International Organization for Standardization

International Accreditation Forum

Date: 13 January 2016

ISO 9001 Auditing Practices Group Guidance on:

Electronic Documented Information Systems

1. Introduction

The growing dependency of organizations on electronic media for the operation and control of their management systems requires certification/ registration bodies and their auditors to look at new approaches to ensuring that audits will be effective and efficient. They will need to redefine the way processes and documented information are evaluated to verify conformance with the audit criteria.

This paper has been developed to give general guidelines for the conduct of audits of management systems that are either fully electronic-based or have a high degree of documented information in electronic media. It also provides guidelines for certification / registration bodies and auditors to consider as a complement to the normal planning and preparation activities that should occur prior to an audit.

This paper focuses on auditing those requirements of ISO 9001 where there is the possibility of use of electronic media for documented information.

This paper is intended for management system auditors who have a broad and varied range of practical experience with regard to the use of electronic media for the operation and control of management systems– i.e. management systems that are dependent on electronic media and software applications for their normal operation. However, it is written in a style that will also allow it to be used by those who only have limited experience of computers and electronic media.

Whether it is a third-party certification body, accreditation body or internal audit function, the organization carrying out the audit ("the auditing organization") is responsible for ensuring the effectiveness of the audit process for the electronic documented information system. This paper utilizes the guidance provided in ISO 19011, and suggests approaches that may be utilized by auditors of ISO 9001, and other management system standards, in order to verify conformance to the referenced standard. Auditors and auditing organizations should make the adjustments necessary to ensure a suitable approach as they perform the audit process steps indicated in ISO 19011.

It should be noted that proficiency in the auditing of electronic documented information should not be viewed as an excuse to reduce audit durations, but as a means of optimizing the effectiveness and efficiency of the audit.

It is not the intention of this paper to provide guidelines for auditing controls associated with information security. Those interested in further controls associated with information security are directed to ISO/IEC 27001 which is a comprehensive standard for these matters.

2. Audit Initiation and Planning

During the audit initiation phase (i.e. the 1st stage audit - see the ISO 9001 Auditing Practices Group paper on “The need for a 2 stage approach to auditing”) the auditing organization should determine the structure of the organization to be audited, and the degree to which its management system uses electronic documented information. A multi-site organization with a centralized process for controlling its electronic documented information, or a "virtual" organization, will require different auditing plans and methods

The auditing organization and the auditee should agree on how the auditors will access and use the electronic documented information system. This may involve consideration of:

- Allowing the members of the audit team an opportunity to familiarize themselves with the auditee’s electronic documented information system (including the scheduling of sufficient time within the audit plan for such an orientation)
- The auditee’s policies for the use of its Information Technology infrastructure
- Instructions for accessing, and the necessary security clearances to access, pertinent organizational documents and records
- Safeguards and processes to ensure that the auditors protect the confidentiality of electronic documented information during, and subsequent to, the audit.

The auditing organization should ensure that there is sufficient competence within its selected audit team to carryout an effective assessment of the electronic documented information system.

3. Review of Documented Information

Depending on whether or not the auditee has the ability to make its information available through a web-based application or through e-mail transmission, the auditing organization may conduct part or all of the documented information review off-site; either on-line or by downloading electronic information submitted by e-mail.

Depending on technical and security factors, it may be not be feasible to conduct a full review of an organization’s electronic documented information system on-line or via e-mail transmission of relevant information, prior to arriving on site. In such instances, audit preparation activities requiring a review of electronic information would need to occur at the facilities of the auditee during the Stage 1 audit.

4. On-Site Operation Activities

The audit approach for electronic documented information systems will depend largely upon how much of the evidence required for determining conformance is in the form of electronic information.

During on-site activities, the auditor’s trail should typically include the physical location of the process being audited. However, with an electronic documented information system the time needed to confirm the evidence for determining whether or not requirements are being met, may be dedicated at a computer workstation, which might not be located near the actual process.

When the computer workstations are in remote areas that are not accessible at the location of the physical process, the actual auditing time at the physical location of the process may be reduced. However, the overall assessment time may not necessarily need to be reduced, given that an electronic evidence review may occur before and/or after confirming the existence of the physical process.

In the case where the associated computer workstation is remotely placed, special consideration should be given to the time required for traveling to and from the physical location of the process.

When the process is dependent on human intervention, the auditor should evaluate the methods employed for interaction between the physical process and electronic media to ensure the accuracy of the associated information.

5. Auditing the Control of Electronic Documented Information

Electronic information that establish operational control of the management system can be in a variety of file formats depending on the software applications that are utilized by the organization to generate the information. Electronic file formats include, text, HTML, PDF, etc. Spreadsheets and databases formats are also considered to be electronic documented information subject to the control elements of the management system to being audited.

Given the relative ease with which users can now create electronic spreadsheets and other electronic information, auditors should ensure that processes governing the controls that apply to management system hard-copy information in-general are also employed for electronic information.

Organizations need to employ suitable and effective methods within the electronic environment for ensuring the adequate review, approval, publication and distribution of its management system documentation. These should be consistent with the methods for the development and modification of electronic information.

In many cases control measures may also be standard features of software applications used for their creation. Therefore auditors should understand these application-specific controls to the degree that these are utilized as a basis for conformance to the applicable management system standard.

Given the increased capacity to modify, update, reformat and otherwise improve documented information within an electronic documented information system, auditors should pay particular attention to control elements such as identification and revision level.

As electronic media facilitates an increased rate of modifications, auditors should verify that the controls being employed for the management of obsolete information are considered within the organizations' control processes.

Auditors should verify that information exists to provide orientation to users with regard to the functional and control aspects associated with electronic information. Additionally, "Point-of-use" requirements associated with the applicable management system standards will typically be addressed in part by the organization's access policies. Auditors should understand the organization's processes regarding user privileges as these become important factors for properly implementing the organization's processes.

External electronic communication with external providers, customers and other interested parties may involve the exchange of documented information. Given that the documented information may contain key parameters that specify the functioning of the organization's processes, auditors should verify the degree to which these are formally introduced and controlled within the electronic documented information system.

Auditors should review the methods employed by the organization for capturing output, in order to ensure that activities provide sufficient confidence in the accuracy of the information.

When evaluating the organization's controls with regard to retention and storage of documented information, auditors should verify if organizations have an understanding of their storage capacity versus:

- the rate of information generation,
- retention timeframes,
- the rate of record disposal,

as these factors may impact the proper functioning of the electronic documented information system..

Given that the knowledge-base and the performance of the organization may be almost entirely in electronic records, Auditors should review the organizations approaches for securing the information contained in electronic means. For more information on Information Security see ISO/IEC 27001.

6. Resources

As organizations migrate to using an electronic documented information system, the I.T. function's role becomes vital. Auditors should verify if the organization has dedicated appropriate I.T. resources (including infrastructure) to ensure that the system operates continually and effectively.

Auditors should also verify if the organization has appropriately defined the level of interaction, support and involvement of I.T. personnel in matters associated with the establishment, implementation and maintenance of the electronic documented information system.

As part of the verification of assignment of appropriate resources, auditors should evaluate how the organization addresses the competence required of persons to operate hardware and software to run the electronic documented information system..

During establishment of an electronic documented information system, it is customary that parallel (hardcopy and electronic) systems are in-place for a period of time to allow users to adapt. In these cases the auditor should verify the organization's approaches for ensuring that the system is actually being assimilated and utilized.

The complexity of an organization's IT infrastructures will vary, depending on the nature and complexity of its business. Auditors should verify an organization's system maintenance processes for its IT platform. Also, auditors should verify how the organization addresses system downtime incidents, as these will impact the normal functioning of the electronic documented information system. Auditors should evaluate whether or not the organization has formal backup systems, and whether or not these are periodically reviewed and tested for adequacy.

In relation to software, the auditors should verify the controls established for internal software, external software, software licensing, and software updates. Since software can be considered to be dynamic, the guidelines provided above for the auditing of electronic information would also be applicable to it.

To the extent that the organizations uses software for its electronic documented information system, auditors should review the functionality of the applications and their relationship to management system elements defined in the applicable criteria.

As environmental factors may impact the functioning of an IT platform, organizations should take measures to protect them against such factors. This may range from the need for adequate facilities or housings through to the need for uninterruptible power supplies (UPS). Auditors should evaluate if the organization's controls take into account aspects such as facility maintenance, temperature, humidity, etc, to the extent that these bear upon the operation of the electronic documented information system.

7. Internal and External Electronic Communication

As the options available for, and ease of use of electronic communication increases, organizations should put the necessary controls in place to ensure consistency in their use and for satisfying the requirements of their electronic documented information system and the applicable management system standard.

When intranets, email, and instant messaging are utilized for satisfying the requirements of the electronic documented information system, auditors should verify that processes address the circumstances under which these means would be employed. Additionally, if the results of internal electronic communication are to be used to satisfy the audit criteria, then auditors should verify that processes for the control of electronic information are being applied.

When the organization relies on its I.T. infrastructure for electronic communications with its customers (e.g. for e-commerce), external providers (e-procurement), external sites and other interested parties, the auditor should verify that the methodology and processes for these communications and associated transactions are formally addressed.

8. Multi-Site Management Systems

Organizations that operate through multiple sites (or from a central location to satellite sites) usually maintain communications and share process and process outputs with their various locations via electronic means, such as the internet, extranets, e-mail and instant messaging.

.

When the I.T. platform and its associated software applications are used to share information that is pertinent to the audit criteria, auditors should understand the different networking means employed by the organization to the extent that it is necessary for ascertaining if the electronic documented information system meets the audit criteria.

Auditors should verify whether the controls over a multi-site management system are appropriately addressed and established within the organization's processes.

9. Auditor Competence

The reliability of the audit process for electronic documented information will depend on the ability of auditors to understand the trends in I.T. as organizations rely increasingly on software for monitoring and controlling their operations.

Auditing organizations should take the necessary measures, including the provision of training, to address the general and individual needs of their auditor base with regard to:

- General trends in I.T. that may impact the operation of management systems

- Audit-specific considerations for each audit assignment that is undertaken

As the innovations in the I.T. sector are relatively rapid as compared to changes in audit criteria, auditors and auditing organizations are challenged with the need to have a practical understanding of the associated trends and how they may be applicable and utilized within an electronic documented information system.

In light of the innovations that influence the functioning of an electronic documented information system, auditing organizations should determine if the experience needed in order to be effective for a given audit is possessed by the audit team itself or whether the assistance of a technical expert would required.

For further information on the ISO 9001 Auditing Practices Group, please refer to the paper: *Introduction to the ISO 9001 Auditing Practices Group*

Feedback from users will be used by the *ISO 9001 Auditing Practices Group* to determine whether additional guidance documents should be developed, or if these current ones should be revised.

Comments on the papers or presentations can be sent to the following email address: charles.corrie@bsigroup.com .

The other ISO 9001 Auditing Practices Group papers and presentations may be downloaded from the web sites:

www.iaf.nu
www.iso.org/tc176/ISO9001AuditingPracticesGroup

Disclaimer

This paper has not been subject to an endorsement process by the International Organization for Standardization (ISO), ISO Technical Committee 176, or the International Accreditation Forum (IAF).

The information contained within it is available for educational and communication purposes. The *ISO 9001 Auditing Practices Group* does not take responsibility for any errors, omissions or other liabilities that may arise from the provision or subsequent use of such information.