
Руководящие указания по аудиту систем менеджмента

Lignes directrices pour l'audit des systèmes de management

Логотип ISO

Номер для ссылки
ISO 19011:2018

© ISO 2018

Заявление о защите авторских прав

Содержание

Страница

Предисловие.....	v
Введение	vi
1 Область применения	1
2 Нормативные ссылки	1
3 Термины и определения	1
4 Принципы аудита	6
5 Управление программой аудита.....	7
5.1 Общие положения.....	7
5.2 Определение целей программы аудита	10
5.3 Определение и оценка рисков и возможностей, связанных с программой аудита	10
5.4 Разработка программы аудита	11
5.4.1 Роли и обязанности лиц(а), управляющих(его) программой аудита	11
5.4.2 Компетентность лиц(а), управляющих(его) программой аудита	12
5.4.3 Определение объема программы аудита.....	12
5.4.4 Определение ресурсов для выполнения программы аудита	13
5.5 Выполнение программы аудита	14
5.5.1 Общие положения.....	14
5.5.2 Определение целей, области и критериев для конкретного аудита	14
5.5.3 Выбор и определение методов аудита.....	15
5.5.4 Выбор членов группы по аудиту	16
5.5.5 Назначение обязанностей руководителя группы по аудиту для конкретного аудита	17
5.5.6 Управление результатами выполнения программы аудита	18
5.5.7 Управление записями по программе аудита	18
5.6 Мониторинг программы аудита	19
5.7 Пересмотр и улучшение программы аудита	19
6 Проведение аудита	20
6.1 Общие положения.....	20
6.2 Инициирование аудита.....	20
6.2.1 Общие положения.....	20
6.2.2 Установление контакта с проверяемой организацией	20
6.2.3 Определение возможности проведения аудита	21
6.3 Подготовка к проведению аудита.....	21
6.3.1 Анализ документированной информации	21
6.3.2 Планирование аудита.....	21
6.3.3 Распределение заданий в группе по аудиту	23
6.3.4 Подготовка рабочих документов	23
6.4 Проведение аудита.....	24
6.4.1 Общие положения.....	24
6.4.2 Назначение ролей и обязанностей сопровождающих и наблюдателей.....	24
6.4.3 Проведение открывающего совещания.....	24
6.4.4 Обмен информацией в ходе аудита	25
6.4.5 Места получения информации для аудита и доступ к ней	26
6.4.6 Анализ документированной информации в ходе аудита	26
6.4.7 Сбор и проверка информации	27
6.4.8 Формирование выводов аудита.....	28
6.4.9 Подготовка заключений аудита	28
6.4.10 Проведение заключительного совещания.....	29
6.5 Подготовка и рассылка отчета об аудите.....	30
6.5.1 Подготовка отчета об аудите	30
6.5.2 Рассылка отчета об аудите	31

6.6	Завершение аудита	31
6.7	Выполнение последующих действий	31
7	Компетентность и оценка аудиторов	32
7.1	Общие положения.....	32
7.2	Определение компетентности аудитора	32
7.2.1	Общие положения.....	32
7.2.2	Личные качества	33
7.2.3	Знания и навыки.....	33
7.2.4	Обеспечение компетентности аудитора	36
7.2.5	Обеспечение компетентности руководителя группы по аудиту	37
7.3	Определение критериев оценки аудитора	37
7.4	Выбор соответствующего метода оценки аудитора	37
7.5	Проведение оценки аудитора	38
7.6	Поддержание и повышение компетентности аудитора	38
	Приложение А.....	39
	Библиография	51

Предисловие

ISO (International Organization for Standardization – Международная Организация по Стандартизации) является всемирной федерацией национальных органов по стандартизации (органов-членов ISO). Работа над подготовкой Международных Стандартов выполняется, как правило, техническим комитетом ISO. Каждый орган-член ISO, заинтересованный в цели, для которой был создан технический комитет, имеет право быть представленным в данном комитете. Международные организации, правительственные и неправительственные, поддерживающие связь с ISO, также принимают участие в работе. ISO также тесно сотрудничает с Международной Электротехнической Комиссией (IEC), ведется совместная работа по всем вопросам электротехнической стандартизации.

Процедуры, использованные при разработке этого документа и предназначенные для дальнейшей поддержки, описаны в Директивах ISO/IEC, Часть 1. В частности, должны быть указаны различные критерии утверждения, необходимые для различных типов документов ISO. Настоящий документ был разработан в соответствии с правилами, изложенными в Директивах ISO/IEC, Часть 2 (см. www.iso.org/directives).

Особое внимание уделено тому, что некоторые элементы данного документа могут являться предметом патентных прав. ISO не должна нести ответственность за идентификацию какого-либо или всех подобных патентных прав. Детали, касающиеся любых патентных прав, установленные в ходе разработки документа, должны быть указаны в разделе Введение и/или в листе патентных деклараций ISO (см. www.iso.org/patents).

Все торговые марки, упомянутые в настоящем документе, приведены для удобства пользователей и не означают рекомендации (одобрения).

Для разъяснения значений, используемых ISO специфических терминов и выражений, связанных с оценкой соответствия, равно как и информации о соблюдении ISO принципов соглашения Всемирной Торговой Организации (ВТО) по техническим барьерам в торговле (ТБТ) см. по следующей ссылке: www.iso.org/iso/foreword.html.

Данный документ был подготовлен Техническим Комитетом ISO/PC 302, Руководящие указания по аудиту систем менеджмента.

Эта третья редакция отменяет и заменяет вторую редакцию (ISO 19011:2011), которая была подвергнута техническому пересмотру.

Основные отличия от второй версии:

- добавление риск-ориентированного подхода к принципам аудита;
- расширение руководства по управлению программой аудита, включая риски по программе аудита;
- расширение руководства по проведению аудита, в частности, раздел планирования аудита;
- расширение общих требований к компетентности аудиторов;
- изменение терминологии, использование термина «процесс», а не «объект» («thing»);
- удаление приложения, содержавшего требования к компетентности для проведения аудита конкретных систем менеджмента (в силу значительного числа отдельных стандартов на системы менеджмента было бы нецелесообразно включать требования к компетентности для всех видов систем);
- расширение Приложения А с целью дать рекомендации по аудиту (новых) концепций, таких как контекст организации, лидерство и обязательства, удаленные аудиты, соблюдение требований и цепочка поставки.

Введение

С того времени, когда в 2011 году было опубликовано второе издание данного документа, был издан целый ряд новых стандартов на системы менеджмента, многие из которых имеют общую структуру, общие основные требования, а также общую терминологию и базовые определения. В результате возникла необходимость рассмотреть в более широком плане подход к аудитам систем менеджмента, а также предоставить руководящие указания более общего характера. Результаты аудита могут служить исходными данными для анализа различных аспектов бизнес-планирования, а также могут вносить свой вклад в выявление потребностей и мер для улучшения.

Аудит может проводиться на соответствие ряду критериев, отдельно или в комбинации, включая, но не ограничиваясь, следующее:

- требования, установленные в одном или более стандарте на систему менеджмента;
- политики и требования, установленные соответствующими заинтересованными сторонами;
- законодательные и нормативные требования;
- один или более процессов системы менеджмента, установленных организацией или иными сторонами;
- план(ы) системы менеджмента, связанный(ые) с достижением конкретных результатов системы менеджмента (например, план по качеству, план проекта).

Данный документ содержит руководящие указания, применимые к организациям любого размера и любого типа, а также к аудитам с разными областями и разных масштабов, включая как те, которые проводятся большими группами по аудиту, как правило, в больших организациях, так и те, что проводятся одним аудитором в большой или маленькой организациях. Это руководство должно быть адаптировано в соответствии с областью аудита, сложностью и масштабом программы аудита.

Данный документ концентрируется на внутренних аудитах (первой стороны) и проводимых организациями аудитах внешних поставщиков и других внешних заинтересованных сторон (второй стороны). Данный документ также может быть полезен при проведении внешних аудитов с целью, отличающейся от сертификации системы менеджмента третьей стороной. Стандарт ISO/IEC 17021-1 устанавливает требования к аудитам систем менеджмента в рамках сертификации третьей стороной; данный документ может дать дополнительные полезные рекомендации (см. Табл. 1).

Таблица 1 — Различные типы аудитов

Аудит первой стороны	Аудит второй стороны	Аудит третьей стороны
Внутренний аудит	Аудит внешнего поставщика	Аудит с целью сертификации и/или аккредитации
	Аудит других внешних заинтересованных сторон	Аудит соблюдения законодательных, нормативных и иных подобных требований

Чтобы повысить читаемость данного документа в нем, как правило, используется единственная форма термина «система менеджмента», но читатель может адаптировать применение руководящих указаний к своей собственной ситуации. Это также применимо к использованию терминов «лицо» и «лица», «аудитор» и «аудиторы».

Предполагается применение данного документа широким диапазоном возможных пользователей,

включая аудиторов, организации, внедряющие систему менеджмента, и организации, нуждающиеся в проведении аудитов систем менеджмента в силу контрактных или законодательных требований. Пользователи данного документа могут, однако, применять эти руководящие указания при разработке собственных требований, связанных с аудитами.

Руководящие указания данного документа могут быть также использованы в целях самодекларации и могут быть полезны организациям, занимающимся подготовкой аудиторов или сертификацией персонала.

Предполагается, что руководящие указания данного документа будут гибкими. Как указано в различных местах текста, применение данных указаний может различаться в зависимости от размера и уровня зрелости системы менеджмента организации. Следует принимать во внимание характер и сложность проверяемой организации, а также цели и область проводимого аудита.

Данный документ включает в себя концепцию комбинированного аудита, когда совместно проверяются две или более различных системы менеджмента. В тех случаях, когда эти системы интегрированы в одну, принципы и процессы аудита остаются теми же самыми, что и для комбинированного аудита (иногда называемого интегрированным аудитом).

Данный документ дает указания по управлению программой аудита, планированию и проведению аудитов системы менеджмента, а также по компетентности и оценке аудиторов и команд аудиторов.

Руководящие указания по аудиту систем менеджмента

1 Область применения

Данный документ содержит руководящие указания по аудиту систем менеджмента, в том числе принципы аудита, указания по управлению программой аудита и проведению аудита систем менеджмента, а также по оценке компетентности лиц, участвующих в процессе аудита. Лица, осуществляющие подобную деятельность, включают тех, кто управляет программой аудита, аудиторов и членов группы по аудиту.

Документ применим ко всем организациям, которым необходимо планировать и проводить внутренние или внешние аудиты систем менеджмента или управлять программой аудита.

Применение данного документа к другим типам аудита возможно при условии, что будут учтены специфические требования к компетентности.

2 Нормативные ссылки

Нормативные ссылки в данном документе отсутствуют.

3 Термины и определения

Для целей настоящего документа применяются следующие термины и определения.

ISO и IEC поддерживают терминологическую базу данных для применения в сфере стандартизации по следующим адресам:

- платформа ISO Online browsing platform: доступна на <http://www.iso.org/obp>
- IEC Electropedia: доступна на <http://www.electropedia.org/>.

3.1

аудит (audit)

систематический, независимый и документированный процесс для получения *объективного свидетельства* (3.8) и его объективной оценки для определения степени, с которой выполнены *критерии аудита* (3.7)

Примечание 1 к определению: Внутренние аудиты, называемые иногда аудитами первой стороны, выполняются самой организацией или в ее интересах.

Примечание 2 к определению: Внешние аудиты включают те, что обычно называют аудитами второй и третьей стороны. Аудиты второй стороны проводятся сторонами, заинтересованными в деятельности организации, например, потребителями или другими лицами в собственных интересах. Аудиты третьей стороны проводятся внешними независимыми проверяющими организациями, например, такими, которые осуществляют сертификацию/регистрацию соответствия, или государственными учреждениями.

[ИСТОЧНИК: ISO 9000:2015, 3.13.1, измененный – примечания к определениям были изменены]

3.2

комбинированный аудит (combined audit)

аудит (3.1), проводимый в одной *проверяемой организации* (3.13) в отношении двух или более *систем менеджмента* (3.18)

Примечание 1 к определению: Если две и более разных систем менеджмента объединены в одну систему менеджмента, то она называется интегрированной системой менеджмента.

[ИСТОЧНИК: ISO 9000:2015, 3.13.2, измененный]

3.3

совместный аудит (joint audit)

аудит (3.1), проводимый в одной *проверяемой организации* (3.13) двумя или более проверяющими организациями

[ИСТОЧНИК: ISO 9000:2015, 3.13.3]

3.4

программа аудита (audit programme)

мероприятия для одного или нескольких *аудитов* (3.1), запланированных на конкретный период времени и направленных на достижение конкретной цели

[ИСТОЧНИК: ISO 9000:2015, 3.13.4, измененный – формулировка определения дополнена]

3.5

область аудита (audit scope)

объем и границы *аудита* (3.1)

Примечание 1 к определению: Область аудита, как правило, включает указание на физическое или виртуальное местонахождение, функции, подразделения организации, виды деятельности и процессы, а также планируемый период времени.

Примечание 2 к определению: Виртуальное местонахождение – это то, где организация выполняет работы или оказывает услуги, используя онлайн режим, давая возможность людям выполнять процессы вне зависимости от физического местонахождения.

[ИСТОЧНИК: ISO 9000:2015, 3.13.5, измененный – Примечание 1 изменено, добавлено Примечание 2]

3.6

план аудита (audit plan)

описание мероприятий и порядка проведения *аудита* (3.1)

[ИСТОЧНИК: ISO 9000:2015, 3.13.6]

3.7

критерии аудита (audit criteria)

совокупность *требований* (3.23), используемых как эталон, с которым сравнивается *объективное свидетельство* (3.8)

Примечание 1 к определению: Если критериями аудита являются юридические (в том числе законодательные или нормативные) требования, то в *выводах аудита* (3.10) часто используются формулировки «соблюдение» или «не соблюдение».

Примечание 2 к определению: Требования могут выступать в форме политик, процедур, рабочих инструкций, законодательных требований, контрактных обязательств и т.д.

[ИСТОЧНИК: ISO 9000:2015, 3.13.7, измененный – определение было изменено и добавлены Примечания 1 и 2]

3.8

объективное свидетельство (objective evidence)

данные, подтверждающие существование или истинность чего-либо

Примечание 1 к определению: Объективное свидетельство может быть получено посредством наблюдения, измерения, испытания или других методов.

Примечание 2 к определению: Объективное свидетельство в рамках *аудита* (3.1) обычно содержит записи, изложение фактов или иную информацию, которая существенна с точки зрения *критериев аудита* (3.7) и может быть проверена.

[ИСТОЧНИК: ISO 9000:2015, 3.8.3]

3.9

свидетельство аудита (audit evidence)

записи, изложение фактов или иная информация, которая существенна с точки зрения *критериев аудита* (3.7) и может быть проверена

[ИСТОЧНИК: ISO 9000:2015, 3.13.8]

3.10

выводы аудита (audit findings)

результаты оценки собранных *свидетельств аудита* (3.9) на соответствие *критериям аудита* (3.7)

ПРИМЕЧАНИЕ 1 к определению: Выводы аудита констатируют *соответствие* (3.20) или *несоответствие* (3.21).

ПРИМЕЧАНИЕ 2 к определению: На основании выводов аудита могут выявляться риски, возможности для улучшения или стандартизации лучших практик.

ПРИМЕЧАНИЕ 3 к определению: В редакции на английском языке если в качестве критериев аудита выступают законодательные или нормативные требования, то вывод аудита формулируется в терминах соблюдения (compliance)/несоблюдения (non-compliance).

[ИСТОЧНИК: ISO 9000:2015, 3.13.9, измененный – изменены Примечания 2 и 3]

3.11

заключение аудита (audit conclusion)

результат *аудита* (3.1), формируемый после рассмотрения целей аудита и всех *выводов аудита* (3.10)

[ИСТОЧНИК: ISO 9000:2015, 3.13.10]

3.12

заказчик аудита (audit client)

организация или лицо, запросившее *аудит* (3.1)

Примечание 1 к определению: В случае внутреннего аудита заказчиком аудита может быть сама *проверяемая организация* (3.13) или лицо(а), управляющее(ие) программой аудита. Запросы на внешний аудит могут поступать из таких источников, как регулирующие органы, стороны контракта или потенциальные или существующие заказчики.

[ИСТОЧНИК: ISO 9000:2015, 3.13.11, измененный – добавлено Примечание 1]

3.13

проверяемая организация (auditee)

организация, во всей или части которой проводится аудит

[ИСТОЧНИК: ISO 9000:2015, 3.13.12, измененный]

3.14

группа по аудиту (audit team)

одно лицо или более, проводящее(их) *аудит* (3.1) при поддержке, если необходимо, *технических экспертов* (3.16)

ПРИМЕЧАНИЕ 1 к определению: Один из *аудиторов* (3.15) *группы по аудиту* (3.14) назначается руководителем группы по аудиту.

ПРИМЕЧАНИЕ 2 к определению: В группу по аудиту могут включаться аудиторы-стажеры.

[ИСТОЧНИК: ISO 9000:2015, 3.13.14]

3.15

аудитор (auditor)

лицо, проводящее *аудит* (3.1)

[ИСТОЧНИК: ISO 9000:2015, 3.13.15]

3.16

технический эксперт (technical expert)

<аудит> лицо в *группе по аудиту* (3.14), обладающее знаниями или практическим опытом в конкретной области

ПРИМЕЧАНИЕ 1 к определению: Знания или опыт в конкретной области связаны с проверяемой организацией, деятельностью, процессом, продуктом, услугой, направлением менеджмента, в отношении которых должен быть проведен аудит, или языком и культурными особенностями.

ПРИМЕЧАНИЕ 2 к определению: Технический эксперт в *группе по аудиту* (3.14) не выполняет функций *аудитора* (3.15).

[ИСТОЧНИК: ISO 9000:2015, 3.13.16, измененный – изменены Примечания 1 и 2]

3.17

наблюдатель (observer)

лицо, сопровождающее *группу по аудиту* (3.14), но не выполняющее функций *аудитора* (3.15)

[ИСТОЧНИК: ISO 9000:2015, 3.13.17, измененный]

3.18

система менеджмента (management system)

совокупность взаимосвязанных или взаимодействующих элементов организации для разработки политик и целей, а также *процессов* (3.24) для достижения этих целей

ПРИМЕЧАНИЕ 1 к определению: Система менеджмента может относиться к одной или нескольким сферам, например, менеджмент качества, финансовый или экологический менеджмент.

ПРИМЕЧАНИЕ 2 к определению: Элементы системы менеджмента определяют структуру организации, роли и обязанности, планирование, функционирование, политики, процедуры, правила, принципы, цели и процессы для достижения этих целей.

ПРИМЕЧАНИЕ 3 к определению: Область действия системы менеджмента может включать всю организацию, определенные и идентифицированные функции организации, определенные и идентифицированные части организации, или одну или более сквозных функций, выполняемых в рамках группы организаций.

[ИСТОЧНИК: ISO 9000:2015, 3.5.3, измененный – удалено Примечание 4]

3.19

риск (risk)

влияние неопределенности

Примечание 1 к определению: Влияние – это отклонение от ожидаемого – положительное или отрицательное.

Примечание 2 к определению: Неопределенность – состояние, даже частичной, недостаточности информации, связанное с пониманием события или знанием о нем, его последствий и вероятности.

Примечание 3 к определению: Риск часто характеризуется указанием возможных событий (определено в п. 3.5.1.3 ISO Guide 73:2009) и последствий (определено в п. 3.6.1.3 ISO Guide 73:2009), или их комбинации.

Примечание 4 к определению: Риск часто выражается в форме комбинации последствий события (включая

изменения в обстоятельствах) и связанной с ним вероятности (определено в п. 3.6.1.1 ISO Guide 73:2009) возникновения.

[ИСТОЧНИК: ISO 9000:2015, 3.7.9, измененный – удалены Примечания 5 и 6]

3.20

соответствие (conformity)

выполнение *требования* (3.23)

[ИСТОЧНИК: ISO 9000:2015, 3.6.11, измененный – удалено Примечание 1]

3.21

несоответствие (nonconformity)

невыполнение *требования* (3.23)

[ИСТОЧНИК: ISO 9000:2015, 3.6.9, измененный – удалено Примечание 1]

3.22

компетентность (competence)

способность применять знания и навыки для достижения намеченных результатов

[ИСТОЧНИК: ISO 9000:2015, 3.10.4, измененный – удалены примечания]

3.23

требование (requirement)

потребность или ожидание, которое установлено, обычно предполагается или является обязательным

Примечание 1 к определению: "Обычно предполагается" означает, что это специфическая или общепринятая практика для организации и заинтересованных сторон, когда рассматриваемые потребности или ожидания предполагаются.

Примечание 2 к определению: Установленным требованием является такое требование, которое определено, например, в документированной информации.

[ИСТОЧНИК: ISO 9000:2015, 3.6.4, измененный – удалены Примечания 3, 4, 5 и 6]

3.24

процесс (process)

совокупность взаимосвязанных или взаимодействующих видов деятельности, которая использует входы для производства запланированного результата

[ИСТОЧНИК: ISO 9000:2015, 3.4.1, измененный – удалены примечания]

3.25

показатель деятельности (performance)

измеримый результат

Примечание 1 к определению: Показатель деятельности может быть связан как с количественными, так и качественными результатами.

Примечание 2 к определению: Показатель деятельности может относиться к управлению задачами, *процессами* (3.24), продуктами, услугами, системами или организациями.

[ИСТОЧНИК: ISO 9000:2015, 3.7.8, измененный – удалено Примечание 3]

3.26

результативность (effectiveness)

степень, с которой запланированные задачи выполнены и запланированные результаты достигнуты

[ИСТОЧНИК: ISO 9000:2015, 3.7.11, измененный – удалено Примечание 1]

4 Принципы аудита

Аудит основывается на ряде принципов. Эти принципы должны помочь сделать аудит результативным и надежным инструментом поддержки политик руководства и средств управления, предоставляя информацию, которую организация может задействовать в целях улучшения результатов ее деятельности. Соблюдение этих принципов является необходимым условием для формирования значимых и достаточных заключений аудита и позволяющим аудиторам, работающим независимо друг от друга, делать схожие заключения в аналогичных обстоятельствах.

Руководящие указания, данные в разделах 5 – 7, основаны на семи принципах, изложенных ниже.

а) **Безупречность:** основа профессионализма

Аудиторам и лицу(ам), управляющему(им) программой аудита, следует:

- выполнять свою работу с соблюдением этических норм, честно и ответственно;
- делать на аудите только то, в чем компетентен;
- выполнять свою работу непредвзято, т.е. оставаться справедливым и беспристрастным во всех своих действиях;
- реагировать на любые вмешательства, которые могут повлиять на их суждения в ходе аудита.

б) **Объективное представление:** обязательство предоставлять правдивый и точный отчет

Выводы, заключения аудита и отчеты по аудиту должны точно и правдиво отражать ход аудита. Существенные затруднения, встретившиеся при аудите, и оставшиеся расхождения во мнениях между группой по аудиту и проверяемой организацией должны быть зафиксированы. Обмен информацией должен быть правдивым, точным, объективным, своевременным, ясным и полным.

в) **Надлежащее профессиональное усердие:** старательность и рассудительность в ходе аудита

Аудиторам следует проявлять должное усердие в соответствии с важностью задачи, которую они выполняют, и доверием, оказанным им заказчиком аудита и другими заинтересованными сторонами. Важным фактором при выполнении их работы с надлежащим профессиональным усердием является способность принимать обоснованные решения в любых ситуациях, возникающих в ходе аудита.

г) **Конфиденциальность:** неразглашение информации

Аудиторам следует проявлять осмотрительность в использовании и защите информации, полученной в ходе исполнения своих обязанностей. Информация по аудиту не должна использоваться аудитором или заказчиком аудита ненадлежащим образом для получения личной выгоды или для нанесения ущерба законным интересам проверяемой организации. Это положение относится и к надлежащему обращению с особо важной и конфиденциальной информацией.

е) **Независимость:** основа беспристрастности аудита и объективности заключений по аудиту

Аудиторы должны быть независимы от ими проверяемой деятельности, где это практически возможно, и во всех случаях действовать таким образом, чтобы быть свободными от предвзятости и конфликта интересов. В случае внутренних аудитов аудиторы должны быть независимы от проверяемых функций, если это практически возможно. Аудиторы должны сохранять объективность в течение всего процесса аудита, чтобы гарантировать, что выводы и заключения аудита основаны только на свидетельствах аудита.

В малых организациях не всегда можно обеспечить полную независимость внутренних аудиторов в

отношении проверяемой деятельности, но должны быть предприняты все усилия, чтобы исключить предвзятость и поддерживать объективность.

ф) Подход, основанный на свидетельствах: рациональный метод получения надежных и воспроизводимых заключений аудита в ходе систематического процесса аудита

Свидетельства аудита должны быть проверяемы. Как правило, они основаны на выборках из имеющейся информации, поскольку аудит проводится в ограниченное время и с ограниченными ресурсами. Следует применять соответствующие методы формирования выборки, т.к. это тесно связано с уровнем доверия к заключению по аудиту.

г) Риск-ориентированный подход: подход к аудиту, при котором рассматриваются риски и возможности

Риск-ориентированный подход должен оказывать существенное влияние на планирование, проведение аудитов и отчетность по аудитам с целью гарантии того, что аудиты были сосредоточены на вопросах, важных для заказчика аудита и для достижения целей программы аудита.

5 Управление программой аудита

5.1 Общие положения

Должна быть разработана программа аудита, которая может включать в себя аудиты, ориентированные на один или несколько стандартов на системы менеджмента, проводимых либо по отдельности, либо в комбинации (комбинированный аудит).

Объем программы аудита должен зависеть от размера и характера проверяемой организации, а также от характера, функционального назначения, сложности, типа рисков и возможностей и уровня зрелости систем(ы) менеджмента, подлежащих проверке.

Функционирование системы менеджмента может быть еще более сложным, когда большинство важных функций передаются на аутсорсинг и управляются под руководством других организаций. Особое внимание необходимо уделить тому, где принимаются наиболее важные решения и кто составляет высшее руководство системы менеджмента.

В случае нескольких мест нахождения/площадок (например, в разных странах) или где важные функции передаются на аутсорсинг и управляются под руководством другой организации, особое внимание следует уделять разработке, планированию и подтверждению программы аудита.

В случае небольших или менее сложных организаций программа аудита может быть масштабирована соответствующим образом.

Чтобы понять контекст проверяемой организации, программа аудита должна учитывать:

- цели организации;
- соответствующие внешние и внутренние факторы;
- потребности и ожидания соответствующих заинтересованных сторон;
- требования к информационной безопасности и конфиденциальности.

Планирование программ внутреннего аудита и, в некоторых случаях, программ аудита внешних поставщиков может быть выполнено для достижения и других целей организации.

Лицо (лица), управляющее(ие) программой аудита, должно гарантировать, что обеспечивается

целостность аудита и что не оказывается неправомерного влияния в ходе аудита.

Приоритет при аудите должен быть отдан выделению ресурсов и выбору методов для элементов системы менеджмента с более высоким уровнем риска и более низким уровнем показателей деятельности.

Для управления программой аудита должны быть назначены компетентные лица.

Программа аудита должна включать информацию и определять ресурсы, позволяющие результативно и эффективно проводить аудит в указанные сроки. Информация должна включать:

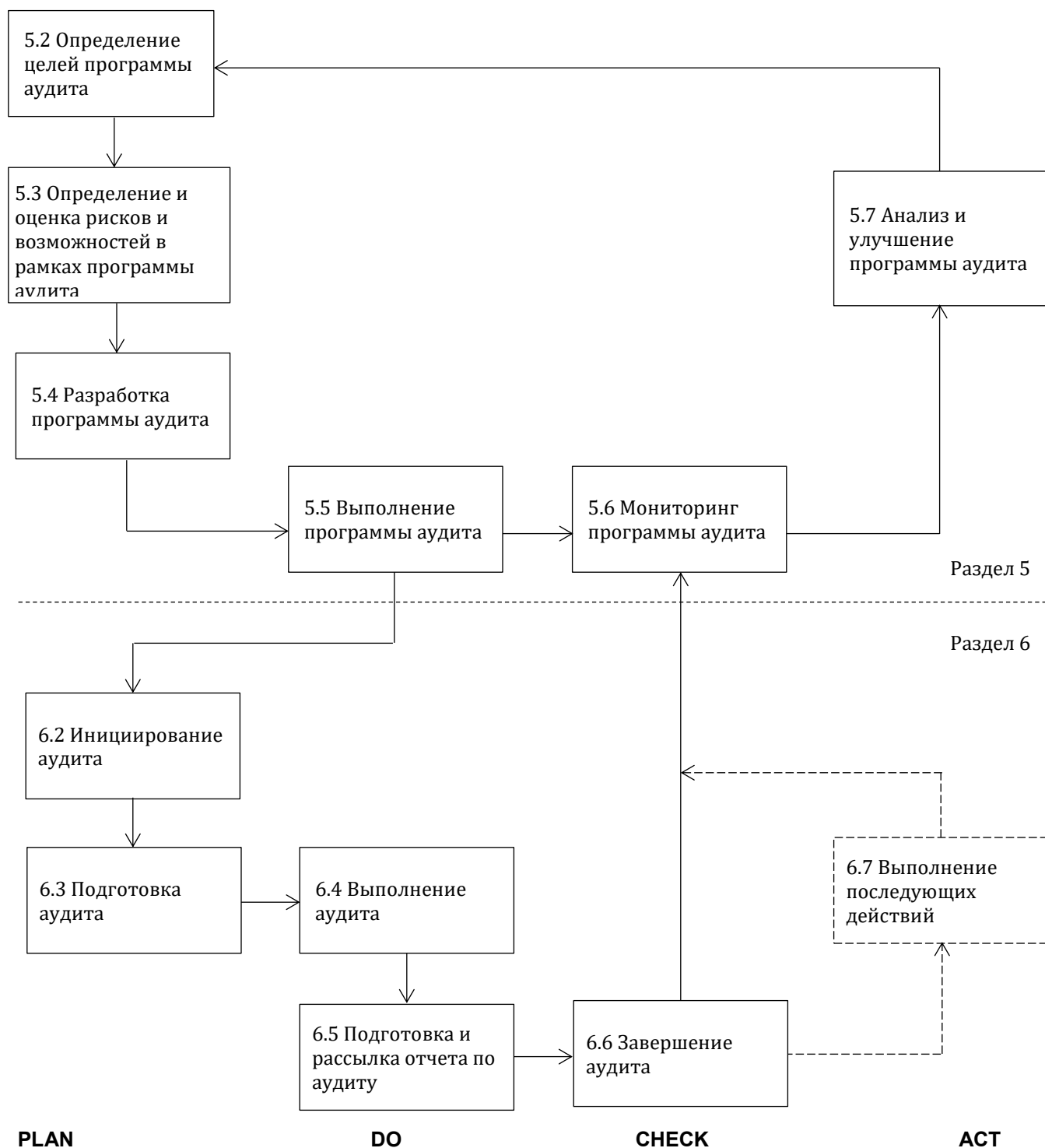
- a) цели программы аудита;
- b) риски и возможности, связанные с программой аудита (см. 5.3), и действия по их обработке;
- c) область (объем, границы, места) каждого аудита в рамках программы аудита;
- d) график (количество/продолжительность/частота) аудитов;
- e) типы аудита, например, внутренние или внешние;
- f) критерии аудита;
- g) методы аудита, которые будут использоваться;
- h) критерии отбора членов группы по аудиту;
- i) соответствующую документированную информацию.

Некоторая часть этой информации может быть недоступна до тех пор, пока не будет завершено более подробное планирование аудита.

Осуществление программы аудита должно контролироваться и оцениваться на постоянной основе (см. 5.6) для обеспечения достижения его целей. Программа аудита должна пересматриваться с целью выявления потребностей в изменениях и потенциальных возможностях для улучшения (см. 5.7).

Рисунок 1 иллюстрирует блок-схему процессов управления программой аудита.

PLAN DO CHECKACT



ПРИМЕЧАНИЕ 1 Этот рисунок показывает применение цикла PDCA в данном документе.

ПРИМЕЧАНИЕ 2 На схеме указаны номера соответствующих разделов/подразделов данного документа

Рисунок 1 - Блок-схема управления программой аудита

5.2 Определение целей программы аудита

Заказчик аудита должен гарантировать, что цели программы аудита для управления планированием и проведением аудитов установлены, и должен обеспечить результативное выполнение программы аудита. Цели программы аудита должны быть согласованы со стратегией развития заказчика аудита, а также быть связаны с политикой и целями системы менеджмента.

Эти цели могут устанавливаться с учетом следующего:

- a) потребностей и ожиданий соответствующих заинтересованных сторон, как внешних, так и внутренних;
- b) характеристик процессов и требований к процессам, продуктам, услугам и проектам, а также любых изменений в них;
- c) требований к системе менеджмента;
- d) необходимости в оценке внешних поставщиков;
- e) уровня функционирования проверяемой организации и уровня зрелости систем(ы) менеджмента, отражаемых соответствующими показателями деятельности (например, KPI), статистикой несоответствий или инцидентов, или претензий от заинтересованных сторон;
- f) выявленных в проверяемой организации рисков и возможностей;
- g) результатов предыдущих аудитов.

Примеры целей программы аудита включают в себя следующее:

- выявить возможности улучшения системы менеджмента и ее функционирования;
- оценить способность проверяемой организации определять ее контекст;
- оценить способность проверяемой организации определять риски и возможности, а также разрабатывать и осуществлять результативные меры по их обработке;
- подтвердить выполнение всех соответствующих требований, т.е. законодательных и нормативных требований, обязательств по соблюдению, требований в рамках сертификации на соответствие стандарту на систему менеджмента;
- получить и поддерживать уверенность в возможностях внешнего поставщика;
- оценить постоянную пригодность, соответствие и результативность системы менеджмента проверяемой организации;
- оценить согласованность целей системы менеджмента со стратегическим направлением развития организации.

5.3 Определение и оценка рисков и возможностей, связанных с программой аудита

Существуют различные риски и возможности, связанные с контекстом проверяемой организации, которые могут повлиять на программу аудита и на достижение поставленных в ней целей. Лицу(ам), управляющему(им) программой аудита, следует выявить и донести до проверяемой организации риски и возможности, учитываемые при разработке программы аудита и требований к ресурсам, с тем, чтобы по ним были приняты надлежащие меры.

Риски могут быть связаны с:

- a) планированием, например, неверным заданием соответствующих целей аудита и определением объема, количества, продолжительности, мест проведения и графика аудитов;
- b) ресурсами, например, с тем, что предусмотрено недостаточно времени, оснащенности и/или подготовки для разработки программы аудита или проведения аудита;
- c) выбором группы по аудиту, например, недостаточностью общей компетентности для результативного проведения аудитов;
- d) коммуникацией, например, плохо работающими процессами/каналами внутреннего/внешнего обмена информацией;
- e) реализацией, например, ненадлежащей координацией в рамках программы аудита или недостаточным вниманием к вопросам информационной безопасности и конфиденциальности;
- f) управлением документированной информацией, например, неверным определением необходимой документированной информации, требуемой аудиторам и соответствующим заинтересованным сторонам, неспособностью соответствующим образом сохранять записи аудита, чтобы продемонстрировать результативность программы аудита;
- g) мониторингом, анализом и улучшением программы аудита, например, неудовлетворительным мониторингом результатов программы аудита;
- h) доступностью и готовностью к сотрудничеству проверяемой организации и доступностью свидетельств, которые должны быть собраны.

Возможности могут включать в себя:

- возможность проведения нескольких аудитов за один раз;
- минимизацию времени и расстояния при переезде с одного места на другое;
- соответствие уровня компетентности группы по аудиту уровню компетентности, требуемому для достижения целей аудита;
- согласование дат проведения аудита с доступностью ключевых сотрудников проверяемой организации.

5.4 Разработка программы аудита

5.4.1 Роли и обязанности лиц(а), управляющих(его) программой аудита

Лицо(а), управляющее(ие) программой аудита, должно:

- a) установить объем программы аудита, соответствующий значимым целям (см. 5.2) и любым известным ограничениям;
- b) определить внешние и внутренние факторы, а также риски и возможности, которые могут повлиять на программу аудита, осуществить меры по их обработке, встраивая эти меры во все соответствующие мероприятия по аудиту, насколько это возможно;
- c) обеспечить формирование группы по аудиту и общую компетентность в рамках мероприятий по аудиту, назначив роли, обязанности и полномочия, а также следуя принципу лидерства, насколько это применимо;
- d) разработать все существенные процессы, включая процессы для:

- координации и формирования графика всех аудитов в рамках программы аудита;
- установления целей аудита, области(ей) и критериев аудитов, определения методов аудита и формирования группы по аудиту;
- оценки аудиторов;
- разработки процессов внутренних и внешних коммуникаций, в зависимости от ситуации;
- разрешения споров и обработки претензий;
- последующих после аудита действий, если это применимо;
- отчетности заказчику аудита и соответствующим заинтересованным сторонам, при необходимости.

- e) определить и гарантировать обеспечение всеми необходимыми ресурсами;
- f) гарантировать, что соответствующая документированная информация подготовлена и управляется, в том числе и записи по аудиту;
- g) осуществлять мониторинг, анализ и улучшение программы аудита;
- h) передавать программу аудита заказчику аудита и, при необходимости, соответствующим заинтересованным сторонам.

Лицу(ам), управляющему(им) программой аудита, следует запросить у заказчика аудита одобрение программы.

5.4.2 Компетентность лиц(а), управляющих(его) программой аудита

Лицо(а), управляющее(ие) программой аудита, должно обладать необходимой компетентностью для результативного и эффективного управления программой и связанными с нею рисками и возможностями, внешними и внутренними факторами, включая знание:

- a) принципов аудита (см. раздел 4), методов и процессов (см. A.1 и A.2);
- b) стандартов на системы менеджмента, иных соответствующих стандартов и нормативных/руководящих документов;
- c) информации, связанной с проверяемой организацией и ее контекстом (например, внешние/внутренние факторы, соответствующие заинтересованные стороны, их потребности и ожидания, виды деятельности, продукты, услуги и процессы);
- d) применимых законодательных, нормативных и других требований, относящихся к деятельности проверяемой организации.

В зависимости от ситуации, может приниматься во внимание знание риск-менеджмента, управления проектами и процессами, а также информационно-коммуникационных технологий (ИКТ).

Лицо(а), управляющее(ие) программой аудита, должно участвовать в соответствующих постоянных мероприятиях по профессиональному развитию для поддержания необходимых знаний и навыков управления программой аудита.

5.4.3 Определение объема программы аудита

Лицо(а), управляющее(ие) программой аудита, должно определить объем программы аудита. Он может варьироваться в зависимости от информации, предоставленной проверяемой организацией относительно ее контекста (см. 5.3).

ПРИМЕЧАНИЕ В некоторых случаях, в зависимости от структуры проверяемой организации или ее деятельности, программа аудита может состоять только из одного аудита (например, небольшой проект или организация).

Другие факторы, влияющие на объем программы аудита, могут включать в себя следующее:

- a) цель, область и продолжительность каждого аудита и количество аудитов, которые должны быть проведены, способы отчетности и, если применимо, последующие действия;
- b) стандарты на системы менеджмента или иные применимые критерии;
- c) количество, важность, сложность, степень сходства и места выполнения видов деятельности, подлежащих аудиту;
- d) факторы, влияющие на результативность системы управления;
- e) применимые критерии аудита, такие как запланированные в рамках соответствующих стандартов на системы менеджмента мероприятия, законодательные, нормативные и другие требования, выполнять которые обязалась организация;
- f) результаты предыдущих внутренних или внешних аудитов, а также анализа руководства, насколько это применимо;
- g) результаты анализа ранее разработанных программ аудита;
- h) язык, вопросы культурной и социальной сферы;
- i) проблемы, указываемые заинтересованными сторонами, такие как претензии потребителей, несоблюдение законодательных, нормативных и иных требований, выполнять которые обязалась организация, или проблемы в цепи поставок;
- j) существенные изменения в контексте проверяемой организации или ее деятельности, а также соответствующих рисках и возможностях;
- k) наличие информационно-коммуникационных технологий для поддержки мероприятий аудита, в частности, использование дистанционных методов аудита (см. раздел A.16);
- l) наличие событий, имевших место как внутри организации, так и за ее пределами, таких как несоответствия продуктов или услуг, утечка информации, несчастные случаи на производстве, инциденты криминального или экологического характера;
- m) бизнес-риски и возможности, включая меры по их обработке.

5.4.4 Определение ресурсов для выполнения программы аудита

При определении ресурсов для программы аудита, лицу(ам), управляющему(им) программой аудита, следует принять во внимание:

- a) финансовые и временные ресурсы, необходимые для разработки, выполнения, управления и улучшения мероприятий по аудиту;
- b) методы аудита (см. раздел A.1);
- c) наличие вообще или конкретных аудиторов и технических экспертов, обладающих компетентностью, соответствующей конкретным целям программы аудита;
- d) объем программы аудита (см. 5.4.3), риски и возможности, связанные с программой аудита (см. 5.3);
- e) время на проезд и стоимость, проживание и другие потребности, связанные с аудитом;
- f) влияние разницы во времени;

- г) наличие информационно-коммуникационных технологий (например, технических ресурсов, необходимых для проведения дистанционного аудита с использованием технологий, обеспечивающих удаленную совместную работу);
- h) наличие любого требуемого инструментария, технологий и оборудования;
- i) наличие необходимой документированной информации, определенной на этапе разработки программы аудита (см. А.5);
- j) требования, связанные с условиями на объекте аудита, включая любые допуски и оснащение (например, проверка анкетных данных, индивидуальные средства защиты, умение пользоваться специальной одеждой для соблюдения режима чистой комнаты).

5.5 Выполнение программы аудита

5.5.1 Общие положения

После разработки программы аудита (см. 5.4.3) и определения необходимых ресурсов требуется осуществить оперативное планирование и координацию всех мероприятий в рамках этой программы.

Лицо(а), управляющее(ие) программой аудита, должно:

- a) довести до сведения соответствующих заинтересованных сторон касающиеся их части программы аудита, включая связанные с ней риски и возможности, и периодически информировать их о состоянии дел, используя установленные каналы для внутренних и внешних коммуникаций;
- b) определить цели, область и критерии каждого отдельного аудита;
- c) выбрать методы аудита (см. А.1);
- d) координировать и определять график аудитов и других мероприятий, имеющих отношение к программе аудита;
- e) обеспечить необходимую компетентность групп по аудиту (см. 5.5.4);
- f) обеспечить необходимые ресурсы для групп по аудиту, как для отдельных членов группы, так и в целом для всей группы;
- g) обеспечить проведение аудитов в соответствии с программой аудита, управляя всеми операционными рисками, возможностями и проблемами (например, неожиданными событиями) по мере их возникновения в ходе развертывания программы аудита;
- h) гарантировать, что соответствующая документированная информация, связанная с мероприятиями аудита, должным образом управляется и поддерживается;
- i) определить и внедрить рабочие процедуры (см. 5.6), необходимые для мониторинга программы аудита;
- j) анализировать программу аудита с целью выявления возможностей ее улучшения (см. 5.7).

5.5.2 Определение целей, области и критериев для конкретного аудита

Для каждого отдельного аудита должны быть установлены цели, область и критерии аудита. Они должны соответствовать общим целям программы аудита.

Цели аудита определяют, что должно быть достигнуто в рамках конкретного аудита, и могут включать в себя следующее:

- a) определение степени соответствия проверяемой системы менеджмента или ее части критериями аудита;

- b) оценка способности системы менеджмента способствовать организации соблюдению соответствующих законодательных, нормативных и других требований, которые организация обязалась выполнять;
- c) оценка результативности системы менеджмента в достижении ожидаемых в ее рамках результатов;
- d) выявление возможностей улучшения системы менеджмента;
- e) оценка пригодности и адекватности системы менеджмента с учетом контекста и стратегического направления развития проверяемой организации;
- f) оценка способности системы менеджмента устанавливать и достигать целей и результативно обрабатывать риски и возможности в условиях меняющегося контекста, включая осуществление соответствующих мероприятий.

Область аудита должна соответствовать программе и целям аудита. Она включает в себя такие элементы, как местонахождение, функции, виды деятельности и процессы, подлежащие аудиту, а также период времени, в который проводится аудит.

Критерии аудита используются в качестве эталона, по которому определяется соответствие. Они могут включать в себя одно или несколько элементов из следующего перечня: применимые политики, процессы, процедуры, критерии результативности, в том числе цели, законодательные и нормативные требования, требования системы менеджмента, информация, связанная с контекстом, рисками и возможностями, установленная проверяемой организацией (включая требования соответствующих внешних/внутренних заинтересованных сторон), отраслевые кодексы поведения или иные запланированные мероприятия.

В случае каких-либо изменений в целях, области или критериях аудита программу аудита следует отредактировать, если это необходимо, и передать заинтересованным сторонам для одобрения, если это необходимо.

Когда проводится аудит по более чем одному направлению менеджмента в одно и то же время, важно, чтобы цели, область и критерии аудита были согласованными в рамках соответствующих программ аудита по каждому направлению. Некоторые системы менеджмента могут иметь область аудита, покрывающую всю организацию, а другие могут иметь область, которая затрагивает часть организации.

5.5.3 Выбор и определение методов аудита

Лицо(а), управляющее(ие) программой аудита, должно выбрать и определить методы для результативного и эффективного проведения аудита, в зависимости от установленной цели, области и критериев аудита.

Аудиты могут проводиться на месте, удаленно или с сочетанием того и другого. Применение этих методов должно быть должным образом сбалансировано с учетом, кроме всего прочего, связанных рисков и возможностей.

Если две или более аудиторских организации проводят совместный аудит одной и той же организации, лица, управляющие различными программами аудита, должны согласовать методы аудита и рассмотреть последствия с точки зрения обеспечения ресурсами и планирования аудита. Если проверяемая организация применяет две или более различных систем менеджмента, то в программу аудита могут быть включены комбинированные аудиты.

5.5.4 Выбор членов группы по аудиту

Лицо(а), управляющее(ие) программой аудита, должно назначить членов группы по аудиту, включая руководителя группы и любых технических экспертов, необходимых для конкретного аудита.

Группа по аудиту должна быть сформирована с учетом компетентности, необходимой для достижения целей конкретного аудита в рамках установленной области аудита. Если есть только один аудитор, он должен выполнять все соответствующие обязанности руководителя группы по аудиту.

ПРИМЕЧАНИЕ Раздел 7 содержит руководство по определению компетентности, необходимой для членов группы по аудиту, и описывает процессы оценки аудиторов.

Чтобы оценить общую компетентность группы по аудиту должны быть выполнены следующие шаги:

- установить необходимую компетентность для достижения целей аудита;
- выбрать членов группы по аудиту таким образом, чтобы группа по аудиту обладала необходимой компетентностью.

При определении размера и состава группы по аудиту для конкретного аудита необходимо обратить внимание на следующее:

- a) общая компетентность группы по аудиту, необходимая для достижения целей аудита, с учетом области и критериев аудита;
- b) сложность аудита;
- c) является ли аудит комбинированным или совместным;
- d) выбранные методы аудита;
- e) обеспечение объективности и беспристрастности, чтобы избежать любого конфликта интересов в ходе процесса аудита;
- f) способность членов группы по аудиту результативно работать и взаимодействовать с представителями проверяемой организации и соответствующих заинтересованных сторон;
- g) соответствующие внешние/внутренние факторы, такие как язык аудита, а также социальные и культурные особенности проверяемой организации. Эти вопросы могут быть решены либо за счет собственной компетентности аудитора, либо при поддержке технического эксперта, а также необходимо учитывать потребность в переводчиках;
- h) тип и сложность проверяемых процессов.

Если необходимо, то лицо(а), управляющее(ие) программой аудита должно проконсультироваться с руководителем группы по вопросу формирования группы по аудиту.

Если выбранные в группу по аудиту аудиторы не обеспечивают необходимой компетентности, то в нее должны быть включены технические эксперты с дополнительной компетентностью.

Аудиторы-стажеры могут быть включены в группу по аудиту, но должны участвовать под руководством и надзором аудитора.

В ходе аудита может потребоваться корректировка состава группы по аудиту, например, в случае возникновения конфликта интересов или проблем с компетентностью. Если возникает такая ситуация, то ее следует обсудить с соответствующими сторонами (например, руководителем группы по аудиту, лицом(ами), управляющим(и) программой аудита, заказчиком аудита или проверяемой организацией), прежде чем будут сделаны какие-либо изменения.

5.5.5 Назначение обязанностей руководителя группы по аудиту для конкретного аудита

Лицо(а), управляющее(ие) программой аудита, должно возложить обязанности по проведению конкретного аудита на руководителя группы по аудиту.

Назначение должно быть сделано с достаточным запасом времени до намеченной даты проведения аудита, чтобы обеспечить надлежащее планирование аудита.

В целях обеспечения результативного проведения конкретных аудитов руководителю группы по аудиту должна быть предоставлена следующая информация:

- a) цели аудита;
- b) критерии аудита и любая имеющая существенное значение документированная информация;
- c) область аудита, включая идентификационные данные организации, ее функции и процессы, подлежащие аудиту;
- d) процессы аудита и связанные с ними методы;
- e) состав группы по аудиту;
- f) контактные данные проверяемой организации, места нахождения, сроки и продолжительность мероприятий по аудиту, которые должны быть проведены;
- g) ресурсы, необходимые для проведения аудита;
- h) информация, необходимая для оценки и принятия мер в отношении выявленных рисков и возможностей для достижения целей аудита;
- i) информация, необходимая руководителю(ям) группы по аудиту в его(их) взаимодействии с проверяемой организацией для обеспечения результативности программы аудита.

Информация о назначении должна также включать следующее, в зависимости от обстоятельств:

- рабочий язык аудита и язык для отчета, если они отличаются от языка, используемого аудитором или проверяемой организацией, или того и другого;
- требуемое содержание отчета об аудите и кому он должен быть направлен;
- вопросы, касающиеся конфиденциальности и информационной безопасности, как это требуется программой аудита;
- любые меры охраны здоровья, окружающей среды и безопасности в отношении аудиторов;
- требования, связанные с переездами и доступом к удаленным местам аудита;
- любые требования, связанные с секретностью и предоставлением прав доступа;
- любые действия, которые должны быть учтены, например, последующие действия, определенные по результатам предыдущего аудита;
- координация с другими мероприятиями аудита, например, когда несколько разных групп проводят аудит схожих или связанных процессов на различных площадках или в случае проведения совместного аудита.

Если проводится совместный аудит, важно достичь соглашения между организациями, проводящими аудиты, до того, как аудит начнется, по конкретным обязанностям каждой из сторон, в частности, в отношении полномочий руководителя группы по аудиту, назначенного для данного аудита.

5.5.6 Управление результатами выполнения программы аудита

Лицо(а), управляющее(ие) программой аудита, должно гарантировать, что выполнены следующие мероприятия:

- a) проведена оценка достижения целей каждого аудита в рамках программы аудита;
- b) рассмотрены и утверждены отчеты по аудитам с точки зрения полноты охвата области аудита и достижения целей;
- c) проведен анализ результативности мер, принятых по результатам аудита;
- d) отчет о результатах аудита разослан соответствующим заинтересованным сторонам;
- e) определена необходимость проведения дополнительного аудита.

Лицо, управляющее программой аудита, должно учитывать, в зависимости от обстоятельств:

- информирование частей организации, не вошедших в область аудита, о результатах аудита и лучших практиках;
- последствия для других процессов.

5.5.7 Управление записями по программе аудита

Лицо(а), управляющее(ие) программой аудита, должно гарантировать, что записи по аудиту создаются и управляются, чтобы продемонстрировать выполнение программы аудита. Должны быть разработаны процессы, гарантирующие, что любые потребности в информационной безопасности и конфиденциальности, связанные с записями по аудиту, удовлетворяются.

Записи могут включать в себя следующее:

- a) Записи, связанные с программой аудита, такие как:
 - график аудитов;
 - цели и объем программы аудита;
 - определяющие риски и возможности в рамках программы аудита, а также соответствующие внешние и внутренние факторы;
 - результаты анализа результативности программы аудита;
- b) Записи, относящиеся к конкретному аудиту, такие как:
 - планы аудита и отчеты по аудиту;
 - объективные свидетельства аудита и выводы;
 - отчеты о несоответствиях;
 - отчеты о коррекциях и корректирующих действиях;
 - отчеты о последующих действиях;
- c) Записи, связанные с группой по аудиту, относящиеся к таким вопросам, как:
 - компетентность и оценка результативности членов группы по аудиту;
 - критерии для формирования групп по аудиту и выбора членов группы;
 - поддержание и повышение компетентности.

Форма и уровень детализации записей должны давать возможность продемонстрировать, что цели программы аудита были достигнуты.

5.6 Мониторинг программы аудита

Лицо(а), управляющее(ие) программой аудита, должно гарантировать оценку:

- a) того, что был ли выдержан график и достигнуты цели аудита;
- b) работы членов группы по аудиту, в том числе руководителя группы по аудиту и технических экспертов;
- c) способности группы по аудиту выполнять план аудита;
- d) обратной связи от заказчиков аудита, проверяемых организаций, аудиторов, технических экспертов и других соответствующих сторон;
- e) достаточности и адекватности документированной информации по процессу аудита в целом.

Некоторые факторы могут указывать на необходимость внести изменения в программу аудита. Они могут включать в себя изменения в:

- выводах аудита;
- продемонстрированном уровне результативности и зрелости системы менеджмента;
- результативности программы аудита;
- области аудита и программы аудита;
- системе менеджмента проверяемой организации;
- стандартах и других требованиях, которые организация обязалась выполнять;
- внешних поставщиках;
- выявленных конфликтах интересов;
- требованиях заказчика аудита.

5.7 Пересмотр и улучшение программы аудита

Лицо(а), управляющее(ие) программой аудита, и заказчик аудита должны анализировать программу аудита для оценки того, были ли достигнуты ее цели. Уроки, извлеченные из анализа программы аудита, следует использовать в качестве исходных данных для постоянного улучшения программы.

Лицо(а), управляющее(ие) программой аудита, должно обеспечить следующее:

- анализ выполнения программы аудита в целом;
- выявление областей и возможностей для улучшения;
- внесение изменений в программу аудита в случае необходимости;
- отслеживание постоянного профессионального развития аудиторов в соответствии с разделом 7.6;
- предоставление отчета о результатах выполнения программы аудита и совместного с заказчиком аудита и, если необходимо, соответствующими заинтересованными сторонами анализа.

При анализе программы аудита следует учитывать следующее:

- a) результаты и тенденции, выявленные при мониторинге программы аудита;
- b) соответствие процессам программы аудита и соответствующей документированной информации;
- c) возрастающие потребности и ожидания соответствующих заинтересованных сторон;
- d) записи по программе аудита;
- e) альтернативные или новые методы аудита;
- f) альтернативные или новые методы оценки аудиторов;
- g) результативность мер по обработке рисков и возможностей, а также внутренних и внешних факторов, связанных с программой аудита;
- h) конфиденциальность и вопросы информационной безопасности, связанные с программой аудита.

6 Проведение аудита

6.1 Общие положения

Этот раздел содержит руководящие указания по подготовке и проведению конкретного аудита в рамках программы аудита. На Рисунке 2 представлена последовательность шагов, выполняемых при типовом аудите. Степень применимости положений настоящего раздела зависит от целей и области конкретного аудита.

6.2 Инициирование аудита

6.2.1 Общие положения

Ответственность за проведение аудита должна оставаться на назначенном руководителе группы по аудиту (см. 5.5.5) до тех пор, пока аудит не будет завершен (см. 6.6).

При инициировании аудита следует иметь в виду этапы, показанные на Рисунке 1; однако, последовательность может отличаться в зависимости от проверяемой организации, процессов и конкретных обстоятельств аудита.

6.2.2 Установление контакта с проверяемой организацией

Руководитель группы по аудиту должен обеспечить установление контакта с представителем проверяемой организации для того, чтобы:

- a) подтвердить каналы связи с представителями проверяемой организации;
- b) подтвердить полномочия для проведения аудита;
- c) предоставить соответствующую информацию о цели, области, критериях и методах аудита, о составе группы по аудиту, в том числе о технических экспертах;
- d) запросить доступ к соответствующей информации для планирования, в том числе информации о рисках и возможностях, выявленных организацией, и мерах по их обработке;
- e) определить применимые законодательные, нормативные и иные требования, относящиеся к видам деятельности, процессам, продуктам и услугам проверяемой организации;
- f) подтвердить соглашение с проверяемой организацией относительно степени раскрытия и обращения с конфиденциальной информацией;
- g) принять меры по организации аудита, включая формирование графика;

- h) определить действия, относящиеся к обеспечению доступа, охраны здоровья и безопасности, секретности, конфиденциальности или иным вопросам, связанным с конкретным местонахождением;
- i) согласовать участие наблюдателей, а также необходимость сопровождающих или переводчиков для группы по аудиту;
- j) определить любые области, представляющие интерес, вызывающие озабоченность или представляющие риски для проверяемой организации в отношении конкретного аудита;
- k) решить с проверяемой организацией или заказчиком аудита проблемы, связанные с формированием группы по аудиту.

6.2.3 Определение возможности проведения аудита

Чтобы обеспечить обоснованную уверенность в том, что цели аудита могут быть достигнуты, должна быть определена возможность проведения аудита.

При определении возможности следует учитывать такие факторы, как наличие следующего:

- a) достаточной и соответствующей информации для планирования и проведения аудита;
- b) надлежащего сотрудничества со стороны проверяемой организации;
- c) достаточного времени и ресурсов для проведения аудита.

ПРИМЕЧАНИЕ Под ресурсами также понимается доступ к соответствующим информационно-коммуникационным средствам.

Если проведение аудита не представляется возможным, заказчику аудита должна быть предложена альтернатива, согласованная с проверяемой организацией.

6.3 Подготовка к проведению аудита

6.3.1 Анализ документированной информации

Соответствующая документированная информация системы менеджмента проверяемой организации должна быть проанализирована для того, чтобы:

- получить информацию для понимания работы проверяемой организации, для подготовки мероприятий аудита и действующих рабочих документов (см. раздел 6.3.4), например, на процессы, функции;
- оценить объем документированной информации, требуемый, чтобы определить вероятное соответствие критериям аудита и выявить возможные проблемные области, такие как недостатки, упущения или конфликты.

Эта документированная информация должна включать, но не ограничиваться: документы и записи системы менеджмента, а также отчеты о предыдущих аудитах. При анализе необходимо принимать во внимание контекст проверяемой организации, в том числе ее размер, характер деятельности и сложность, а также выявленные риски и возможности. Кроме того, должны учитываться объем, критерии и цели аудита.

ПРИМЕЧАНИЕ Рекомендации по тому, как проверять информацию, содержатся в разделе А.5.

6.3.2 Планирование аудита

6.3.2.1 Риск-ориентированный подход при планировании

Руководитель группы по аудиту должен применять риск-ориентированный подход при планировании аудита на основе информации, содержащейся в программе аудита и

документированной информации, предоставленной проверяемой организацией.

При планировании аудита следует учитывать риски, которые создает аудит для процессов проверяемой организации, и формировать основу для соглашения между заказчиком аудита, группой по аудиту и проверяемой организацией, касающегося проведения аудита. Планирование должно облегчить эффективное распределение по времени и координацию мероприятий аудита для результативного достижения поставленных целей.

Степень детализации в плане аудита должна отражать область и сложность аудита, а также риск для недостижения целей аудита. При планировании аудита, руководитель группы по аудиту должен рассмотреть следующее:

- a) состав группы по аудиту и ее общую компетентность;
- b) соответствующие методы выборки (см. раздел A.6);
- c) возможности для повышения результативности и эффективности мероприятий аудита;
- d) риски для достижения целей аудита, создаваемые нерезультативным планированием аудита;
- e) риски для проверяемой организации, создаваемые проведением аудита.

Риски для проверяемой организации могут быть связаны с присутствием членов группы по аудиту, которое негативно влияет на соблюдение требований по гигиене труда и технике безопасности, экологии и качеству, а также представляет угрозу продуктам, услугам, персоналу или инфраструктуре проверяемой организации (например, внесение загрязнения в чистые помещения).

При комбинированных аудитах особое внимание следует уделять взаимодействию между рабочими процессами и любым конкурирующим целям и приоритетам различных систем менеджмента.

6.3.2.2 Подробности планирования аудита

Масштаб и содержание планирования аудита могут различаться, например, для начального и последующих аудитов, а также для внутренних и внешних аудитов. Планирование аудита должно быть достаточно гибким, чтобы сделать возможными изменения, которые могут оказаться необходимыми в ходе аудита.

При планировании аудита следует указать непосредственно или ссылками следующее:

- a) цели аудита;
- b) область аудита, включая информацию об организации, и ее функции, а также процессы, подлежащие аудиту;
- c) критерии аудита и любую документированную информацию, устанавливающую требования;
- d) местонахождение (физическое или виртуальное), даты, ожидаемое время и продолжительность мероприятий проводимого аудита, в том числе встречи с руководством проверяемой организации;
- e) необходимость для группы по аудиту ознакомления с объектами и процессами проверяемой организации (например, путем непосредственного ознакомления на месте (местах) или обзора с помощью информационно-коммуникационных средств);
- f) методы аудита, которые будут использоваться, включая объем необходимой выборки для получения достаточных свидетельств аудита;
- g) роли и обязанности членов группы по аудиту, в том числе действующих как сопровождающие, наблюдатели или переводчики;

h) выделение соответствующих ресурсов с учетом рисков и возможностей, связанных с видами деятельности, подлежащих аудиту.

При планировании аудита, в зависимости от обстоятельств, необходимо учитывать следующее:

- определение представителя(ей) проверяемой организации для аудита;
- рабочий язык и язык отчета по аудиту, если они отличаются от языка аудитора или проверяемой организации, или того и другого;
- разделы отчета об аудите;
- меры по обеспечению логистики и коммуникации, в том числе конкретные мероприятия, связанные с площадками, подлежащими аудиту;
- любые конкретные меры, которые необходимо предпринять для обработки возникающих рисков для достижения целей аудита и реализации возможностей;
- вопросы, связанные с конфиденциальностью и информационной безопасностью;
- любые последующие действия, вытекающие из предыдущего аудита или иного источника(ов), например, извлеченные уроки, анализ проектов;
- любые последующие действия для планируемого аудита;
- координация с другими мероприятиями по аудиту в случае совместного аудита.

Планы аудита должны быть представлены проверяемой организации. Любые проблемы, связанные с планами аудита, должны быть совместно решены руководителем группы по аудиту, проверяемой организацией и, если необходимо, лицом(ами), управляющим программой аудита.

6.3.3 Распределение заданий в группе по аудиту

Руководитель группы по аудиту, советуясь с группой по аудиту, должен назначить каждому члену группы ответственность за аудит конкретных процессов, задач, функций или площадок, а также, насколько это применимо, полномочия для принятия решений. Такие назначения должны делаться с учетом обеспечения независимости, объективности и компетентности аудиторов и результативного использования ресурсов, а также различных ролей и обязанностей аудиторов, аудиторов-стажеров и технических экспертов.

В случае необходимости руководителем группы по аудиту должны проводиться совещания аудиторской группы с целью распределения рабочих заданий и принятия решений по возможным изменениям. Изменения в рабочих заданиях могут быть сделаны и в ходе аудита, чтобы обеспечить достижение целей аудита.

6.3.4 Подготовка рабочих документов

Члены группы по аудиту должны собирать и анализировать информацию, относящуюся к их заданию по аудиту, и готовить документированную информацию для аудита, используя любые соответствующие носители. Такая документированная информация может включать в себя, но не ограничиваться этим:

- a) чек-листы в бумажной или электронной форме;
- b) подробности формирования выборок для аудита;
- c) аудио-визуальную информацию.

Использование этих средств не должно ограничивать объем мероприятий по аудиту, который может

меняться на основе информации, собранной в ходе аудита.

ПРИМЕЧАНИЕ Рекомендации по подготовке рабочих документов по аудиту приведены в разделе А.13.

Документированная информация подготовленная для аудита и полученная в ходе аудита должна сохраняться, по крайней мере, до завершения аудита или как это установлено программой аудита. Сохранение документированной информации после завершения аудита описано в разделе 6.6. Документированная информация, созданная в процессе аудита, и содержащая конфиденциальную или личную информацию должна быть защищена членами группы по аудиту надлежащим образом на всем протяжении аудита.

6.4 Проведение аудита

6.4.1 Общие положения

Мероприятия аудита, как правило, проводятся в определенной последовательности, как это показано на Рисунке 1. Эта последовательность может быть различной в зависимости от обстоятельств конкретных аудитов.

6.4.2 Назначение ролей и обязанностей сопровождающих и наблюдателей

Сопровождающие и наблюдатели могут сопровождать группу по аудиту при наличии соответствующих согласований от руководителя группы по аудиту, заказчика аудита и/или проверяемой организации. Они не должны влиять или вмешиваться в проведение аудита. Если это не может быть гарантировано, то руководитель группы по аудиту должен иметь право запретить присутствие наблюдателей в ходе определенных мероприятий аудита.

В отношении наблюдателей должны выполняться все меры обеспечения доступа, охраны здоровья и безопасности, меры экологического характера, обеспечения секретности и конфиденциальности, согласованные между заказчиком аудита и проверяемой организацией.

Сопровождающие, назначенные проверяемой организацией, должны помогать группе по аудиту и вступать в дело при обращении к ним руководителя группы по аудиту или аудитора, которому они назначены. Их обязанности должны включать в себя следующее:

- a) содействие аудиторам в определении лиц для участия в интервью и подтверждении графика и мест их проведения;
- b) обеспечение доступа к конкретным участкам проверяемой организации;
- c) гарантию того, что правила, касающиеся мер обеспечения доступа, охраны здоровья и безопасности, экологии, секретности, конфиденциальности, связанных с конкретной площадкой, доведены до сведения членов группы по аудиту и наблюдателей и соблюдаются ими, а также того, что меры в отношении любых рисков приняты;
- d) наблюдение за ходом аудита со стороны проверяемой организации в соответствующих случаях;
- e) предоставление разъяснений или оказание помощи в сборе информации, когда это необходимо.

6.4.3 Проведение открывающего совещания

Назначение открывающего совещания состоит в том, чтобы:

- a) подтвердить согласие всех сторон (например, проверяемой организации, группы по аудиту) с планом аудита;
- b) представить группу по аудиту;
- c) гарантировать возможность выполнения всех запланированных мероприятий аудита.

Открывающее совещание должно быть проведено с участием руководства проверяемой организации и, в зависимости от ситуации, лиц, ответственных за функции или процессы, подлежащие аудиту. В ходе совещания должна быть предоставлена возможность задать вопросы.

Степень детализации должна соответствовать тому, насколько проверяемая организация знакома с процессом аудита. Во многих случаях, например, внутренних аудитов в небольшой организации открывающее совещание может состоять просто из информации, что аудит проводится и пояснения характера аудита.

В других ситуациях совещание может быть официальным и должны сохраняться записи об участии. Совещание должно проходить под председательством руководителя группы по аудиту.

В зависимости от ситуации, должны быть представлены:

- участники, включая наблюдателей и сопровождающих, переводчиков, а также краткое описание их роли;
- методы управления рисками для организации, которые могут возникнуть в результате присутствия членов группы по аудиту.

В зависимости от обстоятельств, должно быть рассмотрено подтверждение следующего:

- целей, области и критериев аудита;
- плана аудита и других соответствующих договоренностей с проверяемой организацией, таких как дата и время заключительного совещания, любых промежуточных совещаний группы по аудиту и руководства проверяемой организации, а также любых произошедших изменений;
- официальных каналов связи между группой по аудиту и проверяемой организацией;
- языка, который будет использоваться в ходе аудита;
- того, что в процессе аудита проверяемая организация будет информироваться о ходе аудита;
- наличия ресурсов и технических средств, необходимых для группы по аудиту;
- вопросов, касающихся конфиденциальности и информационной безопасности;
- соответствующих прав доступа, вопросов охраны здоровья и безопасности, обеспечения секретности, действий в чрезвычайной ситуации и иных мероприятий для группы по аудиту.

При необходимости следует рассмотреть предоставление следующей информации:

- метод представления выводов аудита, включая критерии их классификации, если таковые имеются;
- условия, при которых аудит может быть прекращен;
- какие меры принимать в отношении возможных выводов в ходе аудита;
- любой способ обратной связи с проверяемой организацией по выводам или заключениям аудита, включая претензии или апелляции.

6.4.4 Обмен информацией в ходе аудита

В ходе аудита может оказаться необходимым ввести формализованные процедуры обмена информацией в рамках группы по аудиту, а также с проверяемой организацией, заказчиком аудита и, возможно, с внешними органами (например, регулирующими органами), особенно тогда, когда законодательные и нормативные требования устанавливают обязательную отчетность о

несоответствиях.

Группа по аудиту должна периодически обмениваться информацией, оценивать степень выполнения мероприятий аудита, а также проводить переназначение работ между членами группы по аудиту, если необходимо.

Во время аудита руководитель группы по аудиту должен периодически информировать о ходе аудита, существенных выводах и любых затруднениях проверяемую организацию и заказчика аудита, в зависимости от ситуации. Свидетельства, собранные в ходе аудита, которые указывают на возможность непосредственного и значительного риска, должны быть немедленно доведены до сведения проверяемой организации и, в случае необходимости, заказчика аудита. Любая обеспокоенность по поводу проблем, находящихся вне области аудита, должна быть зафиксирована и доведена до сведения руководителя группы по аудиту на предмет возможного общения с заказчиком аудита и проверяемой организацией.

В случае, если имеющиеся свидетельства аудита указывают на то, что цели аудита недостижимы, руководитель группы по аудиту должен сообщить причины этого заказчику аудита и проверяемой организации, чтобы определить соответствующие действия. Такие меры могут включать в себя изменения в планировании аудита, целях или области аудита, или же прекращение аудита.

Любая необходимость изменений в плане аудита, которая может стать очевидной в ходе аудита, должна быть рассмотрена и одобрена, в зависимости от ситуации, как лицом(ами), управляющим(и) программой аудита, так и заказчиком аудита, и представлена проверяемой организации.

6.4.5 Места получения информации для аудита и доступ к ней

Методы, выбранные для аудита, зависят от намеченных целей, области и критериев аудита, а также продолжительности и местонахождения. Местонахождение – это то место, где информация, необходимая для выполнения конкретной задачи аудита, может быть получена группой по аудиту. Оно может быть как физическим, так и виртуальным.

Критически важно для аудита, где, когда и как получить доступ к информации. Это не зависит от того, где создается информация, где она используется и/или хранится. Исходя из этих аспектов и должны быть определены методы аудита (см. таблицу А.1). В ходе проверки можно использовать комбинацию методов. Кроме того, обстоятельства аудита могут вызывать необходимость изменения методов в ходе аудита.

6.4.6 Анализ документированной информации в ходе аудита

Соответствующая документированная информация проверяемой организации должна быть проанализирована, чтобы:

- определить соответствие системы, в той мере, в какой она документирована, критериям аудита;
- получить информацию для обеспечения реализации мероприятий аудита.

ПРИМЕЧАНИЕ Рекомендации о том, как проверять информацию, содержатся в А.5.

Анализ может сочетаться с другими действиями в рамках аудита и может продолжаться в течение всего аудита, при условии, что это не наносит ущерба результативности проведения аудита.

Если соответствующая документированная информация не может быть предоставлена в сроки, указанные в плане аудита, руководитель группы по аудиту должен информировать об этом как лицо(а), управляющее(ие) программой аудита, так и проверяемую организацию. В зависимости от целей и области аудита, должно быть принято решение, следует ли аудит продолжать или он должен быть приостановлен до тех пор, пока проблемы с предоставлением документированной информации не будут решены.

6.4.7 Сбор и проверка информации

В ходе аудита информация, значимая с точки зрения целей, области и критериев аудита, в том числе информация, касающаяся взаимосвязей между функциями, видами деятельности и процессами, должна быть собрана с помощью соответствующих процедур выборки и проверена, насколько это практически возможно.

ПРИМЕЧАНИЕ 1 Для проверки информации см. А.5.

ПРИМЕЧАНИЕ 2 Руководство по выборке дано в А.6.

В качестве свидетельств аудита должна приниматься только та информация, которую можно подтвердить с определенной степенью. В тех случаях, когда степень подтверждения низкая, аудитор должен использовать свое профессиональное суждение для определения степени надежности, с которой эта информация может рассматриваться как свидетельство. Свидетельства аудита, на основании которых делаются выводы аудита, должны быть зафиксированы. Если в ходе сбора свидетельств, группа по аудиту узнает о каких-либо новых или изменившихся обстоятельствах либо рисках или возможностях, то в отношении них должны быть предприняты группой соответствующие меры.

На рисунке 2 представлен общий вид типового процесса от сбора информации до формирования заключений аудита.

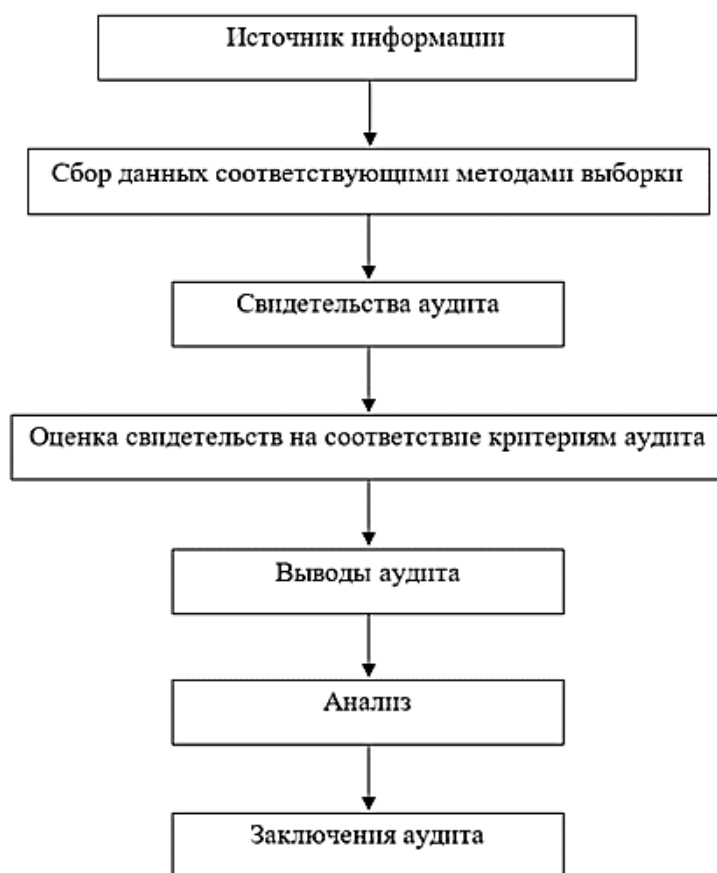


Рисунок 2 – Общий вид типового процесса сбора и проверки информации

Методы сбора информации включают в себя, но не ограничиваются этим, следующее:

- интервью;
- наблюдения;
- анализ документированной информации.

ПРИМЕЧАНИЕ 3 Рекомендации по выбору источников информации и наблюдениям даны в А.14.

ПРИМЕЧАНИЕ 4 Рекомендации по посещению площадок проверяемой организации даны в А.15.

ПРИМЕЧАНИЕ 5 Рекомендации по проведению интервью даны в А.17.

6.4.8 Формирование выводов аудита

Свидетельства аудита должны быть оценены в соответствии с критериями аудита для формирования выводов аудита. Выводы аудита могут указывать на соответствие или несоответствие критериям аудита. Если это предусмотрено в плане аудита, то конкретные выводы аудита должны включать в себя оценку соответствия и лучшие практики с приложением подтверждающих свидетельств, возможности для улучшения, а также любые рекомендации проверяемой организации.

Несоответствия и подтверждающие их свидетельства аудита должны быть зафиксированы.

Несоответствия могут классифицироваться в зависимости от контекста организации и ее рисков. Такая классификация может быть как количественной (например, от 1 до 5), так и качественной (например, несущественное, существенное). Они должны быть рассмотрены проверяемой организацией для того, чтобы получить подтверждение правильности свидетельства аудита, и того, что несоответствия понятны. Должно быть сделано все, чтобы разрешить все разногласия относительно свидетельств или выводов аудита. Нерешенные вопросы должны быть отражены в отчете по аудиту.

В ходе аудита группа по аудиту должна собираться на соответствующих этапах по мере необходимости для анализа выводов аудита.

ПРИМЕЧАНИЕ 1 Дополнительные рекомендации по формированию и оценке выводов аудита даны в А.18.

ПРИМЕЧАНИЕ 2 Соответствие или несоответствие критериям аудита, связанное с законодательными, нормативными или иными требованиями, иногда называется «соблюдение» или «несоблюдение».

6.4.9 Подготовка заключений аудита

6.4.9.1 Подготовка к заключительному совещанию

Группа по аудиту должна провести встречу до заключительного совещания, чтобы:

- a) рассмотреть с точки зрения целей аудита выводы аудита, а также любую другую соответствующую информацию, собранную в ходе аудита;
- b) согласовать заключения аудита с учетом неопределенности, присущей процессу аудита;
- c) подготовить рекомендации, если это предусмотрено планом аудита;
- d) обсудить последующие действия, если это необходимо.

6.4.9.2 Содержание заключений по аудиту

Заключения аудита могут касаться таких вопросов, как:

- a) степень соответствия критериям аудита и устойчивость системы менеджмента, в том числе ее результативность в достижении ожидаемых целей, выявлении рисков и результативности действий, предпринимаемых проверяемой организацией для обработки рисков;

- b) результативное внедрение, поддержание и совершенствование системы менеджмента;
- c) достижение целей аудита, степени охвата области аудита и выполнения критериев аудита;
- d) подобные выводы, сделанные в других частях, где прошел аудит, или при совместном либо предыдущем аудите с целью выявления тенденций.

Если это предусмотрено планом аудита, то на основании заключений аудита могут формироваться рекомендации по улучшению или дальнейшим мероприятиям по аудиту.

6.4.10 Проведение заключительного совещания

Должно проводиться заключительное совещание, чтобы представить выводы и заключения аудита.

Заключительное совещание должно проходить под председательством руководителя группы по аудиту с участием руководства проверяемой организации, а также, насколько это применимо:

- лиц, ответственных за функции и процессы, которые проверялись на аудите;
- заказчика аудита;
- других членов группы по аудиту;
- иных соответствующих заинтересованных сторон, определенных заказчиком аудита и/или проверяемой организацией.

Если это применимо, руководитель группы по аудиту должен сообщить проверяемой организации о ситуациях, возникавших в ходе аудита, которые могли бы снизить степень доверия к заключениям аудита. Если это определено в системе менеджмента или по соглашению с заказчиком аудита, участники должны договориться о сроках выполнения плана действий, вытекающих из выводов аудита.

Степень детализации должна учитывать результативность системы менеджмента в достижении целей проверяемой организации, включая рассмотрение ее контекста, а также рисков и возможностей.

В ходе заключительного совещания должна приниматься во внимание степень знакомства проверяемой организации с процессом аудита, чтобы обеспечить участникам надлежащий уровень детализации.

В некоторых ситуациях совещание может быть официальным и протоколы, в том числе с регистрацией участников, должны сохраняться. В других случаях, например, при внутреннем аудите, заключительное совещание может носить менее формальный характер и включать только обсуждение выводов и заключений аудита.

В зависимости от ситуации, на заключительном совещании проверяемой организации должно быть:

- a) пояснено, что собранные свидетельства аудита основаны на выборке из имеющейся информации и могут не отражать в полной мере результативность проверенных процессов;
- b) указано на способ отчетности;
- c) пояснено, каким образом должны приниматься меры по выводам аудита на основе согласованного процесса;
- d) указано на возможные последствия несоответствующего принятия мер по выводам аудита;
- e) сделано представление выводов и заключений аудита таким образом, чтобы они были понятны и признавались руководством проверяемой организации;

f) обсуждено все, что связано с действиями после аудита (например, осуществление и анализ корректирующих действий, рассмотрение претензий по аудиту, процесс обжалования результатов).

Любые расхождения во мнениях относительно выводов или заключений аудита между группой по аудиту и проверяемой организацией должны быть обсуждены и, если это возможно, устранены. Если устранить не удастся, это должно быть зафиксировано.

Если предусмотрено целями аудита, то могут быть представлены рекомендации по возможностям для улучшения. Следует подчеркнуть, что рекомендации не являются обязательными.

6.5 Подготовка и рассылка отчета об аудите

6.5.1 Подготовка отчета об аудите

Руководитель группы по аудиту должен представить заключения по аудиту в соответствии с программой аудита. Отчет по аудиту должен представлять полную, точную, краткую и ясную информацию об аудите и должен включать в себя непосредственно или в виде ссылок следующее:

- a) цели аудита;
- b) область аудита, в частности, информацию об организации (проверяемой) и проверенные функции или процессы;
- c) информацию о заказчике аудита;
- d) состав группы по аудиту и участников от проверяемой организации;
- e) даты и площадки, где были проведены мероприятия по аудиту;
- f) критерии аудита;
- g) выводы аудита и связанные с ними свидетельства;
- h) заключения аудита;
- i) заявление о степени соответствия критериям аудита
- j) все неразрешенные расхождения во мнениях между проверяемой организацией и командой по аудиту;
- k) пояснение, что аудиты по своей природе носят выборочный характер; таким образом, существует риск, что полученные свидетельства аудита не дают полной и точной картины.

Отчет по аудиту также может включать в себя или ссылаться на следующее, в зависимости от ситуации:

- план аудита, включая график;
- краткое изложение процесса аудита, включая любые встретившиеся препятствия, которые могли снизить надежность заключений аудита;
- подтверждение того, что цели аудита были достигнуты в рамках области аудита в соответствии с планом аудита;
- все, что не было охвачено аудитом, но было включено в область аудита, включая все проблемы с получением свидетельств, ресурсами или конфиденциальностью с соответствующим обоснованием;
- краткое пояснение заключений аудита и основные выводы аудита, на которых они базируются;

- выявленные лучшие практики;
- согласованный план последующих действий, если таковые имеются;
- заявление о конфиденциальном характере содержания;
- любые последствия для программы аудита или последующих аудитов.

6.5.2 Рассылка отчета об аудите

Отчет по аудиту должен быть выпущен в течение согласованного периода времени. Если он задерживается, то причины должны быть доведены до сведения проверяемой организации и лица (лиц), управляющего(их) программой аудита.

Отчет по аудиту должен быть датирован, рассмотрен и одобрен, если необходимо, в соответствии с программой аудита.

Отчет по аудиту должен быть затем разослан соответствующим заинтересованным сторонам, определенным в программе аудита или плане аудита.

При рассылке отчета должны быть учтены соответствующие меры обеспечения конфиденциальности.

6.6 Завершение аудита

Аудит завершается, когда все запланированные мероприятия по аудиту выполнены, или же по согласованию с заказчиком аудита (например, в случае неожиданной ситуации, которая не позволяет завершить аудит в соответствии с планом аудита).

Документированную информацию, имеющую отношение к аудиту, необходимо сохранять или утилизировать по соглашению между участвующими сторонами и в соответствии с программой аудита и действующими требованиями.

Если нет законодательного требования, группа по аудиту и лицо(а), управляющее(ие) программой аудита, не должны раскрывать какую-либо информацию, полученную в ходе аудита, или содержание отчета по аудиту, какой-либо другой стороне без явного согласия заказчика аудита и, в случае необходимости, санкции проверяемой организации. Если же требуется раскрытие содержания документов аудита, заказчик аудита и проверяемая организация должны быть проинформированы как можно скорее.

Уроки, извлеченные из аудита, должны указывать риски и возможности для программы аудита и проверяемой организации.

6.7 Выполнение последующих действий

Результаты аудита могут, в зависимости от целей аудита, указывать на необходимость коррекций или корректирующих действий, или на возможности для улучшения. Решения по таким действиям и их выполнение осуществляется проверяемой организацией в согласованные сроки. В зависимости от ситуации, проверяемая организация должна информировать лицо(а), управляющее(ие) программой аудита, и/или группу по аудиту о состоянии этих действий.

Завершение и результативность этих действий должны быть проверены. Эта проверка может быть частью последующего аудита. Результаты должны быть сообщены лицу, управляющему программой аудита, и заказчику аудита для проведения анализа руководством.

7 Компетентность и оценка аудиторов

7.1 Общие положения

Доверие к процессу аудита и способность достигать поставленных целей зависит от компетентности тех лиц, которые участвуют в проведении аудитов, в том числе аудиторов и руководителей групп по аудиту. Компетентность необходимо регулярно оценивать с помощью процесса, который рассматривает личные качества и способность применять знания и навыки, приобретенные вследствие образования, опыта работы, подготовки в качестве аудитора и опыта проведения аудитов. Этот процесс должен учитывать потребности, вытекающие из программы аудита, и ее цели. Часть знаний и навыков, описанных в разделе 7.2.3, являются общими для аудиторов всех систем менеджмента, вне зависимости от объекта управления; другие являются специфическими для конкретных видов систем менеджмента. Нет необходимости каждому аудитору в группе иметь одинаковую компетентность. Однако, общая компетентность группы по аудиту должна быть достаточной для достижения целей аудита.

Оценка компетентности аудиторов должна планироваться, осуществляться и документироваться, чтобы обеспечить объективный, непротиворечивый, беспристрастный и надежный результат. Процесс оценки должен включать в себя следующие четыре основных этапа:

- a) определение необходимой компетентности для удовлетворения потребностей, вытекающих из программы аудита;
- b) установление критериев оценки;
- c) выбор соответствующего метода оценки;
- d) проведение оценки.

Результаты процесса оценки должны служить основой для следующих действий:

- выбор членов группы по аудиту (как это описано в разделе 5.5.4);
- определение необходимости повышения компетентности (например, дополнительная подготовка);
- постоянная оценка результативности аудиторов.

Аудиторы должны формировать, поддерживать и повышать свою компетентность путем постоянного профессионального развития и регулярного участия в аудитах (см. 7.6).

Процесс оценки аудиторов и руководителей групп по аудиту описан в разделах 7.3, 7.4 и 7.5.

Аудиторы и руководители групп по аудиту должны оцениваться на основании критериев, установленных в разделах 7.2.2 и 7.2.3, а также 7.1.

Требуемая для лица (лиц), управляющего(их) программой аудита, компетентность описана в разделе 5.4.2.

7.2 Определение компетентности аудитора

7.2.1 Общие положения

При принятии решения о необходимых для аудита знаниях и навыках аудитора, относящихся к нижеперечисленному, следует учитывать:

- a) размер, характер, сложность, продукты, услуги и процессы проверяемой организации;

- b) методы аудита;
- c) вид системы менеджмента, подлежащей аудиту;
- d) сложность и процессы системы менеджмента, подлежащие аудиту;
- e) типы и уровни рисков и возможностей, обрабатываемых системой менеджмента;
- f) цели и объем программы аудита;
- g) неопределенность в достижении целей аудита;
- h) другие требования, например, те, что устанавливаются заказчиком аудита или другими соответствующими заинтересованными сторонами, в зависимости от ситуации.

Эта информация должна соответствовать тому, что указано в разделе 7.2.3.

7.2.2 Личные качества

Аудиторы должны обладать необходимыми качествами, обеспечивающими им возможность действовать в соответствии с принципами аудита, описанными в разделе 4. Аудиторы должны проявлять профессиональные качества при выполнении аудита. Желаемое профессиональное поведение предполагает, что аудитор должен быть:

- a) этичным, т.е. справедливым, правдивым, искренним, честным и сдержанным;
- b) открытым, то есть иметь желание рассматривать альтернативные идеи или точки зрения;
- c) дипломатичным, т.е. тактичным в общении с людьми;
- d) наблюдательным, т.е. активно отслеживать окружающую обстановку и действия;
- e) проникательным, т.е. знать и быть в состоянии понимать ситуации;
- f) гибким, т.е. способным легко адаптироваться к различным ситуациям;
- g) упорным, т.е. настойчивым и направленным на достижение поставленных целей;
- h) логичным, т.е. способным своевременно делать выводы на основе логических рассуждений и анализа;
- i) уверенным в себе, т.е. способным действовать независимо, при этом результативно взаимодействуя с другими;
- j) принципиальным, т.е. способным действовать ответственно и в рамках этики, даже если эти действия не всегда могут вызывать одобрение и иногда вести к несогласию или конфронтации;
- k) готовым к совершенствованию, т.е. имеющим желание извлекать уроки из ситуаций;
- l) уважительным к культурным особенностям, т.е. соблюдающим и уважающим культурные традиции проверяемой организации;
- m) настроенным на сотрудничество, т.е. результативно взаимодействующим с другими, в том числе членами группы по аудиту и персоналом проверяемой организации.

7.2.3 Знания и навыки

7.2.3.1 Общие положения

Аудиторы должны обладать:

- a) знаниями и навыками, необходимыми для достижения намеченных результатов аудитов, которые они должны проводить,

- b) общими знаниями и навыками, связанными с видом проверяемой системы менеджмента, а также знаниями и навыками, относящимися к конкретной отрасли.

Руководители групп по аудиту должны иметь дополнительные знания и навыки, необходимые для обеспечения руководства группой по аудиту.

7.2.3.2 Общие знания и навыки аудиторов систем менеджмента

Аудиторы должны обладать знаниями и навыками в областях, указанных ниже.

- a) Принципы, процессы и методы аудита: знания и навыки в этой области позволяют аудитору обеспечить последовательное и системное проведение аудита.

Аудитор должен обладать способностью:

- понимать характер рисков и возможностей, связанных с аудитом, и принципы риск-ориентированного подхода к аудиту;
- результативно планировать и организовывать работу;
- проводить аудит в рамках согласованного графика;
- расставлять приоритеты и фокусироваться на вопросах, имеющих важное значение;
- результативно обмениваться информацией в устной и письменной форме (лично или через переводчиков);
- собирать информацию путем результативного интервьюирования, выслушивания, наблюдения и анализа документированной информации, включая записи и данные;
- понимать пригодность и последствия использования методов выборки для аудита;
- воспринимать и учитывать мнения экспертов;
- проводить аудит процесса от начала до конца, включая взаимосвязи с другими процессами и различными функциями, где это требуется;
- проверять актуальность и точность собранной информации;
- подтверждать достаточность и пригодность свидетельств аудита для обоснования выводов и заключений аудита;
- оценивать те факторы, которые могут повлиять на достоверность выводов и заключений аудита;
- документировать мероприятия по аудиту и выводы аудита, а также формировать отчеты;
- соблюдать конфиденциальность и меры защиты информации.

- b) Стандарты на системы менеджмента и другие ссылочные документы: знания и навыки в этой области позволяют аудитору понимать область аудита и применять критерии аудита, и должны включать в себя следующее:

- стандарты на системы менеджмента или другие нормативные или руководящие/вспомогательные документы, используемые для установления критериев и методов аудита;
- применение стандартов на системы менеджмента проверяемой и другими организациями;
- отношения и взаимодействия между процессами системы (систем) менеджмента;

- понимание значимости и приоритетности в рамках комплекса стандартов или ссылочных документов;
 - применение стандартов или ссылочных документов в различных ситуациях аудита.
- с) Организация и ее контекст: знания и навыки в этой области позволяют аудитору понять структуру, цели и методы управления проверяемой организацией и должны включать в себя следующее:
- потребности и ожидания соответствующих заинтересованных сторон, которые влияют на систему менеджмента;
 - тип организации, построение управления, размер, структуру, функции и связи;
 - общий подход к бизнесу и управлению, процессы и соответствующую терминологию, в том числе планирование, бюджетирование и управление людьми;
 - культурные и социальные аспекты проверяемой организации.
- d) Применимые законодательные, нормативные и другие требования: знания и навыки в этой области позволяют аудитору быть осведомленным о требованиях к организации и работать в рамках этих требований. Знания и навыки, характерные для юрисдикции или деятельности проверяемой организации, процессов, продуктов и услуг, должны включать в себя следующее:
- законодательные и нормативные требования и устанавливающие их госучреждения;
 - основную юридическую терминологию;
 - порядок заключения договоров и контрактные обязательства.

7.2.3.3 Компетентность аудиторов в конкретных видах систем менеджмента и отраслях

Группы по аудиту должны иметь коллективную компетентность, связанную с видами систем менеджмента и конкретными отраслями, подходящие для аудита конкретных видов систем менеджмента и отраслей.

Компетентность аудиторов в отдельных видах систем менеджмента и конкретных отраслях включает в себя следующее:

- a) требования и принципы системы менеджмента и их применение;
- b) основы конкретного(ых) вида(ов) систем(ы) менеджмента и отрасли(ей), связанные со стандартами на системы менеджмента, применяемыми проверяемой организацией;
- c) применение методов, технических средств, процессов и процедур, относящихся к конкретным видам систем менеджмента и отраслям, чтобы группа по аудиту могла оценить соответствие в рамках установленной области аудита и сформировать соответствующие выводы и заключения аудита;
- d) принципы, методы и технические средства, относящиеся к конкретному виду системы менеджмента и отрасли, чтобы аудитор мог определить и оценить риски и возможности, связанные с целями аудита.

7.2.3.4 Общая компетентность руководителя группы по аудиту

В целях содействия результативному и эффективному проведению аудита руководитель группы по аудиту должен обладать компетентностью для:

- a) планирования аудита и назначения задач по аудиту в соответствии с имеющейся компетентностью

конкретных членов группы по аудиту;

- b) обсуждения стратегических вопросов с высшим руководством проверяемой организации с целью определить, учитывало ли оно эти вопросы при оценке рисков и возможностей;
- c) установления и поддержания конструктивных рабочих отношений между членами группы по аудиту;
- d) управления процессом аудита, в том числе:
 - результативного использования ресурсов в ходе аудита;
 - управления неопределенностью в достижении целей аудита;
 - охраны здоровья и безопасности членов группы по аудиту в ходе аудита, включая обеспечение соблюдения аудиторами соответствующих соглашений, касающихся вопросов обеспечения здоровья и безопасности;
 - руководства членами команды по аудиту;
 - руководства и консультирования аудиторов-стажеров;
 - предотвращения и урегулирования конфликтов и проблем, которые могут возникать в ходе аудита, включая, если необходимо, и те, что возникают в группе по аудиту.
- e) представления группы по аудиту в отношениях с лицом(ами), управляющим(и) программой аудита, заказчиком аудита и проверяемой организацией;
- f) руководства группой по аудиту с целью формирования заключений по аудиту;
- g) подготовки и окончательного формирования отчета по аудиту.

7.2.3.5 Знания и навыки для аудита в разных областях

Когда аудит проводится для нескольких систем, член группы по аудиту должен иметь представление о взаимодействии и синергии между различными системами менеджмента.

Руководители групп по аудиту должны понимать требования каждого из стандартов на проверяемые системы менеджмента и осознавать ограниченность своей компетентности в каждом из видов систем менеджмента.

7.2.4 Обеспечение компетентности аудитора

Аудитор может получить надлежащую компетентность, используя комбинации следующего:

- a) успешное завершение учебных программ, которые охватывают общие знания и навыки аудитора;
- b) опыт работы на соответствующих технических, управленческих или профессиональных должностях, связанных с формированием суждений, принятием решений, разрешением проблем и общением с руководителями, специалистами, коллегами, потребителями и другими соответствующими заинтересованными сторонами;
- c) образование/обучение и опыт в конкретной системе менеджмента и отрасли, которые расширяют общую компетентность;
- d) опыт аудита, полученный под руководством аудитора, компетентного в этой области.

ПРИМЕЧАНИЕ Успешное завершение учебного курса будет зависеть от типа курса. Для курсов с экзаменом это может означать успешную сдачу экзамена. Для других курсов это может означать прохождение и завершение курса.

7.2.5 Обеспечение компетентности руководителя группы по аудиту

Руководитель группы по аудиту должен обладать дополнительным опытом аудита для расширения компетентности, определенной в 7.2.3.4. Этот дополнительный опыт должен быть приобретен при работе под руководством другого руководителя группы по аудиту.

7.3 Определение критериев оценки аудитора

Критерии должны иметь качественный характер (например, демонстрируемые желаемые личные качества, знания или реализация навыков при обучении или на рабочем месте) и количественный (например, опыт работы и длительность обучения в годах, количество проведенных аудитов, количество часов подготовки в сфере аудита).

7.4 Выбор соответствующего метода оценки аудитора

Оценка должна проводиться с использованием двух или более методов, указанных в Таблице 2. При использовании Таблицы 2 следует иметь в виду следующее:

- а) описанные методы представляют собой набор возможностей и могут быть неприменимы в некоторых ситуациях;
- б) разные методы из представленных могут отличаться по своей надежности;
- с) для обеспечения объективного, непротиворечивого, беспристрастного и надежного результата следует использовать комбинацию методов.

Таблица 2 - Методы оценки аудитора

Метод оценки	Цели	Примеры
Анализ записей	Проверить подготовку аудитора	Анализ записей об образовании, подготовке, стаже, профессиональной квалификации и опыте аудитов
Обратная связь	Получить информацию о том, как воспринимается работа аудитора	Опросы, анкеты, личные рекомендации, отзывы, претензии, оценка результатов работы, экспертная оценка
Интервью	Оценить желаемые личные качества и навыки общения, подтвердить информацию и проверить знания, получить дополнительную информацию	Личные интервью
Наблюдение	Оценить желаемые личные качества и способность применять знания и навыки	Ролевые игры, наблюдение в ходе аудита, фактическое качество работы
Тестирование	Оценить желаемые личные качества, знания, навыки и их применение	Устные или письменные экзамены, психометрическое тестирование

Метод оценки	Цели	Примеры
Анализ после аудита	Получить информацию о действиях аудитора в ходе аудита, определить сильные стороны и возможности для улучшения	Анализ отчета об аудите, интервью с руководителем группы по аудиту, группой по аудиту и, при необходимости, анализ мнения проверяемой организации

7.5 Проведение оценки аудитора

Информация, собранная об оцениваемом аудиторе должна быть сопоставлена с критериями, установленными в 7.2.3. Если оцениваемый аудитор, чье участие предполагается в программе аудита, не отвечает критериям, то следует провести дополнительное обучение, дать возможность получить дополнительный опыт работы или аудита, после чего следует выполнить повторную оценку.

7.6 Поддержание и повышение компетентности аудитора

Аудиторы и руководители групп по аудиту должны постоянно повышать свою компетентность. Аудиторы должны поддерживать свою компетентность в сфере аудита посредством регулярного участия в аудитах систем менеджмента и постоянного профессионального развития. Это может быть достигнуто с помощью таких средств, как дополнительный опыт работы, обучение, самообразование, наставничество, участие в совещаниях, семинарах и конференциях или других соответствующих мероприятиях.

Лицо(а), управляющее(ие) программой аудита, должно разработать соответствующие механизмы для постоянной оценки деятельности аудиторов и руководителей групп по аудиту.

Постоянное профессиональное развитие должно учитывать следующее:

- a) изменения в потребностях отдельных лиц и организации, ответственных за проведение аудита;
- b) развитие практик аудита, включая применение технологий;
- c) соответствующие стандарты, включая руководящие/вспомогательные документы и другие требования;
- d) изменения в отрасли или направлениях менеджмента.

Приложение А

(Информационное)

Дополнительные руководящие указания для аудиторов по планированию и проведению аудитов

А.1 Применение методов аудита

Аудит может быть выполнен с использованием целого ряда методов. Пояснения по часто используемым методам аудита можно найти в данном приложении. Методы, выбранные для аудита, зависят от намеченных целей, области и критериев аудита, а также продолжительности и местонахождения. Также следует учесть имеющуюся у аудиторов компетентность и любую неопределенность, возникающую в результате применения методов аудита. Применяя разнообразие и сочетание различных методов аудита можно оптимизировать результативность и эффективность процесса аудита и его итог.

Выполнение аудита предполагает взаимодействие между участниками в рамках проверяемой системы менеджмента и средствами, используемыми для проведения аудита. В Таблице А.1 приведены примеры методов аудита, которые могут быть использованы, как по отдельности, так и в комбинации, для достижения целей аудита. Если аудит предполагает привлечение группы по аудиту, состоящей из нескольких человек, могут быть использованы одновременно как методы для работы на месте, так и дистанционные методы.

ПРИМЕЧАНИЕ Дополнительная информация по посещению физических мест приведена в разделе А.15.

Таблица А. 1 – Методы аудита

Характер взаимодействия аудитора и проверяемой организации	Местонахождение аудитора	
	Непосредственно на рабочем месте	Дистанционно
С участием людей	Проведение интервью Заполнение чек-листов и вопросников с участием проверяемого лица Анализ документов с участием проверяемого лица Выборка образцов	С использованием интерактивных средств общения: — проведение интервью; — наблюдение за работой в присутствии удаленного представителя; — заполнение чек-листов и вопросников; — анализ документов с участием проверяемого лица
Без участия людей	Анализ документов (например, записей, данных). Наблюдение за выполнением работы Посещение рабочих мест	Анализ документов (например, записей, данных) Наблюдение за выполнением работы средствами удаленного контроля с соблюдением социальных, законодательных и

	Заполнение чек-листов Выборка образцов (например, продукции).	нормативных требований Анализ данных
--	--	---

Мероприятия аудита непосредственно на рабочем месте выполняются по месту нахождения проверяемого лица. Мероприятия дистанционного аудита выполняются в любом месте, за исключением места нахождения проверяемого лица, независимо от расстояния.

Мероприятия интерактивного аудита предполагают взаимодействие между персоналом проверяемой организации и группой по аудиту. Мероприятия неинтерактивного аудита не подразумевают личного взаимодействия с теми, кто, представляет проверяемую организацию, но предполагают работу с оборудованием, техническими средствами и документацией.

Ответственность за результативное применение методов аудита для любого конкретного аудита на стадии планирования лежит либо на лице(ах), управляющем(ими) программой аудита, либо на руководителе группы по аудиту. Эта же ответственность лежит на руководителе группы по аудиту и за осуществление мероприятий по аудиту.

Возможность дистанционного аудита может зависеть от нескольких факторов (например, уровня риска для достижения целей аудита, уровня доверия между аудитором и персоналом проверяемой организации, а также регламентирующих требований).

На уровне программы аудита должна быть обеспечена уверенность, что использование методов аудита, относящихся к дистанционным и «на месте», является пригодным и сбалансированным для того, чтобы обеспечить удовлетворительное достижение целей программы аудита.

А.2 Процессный подход к аудиту

Использование «процессного подхода» является требованием для всех стандартов ISO на системы менеджмента в соответствии с Директивами ISO/IEC, часть 1, Приложение SL. Аудиторы должны понимать, что аудит системы управления проверяет процессы организации и их взаимодействия в отношении одного или нескольких стандартов на системы менеджмента. Достоверные и предсказуемые результаты достигаются более результативно и эффективно, когда деятельность рассматривается и управляется как взаимосвязанные процессы, которые функционируют как согласованная система.

А.3 Профессиональное суждение

Аудиторы должны выносить профессиональное суждение в процессе аудита и избегать акцентирования внимания на конкретных требованиях каждого раздела стандарта в ущерб оценке достижения намеченных результатов системы менеджмента. Некоторые разделы стандартов ISO на системы менеджмента сложно проверить сравнением содержания процедуры или рабочей инструкции с набором критериев. В этих ситуациях аудиторы должны использовать свое профессиональное суждение, чтобы определить, достигнуты ли цели, заложенные в этом разделе.

А.4 Результаты функционирования

Аудиторы в ходе всего процесса аудита должны акцентировать внимание на предполагаемом результате системы менеджмента. При том, что процессы и то, чего они достигают, имеют существенное значение, результат системы менеджмента и ее показатели – вот что в конечном счете важно. Также важно учитывать уровень интеграции различных систем менеджмента и их ожидаемые результаты.

Отсутствие процесса или документации может быть важным для организаций с высоким уровнем

риска или сложности, но не столь значимо для других организаций.

A.5 Проверка информации

Насколько это практически осуществимо, аудиторы должны проверить, представляет ли информация значимое объективное свидетельство, демонстрирующее выполнение требований, будучи:

- a) полной (в документированной информации имеются все ожидаемые сведения);
- b) правильной (содержание подтверждается другими достоверными источниками, такими как стандарты и регламентирующие документы);
- c) целостной (документированная информация не противоречит сама себе и согласуется с соответствующими документами);
- d) актуальной (содержит сведения на данный момент).

Следует также принимать во внимание, обеспечивает ли проверяемая информация достаточные свидетельства, чтобы продемонстрировать соответствие требованиям.

Если информация предоставляется в ином порядке, нежели ожидался (например, другими лицами, иными средствами), должна быть оценена целостность свидетельств.

Особое внимание необходимо уделять обеспечению информационной безопасности в связи с действующими нормами по защите данных (в частности, в отношении информации, которая не входит в область аудита, но содержится в документе).

A.6 Формирование выборки

A.6.1 Общие положения

Выборка при аудите осуществляется, когда практически невозможно или экономически нецелесообразно изучать в ходе аудита всю имеющуюся информацию, например, слишком много записей или они слишком разбросаны географически, чтобы проверять каждую из них. Выборка при аудите из большого количества – это процесс отбора менее 100% элементов в пределах общего набора данных (генеральной совокупности) для получения и оценки свидетельств по определенной характеристике этой генеральной совокупности, чтобы сформировать заключение, относящееся ко всей совокупности.

Задачей выборки при аудите является получение информации аудитором для обретения уверенности в том, что цели аудита могут или будут достигнуты.

Риск, связанный с выборкой, проявляется в том, что образцы могут быть не репрезентативными для генеральной совокупности, из которой они были отобраны. Таким образом, заключение аудитора может быть искаженным и будет отличаться от того, которое было бы, если бы исследовалась вся генеральная совокупность. Могут быть и другие риски, в зависимости от вариабельности в генеральной совокупности, из которой должны быть взяты образцы, и выбранного метода.

Выборка при аудите, как правило, включает в себя следующие шаги:

- a) установление целей выборки;
- b) выбор объема и состава генеральной совокупности для выборки;
- c) определение метода выборки;
- d) определение объема выборки;

- е) осуществления самой выборки;
- ф) сбор данных, оценка, формирование отчета и документирование результатов.

При выборке следует уделить внимание качеству имеющихся данных, т.к. выборка из неполных и неточных данных не даст полезного результата. Отбор подходящих образцов должен основываться как на методе выборки, так и на типе требуемых данных, например, с целью сделать заключение по конкретным моделям поведения или сделать выводы по всей генеральной совокупности.

Отчет о сделанной выборке может принимать во внимание размер выборки, метод отбора и оценки, сделанные на основе выборки и уровня доверительной вероятности.

Аудиты могут использовать либо детерминированные выборки (см. А.6.2) или случайные выборки (см. А.6.3).

А.6.2 Детерминированная выборка

Детерминированная выборка опирается на компетентность и опыт группы по аудиту (см. раздел 7).

При детерминированной выборке может быть принято в расчет следующее:

- а) опыт предыдущих аудитов в пределах области аудита;
- б) сложность требований (включая законодательные и нормативные требования) для достижения целей аудита;
- в) сложность и взаимодействие процессов организации и элементов системы менеджмента;
- г) степень изменений в технологии, эргономических факторах или системе менеджмента;
- е) ранее выделенные ключевые риски и возможности для улучшения;
- ф) результат мониторинга систем менеджмента.

Недостатком детерминированной выборки является то, что невозможна какая-либо статистическая оценка влияния неопределенности в результатах и выводах аудита.

А.6.3 Случайная выборка

Если принято решение использовать случайную выборку, план выборки должен быть основан на целях аудита и том, что известно о характеристиках генеральной совокупности, из которой должна быть сделана выборка.

Схема случайной выборки использует процесс отбора образцов, основанный на теории вероятности. Атрибутивное выборочное исследование используется, когда есть только два возможных варианта для каждого элемента выборки (например, правильный/неправильный или годный/не годный). Вариационное выборочное исследование используется, когда элементы выборки образуют непрерывный диапазон.

План выборки должен учитывать, какой вид исследования лучше подходит проверяемым результатам – атрибутивный или вариационный. Например, при оценке соответствия заполненных форм требованиям, изложенным в процедуре, мог бы быть использован атрибутивный подход. При изучении случаев инцидентов, связанных с безопасностью пищевых продуктов, или количества нарушений мер защиты, вариационный подход, скорее всего, будет более подходящим.

Элементы, которые могут влиять на план выборки аудита:

- а) контекст, размер, характер и сложность организации;

- b) число компетентных аудиторов;
- c) частота аудитов;
- d) срок конкретного аудита;
- e) любой уровень доверительной вероятности, определяемый внешними требованиями;
- f) имели ли место нежелательные и/или неожиданные события.

При разработке плана случайной выборки важно учесть тот уровень риска выборки, который аудитор готов принять. Это часто называют приемлемым уровнем достоверности. Например, риск выборки в 5% соответствует приемлемому уровню достоверности в 95%. Риск выборки в 5% означает, что аудитор готов принять риск того, что 5 из 100 (или 1 из 20) исследованных образцов не будут отражать действительные значения, которые были бы, если бы исследовали всю генеральную выборку.

Когда используется случайная выборка, аудиторы должны надлежащим образом документировать выполненную работу. Это должно включать описание генеральной совокупности, которая предполагалась для выборки, критерии выбора, использованные для оценки (например, что является приемлемым образцом), статистические параметры и методы, которые были использованы, количество оцененных выборок и полученные результаты.

A.7 Аудит соответствия в рамках системы менеджмента

Группа по аудиту должна проверить, есть ли у проверяемой организации результативные процессы для:

- a) выявления законодательных, нормативных требований и иных требований, которые она обязана выполнять;
- b) управления ее действиями, продуктами и услугами для достижения соответствия этим требованиям;
- c) оценки ее статуса соответствия.

В дополнение к общим указаниям, данным в настоящем документе, при оценке процессов, которые выполняла проверяемая организация чтобы обеспечить соответствие этим установленным требованиям, группа по аудиту должна принять во внимание в отношении проверяемой организации:

- 1) имеет ли она результативный процесс для идентификации изменений в соответствии требованиями и учета их в рамках управления изменениями;
- 2) имеет ли она компетентных лиц для управления процессами обеспечения соответствия;
- 3) поддерживает ли она и предоставляет ли соответствующую документированную информацию о ее статусе соответствия, как это требуется регулирующими органами или другими заинтересованными сторонами;
- 4) включает ли она требования соответствия в ее программу внутреннего аудита;
- 5) принимает ли она меры по всем случаям несоответствий;
- 6) рассматривает ли она показатели соответствия при анализе менеджмента.

A.8 Аудит контекста

Многие стандарты на системы менеджмента требуют от организации определения ее контекста,

включая потребности и ожидания соответствующих заинтересованных сторон, а также внешние и внутренние факторы. Чтобы выполнить это организация может использовать различные методы стратегического анализа и планирования.

Аудиторы должны подтвердить, что для этого разработаны и используются пригодные процессы, в силу чего их результаты обеспечивают надежную основу для определения области действия и развития системы управления. Для этого аудиторы должны рассмотреть объективные свидетельства, связанные со следующим:

- а) используемый(ые) процесс(ы) или метод(ы);
- б) пригодность и компетентность лиц, участвующих в процессе(ах);
- с) результаты процесса(ов);
- д) применение результатов для определения области действия и развития системы менеджмента;
- е) периодический анализ контекста в зависимости от ситуации.

Аудиторы для оценки результативности процессов, используемых для определения контекста, должны обладать соответствующими отраслевыми знаниями и пониманием инструментов управления, которые могут использовать организации.

А.9 Аудит лидерства и обязательств

Многие стандарты на системы менеджмента повысили требования к высшему руководству.

Эти требования включают демонстрацию приверженности и лидерства путем принятия ответственности за результативность системы менеджмента и выполнения ряда обязательств. К ним относятся задачи, выполнение которых руководство должно взять на себя, а также другие, выполнение которых может быть делегировано.

Аудиторы должны получить объективные свидетельства степени, в которой высшее руководство участвует в принятии решений, связанных с системой менеджмента, и как оно подтверждает выполнение обязательств по обеспечению ее результативности. Это может быть достигнуто путем анализа результатов соответствующих процессов (например, политик, целей, доступных ресурсов, коммуникаций со стороны высшего руководства) и интервьюирования персонала для определения степени участия высшего руководства.

Аудиторы должны также стремиться к проведению интервью с высшим руководством, чтобы убедиться, что у него есть адекватное понимание специфических вопросов, связанных с системой менеджмента, а также контекста, в котором организация работает с тем, чтобы оно могло обеспечить достижение системой менеджмента намеченных результатов.

Аудиторы не должны сосредотачиваться на лидерстве только на высшем уровне управления, но также должны проверять лидерство и выполнение обязательств на других уровнях управления, насколько это применимо.

А.10 Аудит рисков и возможностей

Как часть задачи конкретного аудита может быть включено определение и управление рисками и возможностями организации. Основными целями такого аудита являются:

- получить уверенность в надежности процесса(ов) выявления рисков и возможностей;
- получить уверенность в правильности определения и управления рисками и возможностями;

- проанализировать, как организация принимает меры в отношении выявленных ею рисков и возможностей.

Аудит подхода организации к определению рисков и возможностей не следует выполнять как отдельное мероприятие. Он должен быть частью всего аудита системы менеджмента, в том числе и интервью с высшим руководством. Аудитор должен действовать в соответствии с ниже приведенными шагами и собирать следующие объективные доказательства:

а) исходные данные, используемые организацией для определения ее рисков и возможностей, которые могут включать:

- результаты анализа внешних и внутренних факторов;
- стратегию развития организации;
- заинтересованные стороны, связанные с конкретной системой менеджмента, и их требования;
- потенциальные источники риска, такие как экологические аспекты и угрозы безопасности и т. д.

б) методы оценки рисков и возможностей, которые могут различаться для разных систем менеджмента и отраслей.

Принятие организацией мер в отношении рисков и возможностей, включая приемлемый уровень рисков и способ управления ими, потребует применения профессионального суждения аудитором.

A.11 Жизненный цикл

Некоторые системы менеджмента требуют применения концепции жизненного цикла к их продуктам и услугам. Аудиторы не должны рассматривать это как требование принятия концепции жизненного цикла. Идея жизненного цикла предполагает учет степени контроля и влияния, которое организация имеет на протяжении всех этапов жизненного цикла своего продукта и услуги. Этапы жизненного цикла включают в себя приобретение сырья, проектирование, производство, транспортировку/доставку, использование, окончание срока службы и окончательную утилизацию. Этот подход позволяет организации идентифицировать те области, где, рассматривая ее сферу деятельности, он может минимизировать влияние на окружающую среду при одновременном добавлении ценности организации. Аудитор должен использовать свое профессиональное суждение относительно того, как организация применяет концепцию жизненного цикла с точки зрения ее стратегии и:

- а) срока жизни продукта или услуги;
- б) влияния организации на цепочку поставок;
- с) длины цепочки поставок;
- д) технологической сложности продукции.

Если организация, исходя из собственных потребностей, объединила несколько систем менеджмента в единую систему менеджмента, аудитор должен внимательно изучить любое дублирование в части жизненного цикла.

A.12 Аудит цепочки поставок

В соответствии с определенными требованиями может потребоваться аудит цепочки поставок. Программа аудита поставщика должна быть разработана с использованием соответствующих критериев аудита внешних поставщиков. Объем аудита цепочки поставок может различаться,

например, полный аудит системы менеджмента, аудит одного процесса, аудит продукта, аудит конфигурации.

A.13 Подготовка рабочих документов

При подготовке рабочих документов группа по аудиту должна рассмотреть приведенные ниже вопросы применительно к каждому документу.

- a) Какие записи аудита будут созданы с использованием этого рабочего документа?
- b) Какое мероприятие аудита связано с данным конкретным рабочим документом?
- c) Кто будет пользователем этого рабочего документа?
- d) Какая информация необходима для подготовки данного рабочего документа?

При комбинированных аудитах рабочие документы должны быть разработаны так, чтобы избежать дублирования мероприятий за счет:

- группировки аналогичных требований из разных источников;
- координации содержания соответствующих чек-листов и вопросников.

Рабочие документы должны быть достаточными для охвата всех элементов системы менеджмента в рамках области аудита и могут быть представлены на любых носителях.

A.14 Выбор источников информации

Выбранные источники информации могут варьироваться в зависимости от области и сложности аудита и могут включать в себя следующее:

- a) интервью с работниками и другими лицами;
- b) наблюдения за действиями, окружающей рабочей средой и условиями;
- c) документированную информацию, такую как политики, цели, планы, процедуры, стандарты, инструкции, лицензии и разрешения, спецификации, чертежи, контракты и заказы;
- d) записи, такие как протоколы контроля, протоколы совещаний, отчеты об аудитах, отчеты по программе мониторинга и результаты измерений;
- e) сводки данных, результаты анализа и показатели функционирования;
- f) информацию о планах выборки для проверяемой организации и любых процедурах контроля процессов выборки и измерений;
- g) отчеты из других источников, например, отзывы потребителей, внешние исследования и измерения, другая соответствующая информация от внешних сторон и оценки внешних поставщиков;
- h) базы данных и веб-сайты;
- i) результаты моделирования.

A.15 Проведение аудита на месте

Чтобы свести к минимуму влияние, вносимое аудитом в рабочие процессы проверяемой организации, и для обеспечения здоровья и безопасности группы по аудиту во время визита, следует принимать во внимание следующее:

а) Планирование посещения:

- обеспечить разрешения и доступ к тем участкам проверяемой организации, которые необходимо посетить в соответствии с областью аудита;
- предоставить аудиторам достоверную информацию о безопасности, мерах по охране здоровья (например, карантин), вопросах охраны труда и техники безопасности, а также культурных нормах и рабочих часах для посещения, включая запрошенные и рекомендуемые вакцинации и разрешения, если это необходимо;
- получить подтверждение от проверяемой организации, что любые требуемые средства индивидуальной защиты (СИЗ) будут предоставлены группе по аудиту, если необходимо;
- подтвердить договоренности с проверяемой организацией относительно использования мобильных устройств и камер, включая информацию о такого рода записях, как фотографии рабочих мест и оборудования, копии экрана или фотокопии документов, видеозаписи действий и интервью, с учетом вопросов безопасности и конфиденциальности;
- гарантировать, что персонал посещаемой организации будут проинформирован о целях и области аудита за исключением внеплановых – по конкретному поводу – аудитов.

б) Мероприятия на месте:

- избегать любого неоправданного нарушения рабочих процессов;
- гарантировать, что группа по аудиту использует средства индивидуальной защиты должным образом (если это необходимо);
- гарантировать, что действия в чрезвычайной ситуации доведены до сведения (например, расположение аварийных выходов, точек сбора);
- выстраивать коммуникации так, чтобы минимизировать прерывания в работе организации;
- подстраивать размер группы по аудиту и количество сопровождающих и наблюдателей под область аудита, чтобы избежать помех для рабочих процессов, насколько это практически возможно;
- не трогать или не управлять каким-либо оборудованием, если явным образом не разрешено, даже при наличии компетентности или лицензии;
- если произошел инцидент во время работы на месте, руководитель группы по аудиту должен проанализировать ситуацию с проверяемой организацией и, при необходимости, с заказчиком аудита и прийти к согласию о том, следует ли аудит прервать, внести изменения в график или продолжить;
- если производится копирование документов на любом носителе, то следует заранее запросить разрешение и учесть вопросы обеспечения защиты и конфиденциальности;
- при ведении заметок избегать сбора личной информации, если это не требуется целями или критериями аудита;

в) Мероприятия при удаленном аудите:

- обеспечить, чтобы группа по аудиту использовала согласованные протоколы удаленного доступа, включая запрашиваемые устройства, программное обеспечение и т. д.;
- если необходимо снимать копии любых документов любого типа, заранее запросить разрешение

и учесть вопросы конфиденциальности и безопасности, а также избегать съемки людей без их разрешения;

- если произошел инцидент во время удаленного аудита, руководитель группы по аудиту должен рассмотреть ситуацию с проверяемой организацией и, при необходимости, с заказчиком аудита и прийти к согласию о том, следует ли аудит прервать, внести изменения в график или продолжить;
- использовать планы/схемы этажей удаленного места как ссылочный материал;
- соблюдать конфиденциальность во время перерывов в ходе аудита.

Необходимо рассмотреть вопрос об уничтожении информации и свидетельств аудита, независимо от типа носителя, после того, как отпадет необходимость в их сохранении.

A.16 Проведение удаленного аудита

Удаленные аудиты проводятся, когда организация выполняет работу или предоставляет услугу, в режиме онлайн, позволяющего людям независимо от физического местоположения выполнять процессы (например, Интранет компании, “вычислительное облако”). Аудит виртуальных рабочих мест иногда называют удаленным¹ аудитом. Удаленные аудиты связаны с использованием технологий для сбора информации, взятия интервью у проверяемого лица и т.д., когда непосредственные личные встречи невозможны или нежелательны.

Удаленный аудит выполняется в соответствии со стандартным процессом аудита, но с использованием технических средств для проверки объективных свидетельств. Аудитор и группа по аудиту должны соблюдать соответствующие требования к техническим средствам для удаленных аудитов, которые могут включать:

- гарантию того, что группа по аудиту использует согласованные протоколы удаленного доступа, включая запрошенные устройства, программное обеспечение и т. д.;
- проведение технических проверок перед аудитом для решения технических вопросов;
- обеспечение наличия и ознакомления с планами действий в чрезвычайных ситуациях (например, прекращение доступа, использование альтернативных средств), включая предоставление дополнительного времени для проведения аудита, если это необходимо.

Компетентность аудитора должна включать в себя:

- технические навыки использования соответствующего электронного оборудования и других средств при проведении аудита;
- опыт проведения удаленных совещаний для применения при проведении удаленного аудита.

При проведении в удаленном режиме открывающего совещания или аудита аудитор должен учесть следующее:

- риски, связанные с удаленным аудитом;
- использование поэтажных планов/схем удаленных мест в качестве справочного материала или схемы размещения информации в электронном виде;
- принимать меры для снижения негативного влияния прерывания работы на время аудита;

¹ В русском варианте используется несколько терминов: «удаленный аудит», «виртуальный аудит», «дистанционный аудит», «онлайн аудит». Ни один из этих вариантов не является общепринятым на данный момент. В данном переводе используется термин «удаленный аудит» – [прим. пер.]

- получение заранее разрешения на снятие с экрана копий документов или любых записей, а также принятие во внимание вопросов конфиденциальности и безопасности;;
- обеспечение конфиденциальности во время перерывов в аудите, например, отключение микрофона, установление камер на паузу.

A.17 Проведение интервью

Интервью являются важным средством сбора информации и должны проводиться, будучи адаптированными к ситуации и интервьюируемому лицу, либо лично, либо с помощью средств коммуникаций. Однако аудитор должен иметь в виду следующее:

- a) интервью должны проводиться с лицами соответствующих уровней и функций, осуществляющих деятельность или выполняющих задачи в рамках области аудита;
- b) интервью, как правило, должны проводиться в обычное рабочее время и, где это практически осуществимо, на рабочем месте интервьюируемого;
- c) следует стараться создать для интервьюируемого непринужденную обстановку до и во время интервью;
- d) следует пояснить причину интервью и комментировать любые делаемые заметки;
- e) интервью могут начинаться с просьбы к интервьюируемому описать свою работу;
- f) типы вопросов должны тщательно выбираться (например, открытые, закрытые, наводящие вопросы, позитивные вопросы);
- g) понимание ограниченности невербальных средств общения в виртуальной среде; вместо этого следует сосредоточиться на типе вопросов, чтобы использовать их для поиска объективных свидетельств;
- h) результаты интервью должны быть обобщены и проанализированы вместе с интервьюируемым;
- i) следует поблагодарить интервьюируемых за их участие и сотрудничество.

A.18 Выводы аудита

A.18.1 Определение выводов аудита

При определении выводов аудита следует учитывать следующее:

- a) последующие действия по записям и заключениям предыдущего аудита;
- b) требования заказчика аудита;
- c) точность, достаточность и пригодность объективных свидетельств для формирования выводов аудита;
- d) степень, с которой запланированные мероприятия аудита были выполнены и запланированные результаты получены;
- e) наблюдения, указывающие на нечто, выходящее за границы принятой практики, или возможности для улучшения;
- f) размер выборки;
- g) классификация (если используется) результатов аудита.

A.8.2 Регистрация соответствий

При фиксации соответствия должно быть предусмотрено следующее:

- a) указание критериев аудита на основании которых устанавливается соответствие;
- b) свидетельства аудита, подтверждающие соответствие и результативность, если применимо;
- c) заявление о соответствии, если это применимо.

A.8.3 Регистрация несоответствий

При фиксации несоответствия должно быть предусмотрено следующее:

- a) описание или ссылка на критерии аудита;
- b) свидетельства аудита;
- c) заявление о несоответствии;
- d) соответствующие выводы аудита, если это применимо.

A.8.4 Обработка выводов, связанных с множественными критериями

В ходе аудита могут быть выявлены ситуации, оцениваемые по нескольким критериям. Если аудитор при комбинированном аудите выявляет ситуацию, связанную с одним критерием, то он должен проанализировать возможное влияние на соответствующие или аналогичные критерии других систем менеджмента.

В зависимости от договоренностей с заказчиком аудита аудитор может фиксировать либо:

- a) отдельные выводы по каждому критерию; или
- b) один вывод с отсылкой к нескольким критериям.

В зависимости от договоренностей с заказчиком аудита аудитор может указать проверяемой организации, каким образом реагировать на эти выводы.

Библиография

- [1] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*
- [2] ISO 9001, *Quality management systems — Requirements*²
- [3] ISO Guide 73:2009, *Risk management — Vocabulary*
- [4] ISO/IEC 17021-1, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*

² См. www.iso.org/tc176/ISO9001AuditingPracticesGroup
А. Горбунов <http://pqm-online.com/>
Ред. 07.08.2018