International Organization for Standardization

International Accreditation Forum

25 августа 2005 г.

ISO 9001 Auditing Practices Group
Руководство

Аудит систем менеджмента, базирующихся на КИС[1]

1. Введение

Возрастающая зависимость организацией от программных средств поддержки и управления системами менеджмента требует от органов по сертификации/ регистрации, а также их аудиторов, искать новые подходы к обеспечению результативности и эффективности аудитов. Они должны пересмотреть способы оценки процессов и связанных с ними документов (включая записи) с целью проверки соответствия критериям аудита.

Данный документ был разработан, чтобы дать общие указания для проведения аудитов систем менеджмента, которые либо реализованы (основаны) на корпоративных информационных системах (КИС), либо имеют высокую степень документирования в электронном виде. Он также дает руководящие указания органам по сертификации/регистрации и аудиторам, позволяющие учесть как дополнительные к обычным планированию и подготовке действия, которые должны быть выполнены до аудита.

Это руководство нацелено на те требования стандарта ISO 9001, которые дают возможность применения в электронном виде документов, записей и т.д., а также на те случаи, когда доступ к таким документам/записям может обеспечиваться через электронные системы.

Данный документ ориентирован на аудиторов систем менеджмента, кто обладает большим и разнообразным опытом в отношении систем менеджмента, основанных на КИС [далее будет использоваться сокращение КСМ – компьютеризированные системы менеджмента – прим. пер.] – т.е. систем менеджмента, которые зависят от электронных документов, данных и программных приложений, обеспечивающих их нормальное функционирование. Тем не менее, руководство написано так, что оно может быть использовано теми, кто имеет ограниченный опыт в области компьютеров и КСМ.

Неважно, аудит ли это третьей стороны, проводимый органом по сертификации или аккредитации, или внутренний аудит, организация, выполняющая проверку («проверяющая организация») несет ответственность за обеспечение

[1] КИС – корпоративная информационная система

результативности процесса аудита КСМ. Данное руководство использует подходы стандарта ISO 19011, которые могут применяться аудиторами по ISO 9001, а также другим стандартам на системы менеджмента, для оценки соответствия этим стандартам. Аудиторы и проверяющие организации должны вносит необходимые коррективы с тем, чтобы обеспечить соответствующие методы в ходе выполнения этапов аудита, предусмотренных стандартом ISO 19011.

Необходимо помнить, что имеющийся опыт в проверке КСМ не должен рассматриваться как основание для уменьшения продолжительности аудита, но как средство достижения наилучшей результативности и эффективности аудита.

Данное руководство не предполагает указаний по средствам управления, связанным с информационной безопасностью КСМ. Тот, кто заинтересован в таких средствах управления, может обратиться к стандарту ISO/IEC 17799[2], который всесторонне рассматривает эти вопросы.

2. Инициирование и планирование аудита

В ходе инициирования аудита (этап 1) проверяющая организация должна определить структуру проверяемой организации и степень ориентированности системы менеджмента на информационные системы. Организация, имеющая несколько площадок, управляемых через централизованную информационную систему, т.н. «виртуальная» организация, потребует различных планов аудита и методов для каждой площадки.

Проверяющая и проверяемая организации должны договориться о том, каким образом аудиторы будут иметь доступ к КСМ. Для этого следует учесть:

- Возможность членам группы аудита ознакомиться с КСМ проверяемой организации (с включением в план аудита времени на такое ознакомление)
- Политики проверяемой организации в области применения информационных технологий
- Инструкции по доступу, а также необходимые разрешения, связанные с безопасностью, на доступ к требуемым документам и записям организации
- Меры безопасности и процессы, обеспечивающие сохранение аудиторами конфиденциальности электронных документов и записей как во время аудита, так и после него.

Проверяющая организация должна гарантировать, что у членов группы аудита имеются требуемые компетенции для выполнения результативной оценки КСМ.

3. Анализ документов

В зависимости от того, имеет ли проверяемая организация возможность получать доступ к документам через веб-приложения или посредством пересылки по электронной почте, проверяющая организация может провести часть и весь анализ документации вне проверяемой организации; либо в режиме онлайн, либо получив документацию в электронном виде по электронной почте.

В силу технических факторов или условий безопасности может и не быть возможности провести полный анализ КСМ организации в режиме онлайн или посредством пересылки по электронной почте значимых документов, до посещения площадки. В таких случаях может потребоваться провести подготовку к аудиту,

[2] В настоящий момент вместо стандарта 17799 действует стандарт 27001 из семейства стандартов ISO 27000 [прим. пер.]

требующую анализа документов в электронном виде, на каждом из участков в ходе первого этапа аудита.

4. Действия на местах

Подход к аудиту КСМ будет сильно зависеть от того, насколько много свидетельств, требуемых для подтверждения соответствия, существуют в электронном виде.

В ходе аудита на местах маршрут аудитора должен, как правило, включать посещение места, где выполняется проверяемый процесс. Однако, при КСМ свидетельства соответствия требованиям могут быть получены через компьютер, который может находиться как вблизи места выполнения процесса, так и далеко от него.

В тех случаях, когда рабочие станции находятся в удаленных местах, недоступных там, где процесс выполняется, реальное время аудита в месте выполнения процесса может быть уменьшено. Однако это не означает, что обязательно должно быть сокращено общее время аудита, учитывая, что анализ свидетельств в электронном виде может производиться до и/или после подтверждения существования физического процесса.

В том случае, когда соответствующая рабочая станция находится в удаленном месте, необходимо особо учесть время, требуемое для перемещения к и от места физического выполнения процесса.

Когда процесс зависит от человеческого вмешательства, аудитор должен оценить методы, применяемые для взаимодействия между физическим процессом и электронной средой, чтобы убедиться в точности соответствующей информации.

5. Аудит управления электронными документами

Электронные документы, которые устанавливают политики и процедуры системы менеджмента могут быть в файлах различных форматов, в зависимости от применяемых в организации для создания документов программ. Форматы файлов включают в себя текстовые, HTML, PDF и т.д. Файлы форматов электронных таблиц и баз данных также входят в число электронных документов, которые находятся под управлением проверяемой КСМ.

Учитывая определенную легкость, с которой теперь создаются электронные таблицы и другие электронные документы, аудиторы должны убедиться, что политики, определяющие средства управления, которые применяются к системе менеджмента документации в целом, также применяются и к электронным документам посредством соответствующих процедур.

Организации необходимо применять подходящие и результативные методы для электронных документов с тем, чтобы обеспечить соответствующий пересмотр, утверждение, публикацию и распространение документации системы менеджмента. Эти методы должны быть согласованы с методами разработки и изменения электронных документов.

Во многих случаях средства управления документами могут быть стандартными функциями программ, используемых для создания документов. Таким образом, аудиторы должны понимать эти специфичные для разных программ средства в той степени, которая позволяет установить их соответствие применяемым стандартам на систему менеджмента.

Учитывая возрастающие возможности по модификации, обновлению, изменению формата и иных форм улучшения документов в рамках КСМ, аудиторы должны обращать внимание на средства управления, такие как идентификация документов и их версий.

Т.к. электронная среда способствует быстрому изменению документов, аудиторы должны удостовериться, что средства управления, применяемые для управления устаревшими документами, находят отражение в процедурах и политиках управления документацией организации.

Аудиторы должны проверить, что документация КСМ существует для того, чтобы помочь пользователям сориентироваться в различных аспектах, связанных с электронными документами. К тому же, требования к местам применения документов, связанные со стандартами на систему менеджмента, будут, как правило, частично установлены политиками доступа организации. Аудиторы должны понимать политики и процедуры организации, устанавливающие привилегии пользователей, т.к. это становится важным фактором для правильной реализации процессов организации.

Внешние связи посредством электронных коммуникаций с поставщиками, потребителями и другими заинтересованными сторонами могут вести к обмену документами. Учитывая, что документы для внешних сторон могут содержать ключевые параметры, которые раскрывают функционирование процессов организации, аудиторы должны проверить степень, с которой эти документы официально введены и управляются в рамках КСМ.

6. Аудит управления электронными записями

Электронные записи содержат данные о результатах процесса в определенном электронном формате. Эти форматы могут быть от простых электронных таблиц до более сложных форматов систем управления базами данных.

Аудиторы должны понимать, что средства управления, которые организация установила для электронных форм не обязательно должны совпадать с теми, которые организация применяет для электронных записей. Например, в отношении идентификации в случае электронных форм этот термин означает определение вида электронной формы. Когда же термин «идентификация» применяется к электронной записи, то он указывает на уникальное использование электронной формы, связанное с данными, внесенными в форму.

Аудиторы должны анализировать методы, применяемые организацией для получения данных с тем, чтобы убедиться, что они обеспечивают надлежащую точность.

При оценке средств управления, применяемых организацией, для хранения записей аудиторы должны проверить, принимает ли в расчет организация следующее:

- интенсивность генерации записей,
- политики в отношении хранения записей и связанные с этим сроки,
- интенсивность удаления записей,

т.к. эти факторы могут влиять на функционирование КСМ.

Учитывая, что база знаний и данные о деятельности организации могут быть почти полностью в электронных записях, аудиторы должны анализировать подходы организации к обеспечению безопасности информации, содержащейся в

электронных устройствах. Более детальную информацию по информационной безопасности можно получить в стандарте ISO/IEC 17799 [см. примечание 2 на второй странице – прим. пер.]

7. Ресурсы организации

Когда организация переходит на КСМ, роль ИТ-служб становится жизненно важной. Аудиторы должны проверить, выделила ли организация соответствующие ИТ-ресурсы (включая инфраструктуру) для обеспечения непрерывной и результативной работы КСМ.

Аудиторы также должны проверить, определила ли организация соответствующим образом уровень взаимодействия, поддержки и привлечения ИТ-персонала к вопросам, связанным с установкой, документированием, внедрением и поддержкой КСМ.

Как часть проверки назначения соответствующих ресурсов аудиторы должны оценить, как организация поддерживает необходимую компетентность персонала в сфере обслуживания технических и программных средств, обеспечивающих работу КСМ.

Обычно во время внедрения КСМ сохраняется одновременно два способа (бумажный и электронный) ведения документации на местах, чтобы дать пользователям время привыкнуть. В этом случае аудитор должен проверить, каким образом организация гарантирует то, что КСМ действительно осваивается и используется персоналом.

Сложность ИТ-инфраструктуры организаций может быть разной, в зависимости от вида и сложности бизнеса. Аудиторы должны проверить политики и процедуры обслуживания и поддержки организации. Также аудиторы должны проверить, каким образом организация обрабатывает инциденты, связанные с простоем, т.к. они будут влиять на нормальное функционирование КСМ. Аудиторы должны проверить, имеет или не имеет организация официальную систему резервного копирования и тестируется она периодически или нет.

В отношении программного обеспечения (ПО) аудиторы должны проверить средства управления, применяемые для ПО собственной разработки, покупного ПО, лицензий и обновления. Принимая во внимание, что программное обеспечение может рассматриваться как электронный документ, все указания по аудиту документации, данные выше, могут быть также применены и к ПО.

В том объеме, в каком организация использует программное обеспечение для КСМ, аудитор должен проанализировать функциональность приложений и их взаимосвязь с элементами системы менеджмента, определенную в применимых критериях.

Так как факторы, связанные с производственной средой, могут влиять на функционирование информационной техники, организации должны предпринимать меры для защиты ее от этих факторов. Такие меры могут варьироваться от потребности в соответствующих устройствах или местах размещения до потребности в бесперебойных источниках питания (UPS). Аудиторы должны оценить, соответствуют ли меры, предпринятые организацией с учетом таких аспектов, как обслуживание устройств, температура, влажность и т.д., той степени, в которой они влияют на работу КСМ.

8. Внутренний и внешний обмен информацией

Т.к.возможности для электронного обмена информацией и его простота возрастают, то организации должны гарантировать, что документированная система менеджмента предполагает использование этих средств по мере необходимости с тем, чтобы обеспечить согласованное их применение для выполнения требований КСМ организаций и применяемого стандарта на систему менеджмента.

В тех случаях, когда для выполнения требований КСМ применяются интранет, электронная почта и службы быстрых сообщений, аудиторы должны удостовериться, что политики и процедуры принимают во внимание обстоятельства, при которых эти средства должны применяться. Кроме этого, если результаты внутреннего обмена электронной информацией предполагается использовать для оценки соответствия критериям аудита, то аудиторы должны убедиться, что применяются политики и процедуры для управления записями.

В тех случаях, когда взаимодействие организации с потребителями (например, электронная торговля), поставщиками (например, электронные закупки), удаленными площадками и иными заинтересованными сторонами зависит от ИТ-инфраструктуры, аудитор должен убедиться, что методология, политики и процедуры для такого рода взаимодействий предусмотрены в КСМ.

9. Распределенные системы менеджмента

Организации, которые состоят из нескольких равнозначных бизнес-единиц (или одной центральной, управляющей периферийными) обычно осуществляют взаимодействие и размещают в совместном доступе политики, процедуры и данные, относящиеся к процессам, с помощью электронных средств, таких как интранет, экстранет, электронная почта и службы быстрых сообщений.

В тех случаях, когда КСМ и связанные с ней программы используются для обеспечения общего доступа к информации, которая имеет отношение к критериям аудита, аудиторы должны понимать работу различных сетевых приложений, используемых организацией, в том объеме, который необходим для выяснения, соответствует ли КСМ критериям аудита.

Аудиторы должны убедиться в том, что средства управления для распределенной системы менеджмента соответствующим образом учтены и установлены в политиках и процедурах организации.

10. Компетентность аудитора

Степень доверия к результатам аудита КСМ будет зависеть от способности аудиторов понимать направления развития в информационных технологиях, т.к. организации все более зависят от программного обеспечения для мониторинга и контроля их деятельности.

Проверяющая организация должна предпринять необходимые меры, включая проведение тренингов, чтобы учесть общие и индивидуальные потребности своих аудиторов в отношении:

- имеющихся тенденций в развитии информационных технологий, которые могут оказывать влияние на функционирование систем менеджмента,
- специальных аспектов аудита, связанных с каждым конкретным заданием на аудит.

Т.к. инновации в сфере ИТ происходят быстрее, чем изменения в критериях аудита, то от аудиторов и проверяющих организаций требуется практическое понимание соответствующих тенденций и того, как они могут быть применены и использованы в КСМ.

В свете инноваций, которые влияют на КСМ, проверяющая организация должна определить, имеется ли у назначенной на конкретный аудит группы необходимый для результативной работы опыт и нужна ли помощь технических экспертов.

Более подробная информация об ISO 9001 Auditing Practices Group содержится в документе *Introduction to the ISO 9001 Auditing Practices Group* (***Знакомство с ISO 9001 Auditing Practices Group)***

Обратная связь с пользователями для понимания, требуется ли разработка дополнительных руководящих документов или пересмотр существующих версий, будет осуществляться через ***ISO 9001 Auditing Practices Group***.

Комментарии по документам и иным материалам могут быть высланы по следующему электронному адресу:

charles.corrie@bsigoup.com.

Другие документы и материалы ISO 9001 Auditing Practices Group можно загрузить с сайтов

www.iaf.nu

www.iso.org/tc176/ISO9001AuditingPracticesGroup

Ограничение ответственности

Данный документ не подлежит официальному утверждению Международной организацией по стандартизации (ISO), Техническим комитетом 176 ISO, или Международным аккредитационным форумом (IAF).

Информация, содержащаяся в документах, предназначена для образовательных и информационных целей. ***ISO 9001 Auditing Practices Group*** не принимают на себя никаких обязательств и не несут ответственности за любые ошибки и неточности, которые могут произойти в результате получения и последующего использования этой информации.

Переводы документов ISO 9001 Auditing Practices Group на ресурсе «Новое качество»

В феврале 2007 г. «Новое Качество» получило от ISO и IAF официальное разрешение на некоммерческое использование материалов APG. В разделе библиотеки ресурса www.new-quality.ru представлены переводы статей APG по аудиту СМК.

Переводы документов ISO 9001 Auditing Practices Group на сайте журнала «Das Management»

23 октября 2009 г. журнал «Das Management» получил от ISO и IAF официальное разрешение на некоммерческое использование материалов APG. Переводы материалов ISO 9001 Auditing Practices Group представлены в свободном доступе на сайте журнала по адресу http://www.das-management.info/index.php?nmp=02isoiafrec.