

Auditing Computerised Systems

Title: Auditing Computerised Systems					
Auditor Manual: 010					
Prepared by:		Date:		Supersedes:	
Checked by:		Date:		Date Issued:	
Approved by:		Date:		Review Date:	

Audit Training Manual: 010

Auditing Computerised Systems

Auditing Computerised Systems

It is intended to determine if the validation of the computerised system is adequate to satisfy regulatory and company expectations, and that the process is executed consistently and in accordance with established guidelines and procedures.

The audit also determines how computer systems are developed, maintained and used at the facility.

Computerised Systems Management

It is important to establish that computerised systems are managed appropriately within the GMP Facility. They should be covered by a quality management system. This may be the same as the rest of the facility or may be specific (and tailored) for the computerised systems.

Procedures and standards should exist addressing the areas listed below:

- System Development Lifecycle
- Functional Requirements
- Design Specifications Programming
- Testing
- Installation/Implementation
- Support/Maintenance
- Change Control/Configuration Management
- Backup and Restoration
- Business Continuity & Disaster Recovery
- Security
- Decommissioning
- Management of Deviations

It is important to determine the role of Quality Assurance in the management of computerised systems. Quality Assurance may be involved with every step of the validation process or limited to independent approval of the validation deliverables. It is possible that a separate IS Quality Management function (within the IS organization) carries out some or all of the QA activities.

Procedures should describe what level of approval is required for each validation deliverable. As a minimum, QA approval would be expected for Validation Plans, Requirements and Validation Reports and Change Control documentation. If deviations from procedure and standards occur, confirm that they are documented, evaluated and approved.

A systems inventory should exist which identifies all systems owned by the facility detailing the system owner and GMP impact. Any system with GMP impact that is currently operational should be validated. The IT infrastructure should also be identified.

GMP critical systems may include:

- Process Control Systems
 - SCADA
 - Autoclaves
- Environmental Monitoring Systems
- Laboratory Information Management System
- Manufacturing Execution Systems
- Document Management Systems
- Enterprise Resource Planning (ERP) Systems e.g. SAP

Auditing Computerised Systems

Requirements should be unique and prioritized. They should be written at a detailed level, precisely identifying acceptable criteria for success from a users' perspective.

Functional Specification

The Functional Specification (may be referred to as Design Specification) describes how the system is designed to achieve the Functional Requirements. This deliverable is a technical document that identifies the technical solution for the application, underlying software and the hardware necessary to support the system. There should be clear traceability between the requirements and the functional design. This may be achieved using a matrix, cross-referencing, common numbering or any other approach which makes it clear how each requirement is satisfied by the design. It is not necessary to include code or pseudo-code. Some development methodologies may require a formal approach e.g. UML Use Cases. Depending on the complexity of the system it may be appropriate to have a hierarchy of Functional or Design Specification with a high level design specification complemented by more detailed module specific design specifications.

System Programming.

Coding should comply with programming standards for screens, menus, code annotations, etc. Where possible industry standard coding standards should be used. Compliance with coding standards should be assessed through formal code review. A risk based approach can be applied to code review with code selected based on complexity, criticality or experience of the developer.

Defects found during code review should be logged with corrective and preventive actions as appropriate.

Procedures for maintaining and controlling multiple source code versions should be in place. In practice this is often achieved using commercial configuration management software e.g. CVS, Microsoft Visual SourceSafe or IBM Rational ClearQuest.

Where possible separate environments should be used for development and testing. These should be as similar as possible to the production environment for the system in order to assure the validity of system testing. The Development environment is used for developing and unit testing the software. The Test environment is used to test completed components and perform functional and integration testing. The final Production environment is where the application is placed for production roll out.

Test specification

The Test Specification describes the tests to be performed to ensure the system meets the user requirements. Test scripts should be written such that they can be re-executed and the same results can be obtained. Tests should test limit, failure and stress conditions as well as the successful execution of the required functionality. There should be traceability from the requirements, through the Functional Specification to the Test Specification. It should be possible to demonstrate that all required functionality has been adequately tested.

It is good practice for tests to be written by someone other than the developer and executed by another independent person.

Auditing Computerised Systems

Changes to the system may result from problems or changes in business process and system use. The impact of any proposed change on existing functionality should be assessed prior to approval. Testing done in support of a change should demonstrate that (a) the changed functionality works as expected and (b) there is no unexpected impact in related system functions.

On a periodic basis there should be a management review of the system to determine what needs to be done to maintain the validated state. Inputs to the management review may include:

- Amount of system change
- Common user problems
- Technical changes to the infrastructure supporting the system
- Continuing support for any commercially sourced parts of the system (hardware or software)
- Changes in system use
- Changes in business process supported by the system

The output recommendations of the management periodic review should be formally logged and actions tracked.

Where possible, the system should be maintained with current security patches for operating systems, database and application software in order to protect the process and data from unauthorized access and change (hacking)

Where the system can be accessed directly by the software supplier (by dial-in or internet) such access should be controlled so that any changes made are managed in the normal way.

Backup and Restore

In order to secure the system and its data backup and restoration requirements should be identified for all GMP impacted systems. The frequency with which back-ups are taken should be determined according to the criticality of the system. Backed up data should be secured and restore processes tested to ensure successful execution when required.

Business Continuity/Disaster Recovery

Loss of computerised systems can occur for a wide variety of reasons, varying from local equipment failure, network or software failure to site disasters. It is anticipated that most computerised system or infrastructure problems will be resolved quickly by existing support processes to minimize impact on system end users. A serious problem can, however, develop into a disaster if it is left unresolved.

The immediate period surrounding a disaster can result in confusion, chaos and significant interruption to routine business operation. The steps taken in the first hours of a crisis have a significant bearing on the ultimate severity and speed to resume normal business operations. The creation of structured plans will assist management by providing clearly defined responsibilities and actions. These procedures, together with some pre-disaster preparation, will ensure that the impact on the business of any disaster can be managed and minimized.

Auditing Computerised Systems

Data Migration

Data Migration is a one-time process of “moving” data from one system to another system. This can be due to a system upgrade or due to the replacement of an existing system with a new system. This is not an on going process between two systems.

The approach to data migration should consist of a migration plan, identification of the data being migrated, the actual process of migrating the data, and a migration verification process for determining that the migration process was accurate and successful.

Deviations from the Data Migration process should be document and resolved according to its criticality.

Key Parameters in Auditing a Computerised Systems at a GMP Facility

Prior to the audit

- Determine which GMP related products or services the facility provides.
- Determine which regulatory requirements apply.
- Request and review the systems inventory and descriptions to identify which computerised systems to focus on during the audit.
- Contact the Facility and notify them if computerised systems are likely to be included in the scope of the audit. This will enable them to make the relevant staff available.
- Request and review the Facility’s policy or procedure on Computerised System Validation (or equivalent)
- Consider whether an IS Compliance specialist should be included as part of the audit team.

During the Audit

The aim of the audit should be to determine that the computerised systems are developed/procured, implemented, operated and maintained in accordance with GMP principles. It is more important to confirm that the concepts are addressed than the terminology that is used.

- Confirm that a systems inventory identifies all systems owned by the facility and details the system owner and which have GMP impact.
 - Verify that any system with GMP impact, which is currently operational, is validated.
 - Check that there is a clear rationale for which systems have been validated and which haven’t.
- Ensure the review is focused on the system(s) most critical to the component, process or task(s) that the facility performs.
- Determine whether the validation approach chosen is based on categorization of the system. GAMP categorization may be used.
 - Verify that the choice of category is justified
- Confirm that the Facility’s employees understand that their electronic signatures are the equivalent of the hand written signature.

Auditing Computerised Systems

- Confirm that design specification were approved prior to coding commencing.
- Confirm that coding standards exist. If the facility is using industry standard software (e.g. Java, Delphi, .net etc) determine whether industry standard coding standards are used. If not, clarify why not.
- Confirm that code reviews are carried out.
- Determine whether all code is reviewed or a sample. If a sample is used determine how the sample was selected.
- Ensure source code reviewers are independent and suitably qualified.
- Confirm that defects found during code reviews are corrected, tracked and trended.
- Ensure preventative actions are in place to prevent recurrence.

Testing

- Review the testing documentation associated with the system to audit.
- Establish that a test strategy explains the testing done at each stage of development, e.g. module testing, integration testing, interface testing and acceptance testing.
- Confirm through the testing process that the critical functional requirements have been tested.
- Confirm that testing covers limit, failure and stress conditions as well as tests designed to confirm that the system works as expected. Also, ensure that any logical access security controls have been included in the test regime.
- Establish that testing is carried out by people who are independent (of both the developer and test author) and suitably qualified.
- Confirm that test scripts are written so that they will provide the same results if re-executed.
- Confirm that expected results have been clearly identified and that the results obtained have been documented with sufficient evidence to demonstrate success. Verify that deviations from test steps or expected results have been documented.
- Establish that test failures have been evaluated for risk according to the criticality of the functional requirement.
- Establish that where a test has failed the required functionality it is not critical to either the supported process or GMP compliance. Confirm that a suitable procedural workaround exists.
- If automated testing tools are used, establish that:
 - they have been tested/qualified to ensure their proper operation.
 - procedures are available that identify how the tools are to be used.
 - script approval signatures are captured.
 - changes to the tools or electronic scripts are controlled and approved.

Release

- Determine how the system is released for use.
- Evaluate the controls and checks to ensure that all required activities are completed.
- Ensure that roles and responsibilities for release are clear and have been complied with.
- Ensure that all required deliverables were part of the release package. These may include:
 - a confirmed build of the code