quality plan:

Introduction

- Who produced the document, under which authority, and for what purpose

- Contractual status of the document
- Relevant policies, procedures, standards & guidelines
- Relationship and reference to other documents, e.g. verification plan

Overview

- The project and technologies used should be described

Quality plan

- Quality related verification activities
- Responsibilities
- Procedures to be followed

User quality requirements

- Take precedent over supplier QMS
- Relevant company requirements

Supplier quality system

- How the regulated company quality requirements will be met
- Which quality activities will be handled under the supplier QMS, and which under the customer QMS
- The activities to be carried out, the procedures to be followed, and the responsibilities should be defined.

Project Plan

Project organization

- The supplier project team, showing personnel and job title
- Supplier contact for complaints etc.
- The interface between the supplier project team and the supplier quality assurance
- Nominated customer contacts

Deliverable items

- Definition of the deliverables and their identification

Activities

- Project milestones, identifiable project events
- Project activities, design reviews, verification
- Personnel allocated to activities
- Planned start and end date of each activity

Additional information

- Who produces, reviews, and approves the specification of the interfaces
- Who produces, reviews, and approves the test specification
- Is a simulator necessary for the interfaces, if so who designs it
- Who is responsible for testing the interface, FAT & SAT (Factory Acceptance Test, Site Acceptance Test)
- Who is responsible for designing and providing test data
- Who produces, reviews, and approves any test reports associated with the interface

2.8 Project change and Configuration management – appendix M8

Any controlled item that undergoes review, approval, or test should be governed by appropriate configuration and change management. Change management should be applied after the first formal approval, to avoid unintentional change.

All components of a computerized system and the changes to them should be controlled. The exact hardware and software configuration should be documented throughout the life of the system.

Responsibilities, procedure and schedules should be clearly defined; and all activities should be documented.

Key change management steps	
Raising a change	Each change is uniquely identified
Change review	Decision to accept or reject clearly defined Scope of change Impact of change What verification is required The associated risk
Change completion	The change has been implemented, documented, verified, and approved by the project manager.

2.9 Supplier Assessment – Appendix M2

Regulated companies require a high level of confidence that computerized systems will meet their technical, commercial, and regulatory requirements. Knowledge, experience, and documentation must be leveraged from the supplier.

Regulated companies require documented evidence of quality and reliability that the computerized systems will consistently perform as intended.

Quality and integrity must be built into the software by the supplier as it cannot easily be added later. The supplier is best placed to document the required evidence during development.

The assessment process should provide a balanced view of the supplier, including positive observations and a list of concerns.

3 GAMP 5 guidelines and SCFN software compliance

1 The Software must be produced in accordance with a system of quality assurance.	Using SCFN software, you will use a software platform produced under a Quality System Management from SCFN. This assures you that specifications, defects, tests, and test results are managed end to end for all software process development. Customers in any case have to validate their own entire applications, and they should develop and execute the validation plans and protocols themselves or outsource these activities.
2 The system should include built-in checks of the correct entry and processing of data.	This can be accomplished in many ways depending on the user's project. Log in and User authorization, limits on a value can be placed, automatic reactions can be implemented, rechecking of data by a different person before processing can be designed in to a system. Data input can be restricted to defined stations, the station on which an action is executed can be protocolled. SCFN software historical manager can restricts data storage to the server computer only, ensuring that the audit trail is generated from a single location. All audit trail records include date and time stamp, node of origination, and operator name.

3 Data should only be entered or amended by persons authorized to do so.	The User Manager of SCFN software can manage security under the most severe restrictions. Authorization requires User ID and Password, even biometric devices or any other external authorization system can also be used to logon a user. Account policies can be implemented in SCFN software with password aging, minimum password length, and account & system lockout after a reasonable number of unsuccessful login attempts. Internal SCFN software security should be used to limit user access to authorized security areas and applications. Data input can be restricted to defined areas or specific users. Any action executed can be protocolled into Audit Trail. SCFN software architecture restricts data storage only where necessary, ensuring the maximum safety of data.
4 The system should record the identity of operators entering or confirming critical data. Entering or amending critical data should be authorized and record the reason for the change.	The 'Audit trail' is achieved through the appropriated historical table or encrypted file, which records the identity of the person, the data being changed, and possibilities for entering the reason or comment is enabled into the project. All SCFN software audit trail records include date and time stamp, node of origination, and operator name.
5 It should be possible to obtain clear printed copies of electronically stored data	All data in SCFN software can be saved into their a proprietary encrypted format or into tables, using in this case the access security of the OS. There are different ways to access to the data: Integrated tools of SCFN software such as: Audit Trail Viewer, Historical Events Log, Report Designer, Customizable Data Grid. Data can be exported into different formats (CSV, XML) and then be processed in external programs or directly can be printed in PDF format and then be archived.

6 Data should be secured by physical or electronic means against willful or accidental damage.	Storage of the data (Archive or backup) can be local or anywhere on the connected network. The protection of data then falls under the site system/network administrator. Data can be stored in SCFN software specific binary encrypted files, therefore modification by an external system is not possible. The data can be further secured by the security system of the Windows file system or the SQL Server/Oracle user management. Customers should establish policies and procedures to ensure that records are retained for an appropriate duration of time.
7 Data should be protected by backing-up at regular intervals.	SCFN software offer the redundant (hot backup) function, or any kind of data back-up can be put in place. Storage of the data (Archive or backup) can be anywhere on the connected network. The protection of data then falls under the site system/ network administrator. Customers should establish policies and procedures to ensure that records are retained for an appropriate duration of time.
8 There should be adequate alternative arrangements for systems which need to be operated in the event of a breakdown, information required to effect recall must be available at short notice.	SCFN software is a fully redundant system, to guarantee the complete support of a hot backup and failure-proof and mission critical stations.
9 A procedure should be established to record and analyze errors and to enable corrective action to be taken.	Reports for Alarm and statistical analysis can be used to produce alarms & events reports through alarms manager. All data are available for later analysis review, either by the use of SCFN software tools. Additionally data can be exported to external systems.

10 When the release of batches is carried out, the system should allow only a qualified person to release the batch.	SCFN software allows to manage authorization levels, that can be placed on any automatic or manual actions. SCFN software can implement User Administration to set authorization levels and control, Windows Active Directory can be also utilized for central access control. All operations are subject to an audit trail recording. Account policies should implement password aging, minimum password length, and account & system lockout after a reasonable number of unsuccessful login attempts. Data input can be restricted to defined areas. Actions or Users on which actions are executed can be protocolled. SCFN software historical manager restricts data storage only where necessary, ensuring that the audit trail is generated from a single location. It is the responsibility of the customer to ensure that all individuals who develop, maintain, or use the systems are properly educated to perform their task. The 'Audit trail' is achieved through the Historical Log, which records the identity of the person, the data being changed and possibilities for entering the reason or comment is designed into the system.
11 Understanding Critical Quality Attributes (CQA), and facilitate Quality By Design (QBD), ensure quality is built into a system. Identify opportunities for process & system improvements, continuous improvements root cause analysis, corrective and preventive actions	SCFN is a group of companies with a quality system management. All internal process of R&D, testing, quality assurance, support are fully managed under quality control system.
12 Persons developing software have the required training, education & experience.	Any SCFN technician have the required qualifications and experience for software development and project management. Customer training is advised to be carried when a new customer or user is established. Continuance training is available to refresh or advance the knowledge, via specific customer training or consultancy. For the specific customer application, it is the responsibility of the customer to ensure that all individuals who develop, maintain, or use the systems are properly educated to perform their task.

13 Evaluate effectiveness of training, maintain records, and ensure training is maintained.	It is the responsibility of the customer to ensure that all individuals who develop, maintain, or use the systems are properly educated to perform their task. SCFN assist customers that can follow the training programs scheduled by SCFN wordwide: webinar, free trainings, custom training.
14 Persons should be made aware of the relevance and importance of their activities	It is the responsibility of the customer to ensure that all individuals use or maintain the systems are properly educated to perform their task. SCFN assist customers with specific training for pharmaceutical good practice and regulations.
15 Backups should be performed at regular intervals, to include: operating system, software, records & data. Each backup should be documented.	The location of data created and used by our products is configurable by the end user, and so provision can be made in the global system administration to perform backup operations and their documentation.
16 Data Restore	Customers are responsible to establish policies and procedures to enable a system to restored and synchronized. The procedure of the regulated company should enforce a backup operation to be carried before a restore operation. SCFN software perform a backup copy for any project changes and track it, and create e friendly environment for any restore project data.
17 Testing	Customers are fully responsible for a complete project test and validation (offline and on line) for its system. Testing and validation activities must be documented under a regulated system. SCFN software has a simulation mode, local or remote debugger to simplify test and validation operations.

18 Protect against willful or accidental loss, damage, or unauthorized change.	The User Manager of SCFN software can manage security under the most severe restrictions. Authorization requires User ID and Password, even biometric devices or any other external authorization system can also be used to logon a user. Account policies can be implemented in SCFN software with password aging, minimum password length, and account & system lockout after a reasonable number of unsuccessful login attempts. Internal SCFN software security should be used to limit user access to authorized security areas and applications. Data input can be restricted to defined areas or specific users. Any action executed can be protocolled into Audit Trail. SCFN software architecture restricts data storage only where necessary, ensuring the maximum safety of data.
19 System access by User ID & Password	SCFN software implements user administration with user ID & Password, external security system interfaces such as Biometric Identification can be utilized if they are designed so that they cannot be used by anyone other than the genuine owner. All access activities are recorded in the historical log. Account policies allows to implement password aging, minimum password length, and account & system lockout after a reasonable number of unsuccessful login attempts. Internal SCFN software security should be used to

20 System access by User ID & Password	SCFN software implements user administration with user ID & Password, external security system interfaces such as Biometric Identification can be utilized if they are designed so that they cannot be used by anyone other than the genuine owner. All access activities are recorded in the historical log. Account policies should implement password aging, minimum password length, and account and system lockout after a reasonable number of unsuccessful login attempts. SCFN software security can be used to limit user access to authorized security areas and applications. Authorization levels are set on dynamic elements, and authorization levels are given under User administration. Windows Active Directory security and the SCFN software User Management do not permit the creation of duplicate user ID's. SCFN software adopt the appropriate functions that ensure that electronic signatures are unique to one individual and cannot be reassigned to any other individual. Customers in regulated environments must be responsible for verifying the identities of individuals using electronic signatures.
21 Archiving	The location of data created by a SCFN software project is configurable by the user, and so provision can be made in the global system administration to perform archiving operations. SCFN software provides archiving capabilities for production data, where records can be taken off line and stored and back upped elsewhere. Archive location can be located on a remote server under the responsibility of the customer about accessibility of the server.

22 Retrivial	Data stored can be made accessible only by the project, as configured by the user. Data access can be managed by Trends, Reports, Data Tables, Historical Log, Data Analisys. Any data can be managed under a redundant system in order to have a mission critical data retrivial.
23 Production Records	SCFN software's reporting tool allows for full reporting of a system, for both on-line (running) or off-line (backed up or archived) operation. Specific reports can be generated, to create batch records, critical process exceptions, review by exception, etc. All reports can be tailored to suit your means from the recorded data.
24 Patch & Update management	SCFN software is regulated under a specific versioning policy, documented completely within the product documentation, supplied with all new product releases or updates, which track any changes have been made or added. Customers are fully responsible for a complete patch and update management for its system.
25 Performance monitoring	SCFN software debugger offer dynamic information that allows the user to keep always monitored performances of its system, in order to prevent critical situation related to loss of performances.
26 Notification	SCFN software Alarm Dispatcher allows to send events and alerts, and receive acknowledgements. Media supported are email, SMS, Voice (text to speech), Fax, together with traditional methods of screen alarms to display active messages and notifications.

27 Supplier quality	SCFN is a group with a quality system management. All internal process of R&D, testing, quality assurance, support are fully managed under the certified quality control system.
28 Project change and configuration management	SCFN software specifications, quality review documents, test specifications & test results, and manuals/help are created for all modifications. All new revisions and service packs come with detailed descriptions of the changes and new additions that have been achieved in this installation. Customers are fully responsible for a complete project changes tracking and configuration management for its system.
29 Supplier essment	SCFN partners have a 20 years history of successful assessment from a variety of customers in regulated industries as food & beverage, oil & gas, pharma & chemical, cosmetics. SCFN has a certified quality system since over 12 years.

This document has been developed by:
SCFN, Italy
Dated: 19 February 2016
Revision: 02

Copyrights:
© Separeco Srl All Rights reserved
SCFN software is a trademark of SCFN
Windows, SQL Server are trademarks of Microsoft inc. Oracle is a
trademark of Oracle inc.
Any other brands or names are property of their respective holders. This

document is subject to change without prior notice.