

Auditing Electronic-Based Management Systems (EBMS)

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 related documents (including records) are evaluated to verify conformance with the audit criteria.

This paper has been developed to give general guidelines for the realization of audits of management systems that are either fully electronic-based or have a high degree of documentation 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 those requirements of ISO 9001 where there is the possibility of use of electronic documents, records etc., and also where access to such documents/records may be controlled by electronic systems.

This paper is intended for management system auditors who have a broad and varied range of practical experience with regard to electronic-based management systems (EBMS) – i.e. management systems that are dependent on electronic documents, data 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 EBMS.

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 EBMS. 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 EBMS 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 for EBMS. Those interested in further controls associated with information security are directed to ISO/IEC 17799 which is a comprehensive standard for these matters.

Audit Initiation and Planning

During the audit initiation phase (the Stage 1 audit) the auditing organization should determine the structure of the organization to be audited, and the degree to which its management system is electronically-based. A multi-site organization with a centralized EBMS, or a "virtual" organization, will require different auditing plans and methods to a single site and/or physical organization.

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

- Allowing the members of the audit team an opportunity to familiarize themselves with the auditee's EBMS (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 documents and records during, and subsequent to, the audit.

The auditing organization should ensure that there is sufficient competence within its selected audit team to carry out an effective assessment of the EBMS.

Document Review

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

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

On-Site Realization Activities

The audit approach for electronic-based management systems will depend largely upon how much of the evidence required for determining conformance is in the form of electronic records.

During on-site realization activities, the auditor's trail should typically include the physical location of the process being audited. However, with an EBMS the time needed to confirm the evidence for determining whether or not requirements are being met, may be dedicated at a computer workstation which may or 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 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.

Auditing the Control of Electronic Documents

Electronic documents that establish management system policies and procedures can be in a variety of file formats depending on the software applications that are utilized by the organization to generate the documents. Electronic file formats include, Text, HTML, PDF, etc. Spreadsheets and databases formats are also considered to be electronic "documents" 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 documents, auditors should ensure that policies governing the controls that apply to management system documentation in-general are also employed for electronic documents through appropriate procedures.

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 documents.

In many cases document 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 documents within an electronic-based management system, auditors should pay particular attention to control elements such as document identification and document revision level.

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

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

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

Auditing the Control of Electronic Records

Electronic records consist of the process output data combined with the electronic formats that house the data. These electronic formats range from simple spreadsheet documents to more complex database applications.

Auditors should be aware that the control elements that organizations establish for electronic forms are not necessarily the same as that which apply to electronic records. For example, with respect to "Identification", in the case of electronic forms, the term refers to the nomenclature of the electronic form itself. When

“Identification” is considered in the case of an electronic record, this refers to the unique use of the electronic form for a given data set.

Auditors should review the methods employed by the organization for capturing data, in order to ensure that data entry activities provide sufficient confidence in their accuracy.

When evaluating the organizations controls with regard to storage of records, auditors should verify if organizations have an understanding of their storage capacity versus:

- the rate of record generation,
- record retention policies and associated timeframes,
- the rate of record disposal,

as these factors may impact the proper functioning of the EMBS.

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 17799.

Organizational Resources

As organizations migrate to using an EMBS, the IT function's role becomes vital. Auditors should verify if the organization has dedicated appropriate IT resources (including infrastructure) to ensure that EBMS operates continually and effectively.

Auditors should also verify if the organization has appropriately defined the level of interaction, support and involvement of IT personnel in matters associated with the establishment, documentation, implementation and maintenance of the EBMS.

As part of the verification of assignment of appropriate resources, Auditors should evaluate how the organization addresses the competence required of personnel to operate hardware and software to run the EBMS.

During establishment of an EBMS, 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 EBMS is actually being assimilated and utilized by the organization's personnel.

The complexity of organizations IT infrastructures will vary, depending on the nature and complexity of the business. Auditors should verify an organization's system maintenance policies and procedures for its IT platform. Also, auditors should verify how the organization addresses system downtime incidents, as these will impact the normal functioning of the EBMS. 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 a dynamic electronic document, the guidelines provided above for the auditing of documents would also be applicable to it.

To the extent that the organization uses software for its EBMS, 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 EBMS.

Internal and External Electronic Communication

As the options available for, and ease of use of electronic communication increases, organizations should ensure that the documented management system addresses these means, as necessary, to ensure consistency in their use for satisfying the requirements of their EBMS and the applicable management system standard.

When Intranets, Email, and Instant Messaging are utilized for satisfying the requirements of the EBMS, auditors should verify that policies and procedures 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 policies and procedures for the control of records are being applied.

When the organization relies on its IT infrastructure for electronic communications with its customers (e.g. for e-commerce), suppliers (e-procurement), external sites and other interested parties, the auditor should verify that the methodology, policies and procedures for these communications and associated transactions are formally addressed within the EBMS.

Multi-Site Management Systems

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

When the IT 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 EBMS meets with the audit criteria

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

Auditor Competence

The reliability of the audit process for EBMS will depend on the ability of auditors to understand the trends in Information Technology 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 Information Technology that may impact the operation of management systems
- Audit-specific considerations for each audit assignment that is undertaken

As the innovations in the IT 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 EBMS.

In light of the innovations that influence the functioning of an EBMS, 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 be required.

This article is an edited version of ' Auditing Electronic-Based Management Systems (EBMS)' from the website of the ISO 9001 Auditing Practices Group, and is reproduced courtesy of ISO and the IAF. These papers were developed on current best practice and therefore have not been formally endorsed as International Accreditation Forum (IAF) guidance or ISO TC176 interpretations. For further information about the Auditing Practices Group <http://isotc.iso.org/livelink/livelink/fetch/2000/2122/138402/138403/%203541460/customview.html?func=ll&objId=3541460&objAction=browse&sort=name>.

The ISO 9001 Auditing Practices Group is an informal group of QMS experts, auditors and practitioners drawn from the ISO Technical Committee 176 Quality Management and Quality Assurance (ISO/TC 176) and the IAF. It has developed a number of guidance papers and presentations that contain explanations about the auditing of QMSs. These reflect the process-based approach that is essential for auditing the requirements of ISO 9001.

AUGUST 2005