



International Organization for Standardization
Forum



International Accreditation

ISO 9001 Auditing Practices Group **Guidance on:**

Auditando sistemas de gestión en base electrónica (EBMS)

1. Introducción

La creciente dependencia de las organizaciones en medios electrónicos para la operación y control de sus sistemas de gestión, requiere que los cuerpos de certificación y sus auditores vean nuevos enfoques para asegurar que las auditorías serán eficaces y eficientes. Ellos necesitarán redefinir el modo como los procesos y los documentos relacionados (incluyendo los registros) van a ser evaluados para verificar su conformidad con el criterio de auditoría.

Este documento ha sido desarrollado para dar unas directrices generales para la realización de auditorías a sistemas de gestión que estén totalmente basados en sistemas electrónicos o tengan un alto grado de su documentación en medios electrónicos. También proporciona directrices para los cuerpos de certificación y auditores para considerar como un complemento a las actividades de planificación y preparación normal que pudieran ocurrir antes de una auditoría.

Este documento se enfoca a aquellos requisitos de la norma ISO 9001 donde existe la posibilidad de utilizar documentos, registros, etc, electrónicos y también donde el acceso a esos documentos/registros pudiera estar controlado por sistemas electrónicos.

Este documento va dirigido a auditores de sistemas de gestión que tienen una amplia y variada experiencia con respecto a sistemas de gestión en base electrónica (EBMS) – e.g. sistemas de gestión que son dependientes de documentos electrónicos, datos y aplicaciones de software para su operación normal. Sin embargo, está escrito en un estilo que también permitirá ser utilizado por aquellos que solamente tienen una experiencia limitada en computadoras y EBMS.

Sin importar si es un cuerpo de certificación de tercera parte, un cuerpo de acreditación o una función de auditoría interna, quién realice la auditoría (“la organización auditora”) es responsable de asegurar la eficacia del proceso de

Traducción libre realizada por INLAC . Documentos oficiales disponibles en : www.iso.org/tc176/ISO9001AuditingPracticesGroup

auditoría para el EBMS. Este documento utiliza la guía proporcionada en la norma ISO 19011, y sugiere enfoques que pudieran ser utilizados por auditores de ISO 9001, y otras normas de sistemas de gestión, con la intención de verificar la conformidad con la norma referenciada. Los auditores y las organizaciones auditoras deben hacer los ajustes necesarios para asegurar un enfoque apropiado a como desarrollan los pasos del proceso de auditoría indicados en la norma ISO 19011.

Debe resaltarse que la destreza en auditar EBMS (Sistemas de gestión en base electrónica) no debe verse como una excusa para reducir la duración de la auditoría, sino como un medio de optimización de la eficacia y eficiencia de la auditoría.

No se pretende que este documento proporcione directrices para auditar los controles asociados con la seguridad de la información del EBMS. Aquellos interesados en otro tipo de controles asociados con la seguridad de la información se sugiere que se dirijan al documento ISO/IEC 17799 que es una norma para estos temas.

2. Iniciación y planificación de la auditoría

Durante la fase de iniciación de la auditoría (Auditoría fase 1) la organización auditora debe determinar la estructura de la organización a ser auditada, y el grado en que su sistema de gestión está basado electrónicamente. Una organización multisitio con un EBMS centralizado, o una organización "virtual", requerirá diferentes planes de auditoría y métodos que una organización de una sola plaza y/o una organización física.

La organización auditora y el auditado deben acordar como los auditores accederán y utilizarán el EBMS.

Esto pudiera involucrar el considerar:

- Permitir que los miembros del equipo auditor tengan oportunidad de familiarizarse con el EBMS del auditado (incluyendo la calendarización de suficiente tiempo dentro del plan de auditoría para esa orientación)
- Las políticas del auditado para el uso de la infraestructura de Tecnología de la información.
- Instrucciones para acceder, y las licencias de seguridad para acceder y los documentos y registros organizacionales pertinentes
- Los seguros y procesos para asegurar que los auditores protejan la confidencialidad de los documentos y registros electrónicos durante y después de la auditoría.

La organización auditora debe asegurar que existe la competencia suficiente dentro de su equipo auditor seleccionado para realizar una evaluación eficaz del EBMS.

3. Revisión documental

Dependiendo de su el auditado tiene la habilidad para hacer que su documentación esté disponible a través de una aplicación basada en red o a

Traducción libre realizada por INLAC . Documentos oficiales disponibles en : www.iso.org/tc176/ISO9001AuditingPracticesGroup

través de transmisión por correo electrónico, la organización auditora pudiera conducir parte o toda la revisión documental de manera remota; ya sea en línea o por descarga de la documentación electrónica enviada por correo electrónico.

Dependiendo de los factores técnicos o de seguridad, pudiera no ser factible el conducir una revisión total del EMBS de la organización en línea o por la transmisión de documentos relevantes por correo electrónico, antes de llegar al sitio. En estos casos, las actividades de preparación de la auditoría que requieran la revisión de documentos electrónicos necesitaría realizarse en las instalaciones del auditado durante la fase 1 de auditoría.

4. Actividades de realización en sitio

El enfoque para los sistemas de gestión en base electrónica dependerá ampliamente de que tanto de la evidencia requerida para determinar la conformidad está en forma de registros electrónicos.

Durante las actividades de realización en el sitio, el camino del auditor debe incluir típicamente la ubicación física del proceso que está auditando. Sin embargo, con un EBMS el tiempo requerido para confirmar la evidencia para determinar si se cumplen o no los requisitos, pudiera dedicarse en una computadora o estación de trabajo que pudiera estar o no localizada cerca del proceso en cuestión.

Cuando las estaciones de trabajo computarizadas están en áreas remotas que no son accesibles para la ubicación física de operación del proceso, el tiempo real de auditoría en la ubicación física del proceso pudiera reducirse. Sin embargo, el tiempo total de evaluación pudiera no necesariamente reducirse dado que la revisión de la evidencia electrónica pudiera ocurrir antes y/o después de confirmar la existencia del proceso físico.

En los casos donde la estación de trabajo de la computadora es remoto, se debe dar una consideración especial al tiempo requerido de traslado hacia y desde la ubicación física del proceso.

Cuando el proceso es dependiente de la intervención humana, el auditor debe evaluar los métodos empleados para la interacción entre el proceso físico y el medio electrónico para asegurar la precisión de la información asociada.

5. Auditando el control de los documentos electrónicos.

Los documentos electrónicos que establecen políticas y procedimientos del sistema de gestión pueden estar en una gran variedad de formatos dependiendo de las aplicaciones de software que son utilizados por la organización para generar los documentos. Los archivos electrónicos pueden incluir formatos como texto, html, pdf, etc. Las hojas de cálculo y los formatos de bases de datos son también considerados "documentos" electrónicos y están sujetos a los elementos de control del sistema de gestión a auditar.

Traducción libre realizada por INLAC . Documentos oficiales disponibles en : www.iso.org/tc176/ISO9001AuditingPracticesGroup

Dada la relativa facilidad con que los usuarios pueden ahora crear hojas de cálculo electrónicas y otros documentos electrónicos, los auditores deben asegurar que las políticas que gobiernan los controles que aplican a la documentación del sistema de gestión, en general también se apliquen a los documentos electrónicos a través de los procedimientos adecuados.

Las organizaciones necesitan emplear métodos adecuados y eficaces dentro del ambiente electrónico para asegurar la adecuada revisión, aprobación, publicación y distribución de la documentación de su sistema de gestión. Estos deben ser consistentes con los métodos para el desarrollo y modificación de documentos electrónicos.

En muchos casos las medidas de control de documentos pudieran también ser características estándar de la aplicación del software usados para su creación. Por lo tanto los auditores deben entender esos controles de aplicación específicos al grado de que estos sean utilizados como base para la conformidad a la norma de sistema de gestión aplicable.

Dado el incremento de capacidad para modificar, actualizar, reformar y de cierta forma mejorar los documentos dentro de un sistema de gestión electrónico, los auditores deben poner particular atención en los elementos de control como la identificación de documentos y el nivel de revisión de los documentos.

Como el medio electrónico facilita el incremento de modificaciones a documentos, los auditores deben verificar que los controles empleados para la gestión de documentos obsoletos sean considerados dentro de las políticas y procedimientos de control de documentos de la organización.

Los auditores deben verificar que la documentación del EBMS existe para proporcionar orientación a los usuarios respecto a los aspectos funcionales y de control asociados a los documentos electrónicos. Adicionalmente, los requisitos en el "punto de uso" asociados con las normas de sistema de gestión aplicables, típicamente se cubrirán en parte por las políticas de acceso a documentos de la organización. Los auditores deben entender las políticas y procedimientos de la organización que tratan sobre los privilegios de los usuarios ya que estos son factores importantes para comprender apropiadamente los procesos de la organización.

La comunicación electrónica externa con proveedores, clientes y otras partes interesadas pudieran involucrar el intercambio de documentos. Dado que estos documentos externos pudieran contener parámetros clave que especifican el funcionamiento de los procesos de la organización, los auditores deben verificar el grado en que estos documentos son formalmente introducidos y controlados dentro del sistema de gestión en base electrónica.

6. Auditando el control de los registros electrónicos

Los registros electrónicos consisten en los datos de los resultados de los procesos combinados con los formatos electrónicos que contienen los datos.

Traducción libre realizada por INLAC . Documentos oficiales disponibles en : www.iso.org/tc176/ISO9001AuditingPracticesGroup

Estos formatos electrónicos van desde una simple hoja electrónica a las aplicaciones de base de datos más complejas.

Los auditores deben estar concientes de que los elementos de control que establecen las organizaciones para las formas electrónicas no son necesariamente los mismos que los que aplican a los registros electrónicos. Por ejemplo, con respecto a la "Identificación", en el caso de formas electrónicas, el término se refiere a la nomenclatura del formato electrónico mismo. Cuando la "identificación" es considerada en el caso de un registro electrónico, esta se refiere al uso único del formato electrónico para un grupo dado de datos.

Los auditores deben revisar los métodos empleados por la organización para la captura de datos, con la finalidad de asegurar que las actividades de introducción de datos proporciona la suficiente confianza en su exactitud.

Cuando se evalúa los controles de la organización con respecto al almacenaje de registros, los auditores deben verificar si las organizaciones tienen un entendimiento de su capacidad de almacenamiento contra:

- El rango de generación de registros
- Las políticas de retención de registros y tiempos asociados
- El rango de disposición de registros,

ya que estos factores pudieran impactar el funcionamiento apropiado del EBMS.

Dado que la base de conocimientos y el desempeño de la organización pudiera estar casi totalmente en registros electrónicos, los auditores deben revisar los enfoques de la organización para seguridad de la información contenida en medios electrónicos. Para más información sobre Seguridad de la Información ver la norma ISO/IEC 17799.

7. Recursos Organizacionales

Conforme las organizaciones emigran al uso de EBMS, el papel de las funciones de IT (tecnología de la información) se vuelven vitales. Los auditores deben verificar si las organización ha dedicado los recursos de IT apropiados (incluyendo la infraestructura) para asegurar que el EBMS opera continua y eficazmente.

Los auditores deben también verificar si la organización tiene definidos apropiadamente el nivel de interacción, soporte e involucramiento del personal de IT en aspectos asociados con el establecimiento, documentación, implementación y mantenimiento del EBMS.

Como parte de la verificación de la asignación de los recursos apropiados, los auditores deben evaluar como la organización cubre la competencia requerida del personal para operar el equipo (hardware) y el software para correr el EBMS.

Traducción libre realizada por INLAC . Documentos oficiales disponibles en : www.iso.org/tc176/ISO9001AuditingPracticesGroup

Durante el establecimiento de un EBMS, es una práctica común que sistemas paralelos (manuales y electrónicos) estén funcionando por un período de tiempo que permita a los usuarios su adaptación. En estos casos el auditor debe verificar los enfoques de la organización para asegurar que el EBMS ha sido realmente asimilado y utilizado por el personal de la organización.

La complejidad de la infraestructura de IT de las organizaciones variará, dependiendo de la naturaleza y complejidad de los negocios. Los auditores deben verificar los procedimientos y políticas de mantenimiento del sistema de la organización para su plataforma de IT. También, los auditores deben verificar como la organización cubre los incidentes de paros del sistema, ya que esto impactará el funcionamiento normal del EBMS. Los auditores deben evaluar si la organización tiene o no sistemas formales de respaldo, y si éstos se revisan y prueban periódicamente en su adecuación o no.

En relación al software, los auditores deben verificar los controles establecidos para el software interno, el software externo, las licencias de software y las actualizaciones del software. Ya que el software puede ser considerado un documento electrónico dinámico, las directrices dadas con anterioridad para auditar los documentos pudieran también ser aplicables a éste.

Dependiendo de que tanto la organización utilice software para su EBMS, los auditores deben revisar la funcionalidad de las aplicaciones y su relación con los elementos del sistema de gestión definidos en el criterio aplicable.

Como los factores ambientales pudieran impactar en el funcionamiento de una plataforma de IT, las organizaciones deben tener medidas para protegerse contra esos factores. Esto puede variar desde la necesidad de adecuar las instalaciones hasta la necesidad de tener fuentes ininterrumpibles de energía (UPS). Los auditores deben evaluar si los controles de la organización toman en cuenta aspectos como el mantenimiento de instalaciones, temperatura, humedad, etc, en la medida que estos amenacen la operación del EBMS.

8. Comunicación electrónica interna y externa

Dado que las opciones disponibles y la facilidad de uso en la comunicación electrónica aumenta, las organizaciones deben asegurar que el sistema de gestión documentado cubre estos medios, según sea necesario, para asegurar consistencia en su utilización para satisfacer los requisitos de su EBMS y la norma de sistema de gestión aplicable.

Cuando se utilizan intranets, emails y mensajes instantáneos para satisfacer los requisitos del EBMS, los auditores deben verificar las políticas y procedimientos que cubran las circunstancias bajo las cuales estos medios pudieran ser empleados. Adicionalmente, si los resultados de la comunicación electrónica interna serán utilizados para satisfacer los criterios de auditoría, los auditores deben verificar que las políticas y procedimientos para el control de registros se hayan aplicado.

Traducción libre realizada por INLAC . Documentos oficiales disponibles en : www.iso.org/tc176/ISO9001AuditingPracticesGroup

Cuando la organización dependa de su infraestructura de IT para las comunicaciones electrónicas con sus clientes (e.g. para e-commerce), proveedores (e-procurement), sitios remotos y otras partes interesadas, el auditor debe verificar que la metodología, políticas y procedimientos para esas comunicaciones y transacciones asociadas están formalmente cubiertas dentro del EBMS.

9. Sistemas de gestión Multi-sitios

Las organizaciones que operan a través de múltiples sitios (o desde una central a ubicaciones satélites) normalmente mantienen comunicaciones y comparten políticas, procedimientos y datos de procesos entre sus varias ubicaciones vía electrónica, como el Internet, extranets, e-mail y Messenger.

Cuando la plataforma IT y su software de aplicación asociado se utilizan para compartir información que es pertinente al criterio de auditoría, los auditores deben entender los diferentes medios de red que se emplean en la organización en la medida que sea necesario para juzgar si el EBMS cumple con el criterio de auditoría.

Los auditores deben verificar si los controles sobre un sistema de gestión multi sitio son cubiertos y establecidos apropiadamente dentro de las políticas y procedimientos de la organización.

10. Competencia del auditor

La confiabilidad del proceso de auditoría para un EBMS dependerá de la habilidad de los auditores para entender las tendencias en la Tecnología de la Información ya que las organizaciones dependen cada vez más del software para dar seguimiento y controlar sus operaciones.

Las organizaciones auditoras deben tomar las medidas necesarias, incluyendo la provisión de entrenamiento, para cubrir las necesidades generales e individuales de su base de auditores con respecto a:

- Tendencias generales en Tecnología de la Información que pudiera impactar la operación de los sistemas de gestión
- Consideraciones especiales de auditoría para cada asignación de auditoría que se tome.

Como las innovaciones en el sector IT son relativamente rápidas comparadas con los cambios en los criterios de auditoría, los auditores y las organizaciones auditoras se ven retadas con la necesidad de tener un entendimiento práctico de las tendencias asociadas y como ellas pudieran ser aplicables y utilizadas dentro de un EBMS.

A la luz de las innovaciones que influyen el funcionamiento de un EBMS, las organizaciones auditoras deben determinar si la experiencia necesaria para ser eficaces en una auditoría dada, se encuentra en el equipo auditor mismo o cuando se requerirá la asistencia de un experto técnico.