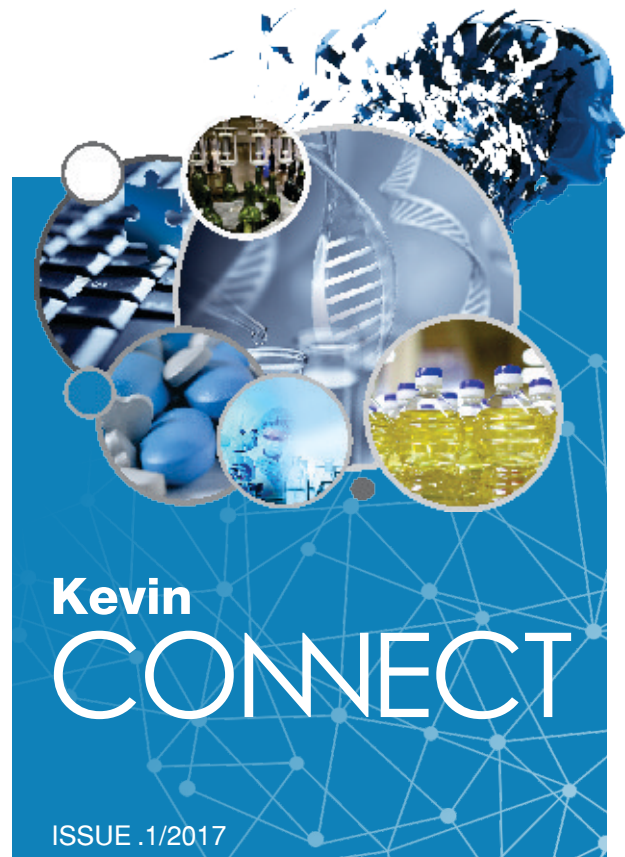




www.kevintech.com

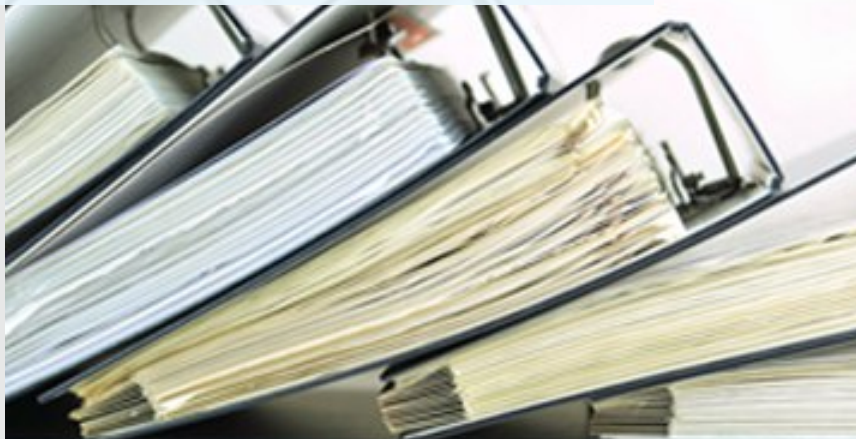
Current Practices of **COMPUTERIZED SYSTEM VALIDATION**



CONNECT INSIDE

- Basics of Computerized System Validation
- Life Cycle of Computerized System
- Life Cycle Approach
- Electronic Records and Electronic-Signatures: Compliance Point of View
- Data Integrity
- Testing as Per Gamp 5 Guidelines
- Auditor's Perspective

The less manual the better
The more automated the better
Less transcripts the better
Electronic documentation
Electronic Signature



Dear Customers / Friends,

Kevin has an impressive legacy of partnership with its customers in successfully applying technology-based solutions and supporting their competitiveness. We are proud of our reputation as a reliable & trustworthy solutions provider for factory automation as well as Regulatory Compliance Services.

Our corporate culture is one of dedication, respect, and continuous improvement. We measure our success by our customers' successes.

In a time marked by rapidly changing customer expectations, I am enthusiastic about the opportunities available for us to address the emerging requirements of our customers.



Yours Sincerely,

A handwritten signature in black ink, appearing to read 'K. Khambhatta', with a horizontal line underneath.

Ketan Khambhatta,
Managing Director

Driving Performance with Technology

Providing world-class technologies and solutions

Founded in 2000, Kevin Technologies is a leader in Automation for Life Sciences, Starch & Edible Oil, Consumer Packaged Goods & MES (Manufacturing Execution Systems) solutions. We are also one of the largest companies, in the area of Regulatory Compliance & Validation for FDA approved facilities across pan India.

We specialize in conceptualization & development as well as engineering of automation and supervisory control systems. Kevin helps clients meet their business objectives by providing effective project management capabilities and expertise in state-of-the-art technologies including Regulatory Compliance & Validation Services.

Our Mission

To provide technical excellence through innovation teamwork and commitment.

Our Ultimate Vision

To be the number one company in the area of expertise that we operate in, especially Factory Automation & Regulatory Compliance Services.

Basics of Computerized System Validation

In recent years, we have observed an upward trend in the use of computerized systems in the pharmaceutical industry. If we talk about guideline-driven industries, the pharmaceutical industry will lead the list. These guidelines pull towards validation and documentation at different stages.

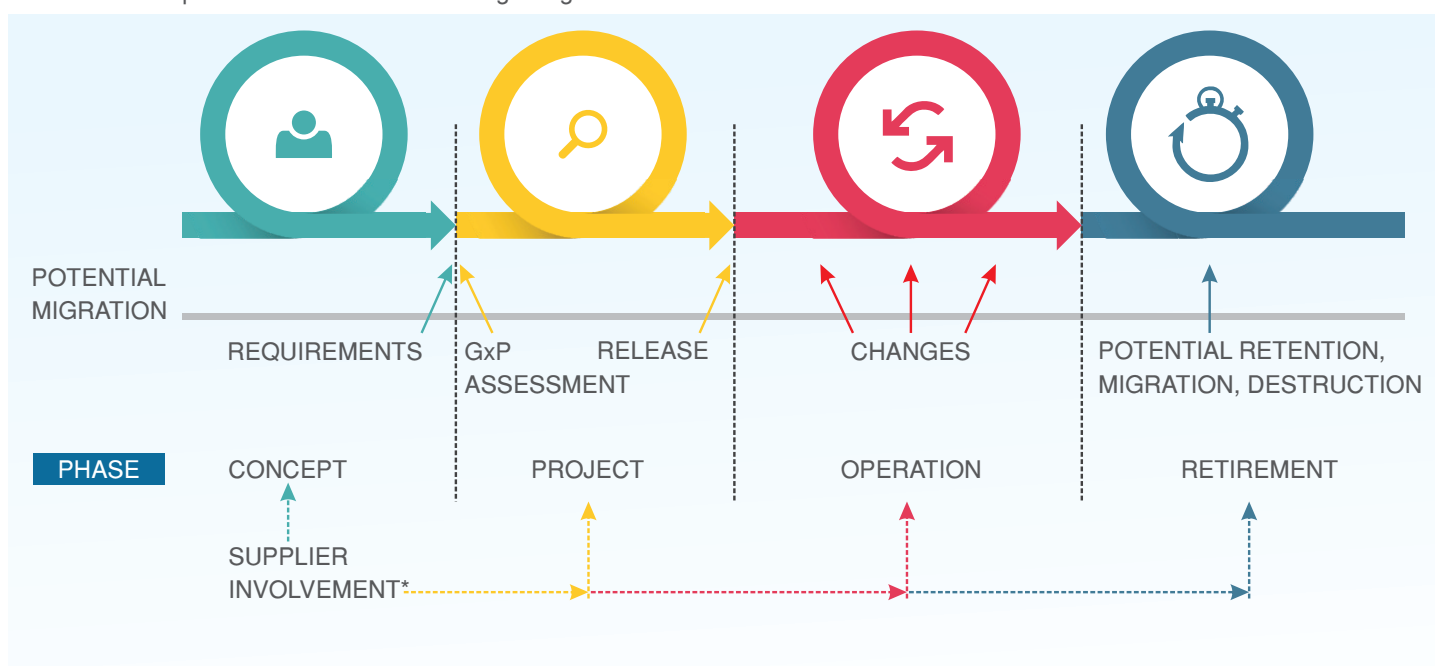
Computerized systems are also not exempted from it. It is required by USFDA, EMA, GMP, GCL, GLP. CSV also helps to increase system uptime and reduce failure rate and identify defects at the initial stage, which costs heavily once the system goes live. It also ensures product and data quality through precise documentation processes. USFDA and EU have given guidelines

If any answer turns to yes in the above table, then it triggers computerized system validation.

Life Cycle of Computerized System

Now we will understand the V-model from GAMP 5, which will be implemented in project and operation phases.

As per guidelines given in GAMP 5, Risk Assessment is involved at different stages of Project and Operation phases of the Life Cycle approach.



* This could be a complex supply chain
Supplier may provide knowledge, experience, documentation, and services throughout lifecycle.

GENERIC LIFE-CYCLE

for handling Electronic records & Electronic signature through guideline like 21 CFR part 11 and EU annex 11 respectively. We show v-model approach of Good Automated Manufacturing Practice version 5 (GAMP 5) is guideline developed by ISPE.

Foremost, we have shown here few general questions to understand requirement of validation for system :

- Does the system create regulated records?
- Does the system maintain regulated records?
- Does the system modify regulated records?
- Does the system archive regulated records?
- Does the system retrieve regulated records?
- Does the system transmit regulated records?
- Does the system support product release?
- Does the system handle data that could impact product purity, strength, identity?

Life Cycle Approach

Life cycle activities should be scaled according to:

1. RISK ASSESSMENT

- System Impact on Patient Safety
- System Impact on Product Quality
- System Impact on Data Integrity

2. RESULT OF SUPPLIER ASSESSMENT

Regulated companies should seek to maximize supplier involvement throughout the system life cycle in order to leverage knowledge, experience and documentation, subject to satisfactory supplier assessment.

3. SYSTEM CATEGORIZATION

System Complexity & Novelty.

One has to understand that specific V-Model will be decided as per software categories.

SOFTWARE CATEGORIES (EACH CATEGORY HAS ITS OWN APPROACH OF VALIDATION).

Apart from these guidelines , one should also be aware of 21 CFR Part 11 and EU Annex 11-Electronic Records and Electronic Signatures(ER & ES):

**Electronic Records and Electronic Signatures:
Compliance Point of View**

Following are the sequential stages to achieve the compliance:

STAGE-A: EDUCATE TEAM

Educate project teams in the new company approach, ensuring an understanding of how compliance and benefits are to be achieved, and a commitment to resolve any non-compliance.

STAGE-B: DETERMINE WHETHER ER & ES REGULATIONS APPLY

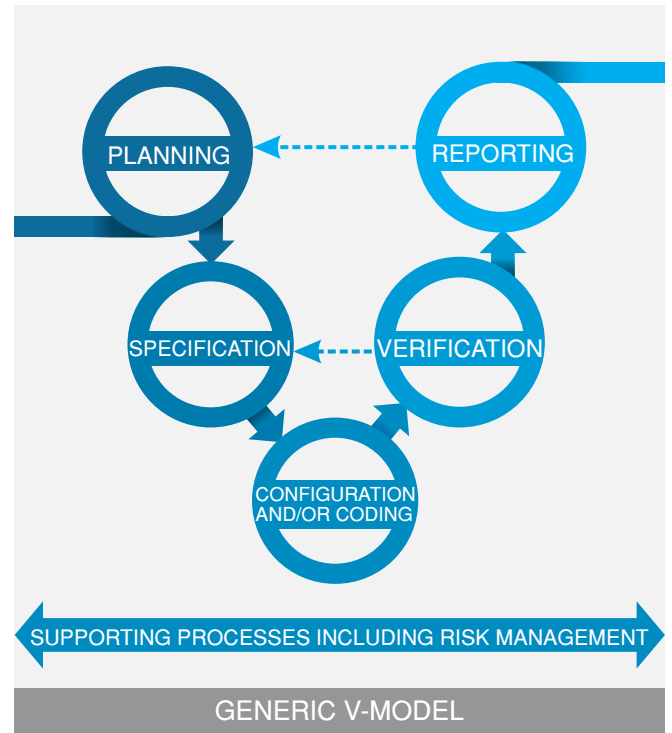
If they do apply, ensure the User Requirements Specification contains requirements for electronic records and signatures that meet current company policies and standards. An initial identification of which electronic records and signatures will exist within the system should be included in the URS.

STAGE-C: ASSESS SYSTEM

The assessment should consider:

- The business processes that create and update records
- The purpose of any electronic signatures which records are being signed
- Any data supporting the electronic records or signatures

Appropriate technological and procedural controls should be selected using GAMP standards.



STAGE-D: IMPLEMENT CONTROLS







- Document and justify decisions
- Update Validation Plan
- Create or update system specifications
- Apply technical and procedural controls
- Test technical controls and verify procedural controls
- Produce Validation Report

STAGE-E: MONITOR EFFECTIVENESS OF CONTROLS DURING OPERATION

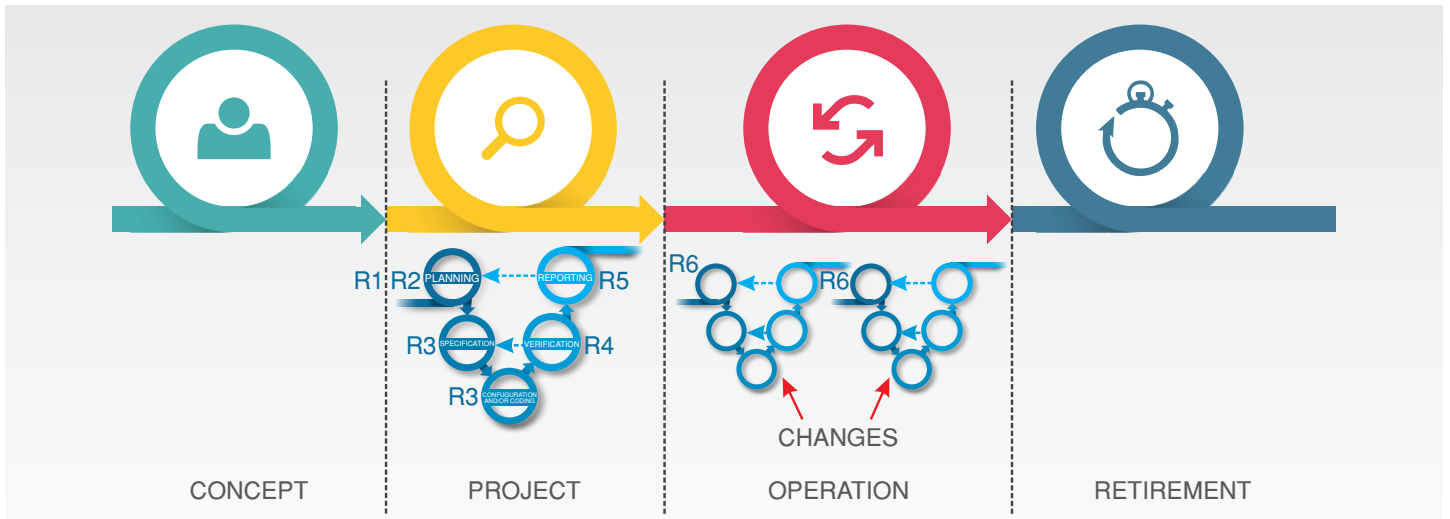
Procedural & Technical Controls

Procedural and technical controls available to reduce risks to an acceptable level include:

- Security management
- Backup and restore
- Disaster recovery and business continuity
- Change control

CATEGORY TYPE	TYPICAL EXAMPLES		
Category-1 Infrastructure Software			
Category-3 Non-Configured Software		Lab Software Micro - Controller	
Category-4 Configured Software			HMI SCADA SAP LIMS
Category-5 Customized Software	- Internally and Externally developed IT Applications & process control Applications - Spreadsheets-Macro		

*logos displayed are the properties of respective companies.



R1-Initial Risk Assessment, R2-Risk-based Decisions During Planning, R3-Functional Risk Assessments, R4-Risk-based Decisions During Test Planning, R5-Risk-based Decisions During Planning of Operational Activities, R6-Functional Risk Assessments In Change Control, R7-Risk-Based Decisions When Planning System Retirement

GENERIC LIFE CYCLE INCLUDING V-MODEL APPROACH



- Record copying controls
- Record retention controls
- Software controls
- Hardware controls
- Policies and procedures
- Training and experience

A combination of these controls may be necessary to adequately manage the risk. The selected measures should be implemented and documented.

- Validation
- AUDIT TRAIL

This shall include following types of controls:

- Type (automatic, manual, combination)
- Date and time stamped
- Identification of time zone
- Amount of information retained (who/what/when)
- Access control and security of the audit trail
- Retention of the audit trail
- Backup and restore of the audit trail
- Procedures for managing the audit trail
- Retention of previous versions of data
- Purpose: e.g., for auditing of planned authorized changes to data or for detecting unauthorized change (fraud attempts)

"Validation is not destination, it's continues journey to achieve high quality"

- Mr. Vivek Chanpura - GM- Project

FACTORY AUTOMATION

REGULATORY COMPLIANCE SERVICES

COMPUTER SYSTEM VALIDATION



HOW TO MAINTAIN THE DATA INTEGRITY ?



DATA INTEGRITY – ALCOA FACTORS

DATA INTEGRITY

Data Integrity refers to maintaining and assuring the accuracy and consistency of data over its entire life-cycle, and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data.

TESTING AS PER GAMP 5 GUIDELINES

To overcome the current issues related to audit/regulatory compliance Testing shall be done as per GAMP5 best practices.

As per GAMP 5, “Testing computerized systems is considered a fundamental verification activity. Appropriate testing is a regulatory expectation”

Also, as stated in EU Annex 11 [8]:
“Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered”

The understanding of both product and process assists in determining appropriate test scope and strategy. Traceability between requirements, identified risks and test cases is an important part of demonstrating this fitness for intended use.

Testing plays a vital role in the project, operational and retirement phases of a computerized system life cycle:

- During all phases, the main purpose of testing is to discover defects. Therefore, avoiding those defects

being present in the operational environment.

- Within the project phase, testing helps to demonstrate fitness for intended use by verifying the correct operation of GxP critical functions and effective implementation of controls identified during risk assessment.
- Within the operational phase, risk-based testing may be required following a system change to demonstrate that:
 - Any new functionality is correct
 - Remaining original functionality has not been adversely affected.
 - Required risk controls are still in place and effective

Within the retirement phase, testing of data migration and/or archive and retrieval methods may be required prior to decommissioning the system.

Testing is an area of the system life cycle in which these are potentially large efficiency gains to be made by the appropriate leveraging of supplier involvement; in particular through the:

- Avoidance of duplication in testing.
- Leveraging of supplier test activities and evidence to the maximum practical extent.

Testing of a system is a combination of:

- Testing conducted by the supplier during basic development of the standard product.
- Testing conducted by the supplier (or integrator) during application-specific development i.e. the development of a solution customized or configured to the customer’s business process.
- Testing conducted by the regulated organization

GENERAL OBSERVATION:

- | | | |
|----------|---|---|
| 1 | Calibration / Inspection
Checking not done | Routine calibration, inspection, checking of automatic, mechanical, electronic equipment is not performed according to a written program designed to assure proper performance. |
| 2 | Computer control of
master formula records | Appropriate controls are not exercised over computers or related systems to assure that change in master production and control records or other records are instituted only by authorized personnel. |
| 3 | Backup file not maintained | Failure to maintain a backup file of data entered into the computer or related system. |
| 4 | Input / Output verification | Input to and output from the computer related systems of formulas records or data are not checked for accuracy. |
| 5 | Written record not kept of
program and validation data | A written record of the program along with appropriate validation data has not been maintained in situations where backup data is eliminated by computerization or other automated processes. |
| 6 | Backup data not assured
as exact and complete | Backup data is not assured as exact complete secure from alteration, erasure or loss through keeping hard copy or alternate systems. |
| 7 | Written calibration /
inspection records not kept | Records of the calibration checks inspections of automatic, mechanical or electronic equipment, including computers or related systems are not maintained. |

Auditor's Perspective
Specific Observation
(Warning Letters)

Example-1

"Your firm failed to exercise appropriate controls over computer or related systems to assure that only authorized personnel institute changes in master production and control records, or other records (21 CFR 211.68(b))."

"Our investigator found that you have not validated 12 computerized systems in your quality control laboratory.

These systems are used for your stability chambers, ultraviolet (UV) and infrared (IR) spectrophotometer, and for thin layer chromatography (TLC)."

Example-2

"Your firm failed to exercise appropriate controls over computer or related systems to assure that only authorized personnel institute changes in master production and control records, or other records (21 CFR 211.68(b))."

"Your stand-alone computer systems lacked controls, such as routine audit trail review and full data retention, to prevent analysts from deleting data. Although you implemented a procedure to begin reviewing audit trails of your high performance liquid chromatography (HPLC) Empower system on January 11, 2016, you had not performed any reviews prior to our inspection."

