

Preparation for the Audit – IT Best Practices

Information Technology (IT) audits are often viewed as difficult and inconvenient. In reality, an audit is a great opportunity for “free” consulting advice regarding the effectiveness of an organisation’s systems, processes, procedures, documentation and controls. This article will provide an overview of IT best practices, and give a step-by-step approach to hosting a successful external IT audit.

By Diane E. Krueger & Earl W. Hulihan

Key Words: IT Audit, FDA, MHRA, Introductory Meeting, Information Gathering and Analysis, Close Out Meeting, Reporting and Follow –up, Regulatory Requirements, GxP, 21 CFR part 11, ALCOA, CAPA, Scope and Objectives, SOP, Training, Internal Audits, External Audits.



In most cases, the scope of an external audit will include a review of systems, procedures, documentation and controls applicable to system development, testing, infrastructure installation and maintenance, general network administration practices, including change control, user account administration, disaster recovery and business continuity.

Audit Process Overview

Most focused IT audits are either conducted by an internal resource, such as the Quality Assurance department or by an external resource, such as a potential or existing customer.

In addition to IT focused audits, the IT department may be asked to contribute to a broad based audit. For example, during a Pharmacovigilance audit, IT would be a component of a more systematic review of processes.

Most audits are conducted in the same fashion regardless of the type of audit. The audit is usually broken down into the following components:

- Request for information
- Introductory or opening meeting
- Information gathering and analysis
- Close-out meeting
- Reporting and follow-up

Request for Information

Prior to the on-site audit, the auditor may submit a request for documentation. Documentation requests may include an

index of Standard Operating Procedures (SOPs) and policies or a completed audit questionnaire.

In some regulatory environments and depending on the type of audit, a completed questionnaire is required. For example, the Medicines and Healthcare products Regulatory Agency (MHRA-UK) requires the completion of a Summary of Pharmacovigilance Systems (SPS) prior to the inspection.

Where appropriate, the Quality Assurance department should be involved with the response to the auditor’s request for documentation.

Introductory Meeting

An on-site audit typically commences with an introductory or opening meeting. The main purpose of the meeting is to introduce the audit participants, review the purpose, scope, and objectives of the audit, as well as confirm the availability of resources, facilities, and documentation required during the audit.

Information Gathering and Analysis

Information gathering and analysis consists of the auditor collecting sufficient information to fulfil the audit objectives through the direct access to documents, interviews, and observations of activities in the areas under review.

Close Out Meeting

At the conclusion of the audit, a close out meeting is typically held. The main purpose of this meeting is for the auditor(s) to summarise the events of the audit and present preliminary observations of non-conformance. The meeting also provides an opportunity to discuss any misunderstandings that may have arisen during the course of the audit.

For planning and scheduling purposes, it is recommended that during the close-out meeting, the auditee inquire about the expected delivery of the formal report. The audit is not over when the auditors leave the site.

Reporting and Follow-up

The specific details regarding the report and follow-up phase of an audit vary. However, the overall approach is consistent. The formal report summarises the events of the audit

including the findings identified during the audit. In most cases, the auditor will submit a request for corrective action along with the formal report.

The request for corrective action typically requires a formal response for each finding and a target date of completion. If not stated in internal procedures, the suggested time period to respond to an auditor's request for corrective action is between two weeks and thirty (30) days.

Auditee upper management and/or Quality Assurance is responsible for developing and implementing a corrective action plan. During the development of the corrective action plan, most auditors require two improvement activity responses for each finding; short term (temporary) and long term (permanent). This two-step improvement approach is often desirable, but not required.

The formal corrective action response with target dates of completion is submitted to the auditor for review. Typically, the auditor will verify whether the corrective action plan will adequately address the finding(s). The auditor(s) will follow-up with the auditee until all corrective action plans have been implemented. Follow-up activities may include a follow-up visit to verify that the findings have been adequately addressed and the corrective action plans have been implemented.

Preparation for an Audit

Being prepared for an IT Audit is more than half the battle. Preparation is essential and is required at all levels of the organisation. As John Wooden, former Head Basketball Coach of UCLA, once said, "you can't have poise and confidence unless you've prepared correctly." His philosophy on preparedness was unmistakable:

"Remember that failing to prepare is preparing to fail. Every (building) block is built on the others. When all are in place, poise and confidence result. You don't force them to happen. They happen naturally from proper preparation."^[1]

In keeping with this creed, preparation begins before the auditor arrives at the facility on the day of the audit. For example, preparation of personnel in knowing what is expected of them (compliance to job description), knowledge of the job before them, understanding of expectation (working knowledge of policies, procedures and work instructions), and documentation (is there *demonstration through documentation*^[2] that is current, complete and correct which demonstrates that systems, processes and performances occur as expected?).

It should be noted that in some cases, "directed audits" or "for cause" audits may be conducted by regulatory or government agencies. Directed audits are conducted in the same manner as a routine audit; the only difference is that a directed audit is initiated because there is credible evidence of a significant violation or there are credible questions concerning subject safety, product quality and/or data integrity. By their nature, there is typically little time to prepare for this type of audit. Given that directed audits can occur with little or no advanced notice, it is important that the IT department be prepared at all times.

In reviewing completed documentation, the ALCOA rule^[3] should apply. In other words, is all data/ documentation: **A**tttributable to an individual, **L**egible, **C**ontemporaneous (created at the time of the activity), **O**riginal (clearly distinguishable between the original and a facsimile), and **A**ccurate? Often personnel in their normal day-to-day IT



operations complete checklists or write up **C**orrective **A**ction and **P**reventative **A**ction (CAPA) reports. It is essential for staff to follow the ALCOA rule in documentation. Staff must be trained and understand that the documentation they create now may answer a question 10 to 15 years later – or longer.

In-depth Understanding of the Applicable Regulatory Requirements, Guidance, and Industry Best Practices

An in-depth understanding of the applicable regulatory requirements, guidance, and industry best practices is an essential element in preparation for an audit.

For example, in the US, if the audited organisation provides a data management solution, such as an electronic data capture (EDC) system for collecting clinical research data to be submitted to the US Food and Drug Administration (FDA), the computerised system falls under the scope of the electronic records/electronic signature [ER/ES] rules - 21 CFR Part 11 and applicable GxP^[4] regulations. It is important for an organization to understand the applicable local, national, and international regulations, guidance, and industry best practices associated with the use for the IT systems under care. The range of regulations, guidance, and industry best practices necessary for measurement and compilation span from GxP's, ER/ES, and Data Protection.^{[5] [6]} In addition to the principle standards associated with healthcare industries noted, increasingly IT departments are involved with audits directed at systems with financial impact due to financial regulations (e.g. Sarbanes Oxley^[7], EROS Project^[8]).

From personal experience, frequently we will observe staff sitting across from us at the audit table not being able to

speak about or discuss the 10-15 procedures they are required to learn and work with on a daily basis. The failure of IT professionals to understand and have a working knowledge of their own SOPs is a common theme found during IT audits. Staff must commit themselves to this working knowledge. IT professionals do not realize their daily actions may affect the lives of others. Simple activities such as selecting an SOP for review during the weekly staff meeting can alleviate this issue and remove it from a negative observation at the audit table. We have also seen IT departments use activities such as a jeopardy game for IT, which makes learning and reinforcement fun and rewarding.

Understanding the Scope and Objectives of the Audit

In addition to knowing the applicable regulatory requirements and industry standards, an equally essential component in the preparation for an IT audit is to understand the scope and objectives of the audit. IT professionals need to be prepared to present information and supporting documentation so that the auditor can meet audit objectives.

An audit notification letter, audit plan, and/or proposed agenda should be submitted to the audited organization prior to the commencement of the audit. The notification letter or audit plan should describe in detail the scope and objectives, the topic areas, and associated documentation to be reviewed during the audit. If this is not the case, the audited organisation should request a written description of the auditor's intentions.

The auditee should carefully review the scope and objectives of the audit. In the event that the topic areas and associated documentation to be reviewed during the audit are not relevant to the scope and objectives, the auditee should discuss these discrepancies with the auditor(s) and come to an agreement prior to the commencement of the audit.

Logistics

To ensure the audit is conducted efficiently, the audited organisation should have the following arrangements in place:

- An escort should be identified to meet the auditor(s) upon arrival. The escort should be available to host the auditor(s) for the duration of the audit. Auditor(s) should not be left alone and should not be permitted to walk freely throughout the organisation. Auditors should also be reminded of facility rules. Rules for an auditor may involve the use of recording devices and/or cameras.
- Availability of management for the opening and closing meeting.
- Availability of personnel who have key roles in relation to areas under review.
- A conference room where the auditor(s) can meet. The room should be in close proximity to the entrance of the facility and should be separate from any locations where auditors would have access to key sensitive areas of the facility. This location serves as the "home base" for the duration of the audit.
- Note: In critical Regulatory audits, our industry makes efficient use of the war room concept. The **war room** is an ancillary room in close proximity to the audit conference room, which allows the review of **all** documents being provided to and received back from the

auditors. By review of questions posed by auditors and consideration of documents reviewed as well as anticipation of audit trends, potential issues become proactive and allow anticipation for future areas of examination/failures.

Audit Training

IT professionals need to be trained to perform their day-to-day job functions, and it is equally important to train IT personnel in the area of hosting an IT audit. One wrong "move" can negatively affect the outcome of the audit and ultimately influence future relations with the prospective customer.

Instead of one-on-one training, a more effective approach to teaching the fundamental principles of hosting an audit is formal training session in a classroom setting. A "mock" audit is an extremely valuable method for preparing IT professionals. Training should include the following:

- Arrival of the auditor(s)
- Documenting the audit
- Audit conduct
- Responding to audit findings

As previously stated, an escort should be assigned to the audit. Typically, the escort is a member of the Quality Assurance group or Legal department and is considered the main point of contact between the auditor(s) and the organisations' audit participants. The escort should be well versed in the applicable regulatory requirements and industry standards appropriate for the audit scope, and it is recommended the escort have experience on both sides of the audit table. The ideal candidate is someone with experience hosting and conducting audits. Most importantly, the escort keeps management informed of the progress of the audit and conveys any areas of concern to management.

The audit escort should meet the auditor(s) at the reception area and request proper identification. Auditors should sign in and be escorted to the appropriate reserved conference room. An e-mail should be distributed to personnel at the facility to inform the staff an audit is in progress. In addition to escorting the auditor(s) to the conference room, the assigned escort should remain with the auditor(s) at all times and document the key activities of audit. Documenting the audit ensures there is a record of personnel interviewed during the audit, documents requested and reviewed by the auditor(s), and any concerns and/or questions raised.

Audit participants should be trained in proper audit conduct and etiquette. At all times the participants should be professional, respectful, and truthful.





When responding to an auditor(s), audit participants should be aware of the following:

- It is extremely important to answer only the questions posed by the auditor. Often the participant's instinct is to elaborate on additional work the IT group is conducting; however, this is not recommended. Participants should also avoid expressing frustrations within the IT organisation by stating and/or revealing problems associated with personnel, compliance to procedures and shortcuts the IT group is taking to get the job done. Before an audit, it is important to have opportunities for the staff to practice answering questions similar to ones they would receive during an audit. The staff must learn to provide an adequate and accurate answer to questions without travelling into murky waters or inadvertently misdirecting.
- If unsure of an answer in an audit, the proper response from the audit participant is to inform the auditor(s) that he or she is not sure or that the question or topic area is outside the scope of responsibility – whichever is appropriate. The participant should let the auditor(s) know that he will either get the answer to their question, or bring in the individual responsible for the topic area.
- Before answering any questions, be sure to understand the question. If a question raised by the auditor is unclear or ambiguous, simply ask for clarification. Do not make any guesses regarding the question at hand.
- Be respectful and professional at all times. Under no circumstances should a participant lose his cool. There are auditors, although rare, who may be condescending and/or antagonistic. The participant should remain calm and answer the questions to the best of his ability. This is a situation where the escort may be required to jump in and facilitate the conversation.
- All questions raised must be answered truthfully. It is never a good idea to stretch the truth or to be misleading in any way.
- If there is a topic area where the participant anticipates a finding, be sure to inform the auditor the awareness of the situation, and briefly explain the plan to correct the situation. In many cases and depending on the severity of the issue, the auditor(s) may accept the approach of correcting the situation and of not reporting the observation as a finding. The observation may be noted as a follow-up item instead.
- It is important for the escort to be cognisant of the discussions between the audit participants and the auditor(s). One of the roles of the escort is to assist the audit participant during these discussions. The escort should let the participant answer the questions; however, the escort can comment on the responses provided by the audit participant to give additional clarification.
- Do not take anything an auditor says personally. The audit is about an organisation's compliance to applicable regulations, internal procedures, industry standards and adequacy of systems, processes and procedures.
- It is important to defend systems and processes; however, one should not become overly defensive and/or argue with the auditor(s). Remember there will be an opportunity to defend an audit finding during the response phase. In practically all cases, the auditor(s) will issue a formal audit report and require a formal written response to all audit findings. This provides an appropriate opportunity to challenge or defend an audit finding.
- Be wary of an auditor who may veer off topic and request information not associated with the scope and objectives of an audit. If this situation should occur, it is the responsibility of the escort to bring the auditor back on track.
- "Unreasonable" requests for information, which may include financial, sensitive and/or intellectual property, may be handled by a 3rd party review. For example, in the event an auditor requests sensitive network security details, it may be necessary to involve a 3rd party to review sensitive information on behalf of the auditor.
- An auditee has the right not to disclose requested information that is deemed proprietary, sensitive and/or highly confidential. It is recommended that the legal and Quality Assurance departments be involved with decisions associated with the disclosure of this information.
- Lastly, the best attitude for each audit participant to possess is a positive one. Look to the upcoming audit as an opportunity for process improvement and do not look at the external audit as "someone coming into your organisation to beat you up." Most auditors strive for a positive win-win situation.

Conduct Regular Internal Audits

Conducting regular internal audits is another great way to prepare for an external audit. An internal audit is designed to measure the organisation's compliance to applicable regulations, as well as its performance, strengths, and weaknesses against its internally established procedures and systems. An important element of an internal audit is that the auditors must have no vested interest in the results of the

audit. The auditor(s) must be independent of and separate from the area being audited. Findings identified during an internal audit should be reported to management so management is aware of the organisation's weaknesses. Appropriate steps should be taken to address internal audit findings. In many cases, the findings identified internally are also identified during an external audit.

It may be beneficial to hire external resource(s) to assist with the conduct of an internal audit, where appropriate. For example, during an internal audit with an objective to assess the organizations network security mechanisms, it may be useful to hire an external resource to perform penetration testing of the network. This is especially important when internal resources do not have the expertise required to assess the strengths and weaknesses of a particular system.

Common Topic Areas of Interest and Expectations of the External Auditor

What will the auditor expect to review during the IT audit process? The bottom line for an auditor is to determine if IT systems and processes are compliant with applicable local, national, and international regulatory requirements, guidance and industry standards. Questions and expectations may include the following:

- Is there a documented and approved disaster recovery plan on file? Has it been tested to ensure reliability?
- How are assets, including data, safeguarded?
- Is there a formal ongoing security awareness and training program to promote computer and network security?
- Has the computerised system been developed in a manner consistent with applicable regulatory requirements, guidance, and industry standards?
- Do personnel have the requisite training, education and experience to perform their job function and is the training documented? Does training include appropriate technical and regulatory training?

Diane E. Krueger

Regulatory Compliance Consultant
META Solutions, Inc.
37 Mountain Boulevard
Suite One
Warren, NJ 07059
860.536.3711 (Office)
860.857.9061 (Cell)
diane.krueger@metasol.com

Diane Krueger is a
Regulatory Compliance
Consultant at META Solutions



Earl W. Hulihan

Vice President
Global Regulatory Affairs
and Quality Assurance
Medidata Solutions, Inc.
79 Fifth Avenue, Eighth Floor,
New York, NY 10003
1.610.393.1109 (Cell)
1.610.588.6091 (PA Office)
1.212.918.1800 (NY Office)
Email: ehulihan@mdsol.com
Medidata web site:
www.mdsol.com

Earl Hulihan is Vice President of Global Regulatory Affairs and Quality Assurance at Medidata Solutions. He is also the chair of the DIA Validation Advisory Committee.



- What is management's involvement with IT operations? Is there adequate oversight?
- Are the Quality Assurance and Quality Control functions built into IT processes?
- Are all changes to the IT environment and systems governed by change control?

The auditor(s) will expect to review written procedures and documentation to demonstrate compliance to the procedures. This may include a review of key logs such as backup and restore logs, disaster recovery plans and results of disaster recovery testing, computerised system validation documentation (including actual results), and evidence that security elements have been tested and deemed adequate.

It would be impossible to provide a comprehensive list of the questions and expectations of an external auditor. If an auditor does not provide a notification letter to include the scope and the expectations, it is strongly recommended that one be requested.

Pulling it all Together

To stay ahead, IT professionals, in conjunction with the Quality Assurance department, should stay abreast of applicable local and national regulatory activities. Understanding industry expectations will help to ensure that an auditor presents no surprises during an audit.

Being prepared, while time consuming, is the most important aspect of an IT audit. Hiring a strong technical team, along with regulatory support and guidance from the Quality Assurance department, will help to ensure the successful outcome of an external audit. In addition to preparation and teamwork, it is important to consider experiences from previous audits.

Hosting an audit is a positive learning opportunity. The audit experience should offer an opportunity to improve internal processes and ultimately provide experience and lessons learned for the next audit. ■

References:

- ¹ From John R. Wooden, Pyramid of Success
- ² Commonly referred to as a 'Hulihanism' phrase
- ³ From the US FDA Compliance Program Guidance Manual
- ⁴ GXP is an all-inclusive reference to 'Good Clinical Practices, Good Laboratory Practices and Good Manufacturing Practices';
- ⁵ Reference is made to locally adopted GXP Regulations such as US 21 CFR 312, US Safe Harbor and Japan GPSP; Guidance examples such as ICH E6, OECD GLP and EU Directives on Clinical Trials and Data Protection are relevant where adopted locally; Industry Best Practice examples include ACDM/PSI Computer Systems Validation in Clinical Research Guide, [V.2, 2004] as well as IEEE, GAMP, PIC/S.
- ⁶ A good site for 'Data Protection information' is: <http://www.privereal.org/> [PRIVIREAL is a EUROPEAN COMMISSION Framework 5 funded project examining the implementation of the Data Protection Directive 95/46/EC in relation to medical research and the role of ethics committees.]
- ⁷ <http://www.sarbanes-oxley.com>
- ⁸ <http://www.pro.gov.uk>