Validation
A supplier and end users perspective

Revised Edition

Contents

Copywrite and Disclamers

Revision 04, 1 July 2011

Preface

This document is designed to assist suppliers who wish to sell equipment, usually computer based, into the highly regulated pharmaceutical environment and to help end pharmaceutical customers understand the equipment supplier's perspective. It describes the details of validation for those who are new to the subject and describes the development of a suitable documentation set, which I refer to as the pre-validation documentation set.

This pre-validation documentation set should be supplied to the pharmaceutical company with the equipment, this way the company can begin the validation immediately. Remember that the validation process must occur before the end customer can product drug; therefore the turnover package is as important to the end customer as the equipment itself. These validation and compliance issues should be discussed with the pharmaceutical company as soon as possible in the sales negotiations. In this way everyone knows what to expect and when to expect it and what it will cost. Suppliers should ask the customer 'what is your need for validation in this project?' If you are dealing with a pharmaceutical company it is a 100% certainty that they will have validation requirements, without question.

In many cases I have observed this issue does not come up until the equipment is due for delivery and then the arguments begin over increasing costs and slipping schedules. This can be avoided if the subject is brought up at an initial sales project meeting with the customer or OEM representative. They may not know the details of the requirements but they will contact the relevant person within the end company and that person will be involved in the next sales project meeting, no question.

What happens in practice is as follows, the project engineer or the sales contact for the OEM (if the equipment is to be fitted to an OEM machine, an increasing occurrence) does not mention validation requirements, so neither does the equipment suppliers salesman.

Neither of these people may have real validation expertise. So the entire project continues until someone from validation or QA on the customer's site becomes involved as asks what provision has been made for validation.

At which point the equipment supplier is contacted and asked by the validation or QA group who have a detailed list of requirements for FS and IOQ documentation sets and may even request additional documentation and an audit of the company, including a source code review for computer based equipment, which of course the supplier cannot supply without adding costs and time to the project.

The supplier says 'you did not ask for this, so we cannot achieve it without extra costs and additional time.' There will not be an option for the pharmaceutical company to do the work themselves; they are reliant on the leveraging information out of the supplier.

- The validation people are angry with the supplier for not giving them what they need
- The supplier is angry with the project manager or OEM agent for not describing their real needs up front
- The pharmaceutical project manager and his management are angry at the supplier for not giving them what they really needed, even if they did not ask for it in the first place

How do we avoid this; simply by asking the question up front – 'what are your validation needs?' And then by understanding and interpreting the answer.

Now if all Pharmaceutical companies have need for validation and they all have slightly different way of achieving this, how does the supplier fit in?

The supplier has an important role in providing equipment that can be validated. If the customer cannot validate the equipment it is of no use to them. More than this, the equipment should be easy to validate, suppliers owe this as a service to their customers.

Different pharmaceutical companies have different way of validation equipment so this sounds like the supplier has a difficult or impossible job. That is just not the case. Once the rules are understood then the supplier can be of help to all customers and everyone will be satisfied.

Also – do not be afraid of telling the end customer or OEM the validation costs. It would cost the pharmaceutical company far more to have a validation consultant, who is not familiar with the equipment perform this work.

So it is more cost effective for the supplier to make the pre-validation pack than anyone else, use this as a sales tool. Remember that the support can be just the documentation set, or providing assistance with the testing. I emphasise assistance because the supplier is not responsible for the testing, the end customer is and it is he who will report in any regulatory audit, not the equipment supplier.

The documentation set will be created by following a set of rules that will be fully described later in this document, these are as follows.

- Defining the scope of the project in order to understand the validation requirement.
- Carry out a risk assessment by defining any Ethical or GMP Risk (Items that would cause a product recall), defining Business and Operational Risk and finally any H&S Risk
- In the GMP assessment defining if the system has the capability to impact on the Product in terms of Quality, Strength, Identity[1] or Purity?
- Does the system keep records and data that are to be provided to regulators? Does the system create, retain, modify, report or approve GMP related data? If so and it is an end customer requirement, define the scope of the 21CFR part 11 procedural controls.

[1] In packaging we particularly seek to confirm identity. Incorrect component such as leaflets labels or cartons are universally identified as cases for recall.

Introduction

During the early 1990's my company made the transition to being a supplier of PC based packaging security systems to the pharmaceutical industry at the same time as the industry itself began to rationalise its approach to the validation of such devices.

I began to attend courses on validation of computer based equipment and found them useful, but not necessarily centred on the task I was trying to carry out, that of the creation of suitable validation documentation sets to provide to our customers. I must state that the task was hindered by the fact that our equipment was to be fitted to a wide variety of machines with a wide variety of functionality. The traditional approach to equipment and machinery validation relies on the fact that an equipment design has been made for a given solution, as is the case in many applications. A given design of blister machine can be qualified in a specific way, dependant on the design documentation created during its development, likewise a specific device for the creation of pure water. Therefore a single documentation set will usually suffice for most applications.

However, because of the nature of the equipment we supplied, I felt unable to create a single, generic, documentation set for all applications. This documentation came out of a series of papers written by myself over the intervening years on this subject, which I wrote as I rationalised the problem from the supplier and end user perspectives and then presented my results to various groups for their thoughts and comments.

This document therefore aims to inform the would-be supplied of computer based equipment what his regulatory obligations are, how to create the documentation set and provide examples and templates to work from. It also seeks to inform end customers of the way to convey information to the supplier that is relevant to the project.

I try to answer what should be the validation approach for standard computer based equipment undergoing configuration prior to use in a cGMP environment and also provides simple and specific ways to improve documentation structure and incorporate such elements as requirements traceability and risk analysis. It seeks to provide tools that can be used to improve the level of compliance to perform the job correctly from the beginning.

Validation - The Background

Let us start at the very beginning. For many, validation, its planning and activity is a grey area and there are good reasons for this, Pharmaceutical and biotechnology are diverse industries comprising:

- Many different and sometimes very complex processes
- Most engineering and scientific disciplines
- Regulations that govern the manufacture of products which are not to be found in a single document, rather they are scattered throughout a variety of sources and often require a fair amount of interpretation

It is probably impossible to find a single person who understands all of the chemistry, engineering, and regulatory aspects related to drug manufacturing. To complicate this further, equipment manufacturing companies often sell to multiple international markets where regulatory expectations vary.

Validation and Qualification

For me the term validation itself is poorly understood, one classical definition is as follows:

'To provide documented evidence which provides a high degree of assurance that systems, operated within their specified design parameters, are capable of repeatedly and reliably producing a finished product of the required quality.'

Good definition, but what does it mean exactly? There is no real definition of the actual testing to be carried out here i.e. the tasks to be performed. This is why validation becomes so confusing to people and is acted out from fear of the consequences of not carrying them out. It therefore often becomes an after-thought.

Many of the same comments that have been made about validation also can be made about qualification. While the terms are a little vague, the physical activity that people actually do is testing.

What's the difference between qualification and testing? Qualification involves testing systems to demonstrate they do what they are supposed to. In other words - Qualification is testing.

So we **Validate** the system by performing **Qualification** on the equipment.

Testing has meaning only when systems are tested against what is required of them. First we need therefore to stipulate 'this is what the system is supposed to do' and then we need to test to show 'this is what it does.'

What we must not do is apply circular logic that states 'this is what the system is because this is what the system is.'

First we need to make the stipulation of what something is and then we can test for that property, for example, if it was first specified that 'a chair is designed to support the weight of an 80 kilogram,' then it would now be possible to devise a rational and quantifiable test that can measure whether the design intent has been accomplished. So, a qualified system is a tested system.

Qualification = Testing

Why Test?

When a system is tested a tested baseline is achieved. For a given set of conditions, the system has a predictable response. Any test result for that system is valid over time provided the system does not change.

Engineers gain confidence in systems by performing tests that show repeatable results, creating understood and communicable baseline measurements defining a systems performance. Confidence is gained that the system is 'repeatable.' By bringing together a number of repeatable parts the overall equipment is created.

Once a system has changed, a test may or may not be valid. A judgment based on the nature of the change would need to be made to determine whether the test results were still considered valid or whether the system would need to be re-tested to find out if that same result is received the second time around. The change may be such that a new test needs to be devised to demonstrate some new system requirements or attributes. It requires the investment of significant time and money to achieve a tested baseline through a rigorous program of specification and testing. Therefore, it makes sense to protect that asset by managing the system so there is confidence that the tested baseline is current over time. In order to achieve this, all aspects of the system need to be controlled, including:

- The physical components of the system
- The people who use and maintain the system
- Associated information and documents
- Ongoing changes made to the system, both planned and unplanned

To summarise, an activity-based definition of validation consists attesting and management to maintain the tested baseline. Testing and management are equally important. A tested baseline that is not managed quickly becomes outdated. Procedures that are implemented to manage a system that hasn't been properly tested, do not improve the assurance of the system response for a given set of inputs, regardless of management efforts.

The tested baseline should be thought of as a physical thing. The majority of the discussion that follows proposes ideas and techniques that can be employed to develop and maintain the tested baseline. The format of the tested baseline and the way in which it is created are critical factors in its ongoing maintainability. The ideas presented are intended to promote and facilitate this maintainability.

Most 'validation' projects are in fact 'qualification' projects. There is often very little management of the tested baseline that is handed over at the end of the project. As a result, the tested baseline is nearly always compromised with the passing of time resulting in systems 'falling out' of validation. This usually results in the whole qualification exercise having to be repeated.

To avoid this situation, it might be useful to focus on the activities being performed. Rather than describing a system as 'validated,' as if it were a property of the system, it would be better practice to say the system is 'under validation.' This better indicates there is a method in place to continuously manage and control the system in an ongoing way to keep the tested baseline current. It is interesting to note that testing and management are commonly understood activities which have been performed by humans for thousands of years to achieve some quite remarkable things. When good science and engineering and good project management are used, validation is nothing new and nothing extra. Now, in order to formulate meaningful tests, there must be pre-determined requirements. There must be a specification that says 'this is what it is supposed to be' and then a corresponding test that shows 'this is what it is.' Where failure can occur is as follows:

- If there are no specified requirements, there can't be meaningful testing.
- If there are no meaningful tests, it is not possible to achieve a tested baseline.
- If there is no tested baseline, there is nothing to manage.
- If there is nothing to manage, the system can't be 'under validation,' i.e. under control.

Therefore, it can be deduced that requirements are fundamental to validation. And yet, it is still common to find 'validated' systems with no definition of what the system is supposed to do.

Regulatory Requirements and CSV

Computers are more and more widely used during manufacturing of drugs and medical devices.

Computers appear in at types of packaging machinery and the ancillary devices that appear on them, like printers and visions systems.

Proper functioning and performance of software and computer systems play a major role in obtaining consistency, reliability and correctness of the manufactured product.

Therefore, computer system validation (CSV) should be part of any good development and manufacturing practice. It is also demanded by groups like FDA regulations and guidelines through the overall requirement that 'equipment must be suitable for its intended use'. Gamp 5[2] itself is specifically named 'A risk based approach to compliant GxP computerized system'

Specific requirements for computers can be found in section 211.68 of the US cGMP regulations:

- Automatic, mechanical, or electronic equipment or other types of equipment, including computers, or related systems that will perform a function satisfactorily, may be used in the manufacture, processing, packing, and holding of a drug product. If such equipment is so used, it shall be routinely calibrated, inspected, or checked according to a written program designed to assure proper performance. Written records of those calibration checks and inspections shall be maintained
- Appropriate controls shall be exercised over computer or related systems to assure that change in master production and control records or other records are instituted only by authorized personnel
- Input to and output from the computer or related system of formulas or other records or data shall be checked for accuracy
- The degree and frequency of input/output verification shall be based on the complexity and reliability of the computer or related system
- A backup file of data entered into the computer or related system shall be maintained except where certain data, such as calculations performed in connection with laboratory analysis, are eliminated by computerization or other automated processes. In such instances a written record of the program shall be maintained along with appropriate validation data

- Hard copy or alternative systems, such as duplicates, tapes, or microfilm, shall be designed to assure that backup data are exact and complete and that it is secure from alteration, inadvertent erasures, or loss shall be maintained

Typical Industrial PC

[2] GAMP 5 a risk based approach to compliant GxP Computerized systems © ISPE 2008. Revision5 issued June 2008.

FDA has developed several specific guidance documents on using computers for other FDA regulated areas. Most detailed is the Industry Guide: General Principal of Software Validation. It deals with development and validation of software used in medical devices. The FDA has released draft guidance on using computers in clinical studies. The guidance states FDA's expectations related to computer systems and to electronic records generated during clinical studies.

Specific requirements for computers and electronic records and signatures are also defined in FDA's regulations 21 CFR Part 11 on electronic Records and Signatures. This regulation applies to all FDA regulated areas and has specific requirements to ensure trustworthy, integrity and reliability of records generated, evaluated, transmitted and archived by computer systems. In 2003 the FDA published guidance on scope and applications of 21 CFR Part 11. In this document the FDA promoted the concept of risk based validation.

By far the most detailed and most specific official document that has ever been developed on using computers in regulated areas is the 'Good Practices Guide on Using Computers in GxP Environments'.

It has been developed by inspectors for inspectors of the PIC/S [3]but is also quite useful for the industry. It has more than 50 pages and includes a six page checklist recommended to be used by for inspectors.

Because of their importance, computer validation issues have been addressed by several industry organizations and private authors:

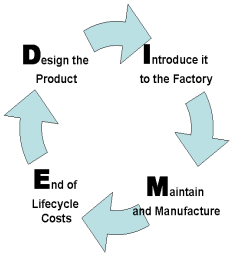
- The Good Automated Manufacturing Practices Forum (GAMP) has developed guidelines for computer validation.
- The PDA[4] has developed a technical paper on the validation of laboratory data acquisition system.

All these guidelines and publications follow a couple of principles:

- Validation of computer systems is not a one time event. It starts with the definition of the product or project and setting user requirement specifications and cover the supplier selection process, installation, initial operation, going use, and change control and system retirement. This is the life cycle model
- All publications refer to some kind of life cycle model with a formal change control procedure being an important part of the whole process.
- There are no detailed instructions on what should be tested. All guidelines refer to risk assessment for the extent of validation

[3] Pharmaceutical Inspection Convention Scheme.
[4] Parenteral Drug Association.

While in the past computer validation was more focused on functions of single user computer systems, recently the focus is on network infrastructure, networked systems and on security, authenticity and integrity of data acquired and evaluated by computer systems. Validation of software loaded on a computer, which is used to control equipments, to capture raw data, to process the data and to print and store. Software typically includes operating systems, standard applications software and software written for a specific user.



Development of Documentation Required by Regulations

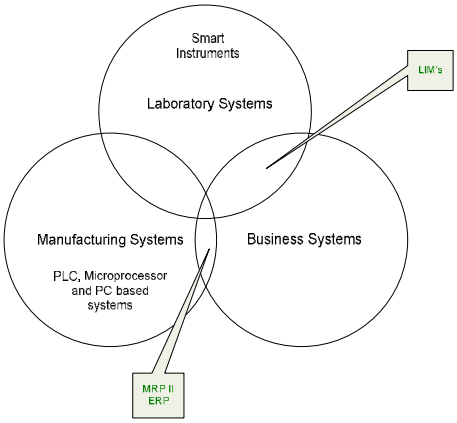
Risk assessment and risk based validation will be discussed for all validation phases to optimize validation efforts vs. costs for systems with different impact and risk on product quality. This is especially important since the FDA has been using and supporting the risk based approaches for compliance as part of the 21st century drug cGMP Initiative.

One of the main purposes of this document is to answer the key question regarding validation: How much validation is needed and how much is sufficient for a specific computer system? This gives a good overview and lists major validation steps and tasks but for an in depth understanding and for easy implementation readers are recommended to read further references.

Computers in the pharmaceutical industry perform three types of task:

1. Control of process and packaging equipment, control of ancillary inspection and printing devices.
2. Data acquisition
3. Data analysis

Most systems do a mixture of some or all of these functions. Again there may be more than one computer in the system and they perform some type of interaction. Computer systems are becoming more integrated, the trend today is to directly send production information to the packaging line to configure the manufacturing equipment directly for example. The computer her will not work in isolation, more often than not the system will by a part of a network of computers exchanging data to provide the required services.



Interaction

Therefore it is important to define the topology of the system as the first step in the validation strategy; this defines the scope of the project. I follow these important steps:

Detail, or have detailed, the system within a separate document, this can be the URS; however I find a well defined Functional Specification (FS) invaluable at this time. Within this FS we define the following:

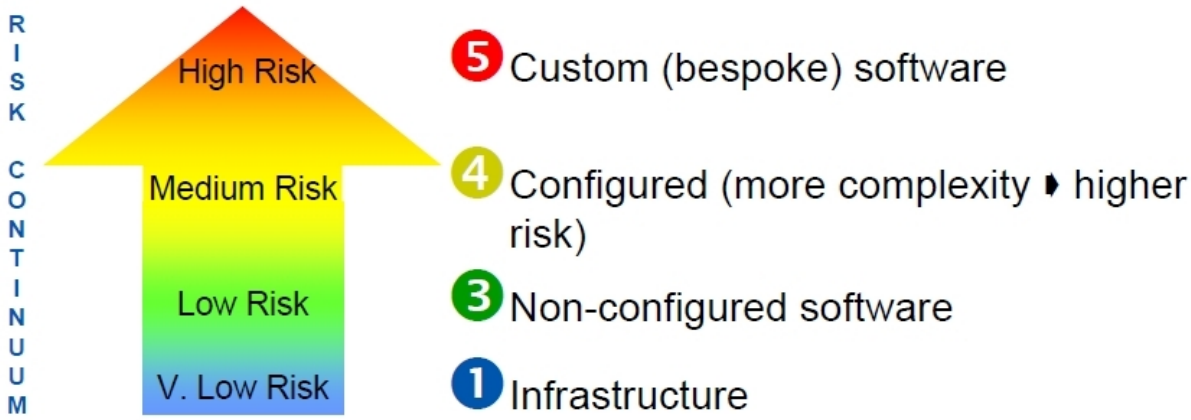
- Identify and list the system functionality as it relates to the end **Product**, the **Process**, the **Plant,** its **People** and its **Procedures** (the five P's)
- Identify the **Software** and **Hardware** of the system
- Identify the **Scope** of the system
- Identify the **Interfaces**

Now assess the system in the following way by a risk assessment. Define any Ethical or GMP Risk (Items that would cause a product recall), define Business and Operational Risk, finally any H&S Risk. In the GMP assessment define if the system has the capability to impact on the Product in terms of Quality, Strength, **Identity** or Purity? Does the system keep records and data that are to be provided to regulators? Does the system create, retain, modify, report or approve GMP related data?

Software categories

Category	Description	Typical Examples	Typical Approach
1. Infrastructure Software	. Layered software (i.e., upon which applications are . Software used to manage the operating environment	· Operating Systems · Database Engines · Middleware · Programming languages · Statistical packages · Spreadsheets · Network monitoring tools · Scheduling tools · Version control tools	· Record version number, verify correct installation by following approved installation procedures · See the *GAMP Good Practice Guide: IT Infrastructure Control and Compliance*
3. Non-Configured	Run-time parameters may be entered and stored, but the cannot be configured to suit the business process	· Firmware-based applications · COTS software · Instruments (See the *GAMP Good Practice Guide: Validation* of *Laboratory Computerized Systems* for further guidance)	· Abbreviated life cycle approach · URS · Risk-based approach to supplier assessment · Record version number, verify correct installation · Risk-based tests against requirements as dictated by use (for simple systems regular calibration may substitute for testing) · Procedures in place for maintaining compliance and fitness for intended

Category	Description	Typical Examples	Typical Approach
4. Configured	Software, often very complex, that can be configured by the user to meet the specific needs of the user's business process. Software code is not altered.	· LIMS · Data acquisition systems · SCADA · ERP · MRPII · Clinical Trial monitoring · DCS · ADR Reporting · CDS · EDMS · Building Systems · CRM · Spreadsheets · Simple Human Machine Interfaces (HMI) Note: specific examples of the above system types may contain substantial custom elements	· Life cycle approach · Risk-based approach to supplier assessment · Demonstrate supplier has adequate QMS · Some life cycle documentation only by supplier (e.g., Design Specifications) · Record version number, verify correct installation · Risk-based testing to demonstrate application works as designed in a test environment · Risk-based testing to demonstrate application works as designed within the business process · Procedures in place for maintaining compliance and fitness for intended use · Procedures in place for managing data
5. Custom	Software custom designed and coded to suit the business process.	Varies, but includes: · Internally and externally developed IT applications · Internally and externally developed process control applications · Custom ladder logic · Custom firmware · Spreadsheets (macro)	Same as for configurable, plus: · More rigorous supplier assessment, with possible supplier audit · Possession of full life cycle documentation (FS, DS, structural testing, etc.) · Design and source code review



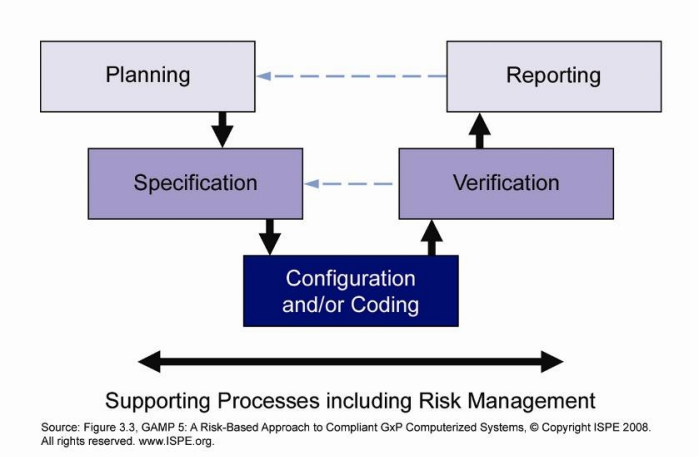
Validation Overview

Validation of computer systems is not a once off event. Annex 11 of the European GMP directive is very clear about this: Validation should be considered as part of the complete life cycle of a computer system. This cycle includes the stages of planning, specification, programming, testing, commissioning, documentation, operation, monitoring and modifying.

For new systems validation starts when a supplier delivers a machine or equipment which is based on computer control. For an existing system it starts when the system owner gets the task of bringing the system into a validated state.

Validation ends when the system is retired and all-important quality data is successfully migrated to the new system. Important steps in between are validation planning, defining user requirements, functional specifications, design specifications, validation during development, supplier assessment for purchased systems, installation, initial and ongoing testing and change control. In other words, computer systems should be validated during the entire life of the system.

Because of the complexity and the long time span of computer validation the process is typically broken down into life cycle phases. Several life cycle models have been described in literature. One model that is frequently used is the V-model [5]as shown here.



Source: Figure 3.3, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

This model comprises of User Requirement Specifications (URS), Functional Specifications (FS), Design Specifications (DS), development and testing of code, Configuration Testing (IQ), Functional Testing (OQ) and Requirement Testing (PQ).

Terms used

Some industry groups however want to eliminate the terms “validation,” “qualification”, and IQ, OQ, PQ The complaint is that these carry baggage and can lead to “over-documentation”.

The use of “Verification” based on “good engineering practice” was advocated.

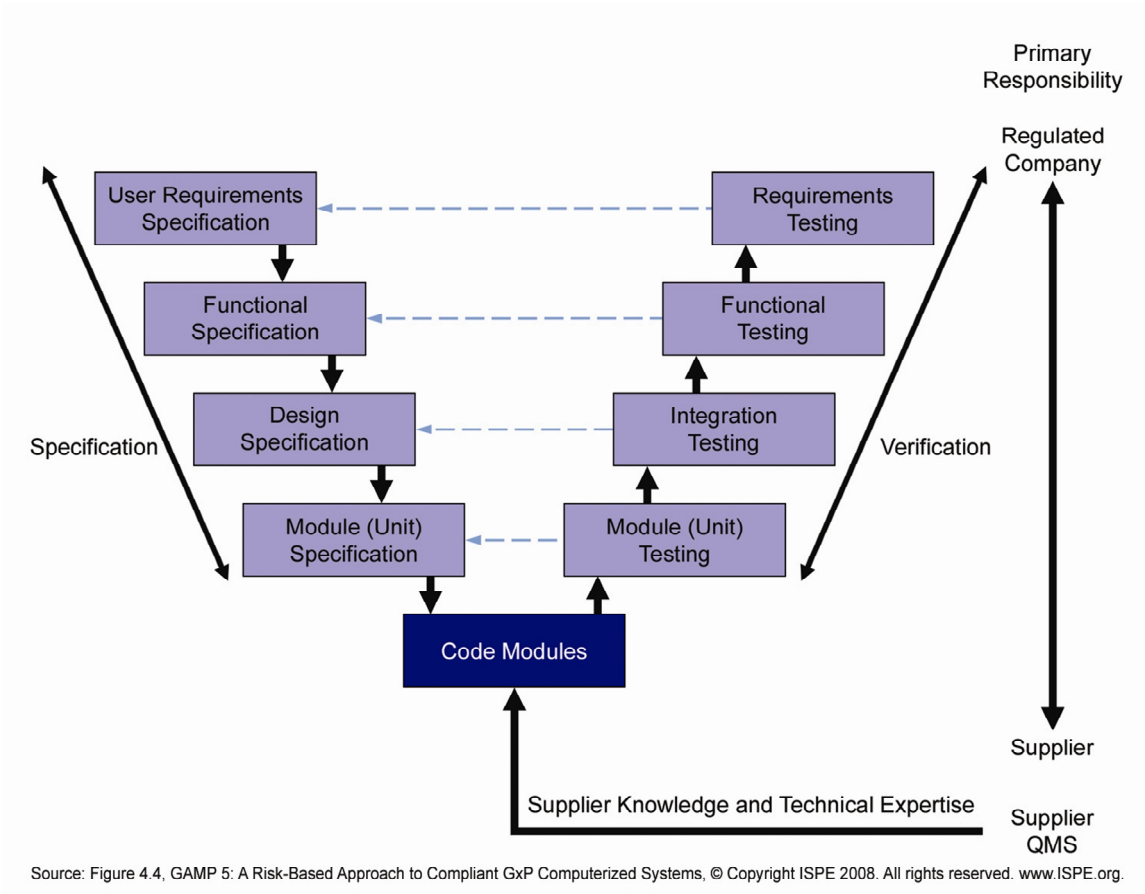
- Many companies are unwilling to abandon terminology that works for them
- *GAMP® 5* strives to be terminology-neutral

[5] GAMP makes great use of the V model.

V-Model Software Development

The **V-model** is a software development process which can be presumed to be the extension of the waterfall model. Instead of moving down in a linear way, the process steps are bent upwards after the coding phase, to form the typical V shape. The V-Model demonstrates the relationships between each phase of the development life cycle and its associated phase of testing.

The V-model deploys a well-structured method in which each phase can be implemented by the detailed documentation of the previous phase. Testing activities like test designing start at the beginning of the project well before coding and therefore saves a huge amount of the project time.



Source: Figure 4.4, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

The V-Model as described above is quite good if the validation process also includes software development.

The extent of validation depends on the complexity of the computer system. The extent of validation at the user's site also depends on the widespread use of the same software product and version. The more that standard software is used and the less customisation made for such software the less testing is required by individual users. GAMP 5 has developed software categories based on the level of customisation. In total there are four categories defined in GAMP 5. We are usually concerned with two of them.

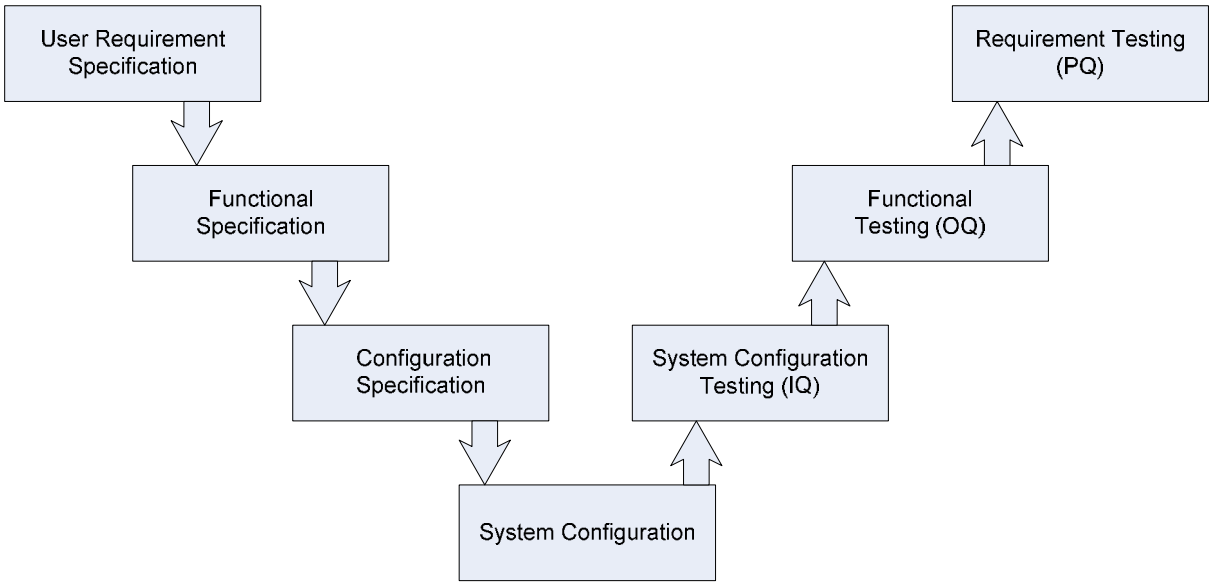
Category one defines operating systems and firmware of automated systems. In the context of this document only categories three, four and five are of interest to us. They are described below. Each computer system should be associated to one of the three categories.

CSV Life cycle for a category 5 system

When considering category 5 system the following must be in existence:

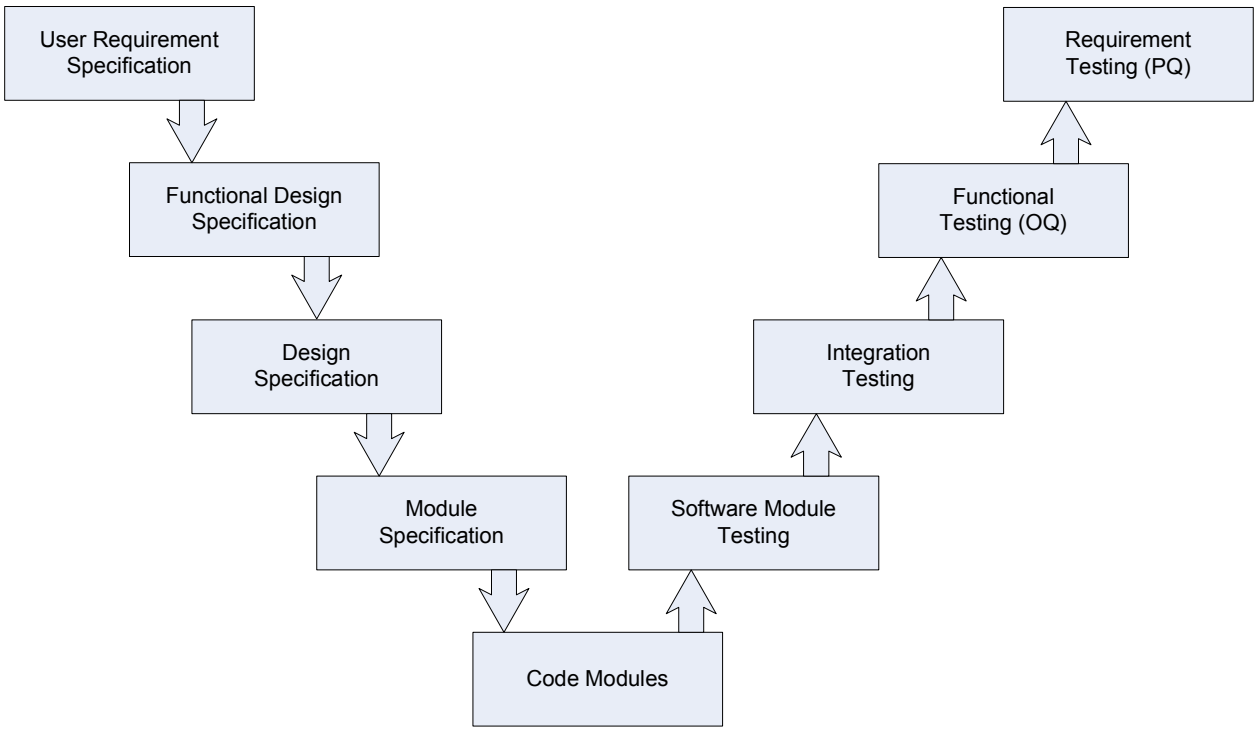
- The existence (and use) of an appropriate quality system during the original development of the computerised system
- Thorough design review during development and manufacture and thorough testing against requirements specifications
- Comprehensive documentation of the full development life-cycle
- Controlled and documented procedures and records for the system's operational life
- Controlled and documented phase-out and data archival/migration at the end of the system's life

GAMP Level 4



A GAMP 5 level 4 system reflects the configuration of a standard system which may be composed of different software and hardware modules.

GAMP Level 5

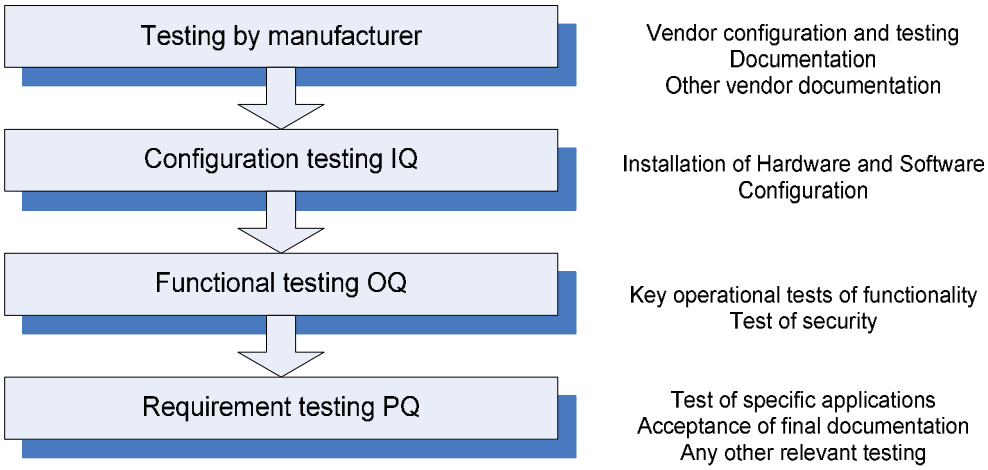


In a GAMP 5 level 5 system we are considering the design of new equipment.

A GAMP 5 level 4 category system, where the system is a standard Hardware and Software product that is in serial production and only configuration is needed to make it operational.

Phases like design specification or code development and code testing are not necessary provided that adequate design and testing documentation exists for the system.

For such systems the simple 4 step model is recommended with just four phases: Testing of system by manufacturer, installation qualification (IQ), operational qualification (OQ), and performance qualification (PQ).



As previously described, the 4 Step model is not suitable when systems need to be programmed for specific applications or when additional software is required that is not included in the standard product and is developed by the user's firm or by a 3rd party.

This means that the system immediately moves into a **GAMP 5 level 5** category system. In this case a life cycle model that combines system development and system integration is preferred. An example is shown on the next page.

GAMP documentation is controlled and issued by the ISPE[6].

[6] International Society of Pharmaceutical Engineers.

Ten Guiding Principles of GAMP 5

1. Guidance will satisfy all current regulatory expectations for CSV.
2. Consolidated framework will fit any automated system.
3. Guidance will cover complete life cycle.
4. Promote benefits of understanding business processes.
5. Fully integrate risk management throughout life cycle.
6. Focus on systems impacting public health.
7. Focus where regulations require controls beyond “good practice”.
8. Clarify Roles and Responsibilities.
    - By discipline / function
    - User / Supplier
9. GAMP® is a trademark, not a certification.
10. GAMP® is based on and consistent with established international standards.

A Definition of the Difference between Level 4 and 5

One definition to apply when discussing level 4 and level 5 systems is as follows:

- With a level 4 system the development life-cycle and all other controls are made by the manufacturing company, the end user is only responsible for the parameterisation of the system
- With a level 5 system the development life-cycle and all other controls are made by the end user.

How then could this these V diagrams apply to a company designing new computer based equipment for a general market, who then have two needs:

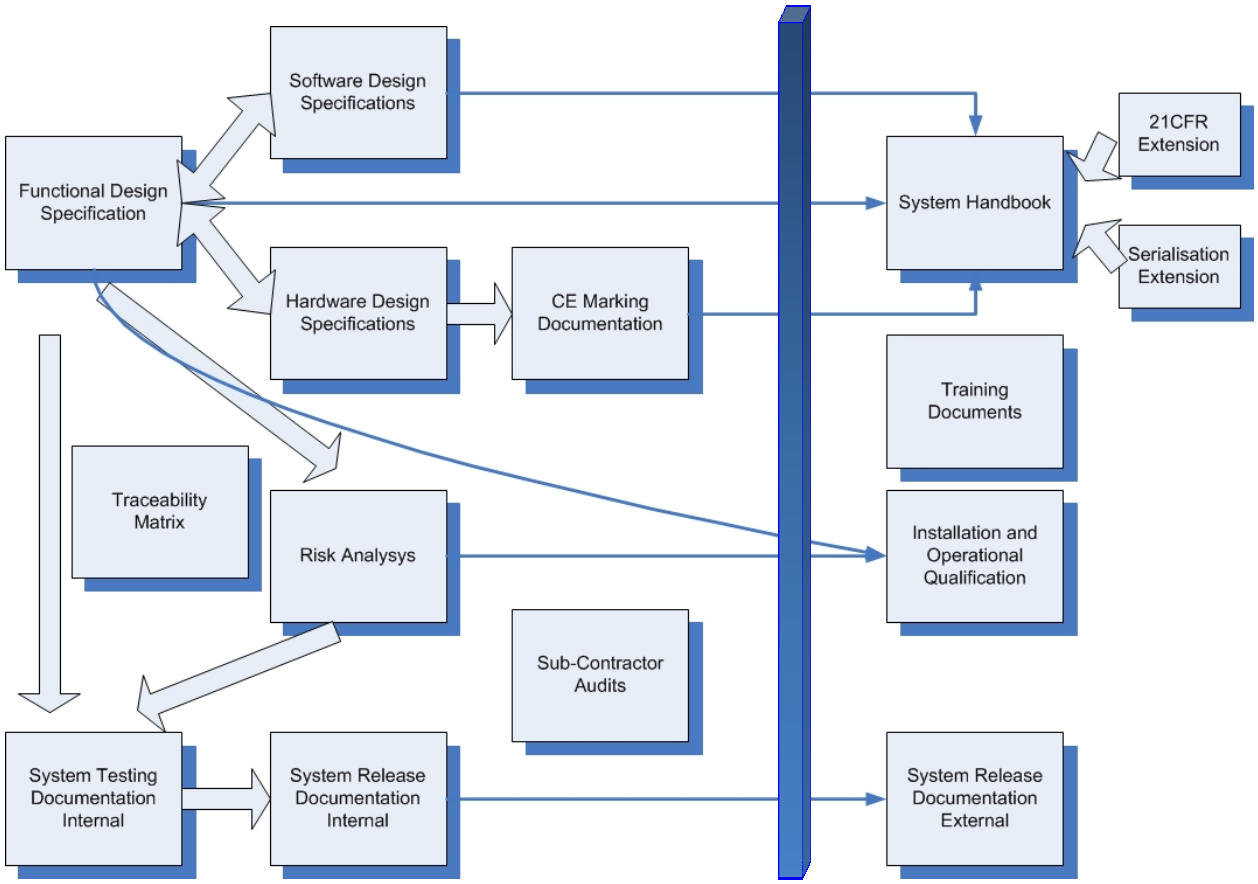
- To supply configured versions of their standard product for say 80% of the market needs
- To perform partial redesign as needed to address the remaining 20% of the market needs

This means that to fulfill all customer requirements there will be a need to redesign equipment for future markets. The following double V diagram or ‘W’ diagram seeks to address that requirement.

General Guidance

Unique, clearly identified, and testable specifications provide greater understanding to all. There is no point in having a specification or requirement if it cannot be tested in some way. How can it be confirmed as even having been delivered by the supplier? In fact this does not just apply to validation in the pharmaceutical industry. Regardless of the industry, at some point suppliers expect to be paid for goods delivered or services rendered. It is common sense to assure oneself that the product is what was wanted and is what it purports to be before it is paid for; this is just prudent contract and financial management.

Master Documentation Relationship



Please note the central importance of the Risk Analysis. The items to be analysed for risk are drawn from the Function Design Specification and directly influence the Qualification testing and internal system testing work.

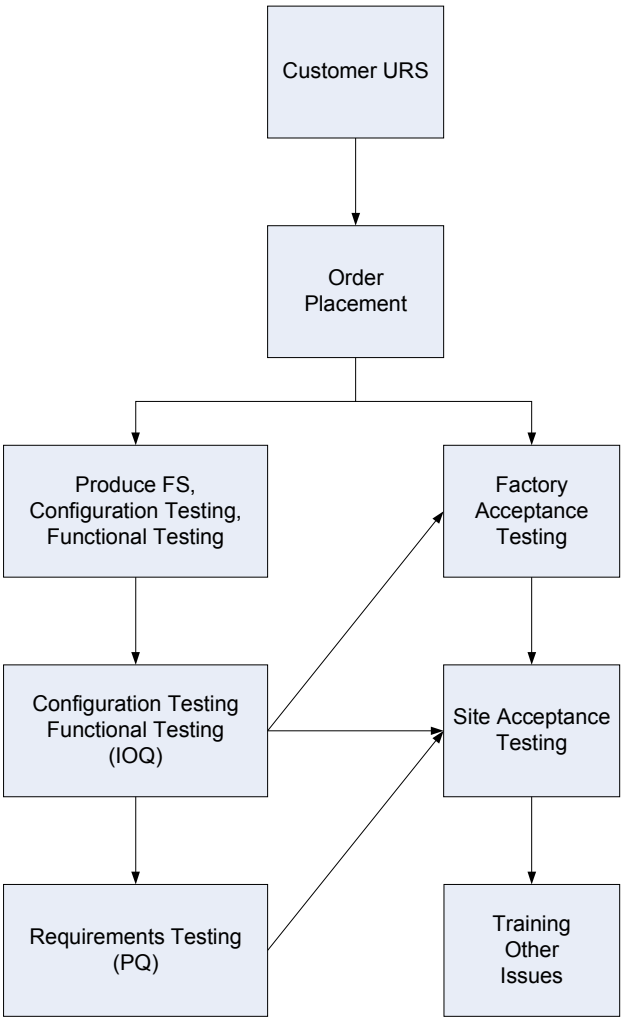
Factory and Site Testing

Testing

During factory acceptance testing most of the Configuration Testing (IQ) can be completed if required. Also, some of the Functional Testing (OQ) can be completed as required.

The System Acceptance Testing FAT and SAT should be fully documented. The completion of Functional Testing for a system confirms that it is ready for use in the manufacturing process.

The Requirements Testing step verifies system performance (PQ). Requirements Testing is conducted under actual running conditions across the anticipated working range. Such testing documentation is usually created by the end customer.



Testing Model

Traceability

Traceability may be achieved in a number of ways, including a Requirements Traceability Matrix (RTM), automated software tools, spreadsheets, or embedding references directly within documents.

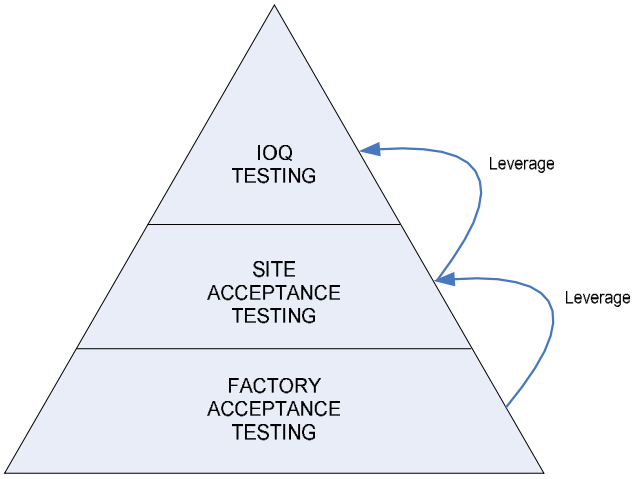
An RTM may be generated as a separate deliverable or as part of an existing deliverable, such as the Functional Specification FS.

	Functional Specification	*System Test*	*IQ*	*OQ*	Risk Analysis
Template Selection. The desired template can be selected.	2.1.2	4100.1.1		9.6.1	2.2
Variable Data. The variable data can be inserted in the printing.	2.1.3	4100.1.1		9.6.1	2.2
Preview. The desired pringing can be viewed for correctness.	2.1.4	4100.1.2		9.6.2	2.2
Save. The desired printing can be saved.	2.1.5	4100.1.3		9.6.3	2.2
Select printer. The desired printer can be selected	2.1.6	4100.1.4		9.6.4	2.2

Leverage

The possibility exists of course to apply leverage to data captured and thus reduce the overall testing overhead. Data captured at FAT time can be referenced to and used at SAT. Likewise, information gathered at both FAT and SAT time can be applied directly into the IOQ data.

This has the effect of drastically reducing the testing time on the project. The key details here are that the various documents used are adequately cross referenced to be of use to any regulatory authority involved in later inspections.

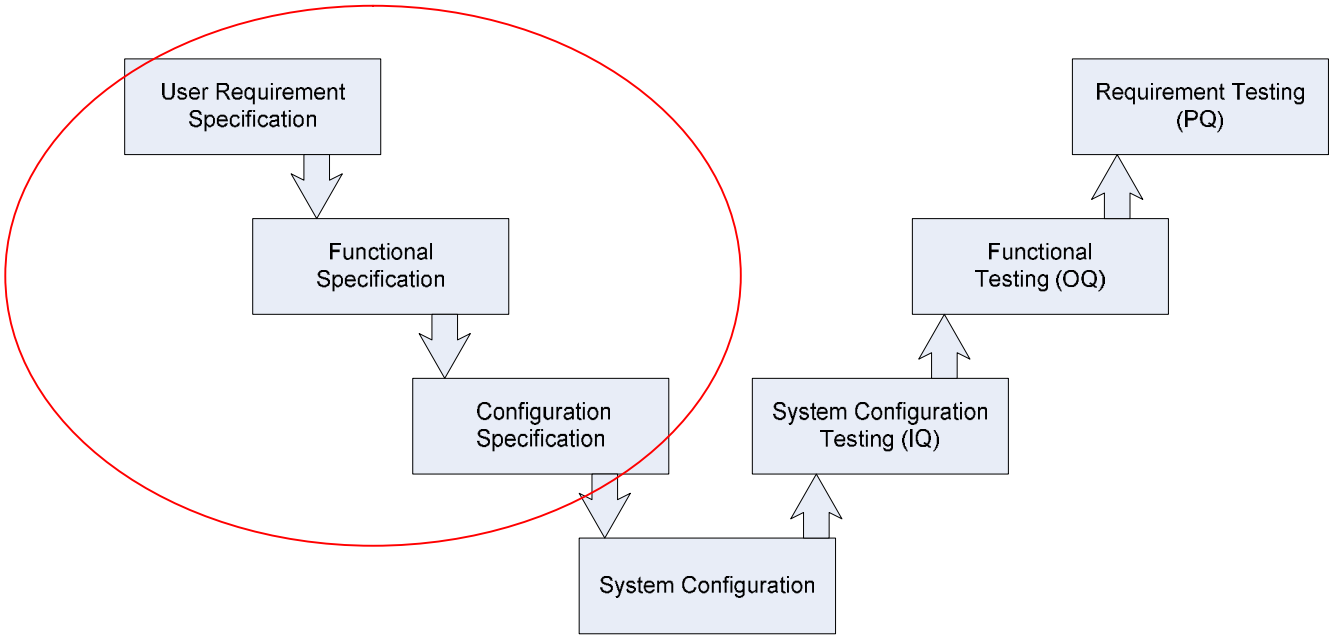


Leverage Model

Specification Phases

GAMP category 4 project

For a GAMP category 4 project we are concerned with the following specifications:



User Requirement Specification

In this phase, the requirements of the proposed system are collected by analyzing the needs of the user. This phase is concerned about establishing what the ideal system has to perform. It describes the system's functional, physical, interface, performance, data, security requirements etc as expected by the user.

This first step in the validation process is the user requirements, created by the customer. When writing User Requirement Specifications, it is crucial to remember the document is not the job. The purpose of the exercise is in fact not to write a document, but to convey information to the reader of that document so they understand what is required. The document exists to be read, not written. To facilitate understanding, it is good practice to:

- Use simple short statements – 'We require a vehicle to hold 6 persons'
- Keep each premise separate – 'It must travel 600Km without refueling'
- Stick to the facts; less text gives rise to more understanding

The end users carefully review this document as this document would serve as the guideline for the system designers (category 5 equipment) or configuration (category 4 equipment) in the system design or system configuration phase.

Defining what the system is supposed to do involves clearly defining in writing what things this system will be designed to accomplish. These are also known as the requirements: functional requirements, user requirements or system requirements. They include things such as the equipment the computer system must interface with, hardware requirements (such as corporate standards for computer hardware), desired graphical user interface, system security requirements (password protection or other scheme), precision of data, the amount of information the system must be able to store, the types of output that must be generated (graphs, reports, tables), and anything else that is important when designing the computer system.

For equipment control systems, one of the requirements is that the computer system be able to control the equipment so it is capable of supporting its intended function. The user acceptance tests are therefore designed in this phase.

An initial version of the URS may be included with the *Invitation to Tender* sent to potential suppliers. This version should include all essential requirements (musts) and if possible a prioritized set of desirable Requirements (wants).

One way to ensure requirement numbers are unique in this way is to use a dynamic outline numbering field code to generate the number. The reference number can then be safely used to refer to a requirement from outside the document with confidence that the reference cannot be broken.

Therefore, to be able to find a specific number and therefore a specific requirement, a Requirement Reference Number Table of Contents is used to list all of the numbers in order and bookmark its page.

There is much additional information that should be supplied with the URS and very often this information is left out, at the cost of the end customer. Besides defining the equipment in terms of its hardware and software, what additional support will be required?

- Software support - In the event of improvements to the system, what is the method of informing the end user of the availability of these improvements? In the event of a system software crash, what are the defined recovery procedures?
- Hardware support - In the event of hardware system failures, what is the exchange mechanism? Is like-for like exchange possible? For how long? In the event on non like-for-like exchanges, what is the revalidation impact?
- Training support – What formal, class based, training is available for the system and how is it documented? Is this included in the sale price?
- Validation support – What formal validation documentation is available for the system, is this included in the sale price?
- Electronic records – Procedures, batch records or test data that is recorded by the system may be required to be controlled by Electronic Record, Electronic Signature (ERES) rules to comply with some markets.

When commercial systems are available either the URS is sent to one or more suppliers (see right site of the diagram). Suppliers either respond to each requirement or with a set of functional specifications of a system that is most suitable for the user's requirements. Users compare the supplier's responses with their own requirements. If none of the suppliers meet all user requirements, the requirements may be adjusted to the best fit or additional software is written to fulfil the user requirements following the development cycle on the left side of the diagram. The supplier that best meets the user's technical and business requirements is selected and qualified.

Functional Specification

In this phase, system engineers analyze and understand the proposed system by studying the user requirements document. They figure out possibilities and techniques by which the user requirements can be implemented. If any of the requirements are not feasible, the user is informed of the issue. A resolution is found and the User Requirement document is edited accordingly.

The Functional Specification document is the reply of the supplier and serves as a blueprint for the development or configuration of the entire system. This document contains the general system organization, menu structures, data structures etc. It may also hold examples of business scenarios, sample windows, reports intended to enhance understanding. The Functional Specification is the defining and controlling document.

GAMP 5 defines the main structure of the Functional Specification as follows:

- Introduction
- Overview
- Functions
- Data
- Interfaces
- General additional information

Other technical documentation like entity diagrams, a data dictionary will also be produced in this phase. The Functional Specification should be written in such a way that it is understood by both supplier and customer. Items to be classified in the Functional Specification include, but are not limited to the following:

- HMI & GUI screens layouts
- Keypad layouts
- Report layouts
- Data Models
- Process Flow (operating process, system process)
- High Level Function of the system
- System Testing conditions, Input values and expected output values

The Functional Specification is a description of the product to be supplied in terms of the functions it will perform and facilities required to meet the user requirements as defined in the URS.

Configuration Specification

Configuration specifications should be provided for configured products and covers the appropriate configuration of the software products that comprise the system to meet specified requirements. This includes the definition of all settings and parameters.

Custom applications require design of hardware and software, and also may require Configuration Specifications.

Software design occurs at two levels. At the higher level it defines the software modules (sub-systems) that will form the complete software system, the interfaces between these modules and also the interfaces to other external systems.

At the lower level the design describes the operation of the individual software modules. These specifications should be unambiguous, clear, and precise.

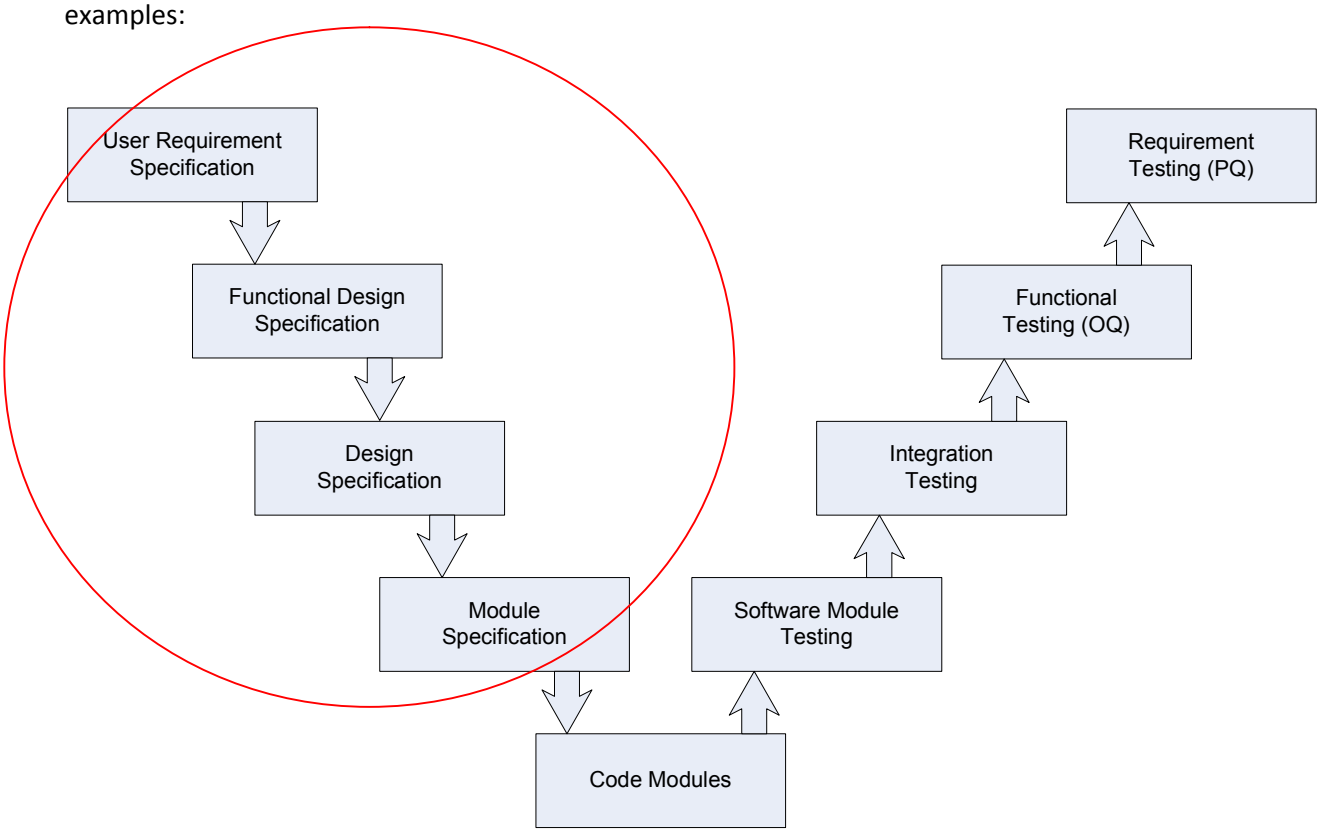
The use of tables and diagrams to illustrate Configuration is highly recommended. If such tables or diagrams are produced elsewhere then these should be cross-referenced in the appropriate specification. Standardized tables can help ensure that all relevant parameters and settings have been defined. Diagrams can be helpful in software design to clarify and explain data flow, control logic, data structures, and interfaces. Diagrams in hardware design can aid understanding of architecture and connectivity.

Configuration and design should cover both hardware and software aspects. Depending on the risk, size and complexity of the system this may be covered by a single specification or may require a hierarchy of specifications covering software and hardware separately. Each specification should be uniquely referenced and traceable back to its appropriate higher level specification.

All specifications should be structured in a way that supports traceability through the life cycle from individual requirements to associated testing.

GAMP category 5 project

For a GAMP category 5 project we are concerned with the following specifications as well as the previous examples:



This is as for the GAMP category 4 project but with the following additions:

Design Specification

The phase of the design of hardware and software architecture can also be referred to as high-level design. The baseline in selecting the architecture is that it should realize all which typically consists of the list of modules, brief functionality of each module, their interface relationships, dependencies, database tables, architecture diagrams, technology details etc. The integration testing design is carried out in this phase.

The Hardware Design Specification is a description of the hardware on which the software resides and how it is to be connected to any existing system or plant equipment.

The Software Design Specification is a description of the software components and sub-systems to be provided as part of the product.

If there is only one module the Software Design Specification should contain enough information to enable the code to be produced. In this case the module design specification, test specification and integration test specification are not required.

For each software sub-system (module) identified in the Software Design Specification, a Software Module Design Specification should be produced. The Software Module Design Specification should contain enough information to enable coding of the module to proceed.

The use of tables and diagrams to illustrate Design is highly recommended. If such tables or diagrams are produced elsewhere then these should be cross-referenced in the appropriate specification. Standardized tables can help ensure that all relevant parameters and settings have been defined. Diagrams can be helpful in software design to clarify and explain data flow, control logic, data structures, and interfaces. Diagrams in hardware design can aid understanding of architecture and connectivity. The following should be considered in each implementation activity:

- Where possible, appropriate implementation methodologies and tools should be used to formalise the production process. The use of these methods and tools should be documented
- Rules and conventions such as programming rules, programming languages, consistent naming conventions, coding and commentary rules should be formally specified and observed

Items to be classified in the Design Specification are:

- Data Structures, including: Message layouts, File layouts, Database tables
- Low Level Functional Decomposition → Module Identification including: Brief Description, Interfaces and dependencies
- Hardware and Software Architecture
- Operating System Specs
- Peripheral Device Specs
- Automation Device Specs
- Integration Test conditions including: Analysis of the interactions among different modules

Module Specification

The Module Design phase can also be referred to as low-level design. The designed system is broken up into smaller units or modules and each of them is explained so that the programmer can start coding directly. The low level design document is built up with a detailed functional logic of all the modules, in pseudocode and/or database tables, with all elements, including their type and size, all interface details with complete API references, all dependency issues, error message lists and complete input and outputs entities. The Unit Testing (Module Testing) design is developed in this stage. Some basic items:

- Module Pseudocode
- Unit Test Conditions, including: Input values and expected output values

Coding

This phase of V-Model scheme produces the application code. It is the deepest phase of the process. If a Version Control System is used, the source files are stored in a repository and it is no possible to have their visibility directly. In such a case, we can assume to keep last release visible in the Project Tree.
Under Version Control, the following files should be stored:

- Libraries
- Resources
- Source code
- Binaries

Verification Phases

Testing Methodology

Goals

- Find and eliminate defects (not just software bugs)
- Determine reliability of the system
- Decide when to release the system in a compliant state
- Use as little resources as possible
- Build confidence that the system will work without error after testing

Good Testing Practices

Tests are executed according to a pre-defined and preapproved test procedure
The test procedure:

- is established on the basis of the appropriate system / equipment specifications
- refers to the relevant specifications
- should enable repetition of the test
- should be based on named documents held under version control

Testing should not start before the test procedure has been approved. All test-related dates must be logically consecutive.

Test Planning

Tests should cover all relevant areas of the relevant equipment or system. Tests should be planned and executed by persons who are:

- qualified to the tasks they are executing
- technically skilled
- knowing the equipment/system
- trained in the requirements of GxP
- be as independent as possible

Test Documentation

The test documentation should:

- include name, position and date for authors, reviewers and approvers
- include the test procedure, described in sufficient detail
- show date and signature on each test by the tester and witness or reviewer
- be retained and properly archived

Test Execution

There should be pre-determined acceptance criteria or statements of expected results for each test During execution test results should be:

- recorded directly onto the test results sheet or
- refer to printouts or computer generated test execution files (e.g. screen printouts)

Each test should be concluded with a statement of whether the test met its acceptance criteria. Test execution should be audited on at least a sample basis by either the user representative or the supplier quality assurance function.

Test Recording

Manual test recording should use permanent ink. Shorthand notations such as tick marks should be avoided. Actual values should be recorded where appropriate. Any corrections should be crossed out with a single line, initialled and dated with a brief explanation. Correction fluid should not be used. See Good Documentation practice later in this document for more details.

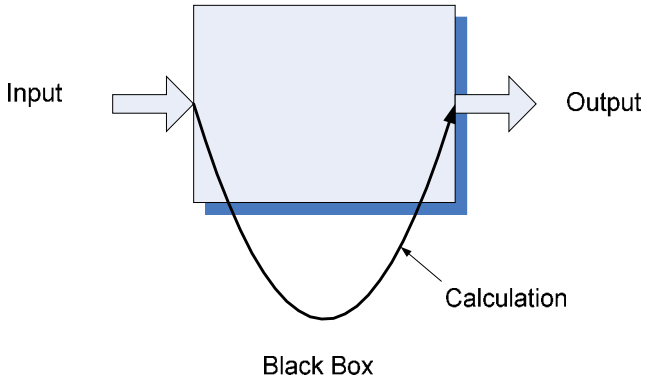
Test Deviations

All deviations should be recorded and be traceable throughout correction and retest into final closure. Deviation corrections may require regression testing to verify that the corrections did not introduce new problems in other tested areas.

Calibrated Tools

Any critical instrument inputs and any test equipment should be calibrated with documented evidence of such calibrations, traceable to international standards. Calibration equipment should be certified, traceable to national standards and referenced.

Black Box Testing

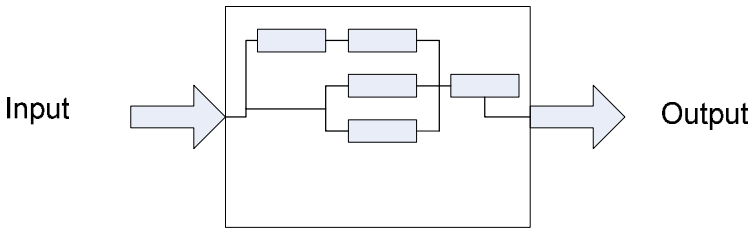


Black Box

Black Box Testing performs the following functions:

- Assess how well a program or system meets the requirements
- Assumes the requirements are accepted
- Checks missing or incorrect functionality
- Compares system result with predefined output
- Performance, stress, reliability, security

White Box Testing



White Box

White Box Testing performs the following functions:

- Reveal problems with the internal structure of a program or system
- Requires detailed knowledge of structure of program or system
- Essentially path testing
- Structures can be tested even when structure is vague or incomplete

Software module testing

- The module or 'Unit' is a function or small library
- Small enough to test thoroughly
- Exercises one unit in isolation of others
- Easier to locate and remove bugs at this level of testing
- Structural testing in test environment
- Done during code development/programming
- Designed, done and reviewed by programmer
- White Box

Integration testing

- Units are combined and module is exercised
- Focus is on the interfaces between units
- Shows feasibility on modules early on
- Tester needs to be unbiased and independent
- White box with some black box

Functional testing

- The whole system: hardware, software, periphery, documentation, incl. manual parts are tested in detail
- Verify the system correctly implements specified functions
- Testers mimic the end use
- Independent testers and formal approval by another independent function (not developer, tester, or user)
- Ensures system features are accurately tested (performance, security, reliability)
- Black box 'Alpha testing'

Requirements testing

- Completed system tested by end users
- More realistic test usage than 'Functional' phase
- Confirms system meets business/user requirements
- Determine if systems is ready for deployment
- Performed in productive environment
- Black box 'beta testing'

Module Structural Testing

Test Objective

The objective of structural testing or "white-box" testing is to ensure that each program statement performs its intended function. Structural testing therefore identifies test cases based on knowledge of the source code. These test cases challenge the control decisions made by the program and the program's data structures including any configuration settings. Structural testing also can identify "dead" code that is never executed when the program is run.

Structural testing is recommended for high risk priority requirements (in addition to functional testing) because testing of all functionality defined by the requirements does not mean that all software code has been tested.

Test Scope

The scope of structural testing should reflect the risk priority associated with the system or function. Some common levels of structural test coverage include:

- **Statement Coverage** - this criterion requires sufficient Test Cases to ensure each program statement is executed at least once; however, its achievement is insufficient to provide confidence in a software product's behavior
- **Decision (Branch) Coverage** - this criterion requires sufficient Test Cases each program decision or branch is executed so that each possible outcome occurs at least once. It is considered to be a minimum level of coverage for most software products, but decision coverage alone is insufficient for high-integrity applications
- **Condition Coverage** - this criterion requires sufficient Test Cases to ensure each condition in a program is executed, to test all possible outcomes at least once. It differs from branch coverage only when multiple conditions should be evaluated to reach a decision
- **Multi-Condition Coverage** - this criteria requires sufficient Test Cases to exercise all possible combinations of conditions in a program decision
- **Loop Coverage** - this criterion requires sufficient Test Cases for all program loops to be executed for zero, one, two, and many iterations, covering initialization, typical running, and termination (boundary) conditions
- **Path Coverage** - this criterion requires sufficient Test Cases to ensure that each feasible path, from start to exit of a defined program segment, is executed at least once. Because of the very large number of possible paths through a software program, complete path coverage is generally not achievable. The scope of path coverage is normally established based on the risk impact or criticality of the software under test
- **Data Flow Coverage** - this criterion requires sufficient Test Cases to ensure that each feasible data flow is executed at least once. A number of data flow testing strategies are available

Test Positioning Within the Life Cycle

Structural testing is carried out primarily within the module test phase. Source code review is a means for documenting the structural verification of a custom coded module. It should include both review against the required coding standards and review against the design requirements. Source code review is normally carried out prior to the start of formal module testing.

Integration Testing

In integration testing the separate modules will be tested together to expose faults in the interfaces and in the interaction between integrated components. Testing is usually black box as the code is not directly checked for errors. It is done using the integration test design prepared during the architecture design phase.

Functional Testing

Functional testing will compare the system specifications against the actual system. The functional test design is derived from the functional design documents. Sometimes System Testing is automated using testing tools. Once all the modules are integrated several errors may arise. Testing done at this stage is called System Testing. Run the testing between two modules and test the gap between two modules whether two modules are interacting with each other.

Test Objective

The objective of functional testing or "black-box" testing is to evaluate the compliance of a system or component with specified functional requirements. Functional testing therefore identifies Test Cases based on the definition of what the software is intended to do. These Test Cases challenge the intended use or functionality of a program, and the program's internal and external interfaces.

Functional testing is required in addition to structural testing because testing of all of a program's code does not necessarily mean that all required functionality is present in the program.

Test Scope

Functional testing should normally cover all stated user and functional requirements. For a particular requirement, however, the number and types of functional tests performed may reflect the risk priority associated with the system or function. Some common types of functional test include:

- **Normal Case (Positive Case) Testing** - testing to show that the system does what it is supposed to do in response to the normally expected inputs (for example checking that a calculation gives the correct result in response to the expected inputs). By itself, normal case testing does not provide sufficient confidence in the dependability of the software product.
- **Invalid Case (Negative Case) Testing** - testing to show that the system does what it is supposed to do in response to specified invalid inputs (for example, giving the correct error message in response to an out-of-range input).
- **Special Case Testing** - testing to show that the system does what it is supposed to do in response to inputs at the limit of the permitted domain (boundary or limit condition testing) or to inputs which form a special case or singularity (for example checking that a calculation produces the correct result for the maximum and minimum values of each input, or checking that a zero input is handled without leading to a 'divide by zero' error).
- **Output Testing** - choosing test inputs to ensure that all software outputs are generated at least once during testing (and if relevant that the outputs are exercised at the limits of their allowed range).
- **Input Combination Testing** - testing combinations of inputs to ensure correct outputs. The input combinations can be selected at random from the possible input domains or selected specifically because they are considered likely to reveal faults.

Test Positioning Within the Life Cycle

Functional testing is carried out during all phases of software testing, from unit or module testing to system level testing.

Design Prototyping (sometimes referred to as Conference Room Pilots or other similar terms), does not form part of formal testing even though it often involves an amount of informal (undocumented) testing. Design Prototyping should be regarded as a means of verifying design requirements and of building confidence prior to formal (documented) testing.

It is in the nature of a prototype to be built up in a rapid, relatively uncontrolled manner. The conversion of a prototype to a real module should, therefore, be approached with caution - as a minimum it is recommended that a baseline be taken and a source code review carried out prior to testing.

Requirements Testing

The objective of performance testing is to evaluate the compliance of a system or component with specified performance requirements. These may include non-functional user requirements (e.g., speed of response to operator input).

Test Scope

Performance testing should normally cover all stated performance requirements. For a particular requirement the number and type of performance tests executed may reflect the risk priority associated with the system or function. Some common types of performance test include:

- **Environmental Tests** - Testing to show that the system is capable of operating reliably in the specified environment (for example under the specified temperature conditions). Testing performed by the Supplier is normally leveraged but additional testing may be necessary if the operating environment falls outside the Supplier's specification for the product.
- **Accuracy Tests** - testing to show that the system is capable of meeting the required accuracy of measurement or control (for example controlling temperature to within a specified range).
- **Repeatability Tests** - testing to show that the system is capable of repeatedly meeting the required performance (for example, by running repeated trials using the same recipe to check that the product is always within specification).
- **Timing or Response Tests** - testing to show that the system is capable of meeting the required timing, throughput or response (for example responding to operator requests within the specified period).
- **Load Tests** - testing to show that the system is capable of meeting the required performance whilst operating under realistic high load conditions (for example, with many concurrent users of a database). Load testing can be a complex area and further discussion is given in section 3.3.4.
- **Usability Tests** - testing to evaluate the combined performance of the system and user (for example checking that the user is able to access and respond to information in a timely fashion via a menu system).

Test Positioning Within the Life Cycle

Performance testing is normally carried out during the factory and site acceptance test phases or prior to 'Go Live'. In order to avoid discovering performance problems when it is 'too late' to remedy them it is important to build in performance tests to earlier stages wherever possible. It may be possible to assess performance at an earlier stage using prototypes or theoretical models or by scaling up of results from unit or module test phases. Where differences exist between the test environment and the production environment, it also may be necessary to carry out some performance monitoring and tuning within the production environment.

Other Testing

Regression Testing

Test Objective

The objective of regression testing is to demonstrate, following a change, that portions of the software not involved in the change were not adversely impacted. This is in addition to testing that evaluates the correct functioning of the changes that were made.

Regression testing is normally achieved by the re-execution of original Test Cases that have already been proven to give the expected outcome. The scope of all regression testing should be based upon regression analysis to determine the scope of functionality potentially impacted by the change and should reflect both the risk priority associated with the system or function and the likely impact of the change being made. The outcome of the regression analysis may indicate that new test cases are required.

Disaster Recovery Testing

Test Objective

Disaster recovery testing has two objectives:

- To check, as part of disaster recovery planning, that elements of a system can be recovered in the event of foreseeable disasters such as loss of the normal operating hardware
- To verify, following a disaster, that recovery of the system has been successful

Decommissioning Testing

Test Objective

The objective of decommissioning testing is to demonstrate, following the decommissioning of a system, that associated systems are not adversely impacted and that archived data can still be accessed. Data migration testing may be an important part of this.

Other Consideration of Testing

The overall system may contain computerised sub-systems within it. Or it may depend on off-the–shelf software products like operating systems and SCADA packages. These should be considered in the plan of testing.

Supplier Maturity

There is a higher probability that a product from a new Supplier will have faults compared to a product from an established Supplier. A mature Supplier is more likely to recognize the importance of quality management and to have established quality management processes.

In these cases, Users may rely on the documented testing conducted by such mature Suppliers and should not repeat such testing.

Supplier Assessment

For systems containing category 4 and/or 5 software (or highly critical software of category 2 or 3) it is usual for an end customer to carry out an assessment of the Supplier. The Supplier should make themselves aware of the areas likely to be covered by that audit Being aware of the requirements and preparing for the audit will assist both parties in determining any shortfalls and where specific remedial actions or testing may be required. The audit may be an important step in developing a long term relationship between the Supplier and the User.

Use of Third Party products

Where the Supplier integrates third party software or hardware at any stage in their product development life cycle they should consider the quality of their own suppliers and their supplier's products when determining an appropriate level of testing. This Guide provides assistance to Users in the pharmaceutical industry as to how they should approach the testing of supplied systems. The same approaches need to be adopted by Suppliers when they make use of third party products.

Suppliers should be in a position to verify that the products they use have been developed using good engineering practices and that they have taken all possible measures to ensure this. This may involve, but not be limited to:

- Assessment of developers of the third party products. This may be restricted to a postal audit but consideration should be given to carrying out a full audit.
- The specific testing of their use of these products, e.g., where specific configurations of automated tools are used these should be tested and documentary evidence provided of fitness for purpose.
- Where third party products are considered to be a "widely used industry standard" then suitable evidence to this should be available.

Just like end customers, suppliers should seek to leverage the testing already executed by their own supplier(s), or testing conducted by themselves on identical systems or pieces of equipment.

System Testing - Why Software is Different from Hardware

There is one consideration here that sets computer based validation apart from all other work and that is the nature of software.

The vast majority of software problems are traceable to errors made during design & development. It is known that 50% of all software errors occur during the design and requirements phase of a project and 40% occur during the coding phase. The quality of software is dependent on design and development with minimum concern for software manufacture, since software manufacturing consists of direct reproduction (copying) that can easily be verified.

It is not difficult to manufacture thousands of program copies that function exactly the same as the original. The difficulty comes in getting the original program to meet all the specifications.

A very significant features of software is branching, i.e., ability to execute alternative commands. Software branching can hide latent defects until long after a software product has been introduced to the market, since branching will create complex possibilities of execution during normal operation, not all of which may have been simulated during testing.

Therefore testing alone cannot fully verify software is complete and correct. Verification techniques such as structured approach and documented development ensure comprehensive validation.

Some other points to understand are as follows; software is not a physical entity and does not wear out therefore failures occur without advanced warning. Software will improve with age as latent defects are discovered and removed. However software that is constantly updated sometimes introduces new defects during the change. Speed and ease of software change cause both software / non-software professionals to believe that software problems can be corrected easily, therefore lack of understanding can lead managers to believe that a tightly controlled engineering development and testing environment is not needed, nor adequate development facilities or resources.

Because of its complexity the development and testing of software should be more tightly controlled and accurate and complete documentation is essential. Software developers are beginning to use off-the-shelf software components for faster and less expensive software development. These 'component-based' approaches require very careful attention during integration. Finally, software engineering needs a greater level of managerial scrutiny and control than hardware. Quality needs to be 'built in' by understanding and applying the above points.

We need to specify the testing of software, its verification and the test documentation in a specific way.

A lot more information can be found in the following document on the FDA website: 'Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices.'

Verification means confirmation by examination and provision of objective evidence that specified requirements have been fulfilled. In a software development environment, software verification is confirmation that the output of a particular phase of development meets all of the input requirements for that phase. Software testing is one of several verification activities intended to confirm that the software development output meets its input requirements. Other verification activities include:

- Code walk-throughs
- Various static and dynamic analyses if relevant
- Code and document inspections
- Module level testing
- Integration testing

Role of the supplier

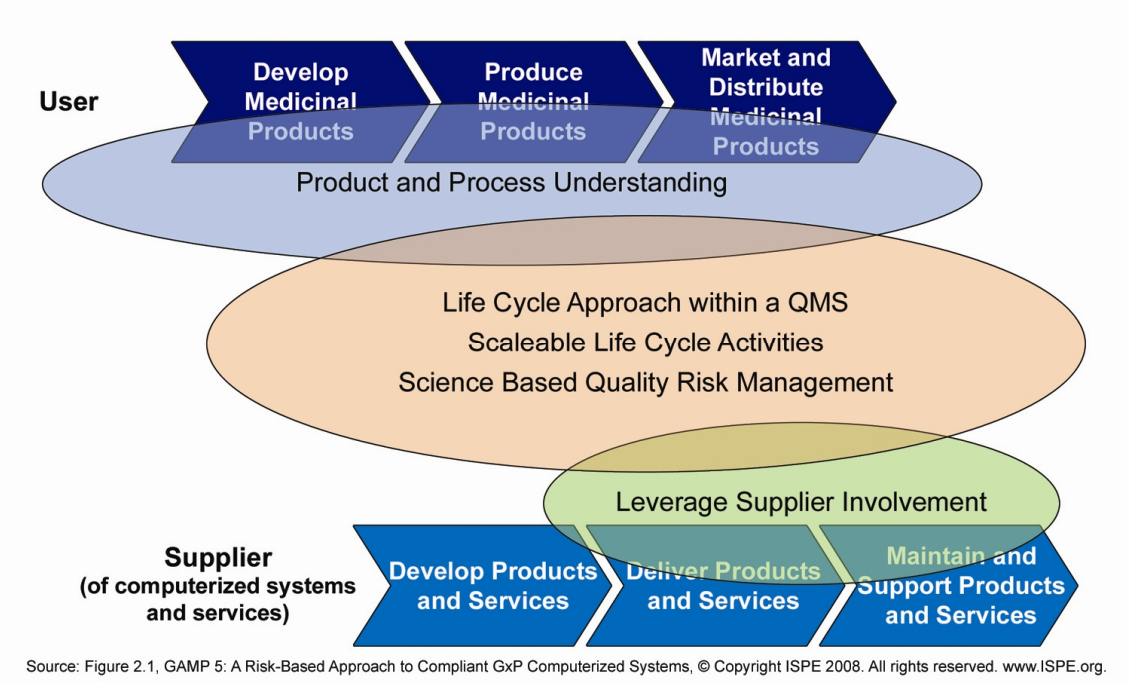
GAMP 5 is an accepted source of guidance for regulators and practitioners worldwide, harmonizing with other guidelines such as:

- ICH Guidance Q8, Q9 and the forthcoming Q10
- FDA Good management practices
- PIC/S guidance on good practices for computerised systems
- ASTM E55 committee on drug development and manufacture

Therefore manufacturing companies worldwide have accepted GAMP methodology and used it in their policies.

Again, looking at GAMP 5 we see some of the key concepts are:

- Product and process understanding
- Life cycle approach within a QMS
- Scalable life cycle activities
- Science based quality risk management
- Leveraging supplier involvement



Source: Figure 2.1, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

Leveraging supplier involvement

Quoting directly from GAMP 5 again:

- Regulated Pharmaceutical companies should seek to maximise supplier involvement throughout the system life cycle in order to leverage knowledge, experience and documentation, subject to a satisfactory supplier assessment
- The supplier may assist with requirement gathering (URS), risk assessment, the creation of functional and other specifications (FS), system configuration (IQ), testing (OQ), support and maintenance
- Justification for the use of supplier documentation should be provided by the satisfactory outcome of supplier assessments, which may include supplier audits
- Documentation should be assessed for suitability, accuracy and completeness. There should be flexibility regarding acceptable format, structure and documentation practices

So what can a company supply as a package to the end customer or OEM to support GAMP 5 level 4 or 5, configurable computer systems?

- Dedicated FS and IOQ documentation set. The type of system supplied decides how generic or dedicated this documentation set must be. Please note that the FS is the application FS
- QMS system overview
- Specifications for the design - equipment design FS or minimum installation documentation
- Design review details. Sometimes called a Design Qualification (DQ)
- Software configuration
- Testing of the system – or reference that documentation can be viewed
- User documentation
- Training details
- CE marking documentation
- System support - details of the system of software release documentation - defining fixes, changes and new features.
- Any system for customer notification of problems
- Reference to results of an audit, including source code review, made by an independent and qualified auditor on your company and its major sub-suppliers

Perspective over the last 10 years

The perspective has changed over the last 10 years. There has been a substantial move towards wide use of configurable commercially-available software packages, with most systems networked. Novel software development methods are increasingly used.

- Main body of *GAMP® 4* was written from perspective that system is based on custom/bespoke systems

- Main body of *GAMP® 5* is written from perspective that system is based on configurable software packages

This allows rapid development techniques to be used.

Project controls example

Supplier generates qualification documents and performs testing

Advantage

- Deep knowledge of the system
- Deep knowledge of validation of the equipment with different customers
- Combination between commissioning and qualification activities can reduce lead time
  Just in time correction of findings possible (under change control)
- Supplier generates qualification documents and performs testing

Disadvantage

- Possibly additional GMP or other customer training required
- Customer has to understand the approach and has to implement supplier standard into internal standard
- Not all tests can be performed by supplier (e.g. SOPs, interfaces to other equipment)

Customer generates qualification documents and performs testing

Advantage

- Documents in accordance to internal company standards
- Experience with inspections by authorities (e.g. FDA)
  Qualification activities are a good (user) equipment training

Disadvantage

- Limited capacities
- Tests partly only with supplier performable
- Generation of test procedures takes a long time due to limited equipment experience

Handovers

3 key areas of documentation are consistent here - Planning, Specifications and Testing:

Planning

- Supplier Project Quality Plan

Specifications

- Functional Design Specification
- Hardware Design Specification
- Software Design Specification
- Traceability Matrix
- Risk Analysis

Testing

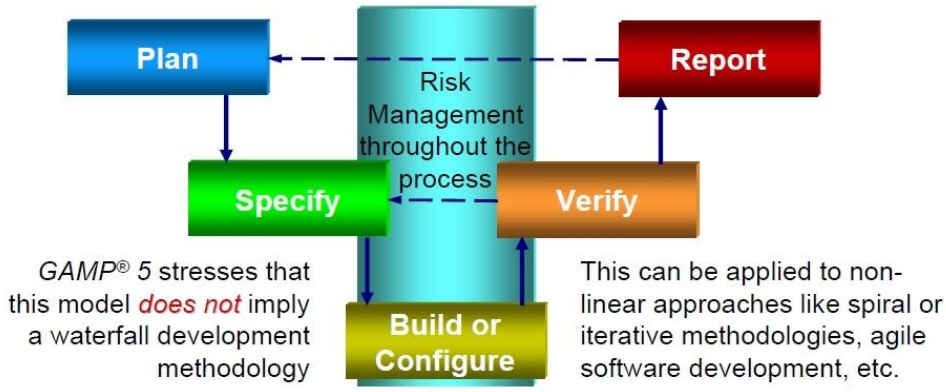
- Acceptance testing
- Verification / Qualification

Consider if the documents provided are to be static (issued and fixed) or dynamic (changing with the progress of the project). Certainly the TM will change.

Everyone wants a smooth handover!

Risk and Risk Analysis

Risk and risk analysis has been mentioned several times, here we will take time to cover this in more detail. Previously we mentioned that risk comes in three types, Ethical or GMP Risk (Items that would cause a product recall), Business and Operational (financial) Risk, finally Safety or H&S Risk.



Risk in the V model

Only the **Ethical Risk** area needs to be validated 100%, during IQ and OQ testing, using the system supplier to help determine the possible risk areas. In this approach, risk is defined as any one single event that can create a fault condition, causing a GMP risk, such risks include:

- Incorrect or contaminated pharmaceutical product
- Incorrect assembly of the 'unit of dose' carrier (blister, bottle, vial...)
- Incorrect packaging component in the final assembly (incorrect carton, missing or incorrect label, missing or incorrect leaflet…)
- Incorrect or illegible lot or batch identification

However the entire operational functionality of the machine needs also to be tested to prove that there is no **Business and Operational Risk** affecting production capacity, or additional GMP risk to product quality. This is also normally included in the system suppliers Validation and Factory Acceptance Testing (FAT) of the machine, these risks include:

- Poor packaging quality (cosmetic defects)
- Excessive machine down time
- Machine damage or wear
- Excessive change-over times
- Slow speed of operation

Finally **H&S Risk** – Although this is usually correct for new machinery regarding CE marking, on older machines subject to retrospective validation there is often potential risk for injury by:

- Guards not operating correctly
- Exposed mechanisms causing human harm
- Open electrical connections
- Human contamination by API's

So there is a requirement for system validation testing for GMP risk, there is also a requirement for system testing for business and operational risk and there may even be some requirement for validation testing for H&S risk. There are various techniques for reducing risk; these are as follows in order of priority:

In general, the documentation provided should:

- Describe the design of the system (FS)
- Document how your design was implemented
- Demonstrate how the device produced by your design implementation was tested
- Show that you identified hazards appropriately and managed risks effectively
- Provide traceability to link together design, implementation, testing, and risk management

Risk Assessment is a formal and systematic approach to identify GMP risks related to equipment and supporting systems. It is a very helpful tool that can be applied to plant, equipment and systems which have been in use for many years. A good validation process with risk analysis will highlight many GMP issues that require standard operating and maintenance procedures to ensure the risks are correctly managed in the production environment. The use of risk analysis helps focus tests on what the machine or process should not do and what can go wrong, rather than what it should do.

One definition of Risk Assessment is as follows: Systematic process of organising information to support a risk decision to be made within a risk management process (ICH Q9).

Risks can be managed in one of several ways:

- Modify the work process in production and system
- Modify the system design.
- Apply technical controls, so fewer people have access
- Apply procedural control as the last resort (SOP)

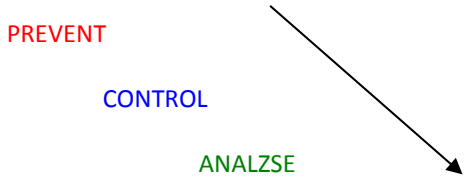
1. Avoidance - Change Process or Approach - Look at modifications to design to prevent an occurrence of the GMP risk.

2. Prevention - Eliminate, Warning, Testing – Like avoidance, seek to remove the risk or warn of its occurrence.

3. Control - Technical, Physical, Procedural – Prevent the occurrence of the risk by procedural or operational controls.

4. Deflection - Dependency on other systems – isolate dependencies to 'shield' the system.

5. Absorption - Proof of negligible probability – analysis and testing of the risk to prove it is of little or no concern.



Risk Mitigation Strategies

1. **Modification of process or system design elements to mitigate risk**

   Modify Process design:

   One or more independent controls are incorporated into the computer-related process e.g., additional data verification checks within the system design in order to reduce data entry errors.

   Introduce External Procedures:

   Introduction of procedures to counter possible failures, such as double checking.

   Modify Product (or System) design:

   Use is made of proven methods, tools and components; fault-tolerance may be built into the automated system (e.g., using replicated parts, system mirroring); the operating environment may be controlled.

2. **Modification of project strategies to mitigate risk**

   Revisit project structure and makeup:

   This refers to the people chosen for the project; their experience and qualifications; the type of project organization preferred; the amount of education and training provided.

   Reconsider amount of (auditable) built-in quality:

   Alter the amount of documentation that is approved and controlled; introduce or remove formal review points to reflect identified risk.

3. **Modification of validation approach to mitigate risk**

   Increased Testing:

   Increase the scope and level of testing applied during various stages of the validation process, including the development of specialized testing aimed at the testing to failure of certain functions.

   Decreased Testing:

   Decrease the scope and level of testing applied during various phases of the validation process due to the extremely low risk associated with occurrence and consequences of the fault conditions.

4. **Eliminate risk**

   Avoidance:

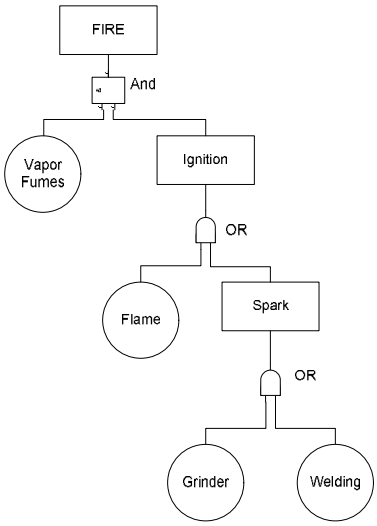
   The risks are so high that the new way of working should not be implemented.

Risk Management tools

- FTA – Fault Tree Analysis
- HACCP – Hazard Analysis and Critical Control Points
- FEMA - Failure Mode and Effect Analysis
- FMECA - Failure Mode, Effects and Critically Analysis
- System impact & component criticality assessment

FTA

The Fault tree Analysis is a team-based method used to identify the causal chain that creates a hazard or a failure mode (effects are typically ignored). FTA represents the sequence and combination of possible events that may lead to a failure mode. Once causes are identified, preventive action can be taken.



FTA example

The limitations of FTA are that it requires time and resources, it requires expert knowledge of the system under review. It can lead to paralysis by analysis (infinite chains of cause and effect), it requires tools like Microsoft Visio or other specialized software to document it and it is more useful as a problem solving than a problem prevention tool.

HACCP

Hazard Analysis and Critical Control Points is a method of identifying and controlling sources of variation at critical process steps that could lead to a hazardous condition. It is similar to a control plan and cannot be used effectively without manual or automated process control methods, including statistical process control.

The main use of HACCP is with new manufacturing process or equipment. Its limitation is that it requires excellent process knowledge. FMEA should precede HAACP to identify critical hazards/failure modes, and then a HAACP could be an action to reduce risk in a FMEA. It also requires use of more complex statistical tools to be effective.

FEMA Analysis

What is a FMEA? It is a team-based approach to ensure that sources of risk are identified and addressed through actions designed to:

- Minimize the impact or severity of the risk
- Prevent the causes of risk from occurring, or to
- Detect the risk early in its life cycle to minimize its effect

The FMEA serves to provide the following services in risk analysis and risk mitigation:

- Breaks down a complex process in single steps
- Breaks down a complex equipment in single parts or functions
- Defines the function of each step / part
- Outlines malfunctions
- Defines steps / functions to reduce the risk
- Can prioritise risks, see FMECA later

The use of Failure Mode and Effects Analysis (FMEA) widely used in the electronics and medical device industries, and Hazard Analysis and Critical Control Points (HACCP) techniques taken from the food industry are beginning to be thought of by the pharmaceutical industry as tools to augment cGMP. Let us look at FMEA in more detail. FMEA was formally introduced in the late 1940s for military usage by the US Armed Forces. Later it was used for aerospace/rocket development to avoid errors in small sample sizes of costly rocket technology. An example of this is the Apollo Space program. The primary push came during the 1960s, while developing the means to put a man on the moon and return him safely to earth. In the late 1970s the Ford Motor Company introduced FMEA to the automotive industry for safety and regulatory consideration.

A FMEA is a cross-functional, concurrent engineering process:

- A FMEA is a living document and should be updated throughout the life of the product
- Because FMEA may determine that a facility, process, or machine design change is needed to reduce risk, FMEA must be initiated as early as possible during the design

There are three areas of a potential risk to consider Severity, Occurrence (Likelihood) and Detection.

Severity

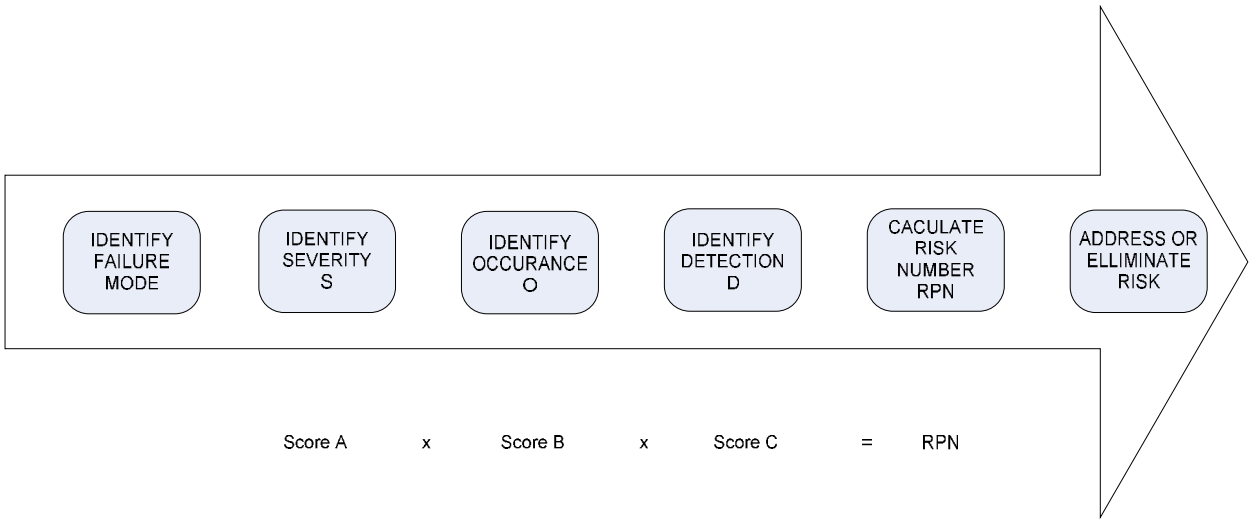
Determine all failure modes based on the functional requirements and their effects and list them. It is important to note that a failure mode in one system area can lead to a failure mode in another area. Therefore each failure mode should be listed in technical terms and for function. Hereafter the ultimate effect of each failure mode needs to be considered. A failure effect is defined as the result of a failure mode on the function of the system as perceived by the user. In this way it is convenient to write these effects down in terms of what the user might see or experience. Examples of failure effects are: degraded performance or even injury to a user. Each effect is given a severity number (S) from 1 (no danger) to 10 (important). These numbers help an engineer to prioritise the failure modes and their effects. If the severity of an effect has a number 9 or 10, actions are considered to change the design by eliminating the failure mode, if possible, or protecting the user from the effect. A severity rating of 9 or 10 is generally reserved for those effects which would cause injury to a user or otherwise result in litigation.

Occurrence or Likelihood

In this step it is necessary to look at the cause of a failure and how many times it occurs. This can be done by looking at similar products or processes and the failures that have been documented for them. A failure cause is looked upon as a design weakness. All the potential causes for a failure mode should be identified and documented. Again this should be in technical terms. Examples of causes are: incorrect algorithms, excessive voltage or improper operating conditions. A failure mode is given a probability number (O), again 1-10. Actions need to be determined if the occurrence is high (meaning >4 for non safety failure modes and >1 when the severity-number from step 1 is 9 or 10). This step is called the detailed development section of the FMEA process.

Detection

When appropriate actions are determined, it is necessary to test their efficiency. Also design verification is needed. The proper inspection methods need to be chosen. First, an engineer should look at the current controls of the system, that prevent failure modes from occurring or which detect the failure before it reaches the customer. Hereafter one should identify testing, analysis, monitoring and other techniques that can be or have been used on similar systems to detect failures. From these controls an engineer can learn how likely it is for a failure to be identified or detected. Each combination from the previous 2 steps, receives a detection number (D). This number represents the ability of planned tests and inspections at removing defects or detecting failure modes. A high detection number indicates that the chances are high that the failure will escape detection, or in other words, that the chances of detection are low.



FMEA in Operation

RPN do not play an important part in the choice of an action against failure modes. They are more of a threshold values in the evaluation of these actions.

After ranking the severity, occurrence and detectability the RPN can be easily calculated by multiplying these 3 numbers: RPN = S x O x D.

Status	Rating	Effect Severity S	Occurrence O	Detection Capability D
Bad	**10**	Injury Resulting / illegal	More than once a day	Failure not detectable
	9	Illegal	Once every 3-4 days	Occasionally sampling only possible
	8	Product Unfit for Use	Once per week	Some systematic sampling only possible
	7	Customer complaints	Once per month	100% manual check, high volume
	6	Partial Failure of product	Once every 3 months	100% manual check, low volume
	5	Performance loss Major	Once every 6 months	Continuous SPC sampling and inspection
	4	Performance loss Minor	Once per year	SPC with action limits acceptable
	3	No performance loss	Once every 1-3 years	SPC and 100% inspection of units outside action limits
	2	Minor effect only	Once every 3-6 years	Automatic inspection possible / automatic elimination
Good	**1**	No noticeable effect	Once every 6-100 years	Defect highly oblivious / easy automatic elimination

Table of values for S, O and D

This has to be done for the entire process and/or design. Once this is done it is easy to determine the areas of greatest concern. The failure modes that have the highest RPN should be given the highest priority for corrective action.

This means it is not always the failure modes with the highest severity numbers that should be treated first. There could be less severe failures, but which occur more often and are less detectable.

After these values are allocated, recommended actions with targets, responsibility and dates of implementation are noted. These actions can include specific inspection, testing or quality procedures, redesign (such as selection of new components), adding more redundancy and limiting environmental stresses or operating range. Once the actions have been implemented in the design/process, the new RPN should be checked, to confirm the improvements. These tests are often put in graphs, for easy visualisation.

Whenever a design or a process changes, an FMEA should be updated.

A few logical but important thoughts come in mind:

- Try to eliminate the failure mode (some failures are more preventable than others)
- Minimize the severity of the failure
- Reduce the occurrence of the failure mode
- Improve the detection

GAMP 5 FMEA

Within GAMP 5 there is a clear definition of the approach for validation testing using risk assessment. During risk assessment the impact of the risks to the system are decided and combined with the probability of the risks happening.

Concentrate on handling the high risks and then the medium risks. The goal is to lower each risk.

Assess the Severity of Impact

Risk Assessment requires not only the identification of the immediate effects of the risk but also the long term and widespread impact on the business of those effects. These effects must take into account a wide variety of issues, including impact on regulatory compliance, financial impact, and company reputation with customers and suppliers. For example, the immediate effect of a hard disk problem may be the corruption of some data stored on that disk, while the business impact of corrupt data relating to product distribution will eventually result in severe problems in conducting a product recall. This would result in a critical non-compliance with the regulatory requirements and could result in regulatory action such as a withdrawn manufacturing license.

The impact of a risk occurring may be described as follows:

Low - Expected to have a minor negative impact. The damage would not be expected to have a long-term detrimental effect.

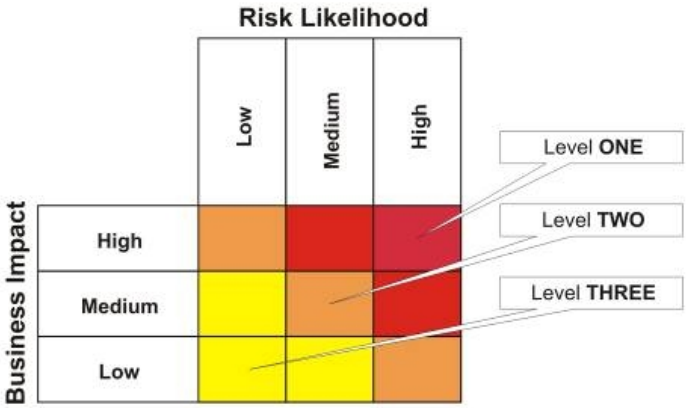
Medium - Expected to have a moderate impact. The impact could be expected to have short- to medium-term detrimental effects.

High- Expected to have a very significant negative impact. The impact could be expected to have significant long-term effects and potentially catastrophic short-term effects.

Status	GAMP Rating	Effect Severity S	Likelihood L
Bad	**High 1**	Injury Resulting / illegal	More than once a day
		Illegal	Once every 3-4 days
		Product Unfit for Use	Once per week
	Medium 2	Customer complaints	Once per month
		Partial Failure of product	Once every 3 months
		Performance loss Major	Once every 6 months
	Low 3	Performance loss Minor	Once per year
		No performance loss	Once every 1-3 years
		Minor effect only	Once every 3-6 years
Good		No noticeable effect	Once every 6-100 years

Assess Risk Classification

Having assigned the *Likelihood* of the risk occurring and the level of *Business Impact* that such an event may have, the risk can be classified. This is achieved by reference to the matrix shown here.



Qualitative Classification (S against L)

Assign Probability of Detection

The purpose of this stage in the assessment process is to identify if the risk event can be recognized or detected by other means in the system. Hence a Level One Risk, if it has a high probability of detection, may not pose such a serious threat because it can be recognized quickly and suitable corrective action taken to mitigate its impact. Conversely if the same fault condition has a low probability of detection, then the team may need to seriously consider a review of the design or the implementation of alternative procedures to avoid the event.

The probability of a risk being detected can be estimated as follows:

Low - Detection of the fault condition is perceived to be unlikely (e.g., less than 1 event in every 3 transactions or operations).

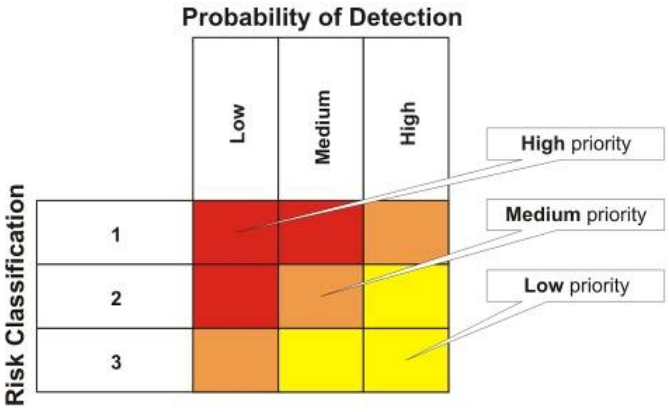
Medium - Detection of the fault condition is perceived to be reasonably likely (e.g., 1 event in every 2 transactions or operations).

High - Detection of the fault condition is perceived to be highly likely (e.g., I event in every 1 transaction or operation).

Status	GAMP Rating	Detection Capability D
Bad	**Low**	Failure not detectable
		Occasionally sampling only possible
		Some systematic sampling only possible
	Medium	100% manual check, high volume
		100% manual check, low volume
		Continuous SPC sampling and inspection
	High	SPC with action limits acceptable
		SPC and 100% inspection of units outside action limits
		Automatic inspection possible / automatic elimination
Good		Defect highly oblivious / easy automatic elimination

Determine Appropriate Measures for Risk Mitigation

By combining the *Risk Classification* with the *Probability of Detection,* it is possible to prioritise the fault conditions associated with each adverse event based upon those areas of greatest vulnerability. Once these priorities have been determined the team can proceed to define and document the appropriate measure(s) to mitigate the adverse event that poses the risk.



Qualitative Prioritisation

The analysis can be drawn on a table which becomes the master plan of risk mitigation.

Function		Risk		Assessment of Risk					Point	Assessment Rational		Remediation
Description	Sub-Function	Number	Risk Scenario	Probability	Severity	GAMP Risk Class	Detection	GAMP Priority				
	Ink Level sensor in print head	1.1	Failure of ink container level sensor in print head.	Low	High	2	Medium	Medium		Occurrence	Ink level sensor in head fails.	No further Design action required. Test during system internal testing.
										Impact	Ink not replenished, head stops printing	
										Detection	Impact visible to operators or automatic camera system.	
	Ink Level sensor in electircal cabinet	1.2	Failure of ink container level sensor in electrical cabinet.	Low	High	2	Medium	Medium		Occurrence	Ink level sensor in electrical cabinet fails.	No further Design action required. Test during system internal testing.
										Impact	Ink not replenished, head stops printing	
										Detection	Impact visible to operators or automatic camera system.	
	Vacuum regulation	1.3	Failure of vacuum regulation sensor.	Low	High	2	Medium	Medium		Occurrence	Vacuum sensor fails.	No further Design action required. Test during system internal testing.
										Impact	Correct printing conditions not maintained. Not correct printing.	
										Detection	Impact visible to operators or automatic camera system.	

FMECA

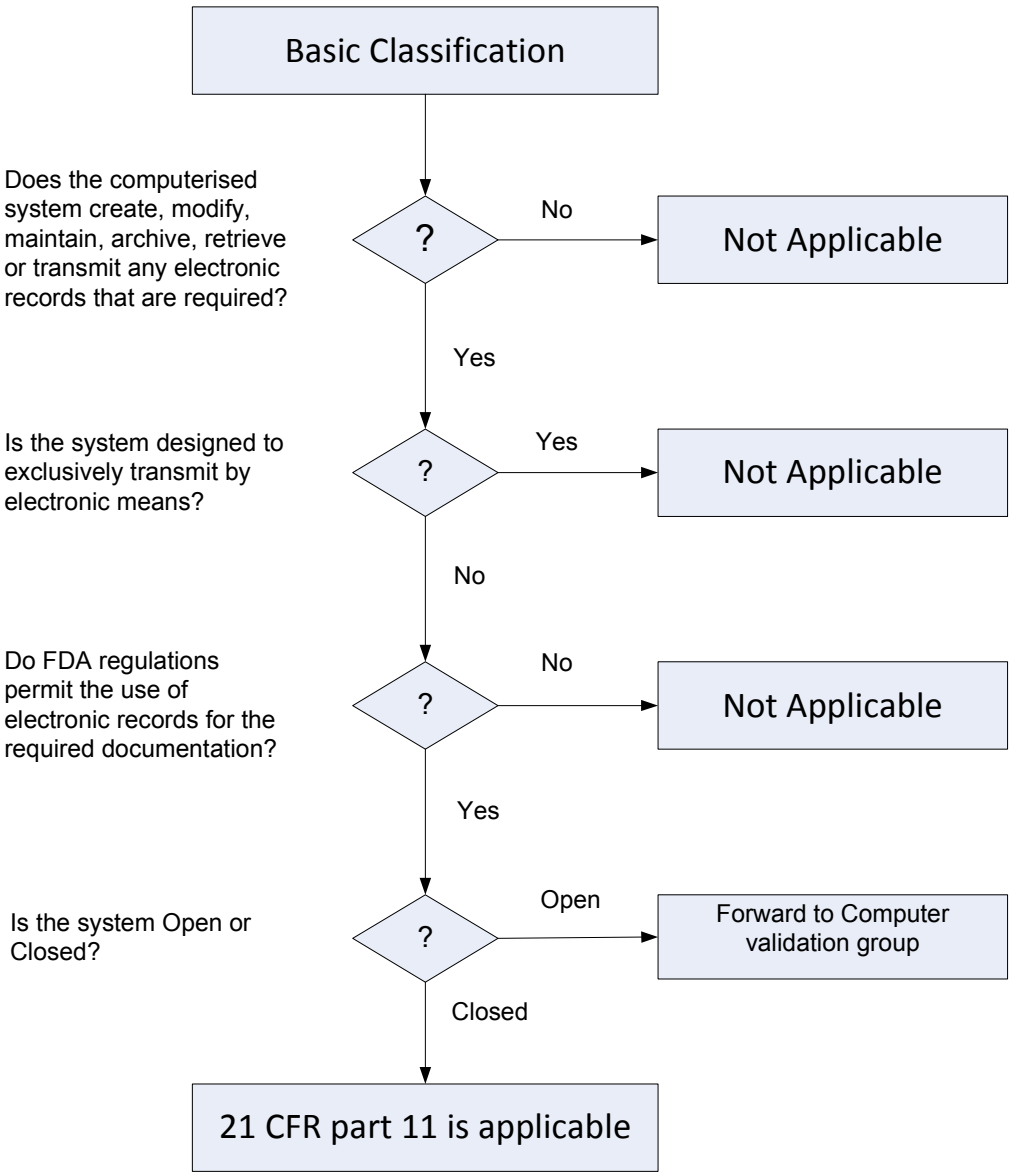
The Failure Mode, Effects and Critically Analysis (FMECA) is the same as FMEA with the additional feature of investigation of the degree of:

- Severity of the consequences
- Probability of occurrence
- Detectability of the failure

Like FEMA it is mainly used in the design phase for equipment and processes. It evaluates the risk and ranks the reduction activities.

21 CFR Part 11 and Annex 11

If requested by the customer, when is 21 CFR part 11 applicable ?



The meaning of 21 CFR part 11

The meaning of 21 CFR part 11 is as follows. 21 CFR — concerns the protection of privacy; Part 11 refers to electronic records and signatures. We are concerned with the GAMP interpretation of 21 CFR part 11.

ISPE's GAMP Forum and the PDA have operated two separate initiatives, but with close cooperation, to deliver industry guidance relative to electronic information. Both initiatives produced work products from different perspectives; however, the approaches are complementary and collectively, they cover the broad issues that are associated with electronic records and signatures.

The Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-operation Scheme (jointly referred to as PIC/S) are two international agreements between countries and pharmaceutical inspection authorities, which provide together an active and constructive co-operation in the field of GMP.

PIC/S 21.5 - Pg 27 states: 'When regulated users elect to use electronic records for GxP applications then it will be necessary for the companies to identify the particular regulations being applied and whether they are to be considered legally binding and equivalent to their paper-based counterparts.'

Annex 11 refers to - Computerised Systems. Draft released for public consultation April 2008. Final revised Annex 11 published January 2011 and consequential amended to GMP Chapter 4 Documentation. This is active at the end of June 2011. Scope - applies to all forms of computerised systems used as part of GMP regulated activities such as packaging.

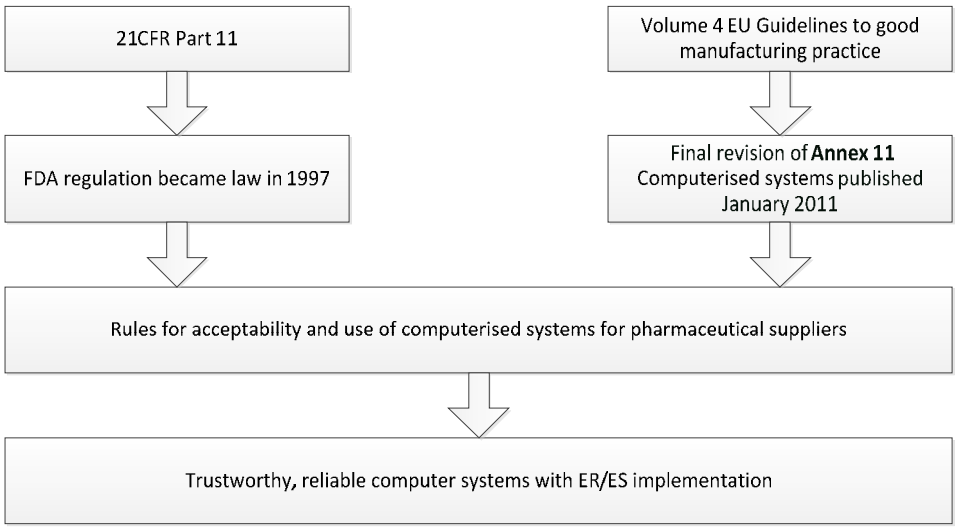
The Food and Drug Administration (FDA) in 1997 issued regulations that provide criteria for acceptance by FDA, under certain circumstances, electronic records and electronic signatures, recorded electronically, to be equivalent to paper records and hand written signatures executed on paper.

This is known as 21 CFR part 11.

So what's new in the rule?

- **Electronic Records = Paper Records.**
- **Electronic Signatures = Hand Written Signatures.**

These are referred to as ER/ES systems



Reaching the ER/ES Model

Can a supplier guarantee compliant system for Part 11? It is not possible for any supplier to offer a 'Part 11 compliant system'. See the later section on interaction for more details.

Anyone who makes such a claim is incorrect. Part 11 requires both procedural controls (training, SOPs, administration) and administrative controls to be put in place by the user in addition to the technical controls that the supplier can offer.

At best, the supplier can offer an application containing the technical requirements of a compliant system.

The concerns are:

- **Data Security** – paper can be locked away
- **Data Integrity** – paper can be seen to have been altered
- **Audit Trail Integrity** – modifications to paper can be tracked
- **Signature Repudiation** – physical signatures are used universally in industry

For Part 11, data integrity is related to the trustworthiness of the electronic records generated and managed by critical systems. The FDA is most concerned about systems that are involved with drug distribution, drug approval, manufacturing and quality assurance because these systems pose the most risk in terms of product quality and/or public safety.

Some definitions

What is **'grand fathering**'? "Grand fathering" simply means the possibility that the rule may not apply to any system in existence before the rule came into effect. Part 11 does not allow for grand fathering of legacy systems. Therefore, systems installed before August 20, 1997 must be made compliant or replaced.

What is '**metadata**'? Literally, it can be defined as 'data about data'. In practical terms, the types of metadata that can be associated with an electronic record may include: details of the record's creation, author, creation date, ownership, searchable keywords that can be used to classify the document and details of the type of data found in the document. Metadata must be stored as an integral part of the electronic document it describes. Alternately, metadata can be configuration information for a device or equipment.

Closed systems [7]- Access control by the company or group, Communication via secure network.

Requirement - Validation of systems, protection of records, limiting system access, checks of devices, operations and authorities and Change control.

Open systems - Company delegate's control, Communication control by the on-line service.

Requirement - As closed systems, plus using open systems to create, modify, maintain, or transmit electronic records must employ procedures and controls to ensure the authenticity, integrity and the confidentiality of electronic records from the point of their creation to the point of their receipt.

What is FDA position on timelines for implementation of 21 CFR Part 11?

There is no fixed date for complete remediation. The Agency had stated often that they would take enforcement discretion if an organisation takes the appropriate steps to put a plan in place that addresses what systems need to be compliant and what the firm will do to get the systems there. These plans must include all applicable systems, be detailed and have reasonable timelines and hold persons responsible for implementing those plans.

[7] All systems we discuss can be considered to be **Closed**.

When are e-signatures required?

The predicate rules mandate when a regulated document needs to be signed.

A predicate rule is any requirements set forth in the Federal Food, Drug and Cosmetic Act, the Public Health Service Act, or any FDA regulation (GxP: GLP, GMP, GCP, etc.). The predicate rules mandate what records must be maintained; the content of records; whether signatures are required; how long records must be maintained, etc. Signatures serve as an authentication. We are not submitting documents; we therefore need signatures to be able to have the log-in facility.

This is the link between 21 CFR and the GMP regulations.

In Part 11.300, controls for identification codes/passwords usage is listed under Subpart C -- Electronic Signatures. Are these requirements only applicable if your system is utilizing e-signatures? It seems that these should be applicable to any system with e-records?

The controls for password/user ID usage apply across the board for ERES systems. They apply to the proper management of electronic records in addition to executing compliant electronic signatures. In previous control systems the access method for controlling the system has been via a simple key-switch system. This however does not force any security regarding the operator making the changes and his proven ability to make these changes. Therefore a more sophisticated system is required. Within 21 CFR this is permitted in three ways:

- Token systems
- Biometrics
- Two part passwords

Most companies have concentrated on method three, for the following reasons.

Token systems for signatures - Using a unique electronic tag system to identify the individual. The system requires this token as the access mechanism. Problems occur with loss, theft or damage.

Biometric signatures use fingerprints; retina scans etc. to identify individuals. There are two types of Biometric, Physical or Behavioural. Problems occur with changes to the characteristic used for the biometric identification - voice, fingerprint, face etc. The Software for good biometrics is still in an immature phase.

Non-Biometric signatures involve a pre-stored account name and a two part access code – user ID and password.

User Name – Publicly known name of user, will be shortened however to say - ‘Osborne’.

Account name – Recorded in the system only, not used for log in but for full identification of the user - ‘Paul M Osborne’.

Password – Private password known only to user – xxx123. This must be unique.

Signature - Repudiation by the Log-in mechanism. Can a single restricted login suffice as an electronic signature?

No. The operator has to indicate intent when signing something, and he has to re-enter the user ID/password (shows awareness that he is executing a signature) and give the meaning for the e-sig. To support this, Part 11 §11.50, states that signed e-records shall contain information associated with the signing that indicates the printed name of the signer, the date/time, and the meaning, and that these items shall be included in any human readable form of the record. Collaboration for falsification is required.

- The two part passwords have a unique combination of I.D. and password
- The names are to be printed out

- The meaning such as issue 1.3.4, etc. are to be included in any human readable form of the record
- The system therefore verifies the identity of the user
- We need to periodically revise
- We need to follow loss-management procedures
- After 3 log-in attempts the user is 'suspended'

Users can be suspended deleted, or edited by the Administrator, or be just suspended by a repeated failed log-in. The Administrator can also be suspended by a repeated failure of log-in.

The audit trail identifies operators by their log in names and from this knows the full name. In the audit trail user must be identified by their full name. Audit trails of electronic records record the following: WHO, WHAT, WHEN and WHY was a change made to a record. This record could be the configuration of a scanning head for example.

However please note that Part 11 itself does not require the audit trail to record the reason why a record was changed, although another control usually requires recording this information.

Classification for 21 CFR part 11 applicable systems

The equipment which is 21 CFR part 11 applicable has to be classified into different Classifications (Supplier or Customer) according to the paragraphs of the FDA rules. All rules outside of the influence of the supplier are classified as 'customer' and must be dealt with by the customer.

Log-in procedures

21 CFR Rule – Access control and Security	Section	Classification
Is system access limited to authorized Individuals? (user ID and password)	11.10(d) 11.10(g)	Supplier
Are there means to identify and authenticate all connected devices?	11.10(h)	
Does the system ensure uniqueness of code and password?	11.300(a)	
Do passwords periodically expire and need to be revised?	11.300(b)	
Will attempts of unauthorized access be detected?	11.300(d)	
Does the system prevent reuse of user ID's?	11.100(a)	

Data storage

21 CFR Rule – Data Security	Section	Classification
Can record changes always be identified? (The records are defined as the creation, modification or deletion of product configuration and actual production data).	11.10(a) 11.10(e)	Supplier
Can a complete copy of records or a complete backup be provided both in electronic record and in readable form?	11.10(b)	
Are all backups readable over the retention period?	11.10(c) 11.10(e)	Supplier

Audit trail and general controls

21 CFR Rule – Audit trail and general controls	Section	Classification
Are secure computer generated time stamped audit trials available for review and copy? (The records are defined as the creation, modification or deletion of product centric configuration data).	11.10(e)	Supplier
Does the audit trail capture modifications without obscuring previously recorded information?	11.10(e)	
Do signed electronic records contain the following related information? The printed name of signer (user ID alone is not acceptable) The date and time of signing The meaning of the signing (such as approved, reviewed)	11.50(a)	
Are signatures linked to their respective electronic records?	11.70	
Are non-biometric signatures made up of least two components, such as an identification code and password.	11.200 (a)(1)	
When several non-biometric signings are made during a continuous session, is the password executed at each signing? (Note: both components must be executed at the first signing of a session).	11.200 (a)(1)	
If signings are not done in a continuous session, are both components of the non-biometric electronic signature executed with each signing?	11.200 (a)(1)	
Is the above information shown on screen based any printed copies of the electronic record?	11.50(b)	

Interaction

21 CFR Rule – General controls		Section	Classification
Is the system validated? Can a vendor audit or qualification be performed?	Supplier system validation protocols	11.10(a)	Supplier
Is a retention period for records defined in a procedure?	SOP	11.10(c)	Customer
Is there a backup and restore procedure?	Application software and SOP	11.10(c)	Customer
Is there a defined procedure for maintaining the records throughout the retention period?	SOP	11.10(c)	Customer
Is system access defined, authorized, periodically assessed and controlled over the retention period of the system?	Application software	11.10(d)	Customer
Is there documented training, Including CV'S and on the job training for system developers and support staff?	Supplier responsibility	11.10(i)	Supplier
Is there a written policy that makes Individuals fully accountable and responsible for actions Initiated under their electronic signature?	SOP	11.10(j)	Customer
Is the distribution of, access to, and use of systems operation and maintenance documentation controlled?	SOP	11.10(k) (1)	Customer
Is there a formal change control procedure for system Documentation that maintains a time sequenced audit trail of changes?	SOP	11.10(k) (2)	Customer

Practical implementation of 21 CFR part 11 applicable systems

The implementation of 21 CFR part 11 controls into a system can be divided into a number of relevant sections, these are as follows:

User access control

Below are the suggested default user access rights for the system as the system is delivered. It is of course possible to change these access rights according to individual company policy.

Functionality	Default	Line Operator	Supervisor	Administrator
Viewing of warnings and alarms.	✓	✓	✓	✓
Reset of warnings and alarms (or automatic reset)		✓	✓	✓
Viewing of counters	✓	✓	✓	✓
Reset of counters			✓	✓
View device parameters		✓	✓	✓
Control (modify) device parameters				✓
View product data		✓	✓	✓
Control (modify) product data				✓
Report generation		✓	✓	✓
Audit trail access and export				✓
User management				✓

Password Controls

The following parameters control the password use.

Name	Operation
Lowercase chars allowed in password	Lowercase characters are allowed in passwords. Set to True/False.
Numeric chars allowed in password	Numeric characters are allowed in passwords. Set to True/False.
Special chars allowed in password	Special characters are allowed in passwords. Set to True/False.
Uppercase chars allowed in password	Uppercase characters are allowed in passwords. Set to True/False.
Password inactivity limit (days)	Number of days a password will expires for long inactivity; if a non-positive number is set no password will expire.
Case sensitive. comparison in password	Make case sensitive password comparisons. Set to True/False.
Password duration in days	Number of days a password can live before expiring; if a non-positive number is set no password will expire.
Maximum password length	The maximum password length in characters; if a non-positive number is set no password will be checked.
Minimum password length	The minimum password length in characters; if a non-positive number is set no password will be checked.
Lowercase chars obliged in password	At least one lowercase character must be entered in passwords. Set to True/False.
Numeric chars obliged in password	At least one numeric character must be entered in passwords. Set to True/False.
Special chars obliged in password	At least one special character must be entered in passwords. Set to True/False.
Uppercase chars obliged in password	At least one uppercase character must be entered in passwords. Set to True/False.
Maximum number of password retries	Maximum number of retries when entering a wrong password will expires for long inactivity, before the user will be blocked. If a non-positive number is entered an infinite number of retries will be permitted.
Number of reused password	Number of previously used passwords that cannot be entered as new password; The maximum number managed in the system is six. If a non-positive number is entered, All previously used passwords can be reused.
Timeout	The maximum inactivity time in minutes before the system automatically logs the user out; if a non-positive number is set no log out is made.

Audit Trail

We must ensure that an audit trail is maintained, the user cannot influence the audit trail process. Audit trail recording is always active and it is on for the entire life of the system. All GMP relevant product data is captured during a production batch, this includes all production relevant data.

Additionally any change to the user accounts is logged. The security audit trail history contains the user name of the user, the full user name, the date and time stamp when the record was created, modified or deleted, the new value, the old value and the type of modification (e.g. insert, delete, modify).

- The Audit trail designed into the system is a recorded series of chronological events that monitor any GMP relevant changes to the product or system configuration. It is not a production record of system. However Batch reports are usually a customer requirement
- The previous changes made to the audit trail must not be overwritten by subsequent changes
- The sections of the audit trail required fall into a number of major categories

Product Parameters

Select a product from the audit trail list of all products and in the 'view audit trail' menu, the product data is displayed as a chronological list of events: the title of the product, the time and date at which the event occurred and what the event was:

- Created – new product was created
- Deleted – product deleted
- Modified – product was modified
- Accepted – the new product was accepted and saved (if this method is adopted)

By selecting a product for further investigation, the following items are now viewed:

- Name of product
- Timestamp of event (format: YYYY-MM-DD HH:MM:SS) (**When** it was changed)
- Account that caused the event and with his complete user name (**Who** changed it)
- Event i.e. Created, Deleted, Modified or Accepted (**What** was changed)
- Description of event, difference to the previous status (old and new values)

Please note in the above we do not record why the change was made, this is not in the regulation but a small field can be provided for comments.

System Parameters

Select system parameters from the audit trail list and in the 'view audit trail' menu, the system data is displayed as a list of parameters: the time and date at which the change occurred and what the change was:

- Modified – parameter was modified
- Accepted – the new parameter was accepted and saved (if this method is adopted)

By selecting a parameter for further investigation, the following items are now viewed:

- Name of parameter
- Timestamp of event (format: YYYY-MM-DD HH:MM:SS) (**When** it was changed)
- Account that caused the event and with his complete user name (**Who** changed it)
- Event i.e. Modified or Accepted (**What** was changed)
- Description of event, difference to the previous status (old and new values)

Please note in the above we do not record why the change was made, this is not in the regulation but a small field can be provided for comments.

User Administration

Select a user from the audit trail list of all users and in the 'view audit trail' menu the number of the user is displayed as a chronological list of events, the username and details of the account, the time and date at which the event occurred and what the event was:

- Created
- Suspended
- Deleted
- Reactivated
- Modified

By selecting a user event for further investigation, the following items are now viewed:

- Name of Account
- Timestamp of event (format: YYYY-MM-DD HH:MM:SS) (**When** it was changed)
- Account that caused the event and with his complete user name (**Who** changed it)
- Event i.e. Created, Deleted, Suspended, Modified or Reactivated (**What** was changed)
- Description of event, difference to the previous status (old and new values)

Reports for the system

The system should supply the following reports**:**

Current batch report

Status: the status of the system showing correctly functioning items. Batch counts for current batch.

Alarms: all details about the alarms generated in the history of the current production batch.

Warnings: all details about the warnings generated in the history of the current production batch.

System Parameters: all parameters that are related to the operation of the C-TTS system for the current batch.

User Management: This screen shows all details about any user management changes made in the current batch.

Historical batch report

Status: the status of the system showing correctly functioning items for a given batch. Batch counts for that batch.

Alarms: all details about the alarms generated in the history of the selected production batch.

Warnings: all details about the warnings generated in the history of the selected production batch.

System Parameters: all parameters that are related to the operation of the C-TTS system for the selected batch.

User Management: This screen shows all details about any user management changes made in the selected batch.

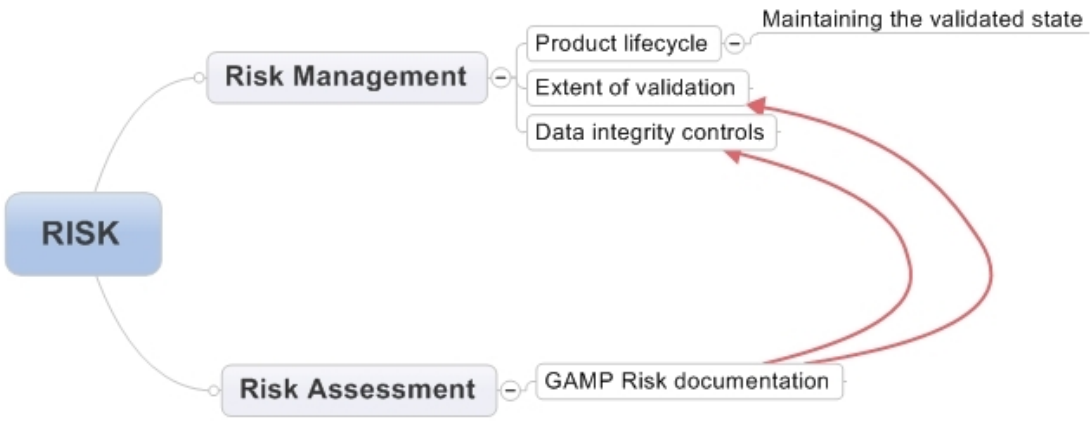
Annex 11 – Computerised systems

Volume 4, EU Guidelines to Good Manufacturing Practice, Medicinal Products for Human and Veterinary Use. Covered by EU Commission Directives 91/356/EEC, as amended by Directive 2003/94/EC, and 91/412/EEC respectively. In the UK this is the so-called 'Orange Guide' known by all pharmaceutical manufacturers as the 'bible' of drug manufacturing.

Annex 11 refers to - Computerised Systems. Draft released for public consultation April 2008. Final revised Annex 11 published January 2011 and consequential amended to GMP Chapter 4 Documentation. Active at the end of June 2011. Scope - applies to all forms of computerised systems used as part of GMP regulated activities such as packaging.

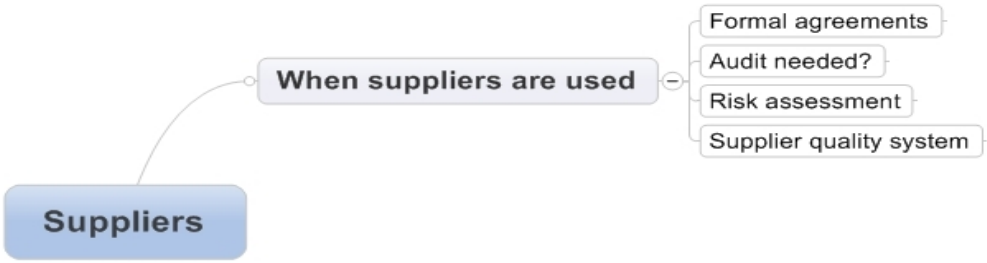
Key Points in the Annex

Risk



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.

Supplier and Service providers

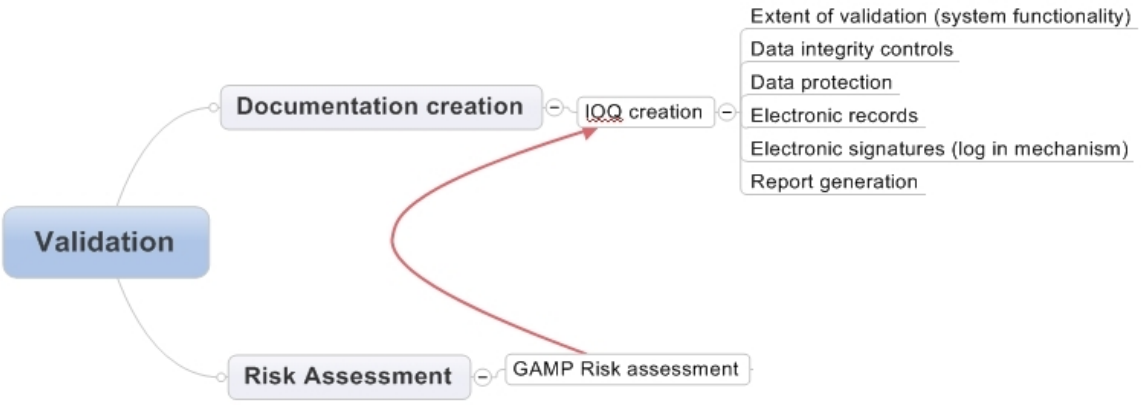


[When] third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing.

[Then] ... 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.

The need for an audit should be based on a risk assessment. Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.

Validation



Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.

Data Migration

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.

Data Integrity

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. 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
- 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
- Regular back-ups of all relevant data
- Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically
- 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")
- Physical and/or logical controls should be in place to restrict access to computerized system to authorised persons
- Data may be archived. This data should be checked for accessibility, readability and integrity

Testing

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.

Electronic Signatures

Have the same impact as hand-written signatures. Permanently linked to their respective record Include the time and date.

Good documentation practice

The pre-validation documentation set should be supplied to the pharmaceutical company along with or shortly after the equipment, this way the company can begin the validation immediately. Remember that the validation process must occur before the end customer can product drug; therefore the pre-validation documentation set is as important to the end customer as the equipment itself.

To date, Major pharmaceutical companies have expended large amounts of money creating all supplier validation documentation in their standard format. This has often meant teams of either supplier or manufacturer's technical teams rewriting documentation sets. This is clearly a wasteful and unneeded practice.

GAMP 5 has tried to rectify this by making the following statements:

- Justification for the use of supplier documentation should be provided by the satisfactory outcome of supplier assessments, which may include supplier audits
- Documentation should be assessed for suitability, accuracy and completeness. There should be **flexibility regarding acceptable format, structure and documentation practices**

So GAMP 5 sets out, in their words to 'leverage supplier involvement', so this means that suppliers can adopt their own documentation formats and providing the above applies, then the documentation should be considered as acceptable. The considerations to be made in good documentation practice are well defined in GAMP 5 and are as follows:

The GMPs require written records and the definition of validation contains the words 'documented evidence.' Documentation is any written record of information used for quality assurance, evidence of adherence to specifications, or any validation purposes. In supplying equipment to the pharmaceutical industry, you are most likely to be working with documentation such as:

- Procedures
- Test reports
- Certificates
- Manuals
- Validations
- Functional Specifications
- Drawings

Documentation is critical to GMP and validation. In this industry, everything you do must be documented, or it is like you didn't do it. You have to prove everything in writing, and we mean everything. Keep in mind that when requirements are specified as part of an order, proof of meeting those requirements is expected in writing. Also keep in mind that information written on a piece of paper may not be acceptable to the pharmaceutical industry if it doesn't meet their standards for proper documentation. It's not that the pharmaceutical people don't trust their suppliers, but these are the rules.

Commercially supplied, mass-produced instruction manuals are also documentation, but these are generally accepted without question as proper documentation. The rules come into play when information about specific equipment is documented as part of the official documentation provided to the pharmaceutical companies. This is where they expect the rules described below to be followed.

We refer to these as the pharmaceutical industry's expectations because these documentation rules are not all stated in the federal regulations. These are good industry conventions that have become the accepted standards. Therefore, the FDA and other authorities expect this as well.

Rule 1 All entries must be in Permanent Ink

Any information written, printed, or drawn must be done using ink or some other method that cannot be erased or altered (pencils and erasable pens are not acceptable). The convention used to be to use only black ink. This is based on the belief that black can be copied more easily than other colours.

I know some people argue that blue should be the standard, since it distinguishes original from the copy.

There are differences of opinion, but ink colour is not specified in the GMPs. An acceptable rule is to always use dark, permanent ink (a lot of companies insist on blue).

Rule 2 Never Obliterate Data

When you need to make changes to documented information, always do the following:

- Strike out the original entry with a single line
- Rewrite the entry
- Write a brief explanation of why it was changed
- Initial and date the change

Never do either of the following:

- Obliterate the original entry by scribbling over it or writing over it
- Cover up the original entry using white paint

These are standard practices in banking as well as GMP businesses.

Rule 3 All Record must be signed twice

All manual records (forms, certificates, etc., with handwritten information) should be signed and dated by the person who did the work, and signed and dated by a second person who checks the work to make sure it is correct. Usually, there are blank lines for these signatures at the bottom of each page or on the cover page of a package of multiple sheets. This is common practice for documentation in the pharmaceutical industry. One person does the work and one person checks it. The GMPs mention that records 'shall be prepared, dated, and signed (full signature, handwritten) by one person and independently checked, dated, and signed by a second person.' The preparation of master production and control records shall be described in a written procedure and such written procedure shall be followed.

Some people think this means the second person has to look over the shoulder of the first person to make sure everything is done right. This seems like requiring two people to do the work of one, a costly requirement.

What is needed is for the person who did the work to sign and date the form to verify the work was completed correctly. This also provides a record of who did the work and when. The second person signs the form to verify that he or she reviewed the first person's work, that the first person did do the work, and that the work is complete and correct. That means the second person must have an understanding of what the work involves and what the results should be.

This second person is typically a supervisor or co-worker, since this person would know what is going on and what the form should look like when it is filled out. The second person can also be a customer representative, since the customer knows what the requirements are. There can also be more than two signatures; there can be as many as you want. But there must be at least two. Remember that these signatures must be in permanent ink. Think of it as signing a contract.

Rule 4 Original Records are the most important

For data that are manually recorded (handwritten as they are measured or read), always keep the original records. The original records contain the information as it was first recorded. Even if this information is going to be entered into a computer and printed in a formal report, keep the original data and give them or a copy of them to the pharmaceutical company.

If this information is GMP documentation (calibration certificates, cleaning records, etc.), do not write the original entries on scrap paper and copy it over onto the form you intend to turn over to the pharmaceutical company. Always enter the information directly onto a form. Remember that neatness doesn't count, but accuracy does.

Do not copy raw data into another form and discard the original. There is always the concern of transposition error. This means copying things incorrectly or making mistakes when entering data onto another form or into a computer. If you print out the results in a formal, computerized summary report, that's great, but you still need to provide the pharmaceutical company with copies of the original data entries. If FDA or other inspectors see typed reports or perfect handwritten documents without mistakes, they will pick up on this.

They have been known to ask pharmaceutical companies questions such as, "Where's the real data?"

If the data are being typed directly into a computer as it is originally recorded, the computer file is the original data. These data still need to be signed and reviewed. This is accomplished either by printing out the data and signing it by hand as described in Rule 3, or it can be approved electronically. If the data is printed out and the paper copy is signed by hand, this signed paper copy becomes the original or master copy of the data. All copies of this data should be obtained by photocopying or reproducing an exact copy of the signed master document.

The regulations for electronic approval are more complex. Approving the data electronically means the data in the computer file can be approved in the computer without printing it out. The master copy or original is stored in the computer and it can be printed out as an approved document directly from the computer.

With electronic forms, the FDA and other authorities get concerned about data integrity, information manipulation, and security. Since it is possible to change data in a computer file, there will always be the lingering question, 'Has this information been altered?' That is one of the reasons we need two persons to approve the documents and attest to their accuracy.

The concern here is making sure no changes have been made to what you signed. You must be sure that what you think you signed is the same as what may be printed out in the future. Could somebody go into the computer and change a piece of information and then reprint the document without your knowing

about it or being able to do anything about it? This is what the FDA's concern is with electronic GMP documents.

The final ruling on electronic signatures was recently published in the Federal Register by the FDA (21CFR 11, effective August 1997) is detailed in this book.

Rule 5 Use Templates and Forms

Standardised fill-in-the-blank forms are the preferred way to document manually entered information. This method of documentation is easier to write up and easier to review than free-form information. Pharmaceutical companies, the FDA and other authorities like to see these standard certificate-type forms. This shows consistency and it shows that a standard procedure is being followed. It also makes understanding the paperwork much easier. If you calibrated an instrument and recorded all the readings and adjustments on a blank sheet of paper, you may accidentally leave out some important piece of information and it may not be easy to follow the information. If you have a pre-printed form, this saves you the trouble of writing everything you do as you do it. This is especially helpful for repetitious jobs such as inspection or calibration or testing.

Also, when you have a form, there are blank lines to remind you of every piece of information you should be recording. This ensures that your paperwork is consistent and easy to follow. You won't give more information for one thing and less for another. The FDA, other authorities and pharmaceutical people can pick out inconsistencies right away. If more information is provided for the testing of one piece of equipment than for another similar piece, they may think something is being covered up or no control is being maintained over the work done.

Rule 6 Leave no Missing Information

Complete all the entries on data forms. Do not leave missing information or gaps or blanks, even worse do not leave completely blank pages. Fill in all the blanks, take out blank pages.

Items left blank - this is something that draws questions right away: ‘Why didn't you do it?’ will be the question. It looks as if someone forgot to complete something or didn't finish things or intentionally left something out or never got back to it. If there is reason information doesn't need to be entered, and there often is, the blank should be filled in N/A or Not Applicable and a brief reason should be stated. In this example, the appropriate entry would be:

Steam Supply Pressure: N/ A - This unit is electrically heated.

By putting something in the blank, it shows that someone checked into this item and thought about it. If this information entry is in the documentation, it's important to check. If it's not filled in, it's not clear whether anything was checked. This is something you can do to save yourself questions later. The pharmaceutical company is going to want to know why there are blank items because it may be asked by the FDA or any other regulatory authority and it needs to have a good answer. If it's not applicable or not required, just say so.

If it is something you should have completed but didn't, it's still better to write "Not Tested" or "Needs To Be Retested" than to leave it blank. This way the pharmaceutical company knows that this work needs to be completed. Honesty is the best policy, and it's also GMP.

Rule 7 Reference Procedures and Standards Wherever Possible

The pharmaceutical industry thrives on standardization and consistency to ensure quality. Following procedures and using accepted standards is always the right thing to do. It shows that you are doing something consistently and are following widely accepted methods.

Whenever validation or GMP work is being done for the pharmaceutical companies, written procedures or accepted standards should be followed and this should be noted in the documentation supplied to the pharmaceutical company. Information generated based on a written procedure may be used by the pharmaceutical people as part of their validation data, if they agree with the procedure that was followed. However, if no procedure was followed, they will most likely have to redo the work to generate information that can be used for validation. The GMPs require that written procedures must be in place:
There shall be written procedures for production and process control designed to assure that the drug products have the identity, strength, quality, and purity they purport or are represented to possess. Such procedures shall include all requirements in this subpart. These written procedures, including any changes, shall be drafted, reviewed, and approved by the appropriate organizational units and reviewed and approved by the quality control unit.

Written production and process control procedures shall be followed in the execution of the various production and process control functions and shall be documented at the time of performance. Any deviation from the written procedures shall be recorded and justified.

Having a procedure and referencing it in the documentation shows consistency and provides a level of assurance that the work was done the right way. Procedures can be internally generated (procedures that you write up), they can be manufacturer's procedures (maintenance procedures, calibration procedures, installation procedures, etc.), or they can be industry-accepted procedures such as standards published by professional organisations.

Examples of GMP/validation-related information supplied to pharmaceutical companies are:

- Validation records
- Calibration records
- Installation records
- Inspection reports

In addition to following standard procedures, the pharmaceutical industry also expects adherence to standards for quantitative measures. This means quantitative information or data must be traceable to an accepted standard of measure to be used for GMP purposes. These standards should be referenced or noted in the documentation of the data provided to the pharmaceutical companies.

An example of quantitative standards is measuring devices whose accuracy is traceable to standards. This means someone calibrated either the measuring device or the instrument used to calibrate the measuring device.

Rule 8 Drawings should be an accurate representation of the equipment being supplied

This rule applies to drawings, schematics, wiring diagrams, piping diagrams, flow charts, installation drawings, and layout drawings. These are an important part of the documentation that the pharmaceutical companies need to validate the equipment, so they must be correct. To show the FDA and other authorities that the equipment is suitable and in a state of control, the pharmaceutical company needs to understand how it works. To accomplish this, it needs to have accurate drawings and diagrams. All the drawings should contain the most current correct information. All this information on the drawing should correlate with what is installed in the equipment. For example, all the wire numbers or valve IDs should match the tags in the equipment. All the wires should connect to the components and terminals indicated in the diagrams. All the piping flows should be as they are depicted in the drawings. All the components included in the equipment should be noted in the drawings and all the components included in the drawing should be installed in the equipment unless specifically noted. The

bottom line is that when someone looks at these drawings, they should be confident that this is what the equipment is, not something different, not something similar, but exactly what is shown.

Final drawings should be certified "As-Built" before they are turned over to the pharmaceutical company. This means that someone who is familiar with the equipment, such as a design engineer or mechanic, has reviewed the drawing and verified its accuracy. It is then customary to stamp or sign the drawing "As-Built" with the signature of the person who verified its accuracy.

Any changes made to the equipment before its release to the pharmaceutical company should be noted on the drawings. The drawings supplied to the pharmaceutical company should be the final updates with all the changes included so that the drawings accurately represent the equipment. The drawings should contain accurate identification information for traceability to the original project. This means all the information noted on the drawings (model numbers, serial numbers, project numbers, drawing numbers, revisions dates, file names, etc.) should be verified as accurate. Handwritten changes to drawings should be handled in the same manner as handwritten changes to other types of documentation. See Rule #2.

Rule 9 Provide all the Manuals with the Equipment

When the equipment or system is delivered to pharmaceutical companies, they should be given all the manuals they need to properly operate, maintain, and understand the equipment. This includes all operations manuals, instruction manuals, service manuals, maintenance manuals, and/or user manuals. These manuals should include individual component manuals and system manuals for complex multi component systems.

As an example, a production line that contains motors, conveyors, check-weighers, and controllers is a multi-component equipment system. In this case, the manuals needed are the manuals for each of the components listed, plus a general operating and maintenance manual for the entire line. This list of component manuals includes:

- Conveyor line
- Controllers
- Pumps
- Balances
- Cameras
- Printers
- Motors
- Solenoid valves
- Ejection Mechanisms

In addition, the system manuals include:

- Operation of the filling line
- Safety guidelines
- Proper settings and set-up procedures
- How to run the line-sequence of operations
- Maintenance of the filling line
- Routine preventive maintenance
- Non-routine repairs
- Troubleshooting guidelines

Individual component manuals are usually produced by the component manufacturer, and the system manual is usually produced by the equipment system manufacturer. The manuals must be appropriate (correct revision and model numbers, etc.) for the equipment. All of this information is important to ensure that the pharmaceutical people know how to properly operate and maintain the equipment so it will consistently produce quality drug products. These are the written procedures they need to follow to ensure GMP compliance when they use this equipment.

The best way to provide the information and paperwork to pharmaceutical companies is to put them all together in one package and give that to them with the equipment. This is what we refer to as the prevalidation package or turnover package. This is the ideal scenario. Sending things to the pharmaceutical company in dribs and drabs over an extended time typically results in things being misplaced, forgotten, or lost. In addition, the people involved in the project typically change over its life. By the time the equipment is delivered, there may only be one or two persons who were involved in the planning stage.
My recommendation to avoid a lot of stress and headaches is to put everything into one neat package, like a binder or series of binders, and hand it in all at once. If you want to impress the pharmaceutical people, separate the sections by tabs and put in an index. This sounds like trivial stuff that shouldn't be nearly as important as the equipment, but in this business paperwork is valuable because of the reasons mentioned earlier. The up side of this is that you can please the customers by doing these little things without adding a lot of extra cost to the project.

What if the pharmaceutical companies want to see some of the documentation before the equipment is delivered? Provide them with copies of what they want as a PDF, but still keep a printed copy for the turnover package. The turnover package is the official master copy of the documentation they will use for validation. Whatever happens, make sure the turnover package is complete, the documentation is up to date, and it is provided to the pharmaceutical company in a timely manner.

In the ideal scenario, the turnover package is provided to the pharmaceutical company at the same time as the equipment; this way they have what they need to start working on validation right away. Don't assume they will accept the equipment and wait to get the complete documentation package. If this information is going to be delayed for any length of time, it is important to let the pharmaceutical companies know this as soon as possible. Otherwise, they will keep after you until they get what they need. Remember that they cannot use the equipment to make drug products until it has been validated, and they cannot validate the equipment without all the necessary documentation. This turnover package has a significant value to them in getting on-line as quickly as possible.

Remember these rules when you submit paperwork to the pharmaceutical companies. These are the things they are looking for and expect. It's always easier to get them right the first time. I have been involved in projects where it took months to fix the paperwork. This was typically because:

- The people who did the original work were working on other projects
- The extra time needed to fix the paperwork was not in the original budget
- It was not possible to generate the information after the fact (the information was not recorded when the work was done)
- The supplier didn't realise this information was important

Meanwhile, the paperwork went back and forth, while the project completion time got longer and tempers got shorter. Believe me; take the extra time needed to make sure the paperwork will be acceptable to the pharmaceutical companies before you submit it. It could save you a lot of unnecessary headaches later. Please remember:

- Documentation is an important part of GMP compliance and validation
- Validation documentation is recorded information that is used to provide evidence of quality and adherence to specifications
- The pharmaceutical industry has standard practices for acceptable documentation. The specifics of these rules are not detailed in the USA federal regulations or un ant EU regulations
- It is important to know and understand the rules to provide acceptable documentation to pharmaceutical companies

Rule 10 No Tick boxes

The current trend is not to allow the use of tick boxes at all, previously it was acceptable to write:

Did the system pass the test Yes ( ) No ( ).

Now the trend is to write the result as follows:

Have all acceptance criteria been met Yes/No?: _____

Rule 11 detailing the actual result

During testing it is necessary to detail the actual result and not just write 'as specified', below is an example:

No	Procedure	Specified Result	Actual Result	Pass/Fail?	Initials / Date
1	System to be run at 220 cartons per minute, with correct packaging components.	The bar code reading system evaluates the correctly barcoded leaflets and the complete, filled cartons are accepted, and pass out of the machine.	BARCODED LEAFLETS CORRECTLY EVALUATED AT 220/MIN.	PASS	GMO 11 AUG2011

Company Audits

The objective of supplier qualification is to get assurance that the supplier's products development and manufacturing practices meet the requirements of the user's company, regarding quality. For software development this usually means that the software is developed and validated following documented procedures.

Supplier assessment should answer the questions: 'What type of assurance do you have that the software has been validated during development" or 'How can you be sure that the software supplier followed a quality assurance program?'. Depending on the risk and impact on (drug) product quality answers can be derived from:

1. **Documentation of experience with the supplier**. Experience may come from the product under consideration or from other products.
2. **External references**. Useful if there is no experience within the supplier.
3. **Assessment checklists** (mail audits). Use checklists available within your company, through public organizations, e.g., PDA and from private authors.
4. **3rd party audits**. Gives an independent assessment of the quality system and/or product development.
5. **Direct supplier audits**. Gives a good picture on the supplier's quality system and software development and validation practices.

One point of interest is that the principal supplier is responsible for the auditing of sub-suppliers if they are working outside the QMS of the principal. This means the principle supplier himself must make the above assessment on his sub-supplier and provide documentary evidence. The following Supplier risk assessment is based on the Parenteral Drug Association (PDA) Technical Report number 32, published in October 1999 entitled 'Auditing of Suppliers Providing Computer Products and Services for Regulated Pharmaceutical Operations.'

The audit scope includes two parts:

1. Product risk
2. Supplier risk

Factors for product risk include:

- System complexity
- Number of systems to be purchased
- Maturity of the system
- Level of networking
- Influence on other systems, e.g., through networks
- Impact of the system on drug quality
- Impact of the system on business continuity
- Level of customization

Factors for supplier risk include:

- Size of company
- Company history
- Future outlook
- Representation in target industry e.g. pharmaceutical
- Experience with the supplier

The Supplier Audit Checklist is intended as an aid to make supplier auditing easier, faster, more consistent, and ensure proper audit coverage. The checklist is one element of the Supplier Audit Guideline written by most large pharmaceutical companies. Most will follow the procedure of auditing the following topics within a supplier's organisation.

Module Number	Topics
1	Supplier Organisation
2	Viability
3	Quality Management System (QMS)
4	Systems Lifecycle Procedures (SLC)
5	Document Control
6	Requirements and Design
7	Electronic Record and Electronic Signature
8	Programming
9	Security
10	Testing
11	Change Control
12	Support

Supplier Organisation - General Expectations:

1. The supplier has a current organization chart and an organization structure to address the key aspects of the supplier's responsibilities concerning the computer system.
2. The supplier has written qualification requirements or job descriptions for persons in the positions that impact the computer system.
3. The supplier has evidence that the personnel currently in place meet the requirements for their positions.
4. The supplier has evidence that key personnel maintain the education, experience, and training required for their positions.
5. The supplier can demonstrate how the quality responsibilities are assigned to member(s) of the supplier's organization who are independent of development.

Viability - General Expectations:

1. The system's viability is not at risk from associations with third party or contracted products or services.
2. The source code is available for any required regulatory review or use in the event the product can no longer be supported by the supplier.
3. New releases of the system will enable the user to access or convert data created by previous releases.
4. The supplier demonstrates control over systems via an inventory of their systems and versions.

QMS - General Expectations:

1. The supplier has a Quality Management System, or equivalent, in place to ensure the quality of computer system development, validation, management, and control.

SLC Procedures - General Expectations:

1. The supplier has current written procedures in place to control the development, testing, and maintenance of the computer system.
2. The supplier's written SLC procedures adequately address applicable regulatory expectations for these procedures, as reflected in company policy.

Document Control - General Expectation:

1. The supplier uses documented practices to control the preparation, approval, issuance, and modification of documents related to the computer system.

Requirements and Design - General Expectations:

1. The supplier maintains current Requirements indicating the required content of functions for the computer system.
2. The supplier maintains current Design documentation specifying how the requirements for the system are met.
3. For Bespoke Hardware, the supplier has applicable hardware layout diagrams for the system.

Electronic Record and Electronic Signature - General Expectations:

1. If applicable, a preliminary high-level review indicates that the supplier's system or service may comply with applicable regulatory requirements for electronic records and signatures as reflected in customer policy, when used in combination with existing customer user controls.

Programming - General Expectations:

1. The supplier constructs source code in accordance with pre-defined programming standards.
2. The supplier's programming standards address programming conventions to be used, including annotations and dead code handling.
3. The supplier reviews code for conformance with programming standards.

Security – General Expectations:

1. The supplier maintains a secure environment for system development to ensure that physical and electronic access to the computer system is limited to authorized personnel.
2. The supplier has procedures for Contingency Planning, Virus Handling and Backup / Restoration of software to ensure security from natural disasters and malfunctions.
3. The supplier periodically backs up their software.
4. The supplier has documented testing of their Contingency Plan.

Testing – General Expectations:

1. The supplier performs documented testing to demonstrate that the structure and functionality of the computer system meet the pre-defined requirements.
2. The testing complies with written system development procedures.
3. The testing is based on the pre-defined approved requirements and specifications and is traceable to these documents.
4. The supplier has a procedure in place to resolve test failures and errors discovered during testing.
5. The supplier's testing includes written test plans with defined expected results, documented test results, and documented release of the system.

Change Control – General Expectations:

1. The supplier controls, implements, and tracks changes to the system.
2. The system is controlled to ensure traceability and security through the use of a configuration management system or procedures.
3. The supplier can recreate past and present software versions.
4. The supplier maintains a link between their fault reporting mechanism and the change control program.

Support – General Expectations:

1. The supplier has written documentation available detailing the instructions for hardware and software installation for the system.

2. If the supplier participates in the installation of hardware or software for the customer's system, the supplier produces installation reports and has procedures for documenting and resolving installation problems.
3. The supplier provides the appropriate level of training to support the customer's use of the computer system.
4. The supplier maintains a technical support program to support the customer's use of the computer system.
5. The supplier maintains a process to adequately record, track, analyze, and correct defects reported or discovered in the system.

Note - Auditor Code of Ethics - from: PDA Computer Products Supplier Auditor Training, Baltimore February 2000.

1. I will be honest, impartial, and candid and will demonstrate freedom of mind and approach that will ensure objective viewing of the operation being audited.
2. I will conduct myself in a dignified manner that reflects well upon my profession and my company.
3. I will inform my company of any personal involvement (business connections, financial interests, employment history, or personnel or family affiliations) that might influence, or appear to influence, my judgment or jeopardize my independence in my ability to assess the suitability of the operation being audited.
4. I will undertake only those audits compatible with the degree of training, experience, and proficiency I hold with regard to the operation being audited.
5. I will issue reports that clearly, factually, and accurately describe the operation being audited, and that are constructive in nature.
6. I will not disclose information concerning the business affairs or technical processes of the c1ient/ supplier without obtaining prior written consent to do so from the c1ient's/supplier's management.
7. I will not disclose any proprietary information or confidential data provided by a company being audited without obtaining consent to do so from that company's management.
8. I will strive to contribute to the development of improved audit techniques and methods within the quality audit profession and the PDA Process Model.

Training

The supplier should identify training needs and provide appropriate training. They should consider the specific methods, tools, techniques, and hardware to be used. Records of relevant training and experience should be maintained and should be available as part of the project documentation.

The requirement is for formal classroom training with notes and a test to be made at the end, in both theory and practice.

Trainers must be both qualified in the technical disciplines relevant to the training and the actual equipment itself.

Additionally the trainer should also have attended some type of 'train the trainer' course. These typically last one to two days and teach important lessons, such as:

- Writing a talk
- Delivery methods and systems
- Body language
- Learning to cope with nerves
- Practicing and rehearsing
- Relaxation exercises
- Understanding your audience
- Making and using visual aids
- Humour and wit
- Writing a script to be read, hints on reading a script

At the end of the training the delegates should be issued with a certificate of training. These certificates can state that the individual has 'attended' a course or has 'successfully participated' in a course.

The certificate must not state that the individual has achieved an addition qualification as a result of attending the course. This type of certification is only for professional bodies like Universities to issue against a rigorous syllabus and examination system.

Additionally the certificate should contain the following details:

- The name of the training person, this is necessary for traceability and their professional credentials may be asked for
- All dates must contain the date of the training and the duration. The style usually adopted to start and finish dates in the form DD/MM/YYYY. Or the start date and the duration
- The signature of the training person
- The address of the company and brief contact details like phone number need to be on the certificate
- A unique serial number to identify the document

Maintenance

Procedures must established to ensure that backup copies of all software and other relevant data are taken, maintained, and retained within safe and secure areas. Backup and recovery procedures should be verified.

Identify and define system components. Record and report the status of items and modifications to items. Ensure the completeness, consistency, and correctness of items of the machine. Control storage, handling, and delivery of items.

All changes proposed during the operational phase of an automated system should be subject to a formal Change Control process, and should be reviewed, impact and risk assessed, authorised, documented, tested, and approved before implementation.

Consider that some elements of the machine must require routine maintenance - This is a planned activity.

Periodic review – at routine intervals, once per year, review the status of the above.

Document the review.

Change Control

Baseline Definition of the FDA (1995):

'A specification or product that has been formally reviewed and agreed upon, that serves as the basis for further development, and that can be changed only through formal change control procedures.'

Change Management Regulations/Guidelines

' ..... change control measures can apply to equipment, standard operating procedures, manufacturing instructions, environmental conditions, or any other aspects of the process system that has an effect on its state of control, and therefore on the state of validation.' – 21CFR parts 210 and 211 May 1996.

Change Management – Attributes

- There can by responsibility of system owner together with the end-user
- No universal procedure
- More than one procedure may be appropriate, depending on: organisation, infrastructure, components being changed and position in life cycle
- Change requests are typically initiated by users

The Phases

- Request
- Approval
- Implementation
- Recording of change
- Periodic evaluation Sign-off

Responsibilities

- Quality Assurance – Compliance audit of system, reporting of findings to responsible management
- Validation Team - determination of impact of changes on the computerised system, Review/Authorization/Reject of changes accord. to system SOP, update of validation documentation and revalidation/revalidation planning
- QP (Qualified Person) - Legal Responsibility

Types of Change

- Planned - An intentional change to a validated system for which the implementation and evaluation program is predetermined. Intended to enhance capabilities, to correct non-critical problems. It is evaluated prior to change. This may require verification of the system in some form of re-validation, see below
- Unplanned - An unanticipated, necessary change to a validated system requiring rapid implementation. Here we have little or no advanced warning, it is time-driven and a result of malfunctions and or faults in equipment and or software. It requires rapid assessment and may require temporary quarantine. This may require verification of the system in some form of re-validation, see below
- Repetitive - Time-driven but periodic, probably part of preventative maintenance, replacement of parts or re-calibration. This may require verification of the system in some form of re-validation, see below
- Pending – System being evaluated prior to planned changes

Classification of Change

- Major change - A change to a validated system that, in the opinion of change-control reviewers, necessitates a revalidation of the system
- Minor change - A change to a validated system that, in the opinion of change-control reviewers, does not require a revalidation of the system

Documentation of change

Consideration should be given to how the change will be made, who will make the changes, the change review and finally the change approvals. How will this be documented?

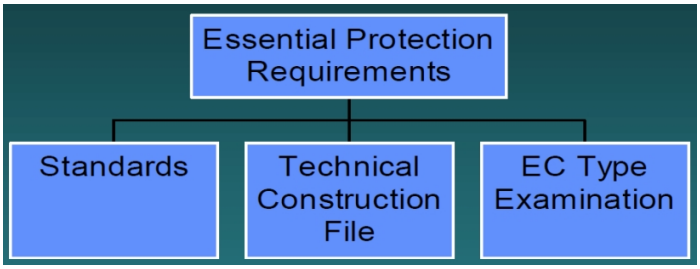
Possible documents affected by the change:

- Sop's
- Problem report / incident log
- Change request
- Qualifications
- Change report

The EMC Regulations and the Technical Construction File

EMC is controlled in Europe by regulation:

The EU EMC Directive 89/336/EEC are the controlling standards, this is implemented by all member states. 89/336/EEC covers all electrical and electronic equipment and their phenomena. The way to CE marking of the product is to ensure the essential protection requirements are met, these are as follows:



The standards are a number of harmonized EC standards to consider for CE marking of a product and the EMC Directive 89/336/EEC mandates that all electronic equipment must comply with the applicable EN specification for EMI (Electro Magnetic Interference). Some typical EN specifications follow, highlighted are the one's necessary for RedCube:

Harmonised standards for Electronic Equipment

Radio Disturbance characteristics

EN55011 Industrial, scientific and medical equipment

EN55013 Broadcast receivers and associated equipment

EN55014 Electrical motor-operated and thermal appliances for household and similar purposes, electrical tools and similar apparatus

EN55015 Electrical lighting and similar apparatus

EN55022 Information technology equipment

Immunity

EN61000-4-2 ESD (ElectroStatic Discharge)

EN61000-4-3 Radiated immunity

EN61000-4-4 EFT/S (Electrical Fast Transients)

EN61000-4-5 Surge

EN61000-4-6 Conducted RF

EN61000-4-8 Power frequency magnetic

EN61000-4-11 Voltage dips and interruptions

The Technical Construction File

General

Products which are to be provided with the CE marking shall be designed to comply with relevant requirements.

Products with the CE marking shall be produced in accordance with the design that was found to comply with relevant requirements.

This leaflet provides information about the "Technical Construction File" which is the basis of the conformity assessment of the design.

For each product with the CE marking the manufacturer shall issue a "Declaration of Conformity"; this document states that the product is in conformance with the approved design. A separate information leaflet on this declaration is available.

The File

Essentially the file shall provide the necessary evidence that the design is in accordance with relevant requirements.

The file shall identify the product and the requirements. It shall describe the assessment-activities, and contain the results of these activities.

Suggestions for file-elements are:

- Name of the company responsible for the design
- Name and function of the employee responsible for the file
- Name (of the product)
- Type-designation
- Description
- photographs, brochures
- technical construction drawings
- material compositions
- schematic diagrams
- parts lists of components
- descriptions of components

All different versions shall be described, as far as relevant:

- Copies of the user manual and service instructions, as far as applicable,
- List of applicable EU-directives,
- List of normative technical documents or standards used for the conformity assessment,
- Design calculations,
- Hazard (Risk) analysis,
- Description of measures to reduce or eliminate hazards (Risk Analysis),
- Evaluation and test reports, indicating:
- which evaluations and tests were performed,
- methods of evaluations and tests,
- evaluation- and test-equipment,
- results of evaluations and tests,
- acceptance criteria.
- Conclusion, indicating that the product complies with all relevant requirements.

If considered appropriate, descriptions and explanations to properly understand the documents, shall be provided.

It is the responsibility of the manufacturer to decide about the assembly of the file.

Information sources

The manufacturer may use outside-sources for the file or sub-contract the file, in parts or completely.

Manufacturers may not have available all evaluation- and test-equipment as required by the technical standards. Specialized laboratories, like CEBEC, provide relevant evaluation and testing services.

In all cases the manufacturer remains responsible for the contents of the file and should operate an adequate system to verify the contents of information received. This verification can be asked from third-party certification institutes or Notified Bodies.

Administration of the file

The file-elements need to be available. It is not an absolute requirement that the file is available as a "physical" entity. Manufacturers usually operate quality management systems or administration systems with document control procedures. The file-elements can be made available in accordance with these procedures. Authorities and Notified Bodies will require insight in the administration system of the manufacturer. Upon their request, the file, as a "physical" entity, shall be made available on short notice (a few days).

Notified Body

The conformity assessment scheme, require the involvement of a Notified Body in the design-stage. It is the obligation of the Notified Body to verify the contents of the file and to repeat evaluations and tests if considered necessary.

Suggested inclusion in the installation or user manual

EC Directive **EMC Guidelines 89/336/EEC**
Applied Harmonised Standards **DIN EN 55022/A Radio disturbance characteristics** **DIN EN61000-4-2 ESD** **DIN EN 61000-4-3 Radiated immunity** **DIN EN 61000-4-4 EFT/S**

Terms used

A

Application - Software specifically produced for the functional use of a computer system. Software written to perform a task on a computer.

Application Software - A program adapted to the specific requirements of a user for the purposes of data manipulation, data archiving or process control.

Approved Document (Approval) - A written document (protocol, technical report, procedure, test method, etc.) has been approved after it has been reviewed and signed by a pre-defined group of responsible individuals representing manufacturing, engineering, QC, R&D and QA/regulatory or their designates.

Archived Master - A software library which contains formally approved and released versions of software and documentation from which copies are made.

Audit *(Quality Audit)* - 1] A documented activity performed on a periodic basis in accordance with written procedures to verify, by examination and evaluation of the objective evidence, compliance with those elements of a quality program under review. 2] An independent review to assess compliance with requirements, specifications, baselines, standards, procedures, instructions, codes and contractual and licensing requirements. 3] A qualitative and quantitative.

C

cGMP - Current Good Manufacturing Practice.

Calibration - Documented comparison, by written and approved procedures, of a traceable measurement standard, of a known accuracy, with another measuring device to respond to, detect, correlate, report or eliminate any variation in the accuracy of the item being compared over an appropriate range of measurements.

Calibration Verification - The assaying of *Calibration* materials to confirm that the *Calibration* of the instrument, kit or test system has remained stable throughout the reportable range for test results. Performance and documentation of *Calibration Verification* is required to substantiate the continued accuracy of a quantitative test method for the reportable range of test results.

Calibrator - A device intended for use in a test system to establish the points of reference for the determination of values in the measurement of the test instrument. 2] Special samples of known values specifically prepared to set up a standard curve, or cut-off point, of an assay. Used in the *Calibration* of a diagnostic assay.

Certification - A documented statement, by authorized and qualified individuals *(Validation Committee),* that an equipment/system validation, revalidation, qualification, requalification or calibration has been performed appropriately with acceptable results. Certification may also be used to denote the overall acceptance of a newly validated manufacturing facility. 2] A written guarantee that a system, instrument, test or computer program complies with its specified requirements.

Challenge - The performance of tests to determine the limits of capability of a component in a manufacturing process. Limits of capability do not necessarily mean challenging until destruction, but rather the limits of variation within which a defined level of quality can be assured.

Change Control - A formal monitoring system by which qualified representatives *(Validation Committee)* of appropriate disciplines review proposed or actual changes that might effect a validated status. This is done to determine the need for *Corrective Action* to ensure that the system retains its validated state. 2] Management and implementation methodologies associated with increasing or correcting system capabilities, a partial system redesign or the determining of software obsolescence.

Closures - Those portions of drug or diagnostic systems, such as stoppers, caps or other barriers, which may be removed or otherwise altered in order to grant access to the container contents.
Code - To represent data or a computer program in a symbolic form that can be accepted by a processor. Loosely, one or more computer programs, or part of a computer program.
Code Audit - An independent review of *Source Code* by a person or team of persons, or a tool to verify compliance with software design documentation and program standards.
Critical Process Parameter - A control parameter that has a direct relationship to the quality, safety, effectiveness or performance of the intermediate or final product.
Critical System - A system whose performance has a direct and measurable impact on the quality of the intermediate or final product. A system determined to be "critical" must be designated as such, and must be maintained and operated using approved *Standard Operating Procedures (SOP)*.

D

Design Review (Architectural Review) - A planned, scheduled and documented audit of all pertinent aspects of a design that can affect performance, safety or effectiveness of a piece of equipment, system or facility. 2] A comprehensive, systematic examination of a design to evaluate the adequacy of the device requirements to evaluate the capability of the design to meet those requirements and to identify problems with the design and design requirements so solutions can be proposed to all such problems. 3] A technique of evaluating a proposed design to ensure that the design: a) Is supported by adequate materials that are available on a timely basis; b) Will perform successfully during use; c) Can be manufactured at low cost; and d) Is suitable for prompt field maintenance.
Design Validation - The comparison of the product against the user requirements that were agreed to, at contract review stage, and detailed in the design outputs. 2] Establishing by objective evidence that device specifications conform with user needs and intended uses.
Design Verification - The comparison of design output with design input. 2] Confirmation (by examination and provision of objective evidence) that the design output meets the design input requirements.
Device - An instrument that will give analytical answers as a result of electrical or mechanical measurements on an element, compound, solution, instrument, system, etc.

E

Enterprise Resource Planning (ERP) - A computerized system for integrating company-wide data in order to improve planning activities, provide better control of operations, and enable products to get to market more quickly.

F

Functional Design Specification (FDS) - provides a written definition of what the system does, what functions it has and what facilities are provided by the equipment/system.

Q

Qualification (IQ) - The performance of documented verification that an equipment/system installation adheres to approved contract specification and achieves design criteria. The IQ is developed from P&IDs, electrical drawings, piping drawings, purchase specifications, purchase orders, instruments lists, engineering specifications, equipment operating manuals and other necessary documentation. All developmental documentation will be included in an IQ. The manufacturer's recommendations, local and state codes and the cGMP should also be considered. The IQ precedes the Operational Qualification (OQ). 2] Establishing the documentary evidence that a sub-system or equipment is installed in compliance with the technical specifications, standards, codes and regulations. 3] Documented verification that all key aspects of hardware installation adhere to appropriate codes and approved design intentions and that the recommendations of the manufacturer have been considered.

L

Life Cycle - An approach to computer system development that begins with identification of a user's requirements and continues through design, integration, qualification, validation, control and maintenance, ending only when commercial use of the system is discontinued.

M

Manufacturer - Any person, who designs, manufacturers, fabricates, assembles or processes a Finished Device. This includes contract sterilizers, specification developers, repackers, relabelers and initial distributors of import devices.

Manufacturing Execution System (MES) - A real-time system for coordinating all data relating to the manufacture of products and applying them directly to shop floor activities.

Manufacturing Resource Planning (MRP) - An automated system for handling information directly relating to manufacturing. This includes inventories, bills of materials (BOM) and orders from purchasing.

Manufacturing Resource Planning II (MRPII) - An expanded version of *MRP* that includes enhanced capacity for planning and scheduling the use of manufacturing resources.

Marking - Information about the contents and shipment of a package which is printed on or affixed to the surface of the package.

O

Objective Evidence - Information which can be proven to be true based on facts obtained through observation, measurement, test or other means.

Ongoing Evaluation - A term used to describe the dynamic process employed after a system's initial validation in order to maintain the validation status of the computer system.

Operating Parameter (Operating Variable) - The *Process* variables which are measured to monitor and maintain the normal state of a *Process* or system. All factors, including *Control Parameters,* which may potentially affect the *Process State of Control* and/or fitness for use of the final product.

Operating System - A set of programs provided with a computer that function as the interface between the hardware and the applications program.

Operational Qualification (OQ) - 1] The documented verification that the equipment/system performs per design criteria over all defined operating ranges. The OQ includes qualification of operating and maintenance records. The OQ precedes the *Performance Qualification (PQ).*

Original Observations - The first occurrence of human-readable *Information.*

Out-of-Specification Event - When one or more of the requirements included in *Standard Operating Procedures* for *Controlled Environments* are not fulfilled.

P

Package - The completed product of a packing operation. It consists of the packaging and its contents prepared for shipment.

Packaging - Assembly of one or more containers, and any other components, which are necessary to ensure compliance with minimum packaging requirements of applicable regulations.

Packing - The art and operation by which an article, material, or substance is enveloped in a wrapping and/or packaging or otherwise secured.

Parenteral - Products administrated to patients by routes other than the mouth, such as intravenous (IV) or intramuscular.

Performance Qualification (PQ) - Documented verification that equipment, systems or processes operate the way they are purported to do. This operation must be reliable and reproducible within a specified, predetermined set of parameters, under normal production conditions and must be in a *State of Control.* Establishing documentary evidence that operating characteristics and product are in conformity with the limits defined in the specifications. Critical parameters (temperature, pressure, flow rate, humidity, etc.)

must be stable over time under both normal and worst-case conditions.

Procedure - An approved document listing a specific set of instructions which, when followed, will produce a product or result defined by a specification. Procedures are used to define and control the manufacture of materials as well as the operation and/or maintenance of equipment, systems or processes.

Production - All activities subsequent to design transfer up to the point of distribution.

Programming - Coding of program modules that implement a design.

Prospective Validation - Establishing documented evidence that a system does what it purports to do based on a written and approved, preplanned protocol. The validation is performed prior to the manufacture of clinical or marketable product, and the product is not sold until the equipment, system and process meet the validation acceptance criteria.

Protocol - The written and approved document of an experimental sequence of tests that, when executed as prescribed, are intended to produce documented evidence that the equipment or system does what it is designed or claims to do reproducibly. The protocol will address all elements of the validation sequence relevant to the assay, process, equipment or system being challenged. The results of the performance of the protocol shall be documented in a *Validation Final Report.*

Q

Qualification - Used to describe the *Testing* and review of a piece of equipment, system or sub-system of a process to assure its fitness for use. *Qualification* deals with components or elements of a process, while *Validation* deals with the entire manufacturing process for a product. The qualification procedure is determined by a written and approved *Protocol* or *Testing* defined by the *Validation* review committee. 2] Operation aimed at proving, with regard to either materials, equipment or personnel, that the required conditions are met and that they actually provide the expected results. 3] Action of proving that any equipment works correctly and actually leads to the expected results. The word *Validation* is sometimes widened to incorporate the concept of qualification.

Quality - The totality of features and characteristics, including safety and performance, which bear on the ability of a device to satisfy fitness for-use.

Quality Assurance (QA) - The activity of providing, to all concerned, the evidence needed to establish confidence that the quality function is being performed adequately. 2] All activities necessary to assure and verify confidence in the quality of a process used to manufacture a *Finished Device.* 3] *Quality System* - International Standard, ISO 9004 replacement term for Quality Assurance. 4] All the planned and systematic activities implemented within the *Quality System* which can be demonstrated as needed to provide adequate confidence that an entity will fulfill requirements for *Quality.*

Quality Assurance Unit - Any person or organization element designed by laboratory management to monitor the LIMS functions and procedures.

Quality Audit - An established systematic, independent, examination of a manufacturer's entire *Quality System* that is performed at defined intervals and with sufficient frequency to ensure that both quality system activities and the results of such activities comply with specified quality system procedures. It is also used to determine that these procedures are implemented efficiently, and that that they are suitable to achieve quality system objectives. *Quality Audit* is different from, and in addition to, the other *Quality System* activities required.

Quality Control (QC) - The regulatory process, through which industry measures actual quality performance, compares it with standards and acts on the difference.
Quality Function - The entire collection of activities from which industry achieves fitness for use, no matter where these activities are performed.
Quality Plan - A document setting out quality practices, resources and sequences relevant to a particular product, service, contract or project.
Quality Policy - The overall quality intentions and direction of an organization with respect to quality, as formally expressed by the executive management.
Quality System - All planned and systematic activities necessary to provide adequate confidence that a product, process or service will satisfy given quality requirements (International Standard, ISO 9004). See *Quality Assurance.* 2] The organizational structure, responsibilities, procedures, specifications, processes and resources for implementing quality management. 3] Organizational structure, procedures, processes and resources needed to implement quality management.

S

Recertification - The repetition of a documented qualification procedure after minor alterations, maintenance or repair. The extent of the requalification is determined by the Validation Committee.
Record - Any written or automated document (books, papers, maps, photographs, machine-readable materials, etc.), including specifications, procedures, protocols, standards, methods, instructions, plans, files, notes, reviews, analyses, and reports - regardless of physical form or characteristics - made or received by an agency of the United States Government under federal law or in connection with the transaction of public business and preserved, or appropriate for preservation, by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the government or because of the informational value of the data in them.
Repeatability - The *Precision* of a method performed under the same operating conditions (e.g., same operator and equipment) over a short period of time. Also known as intra-assay precision.
Reproducibility - The measure of a test method's variability with different analysts, laboratories or other conditions.
Requalification - The approved written procedure used to return a process, piece of equipment or system to a validated or qualified state after maintenance or minor changes have been made to it. Especially applicable to those systems used to control or measure critical parameters. The *Validation Committee* determines the extent of the requalification required, depending on the repair or maintenance procedures performed.
Retrospective Validation - Establishing documented evidence that a system does what it purports to do based on a review and analysis of historical data and information obtained during the production of clinical or marketable product.
Revalidation - The repetition of the *Validation* sequence or a specific portion of it, to assure that the system is suitable for use after modification, repair or maintenance that could alter the product characteristics or performance. *Revalidation* is also required periodically.

S

Standard Operating Procedures (SOP) - Written procedures describing operations, *testing,* sampling, interpretation of results and *Corrective Actions* that relate to the operations that are taking place in a *Controlled Environment* and auxiliary environments. Deviations from the SOPs should be noted and approved by responsible managers.

T

Test Case (Test Script) - A specific set of test data and associated procedures developed for a specific objective. Some examples are: To exercise a specific program path, or to verify compliance with a specific requirement.

Testing - The determination, by technical or scientific means, of the properties or elements of a product or its components. This includes functional operation and involves the application of established scientific principles and procedures.

V

Validation - The overall term for the establishing of documented evidence through defined tests and challenges, that a system, manufacturing process, analytical method and/or piece of equipment meets design criteria and that adequate provisions have been established to keep it in a *State of Control* so it will produce a product that meets predetermined specifications and quality attributes.

Validation Capability/Maturity Model - A model (borrowed from Carnegie-Mellon) used to describe the level of knowledge of *Validation.* There are four levels to the model:

1. Level 1 - Validation Unaware: No knowledge of the Theory of Validation
2. Level 2 - Validation Aware: Basic knowledge of the Theory of Validation
3. Level 3 - Validation Active: Forced to participate by regulation or customer demand.
4. Level 4 - Validation Enthusiast: Experienced in practice; recognising the benefits and limitations and encouraging others to participate.

Validation Change Control - A formal monitoring procedure during which qualified members of a *Validation Committee* (and/or others from appropriate disciplines) review the affect of proposed or actual changes on the manufacturing process to determine the impact on the *Validation* status. These representatives may initiate corrective action to ensure the system or process retains, or is returned to, a validated condition or *State of Control.*

Validation Committee - A cross-functional group of qualified individuals representing each major division in a company [manufacturing, engineering, development, engineering services, facilities, production, quality services, R&D, and QA/regulatory affairs] that is assembled to review, evaluate and approve all *Validation* and/or *Qualification* functions and/or activities.

Validation Master Plan - The establishment of a dynamic written plan that defines the overall approach to a *Validation* project. It will define the terminology to be used in all subsequent documentation, outline descriptions of the facility site, the manufacturing processes and the scope and implementation of the *Validation Sequence.* This document is prepared concurrently with the construction phase of a project after all equipment and materials have been specified.

Validation Plan - The collection of activities that include, and are specifically related to, computer system validation itself.

Validation Sequence - The specific set of steps undertaken to validate a system, equipment or process. The *Validation Sequence* may contain any one (or more) of the following steps, depending on the size, complexity, function and criticality of the equipment or system. A subsequent step in the *Validation Sequence* should not be initiated prior to the completion of a prior step. No step can be implemented prior to securing an *Approved Document* (protocol) directing the method of the execution of the document.

1. Design/Specifications Qualification
2. Construction Qualification or Architectural Review *and* Commissioning (Pre IQ)
3. Calibration
4. Installation Qualification Operational Qualification
5. Performance Qualification or Process Qualification (Process Validation)