International Organization for Standardization

International Accreditation Forum

Дата: 13 января 2016 г.

Группа по практикам аудита на соответствие ISO 9001

Рекомендации

Системы с электронной документированной информацией

1. Введение

Возрастающая зависимость организацией от электронных носителей для функционирования и управления их 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 документированной информации с целью проверки соответствия критериям аудита.

Данный документ был разработан, чтобы дать общие рекомендации для проведения аудитов систем менеджмента, в которых документированная информация представлена либо только в электронном виде, либо высок уровень информации на электронных носителях. Он также дает рекомендации 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 документированной информации на электронных носителях.

Данный документ ориентирован на аудиторов систем менеджмента, кто обладает большим и разнообразным практическим опытом использовании электронных носителей для функционирования и управления системами менеджмента, т.е. систем менеджмента, нормальная работа которых зависит от электронных носителей и программного обеспечения. Тем не менее, документ написан так, что позволяет применение теми, кто имеет ограниченный опыт в области компьютеров и электронных носителей.

Неважно, аудит ли это третьей стороны, проводимый органом по сертификации или аккредитации, или внутренний аудит, организация, выполняющая проверку («проверяющая организация») несет ответственность за обеспечение результативности процесса аудита системы с электронной документированной информацией. Данный документ использует рекомендации, данные в ISO 19011, и других стандартах на системы менеджмента, и поддерживает подходы, которые могут применяться аудиторами ISO 9001, а также других стандартов на системы менеджмента, для оценки соответствия этим стандартам. Аудиторы и проверяющие организации должны вносит необходимые коррективы с тем, чтобы обеспечить соответствующий подход при выполнении этапов аудита, предусмотренных стандартом ISO 19011.

Необходимо помнить, что имеющийся опыт в аудите систем с электронной документированной информацией не должен рассматриваться как основание для уменьшения продолжительности аудита, но как средство достижения наилучшей результативности и эффективности аудита.

Данный документ не предполагает рекомендаций по аудиту механизмов, связанных с информационной безопасностью. Тот, кто заинтересован в средствах управления, связанных с информационной безопасностью, может обратиться к стандарту ISO/IEC 27001, который всесторонне рассматривает эти вопросы.

2. Инициирование и планирование аудита

В ходе инициирования аудита (т.е. первого этапа аудита – см. документ Группы по практикам аудита «Необходимость двухэтапного подхода к аудиту»[*]) проверяющая организация должна определить структуру проверяемой организации и степень применения электронной документированной информации. Организация с несколькими площадками, имеющая централизованный процесс управления своей электронной документированной информацией, или иначе «виртуальная» организация, потребует различных планов аудита и методов.

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

- Возможность членам группы аудита ознакомиться самим с системой электронной документированной информации (включая резервирование в плане аудита достаточного времени на такое ознакомление)

- Политики проверяемой организации в области применения информационных технологий

- Инструкции по доступу, а также необходимые разрешения, связанные с доступом к документам и записям организации

- Меры безопасности и процессы, гарантирующие, что аудиторы обеспечивают

[*] Дано название документа из пакета рекомендаций по ISO 9001:2008. В пакете документов Группы для ISO 9001:2015 он называется «Два этапа начального сертификационного аудита» [прим. пер.]

сохранение конфиденциальности электронной документированной информации как во время аудита, так и после него.

Проверяющая организация должна гарантировать, что у отобранной группы аудита имеется достаточная компетентность для выполнения результативной оценки системы электронной документированной информации.

3. Анализ документов

В зависимости от того, имеет или нет 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 системы электронной документированной информации организации в режиме онлайн или посредством пересылки по электронной почте соответствующей информации до посещения площадки. В таких случаях может потребоваться провести подготовку к аудиту, требующую анализа электронной информации на каждом из участков проверяемой организации в ходе первого этапа аудита.

4. Действия на местах

Подход к аудиту систем электронной документированной информации 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 наличии системы электронной документированной информации время, необходимое для подтверждения, выполняются или нет требования, могут быть получены через компьютер, который может и не находиться вблизи места выполнения процесса.

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

Электронная информация, которая обеспечивает оперативное управление системой менеджмента, может быть в файлах различных форматов, в зависимости от применяемых в организации для создания информации программ. Форматы электронных файлов включают в себя текст, HTML, PDF и т.д. Файлы форматов электронных таблиц и баз данных также рассматриваются как электронная документированная информация, находящаяся под управлением проверяемой системы менеджмента.

Учитывая определенную легкость, с которой пользователи могут сегодня создавать электронные таблицы и другую электронную информацию, аудиторы должны убедиться, что процессы, регламентирующие средства управления, которые обычно применяются в системе менеджмента информации на неэлектронных носителях, также применяются и к электронной информации.

Организации необходимо применять подходящие и результативные методы в рамках электронной среды, чтобы обеспечить соответствующий пересмотр, утверждение, публикацию и распространение документации системы менеджмента. Эти методы должны быть согласованы с методами разработки и изменения электронной информации.

Во многих случаях средства управления документами могут также быть стандартными функциями программ, используемых для их создания. Таким образом, аудиторы должны понимать эти специфичные для разных программ средства в той степени, в которой они применяются для свидетельства соответствия действующим стандартам на системы менеджмента.

Учитывая возросшие возможности по модификации, обновлению, изменению формата и иных форм улучшения в рамках системы электронной документированной информации, аудиторы должны обращать особое внимание на средства управления, такие как идентификация и учет версий.

Т.к. электронная среда способствует повышенной скорости изменений, аудиторы должны удостовериться, что средства управления, применяемые для управления устаревшей информацией, находят отражение в процессах управления организации.

Аудиторы должны проверить, что имеется информация для того, чтобы помочь пользователям сориентироваться в вопросах функциональности и управления, связанных с электронной информацией. К тому же, требования к местам применения, связанные с действующими стандартами на системы менеджмента, будут, как правило, установлены в рамках политикам доступа организации. Аудиторы должны понимать процессы организации, устанавливающие привилегии пользователей, т.к. это становится важным фактором для правильной реализации процессов организации.

Внешние электронные коммуникации с внешними поставщиками, потребителями и другими заинтересованными сторонами могут предполагать обмен

документированной информацией. Учитывая, что документированная информация может содержать ключевые параметры, которые раскрывают функционирование процессов организации, аудиторы должны проверить, в какой степени она официально введена и управляется в рамках системы электронной документированной информации.

Аудиторы должны рассмотреть методы, применяемые организацией для сбора результатов с целью гарантии того, что деятельность обеспечивает достаточную уверенность в точности информации.

При оценке средств управления организации, связанных с хранением документированной информации, аудиторы должны проверить, имеет ли организация представление о своих возможностях по хранению в плане:

- объема создаваемой информации,
- времени хранения,
- объема удаляемых записей.

как эти факторы могут влиять на надлежащее функционирование системы электронной документированной информации.

Учитывая, что база знаний и показатели деятельности организации могут быть почти полностью в форме электронных записей, аудиторы должны проанализировать подходы организации к обеспечению безопасности информации, находящейся на электронных носителях. Для большей информации по информационной безопасности см. ISO/IEC 27001.

6. Ресурсы организации

Когда организация переходит к использованию системы электронной документированной информации, роль ИТ-служб становится жизненно важной. Аудиторы должны проверить, выделила ли организация соответствующие ИТ-ресурсы (включая инфраструктуру) для гарантии непрерывной и результативной работы системы.

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

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

Обычно во время внедрения системы электронной документированной информации действуют параллельно (бумажная и электронная) системы, чтобы дать пользователям время привыкнуть. В этом случае аудитор должен проверить, каким образом подходы организации к гарантии того, что система действительно осваивается и используется.

Сложность ИТ-инфраструктуры организаций может быть разной, в зависимости от характера и сложности бизнеса. Аудиторы должны проверить процессы обслуживания системы организации в рамках ее ИТ-платформы. Также аудиторы должны проверить, каким образом организация обрабатывает инциденты, связанные с простоем, т.к. они будут влиять на нормальное функционирование системы электронной документированной информации. Аудиторы должны проверить, имеет или нет организация формализованные системы резервного копирования, тестируется и анализируется ли она периодически на предмет соответствия или нет.

В отношении программного обеспечения аудиторы должны проверить средства управления, применяемые для программ собственной разработки, покупных программ, лицензий и обновлений. Принимая во внимание, что программное обеспечение может рассматриваться как динамически меняющееся, рекомендации по аудиту электронной информации, данные выше, могут быть также применены и к программам.

В том объеме, в каком организация использует программное обеспечение для системы электронной документированной информации, аудиторы должны проанализировать функциональность приложений и их взаимосвязь с элементами системы менеджмента, определенную в действующих критериях.

Так как факторы, связанные с производственной средой, могут влиять на функционирование ИТ-платформы, 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, учитывают ли меры, предпринятые организацией, такие аспекты, как обслуживание устройств, температура, влажность и т.д., той степени, в которой они влияют на работу системы электронной документированной информации.

7. Внутренний и внешний обмен информацией

Т.к. возможности для электронного обмена информацией и его простота возрастают, то организации должны внедрить необходимые средства управления, чтобы гарантировать согласованность в их применении и для выполнения требований системы электронной документированной информации, а также действующего стандарта на систему менеджмента.

В тех случаях, когда для выполнения требований системы электронной документированной информации применяются интранет, электронная почта и службы быстрых сообщений, аудиторы должны удостовериться, что процессы учитывают 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 процессы управления электронной информацией применяются.

В тех случаях, когда организация использует ИТ-инфраструктуру для электронных

коммуникаций с ее потребителями (например, для электронной торговли), внешними поставщиками (электронные закупки), внешними сайтами и иными заинтересованными сторонами, аудитор должен убедиться, что методология и процессы для такого рода коммуникаций и связанных с ними операций разработаны.

8. Распределенные системы менеджмента

Организации, которые осуществляют деятельность на нескольких производственных площадках (или по схеме центр – региональные единицы) обычно осуществляют взаимодействие и процессы общего доступа, а также хранят данные процессов с различных мест при помощи электронных средств, таких как интранет, экстранет, электронная почта и службы быстрых сообщений.

В тех случаях, когда ИТ-платформа 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 система электронной документированной информации критериям аудита.

Аудиторы должны убедиться в том, что средства управления для распределенной системы менеджмента соответствующим образом учтены и включены в процессы организации.

9. Компетентность аудитора

Надежность процесса аудита системы электронной документированной информации 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.

Проверяющие организации должны предпринять необходимые меры, включая проведение тренингов, чтобы учесть общие и индивидуальные потребности своих аудиторов в отношении:

- основных тенденций в развитии информационных технологий, которые могут оказывать влияние на функционирование систем менеджмента,

- вопросов, связанных с конкретным аудитом.

Т.к. инновации в сфере ИТ происходят быстрее, чем изменения в критериях аудита, то от аудиторов и проверяющих организаций требуется иметь практическое понимание соответствующих тенденций и того, каким образом они могут быть примененными и использованы в системе электронной документированной информации.

В свете инноваций, которые влияют на функционирование системы электронной документированной информации, проверяющая организация должна определить, имеет ли назначенная на конкретный аудит команда необходимый для результативной работы опыт или же нужна помощь технических экспертов.

Для более подробной информации о ISO 9001 Auditing Practices Group посмотрите, пожалуйста, документ *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 ***Группой по практикам аудита на соответствие ISO 9001*** (***ISO 9001 Auditing Practices Group)***.

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

charles.corrie@bsigroup.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 форумом по аккредитации (IAF).

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