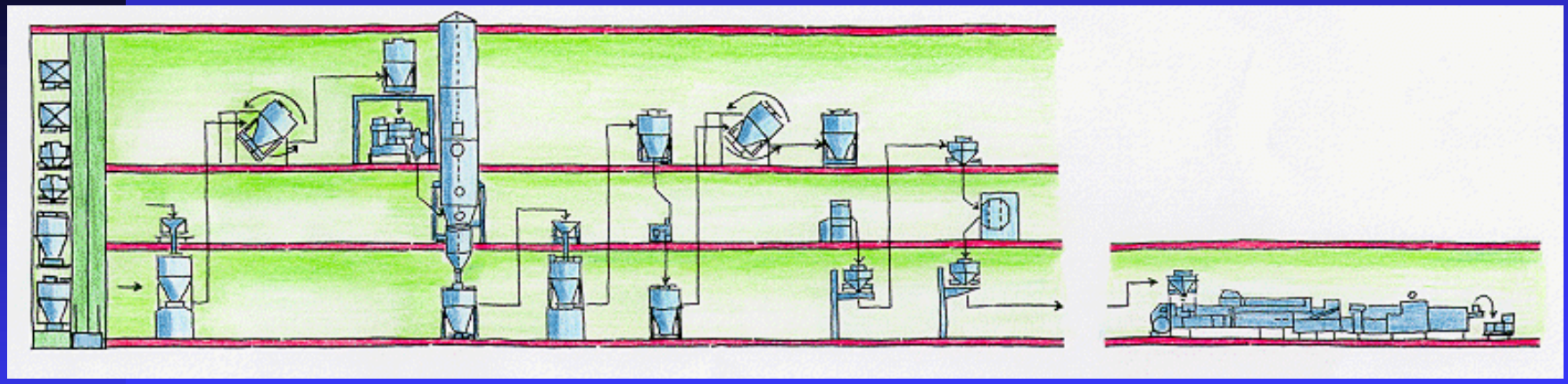
GAMP4

IKEV - Istanbul

02-03 May 2002

by Danny Eykholt

SNC·LAVALIN Pharma



Increased Focus of Regulators

483s on FDA website

- www.ISPE.org
- www.GAMP.org
- www.FDA.gov
- dg3.eudra.org

SNC·LAVALIN Pharma

483s on Specifications

- Specification documents for computer process control did not **detail** system / software development
- System specification documents were prepared and **signed-off after** vendor acceptance testing
- Specification documents lack details to support future changes to code
- No formal requirements for software design
- System developer audit was cursory and failed to demonstrate contractor qualifications
- Computer used in the shipping / receiving area to log / track raw materials had inadequate security (this is a direct reflection of **poor specification** of the needs)

483s on Testing

- Functional requirements **not tracked** through software development life cycle
- Failed to identify and analyze system / software safety **critical** functions
- Qualification criteria were not tracked through systems development
- Data transferred from working hard copy to computer database without data **verification**
- Formal error / incident **logs** were not kept during installation and qualification of software
- No procedures to **audit** computer generated data, results and/or error corrections

483 on Comp. Systems in Labs

"During the validation of the laboratory computer system at installation only calculations producing results within expected ranges were verified versus manual calculations. No testing was done of other conditions such as results at and outside of the expected range limits, inappropriate data entry, and error condition recovery. There were no written specifications for allowable variations in calculation check comparisons, and comparison records were not signed / dated to indicate review and approval."

483s on Change Control

- Undocumented software changes
- **Master** hardcopy for all source code not maintained
- New revision number not issued after software modifications arising from IQ / OQ results
- No records of changes to original source code made prior to installation; no audit trail provided
- Release and implementation dates of source code not recorded
- Hazard analysis for safety critical functions / components not required after software changes

483s on Change Control (contd.)

- Version numbers not assigned to all programs
- Not all documented software changes had clear specific rationale for the change
- Software changes resulting from IQ / OQ were not documented
- User profile codes allowing access to screen editing capability were not fully validated
- No procedure for evaluating / updating overall system configuration after code modifications

GAMP 4 objectives

- Assist Users and Suppliers
- To easily determine the extend and scope of validation
- Framework for convergence with existing standards (e.g. TickIT, ISO 9000)
- Introduce sample procedures to easy the introduction of the defined principles

History

- 1994, 96, 98, 2001 – GAMP v1, 2, 3, 4
- 1996 links to APV and GMA/NAMUR
- JETT (Process Ctrl USA, Can) join GAMP
- 2001 – GAMP becomes part of ISPE

GAMP4 Contents

SNC·LAVALIN Pharma

Amsterdam keywords 3,4 Dec 01

- Increased focus on CSV
- Calibration
- Auditing, SLA
- Ongoing support
- Change Control
- Risk Assessment
- System Security
- Business Continuity Planning

Definition: Life cycle Validation

demonstrated conformance to user, design and functional specifications

- Establishing documented evidence
- which provides a high degree of assurance
- that a specific process will consistently produce
- a product meeting its pre-determined specifications and quality attributes.

ongoing quality audits, structural, functional and integration testing

Test Plans and Protocols

Phases of Qualification

- URS - Process Oriented Description
- FS - Tasks
- DS - Technical Detailed Documents

DQ

- Build
- IQ - install., configuration, completeness, calibration
- OQ - functionality, dry run in normal range
- PQ - product, repeatability

Validation Plan & PQP

- Validation Plan ⇨ Compliance
  - regulations.
  - Validation evidence
- Project en Quality Plan ⇨ Quality
  - deliverables
  - Progress reporting
  - Approved by suppliers

GAMP Category	1	2	3	4	5
Description of software category	Operating Systems	Firmware	Standard Software packages	Configurable software packages	Custom or bespoke systems
Change Control	〈	〈	〈	〈	〈
SOPs		〈	〈	〈	〈
Training		〈	〈	〈	〈
Supplier Audit		(〈)	(〈)	(〈)	〈
User Requirements testing in OQ			〈	〈	〈
Full Life Cycle Approach				〈	〈
Address Layers of Software				〈	〈
Mitigation Strategies for weakness in supplier's development process				〈	〈

Firmware = incorporated in instruments and controllers (〈) = Optional

Example traceability matrix (vertical type)

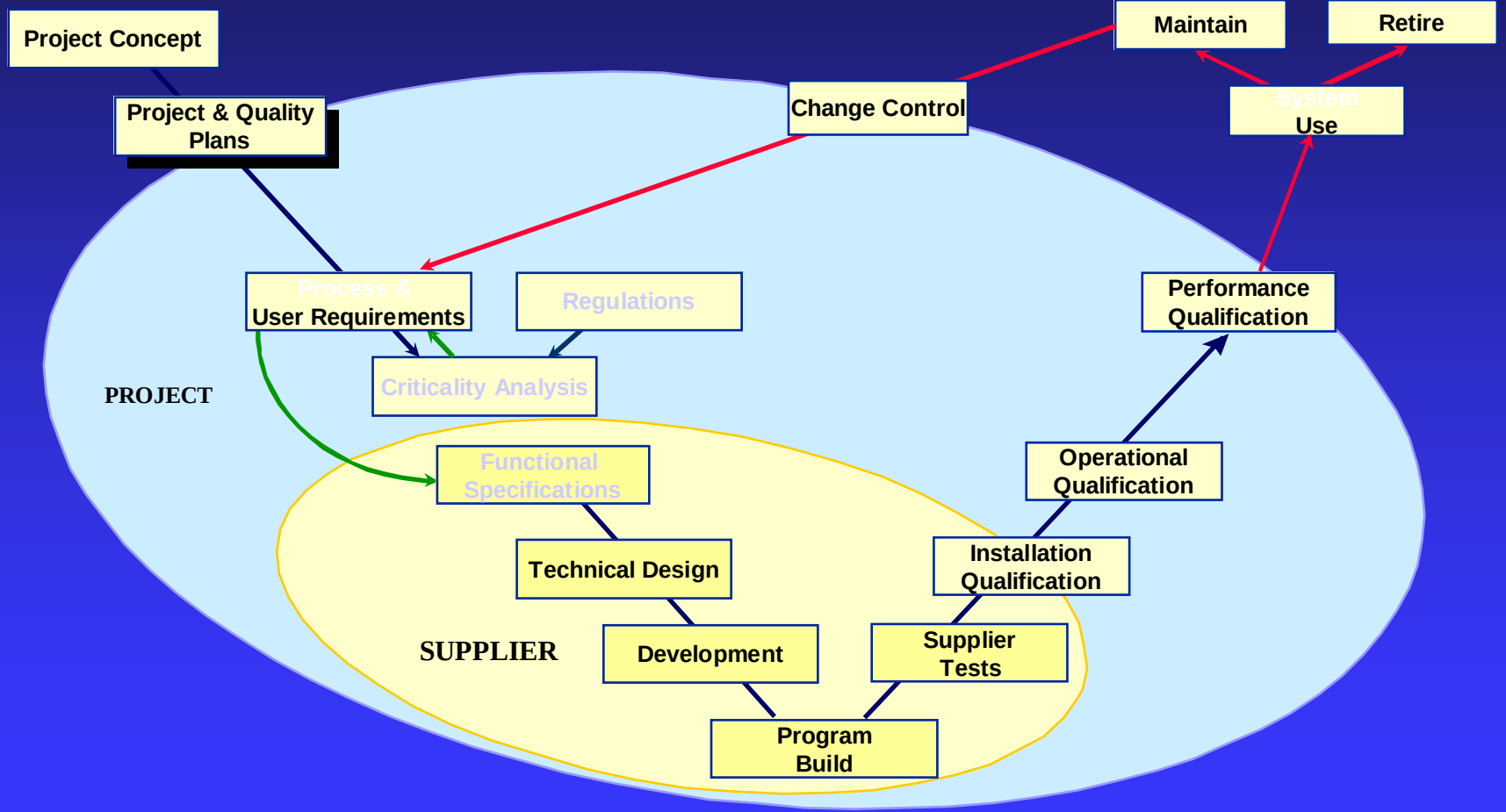
User Requirements / Functional Specifications	U-FAM-1	U-FAM-2	U-LEEF-1	U-LEEF-2	U-LEEF-3	U-STIJL-1	...	
F-VORM-1						X		OK
F-VORM-2								?
F-BINNEN-1	X	X		X				OK
F-BINNEN-2	X	X		X				OK
F-BINNEN-3			X					OK
F-ELEC-1					X			OK
F-ELEC-2					X			OK
...								
	OK	OK	OK	OK	OK	OK		

Life Cycle Model following GAMP4

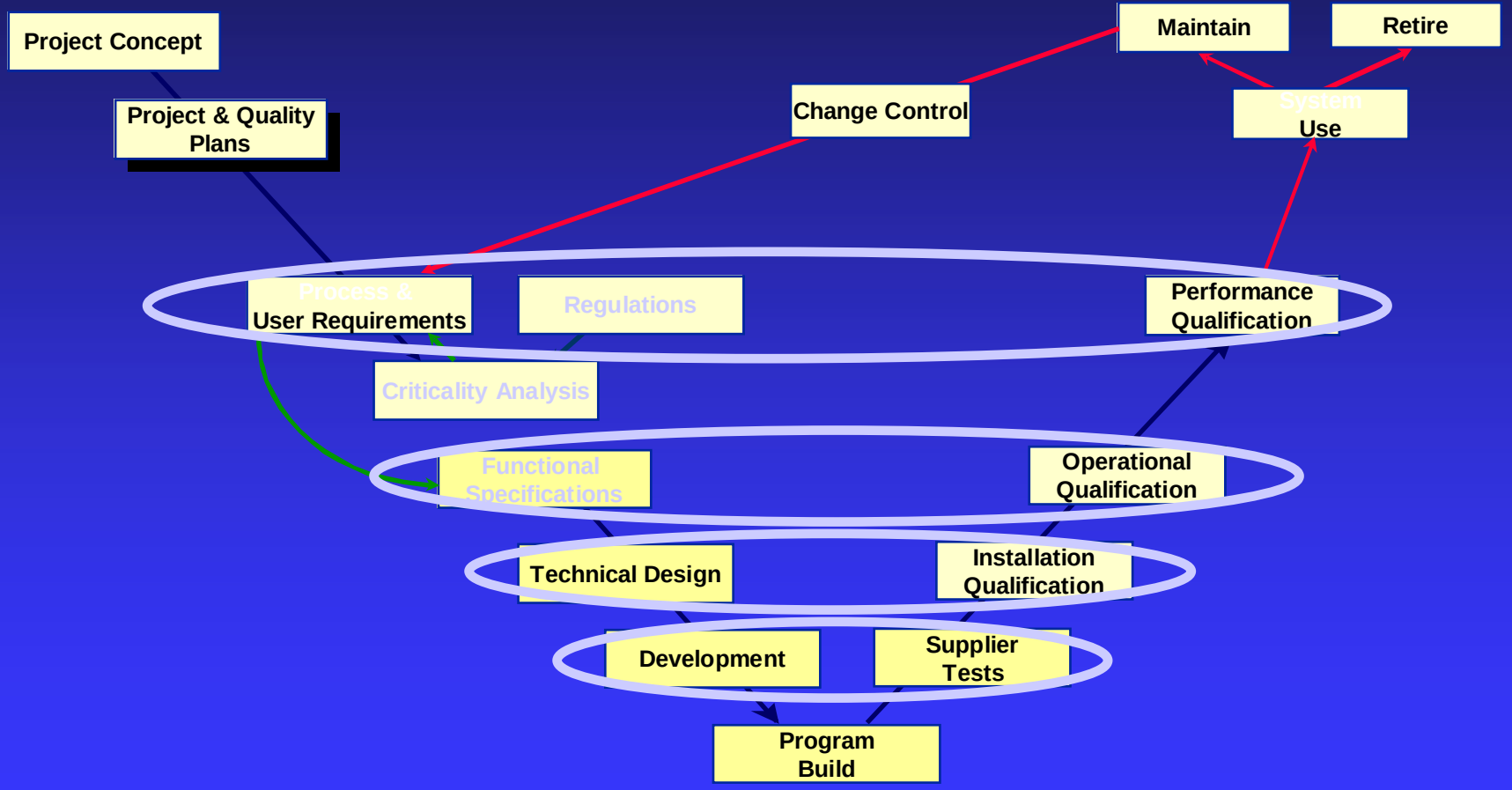
Detailed step by step guide

SNC·LAVALIN
Pharma

The V model


Project Concept
Project & Quality Plans
Maintain
Retire
Change Control
System Use
Process & User Requirements
Regulations
Performance Qualification
PROJECT
Criticality Analysis
Functional Specifications
Operational Qualification
Technical Design
Installation Qualification
SUPPLIER
Development
Supplier Tests
Program Build

The V model


Project Concept
Project & Quality Plans
Change Control
Maintain
Retire
System Use
Process & User Requirements
Regulations
Performance Qualification
Criticality Analysis
Functional Specifications
Operational Qualification
Technical Design
Installation Qualification
Development
Supplier Tests
Program Build

Validation Policy

- *Standardised Approach*
- *GXP Compliance*
- *System Life Cycle*
- *Management responsibility*
- *Quality Assurance*
- *External Supplier Relationship*

Validation Policy

- *Internal Partners*
- *Validation Master Plan*
- *Validation Documentation*
- *Signatures and Electronic Records*
- *Training*
- *Maintaining the Validated Status*

Validation Master Plan

- *Purpose*
- *Scope*
- *Objective*
- *References to policies and plans*
- *References to other documents*
- *Description of levels of planning*
- *General Description of Production Plant*
- *Description and locations of the areas being covered at this level*
- *Organisation of Validation Activities*

Validation Master Plan

- *Validation Team*
- *The Validation Execution Group*
- *Validation Strategy*
- *Production Plant Validation Policy*
- *Life Cycle Model Applied*
- *Validation Reporting*
- *GxP Criticality Assessment Process*
- *Requirements to determine Level of GxP*
- *Procedure for performing the assessment*
- *Status of the process*
- *Phases of Qualification*

Validation Master Plan

- *Automated System Validation Procedures*
- *EU GMP Vol4, Annex 11 requirements*
- *Testing of an Automated System*
- *Calibration*
- *Deviations (handling) and Action Plan*
- *Change Control*
- *Documentation Management*
- *SOP's and Training*
- *Timeline and Resources*
- *Environmental Monitoring*
- *Process Validation*

Validation Master Plan

- *Additional Programs*
- *Facility cleaning and sanitation*
- *Process Equipment Changeover cleaning*
- *Preventive Maintenance*
- *Equipment/System history files (log book)*
- *Status Tagging and checklists*
- *Room history files (Room log books)*
- *Periodical Recalibration program*
- *Periodical Revalidation program*
- *Lexicon*

Validation Procedure

- *Overview of Validation*
- *The Validation Process*
- *Validation Elements*
- User Requirement Specification
- Design Qualification
- Installation Qualification
- Operational Qualification
- Performance Qualification
- Validation Summary Report

Validation Procedure

- *Validation Procedures*
- Document Templates
- Qualification Protocols
- Validation Summary Report
- Changes and Revalidation
- Completion of Validation documentation
- Document Control

IQ Protocols

- Targeted Audience
- Scope
- Objectives
- Qualification Method
- Preparation
- Verification
- Reporting, logging en resolving of deviations
- Qualification Acceptance Criteria

IQ Protocols

- Project Deliverables
- Project- and Quality Plan
- Suppliers audit
- User Requirements Specification Document
- GMP- Analysis
- Review ‘safety Plan’
- Criticality Analysis
- Functional Specification
- Traceability matrix URS vs. FS
- Traceability matrix FS vs. tests
- Approved Design Drawings

IQ Protocols

- Systeem In- and Outputs
- Installation Instructions
- Design Tests
- Calibration Procedures en Protocols
- User
- Program Description
- User Manuals
- Training Plan
- Environment
- Access Control
- Utilities

IQ Protocols

- Environmental Conditions
- Installation
- As-Built approved drawings
- Systeem In- and Outputs
- Source Code for Control System
- System Configuration
- Devise Inventory List
- Instrument List
- Spare Parts List
- Installation Tests Hardware
- Installation Tests Software

IQ Protocols

- System Management
- GMP check SOP System Management
- Maintenance and Logbook
- Service Level Agreements
- Verification List
- Verification Notes List
- Verification Deviation List
- Verification General Remarks List
- General Acceptance
- Responsibilities

OQ Protocol

- General as for IQ
- Operational Tests Hardware
- Operational Tests Software
- Operational Tests System
- calibration
- Verification List
- General as for IQ

PQ Protocol

- General as for IQ, OQ
- Qualification Acceptance Criteria
- Performance Tests
- Verification and general as per IQ, OQ

Test Concept

- Categorisation of the various tests
- See example

e Records & e Signatures

SNC·LAVALIN Pharma

Definitions

- Electronic Record - any combination of text, graphics, data, audio, pictorial or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system
- Electronic Signature - a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature

Definitions

Closed Systems - an environment in which system access is controlled by persons who are responsible for the content of the electronic records that are on the system

- Open Systems - an environment in which system access is not controlled by persons who are responsible for the content of the electronic records that are on the system

What is 21 CFR Part 11?

- A set of rules governing access, storage, retrieval, control and security of electronic records
- A set of rules governing security, control and use of electronic signatures

- Provides the basis by which electronic records and electronic signatures may be used as equivalents to paper records and traditional handwritten signatures

Where did the regulation come from?

- Initial drafts of ANPRM were presented in 1992
- Proposed rule was issued in 1994
- Final Rule was issued March 20, 1997 to become effective August 20, 1997
- Compliance Policy Guide was issued May 1999

Industry comment and technical interchange was key at each phase of development.

What is Scope of 21 CFR 11?

- Records maintained on site for inspection
- Records submitted to the agency
- All ER/ES created since August 20, 1997 are subject to Part 11
- Legacy systems are not exempt if they continued to be used after August 20, 1997

21 CFR Part 11's Legal Status

Part 11 . . .

- is a substantive regulation
- has the force and power of law
- is a "minimum" standard

When do we have e signature?

- ID
- Password
- States what one signs for
- Action to execute the “signing”
- Within a policy/certificate framework

- =/= Records
- =/= Security

In a nutshell for closed system with no electronic signatures

- Audit Trail (and system event log)
- Security
- Archiving and Record Retention

E signatures & security

- Trustworthiness of information:

- Privacy
- Integrity
- Non-repudiation
- Authentication

Security Considerations for Electronic Records

- limit system access
- use secure, independent, computer generated time-stamped audit trails that do not obscure the original data
- self-monitor operational sequences
- use authority checks
- limit distribution / access to documentation for system operation and maintenance

General Security Principles Common to Both ES & ER

- Validation!
- Written procedures must govern system use
- Adequate controls over access / availability
- Appropriate training and control for all users
- Periodic testing of devices
- Maintenance
- Change Control

Storage of Electronic Records

- What?
  - Any record or supporting documentation required by the predicate rule(s)
  - Electronic records must be stored with all “meta data” and must be capable of providing records in human readable form
- Where?
  - Secure location
  - Durable media
  - Accessible for audit / inspection

Storage of Electronic Records (continued)

- How?
  - With suitable audit trails / security
  - Periodically inspected
  - Transcribed (with validation) as technology progresses, if required
- How Long?
  - For the duration dictated by the predicate rule
    (e.g., 1 year beyond expiration, 3 years, device life, etc.)

System Security (Information Protection Worksheet)

- Protection
  - Confidentiality (access control or encryption)
  - Integrity (access control or digital signatures)
  - Availability of Information (redundancy or file backup)
- Seriousness & Likelihood (H,M,L)
  - Disclosure
  - Modification
  - Loss
- Security = Loss Prevention
- Classify systems subject to regulatory control or inspection
- Your policy must ensure the validation status of PCs is not compromised. (office/validated data)

Hybrid Systems

- Mixing of manual records / signatures with electronic records / signatures is permitted by the final rule -- so called “hybrid systems”
- Ensure that all Part 11 rules are complied with for the electronic portions
- Ensure that manual records are not really “electronic records” in disguise

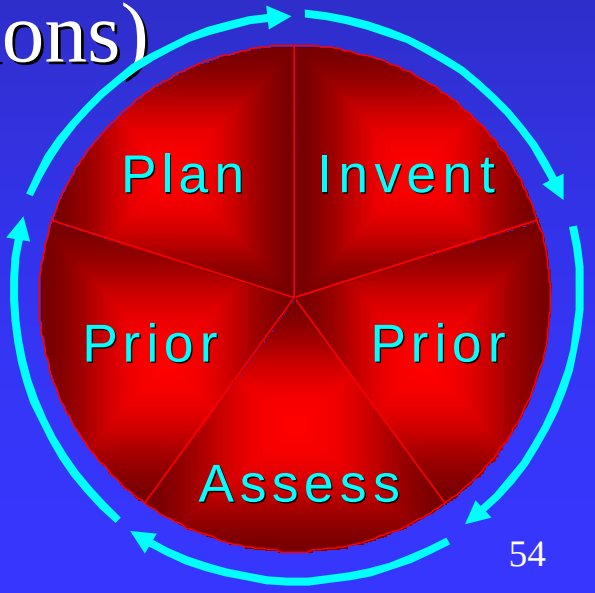
E Records & E Signatures

Steps towards compliance

SNC·LAVALIN Pharma

21 CFR Part 11

- Inventory (assessment forms, architecture)
- Prioritisation
- Assessment (GAP analysis)
- Remediation (corrective actions)



Step 1- Inventory...

- Identification of all recorded/stored data and signatures of automated systems as described in the scope. Such as:
  1. Operating systems (WinNT, Unix,...)
  2. Development packages (FIX, win CC,...)
  3. Application code & specific configurations
  4. Recipe data (production parameters & info)
  5. Operations data (audit trails, trends, reports)

...Inventory

- Templates for collection of

  1. General details (system classification, architecture, configuration, access,…

  2. Documented evidence for the fixed and variable data types and storage, backup and deletion details

- Data model & Database

Step 2- Prioritisation

- Spreadsheet used to calculate the risk
  - Impact on the business
  - “Probability” of non-compliance
- Alternatively a checklist can be used to add all the non-compliance's

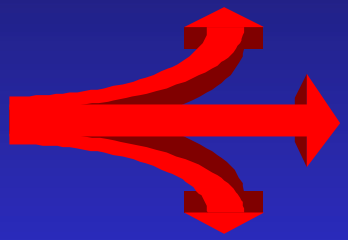
Step 3- Assessment

- "Compliance report" with ratings (high, moderate, low) based on
  - GxP risk
  - Priority
- Indicating the type of compliance gap

Step 4- Remediation

- Plan of corrective actions
- Possible actions for not-compliant system:
  - Repair, retire, re-engineer, replace, update controls and procedures
- The classification (H,M,L) allows for the appropriate corrective action:
  - Resolve, manage, accept

Detailed Corrective Actions
Determination of Solutions



- Technological
- Procedural
- Procedural fixes for technological problems *

** cannot be used to avoid parts of the regulation*

Recommendations for Data Management

- Automated Systems Register
- Backup and Storage Register
- System Access and Security
- Software Changes and Revision Control
- Recipe Creation and Control
- System Recovery
- Control of Programming Devices
- Auditing of Automated Systems
- Validation and Training

Risk Management

and Validation

SNC·LAVALIN Pharma

Relation with Validation?

- Validation avoids intolerable risk to patient safety.
- And it maximises business profit
- Risk Assessment answers to the question “how much validation is required?”
- It provides justification called for by regulators and cost benefits sought by the business

Risk Assessment as per GAMP

- Identify Processes
- Identify GxP Risk (Criticality Analysis)
- Identify Business Risk
- Identify Risk Scenario’s
- Assess the Likelihood
- Assess the severity of the impact
- Assign Risk Classification
- Assess Probability of detection
- Determine risk mitigation measures
- Risk Assessment of Changes

Contingency Planning

- It’s a regulatory requirement!
- EU GMP annex 11 & 15 require adequate alternative arrangements for systems in event of breakdown

Business Continuity Planning

- Business Impact Analysis
- Business Contingency Planning
- Emergency Response Planning
- Disaster Recovery Planning

BIA determines the cost of risk

- Financial Impacts
  - Lost Revenue
  - Lost Trade Discounts
  - Contractual Penalties / Fines
- Operational Impacts
  - Negative Public Image
  - Loss of Shareholder Confidence
  - Employee Morale
- Extraordinary Expenses
  - Rental/moving premises equipment, media reconstruction…

BIA

- Analysis Form
  - Business Processes
  - Systems
  - Stakeholders
  - Supporting Infrastructure
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)
  - Service Level Agreement (SLA)
  - Threats to the process
- Matrix
  - BIR =(B*BW)+(P*PW)

BCP

- Act of planning for the continued operation of systems and facilities in the event of a known adverse incident or fault condition occurring. (Procedures to prepare and respond to threats to the continuation of normal business)
- Backup and Recovery
- Record Retention / Archiving and Retrieval
- System Security

ERP

- The preparation of site level plans that will ensure the provision of critical infrastructure services to a site as well as timely status communications.

DRP

- Act of planning for the restoration of a system and facilities after a major incident
- Detailed plans for the recovery of loss of IT systems and data.

- Practice (“test”) the Procedures !!!