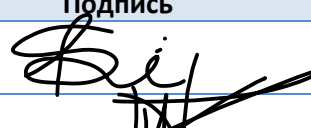


Программа Внутреннего Аудита

Version 1.0, 1.12.2020

Одобрение документа

Нижеподписавшиеся подтверждают, что они ознакомились с процессом управления доступом и полностью одобряют содержание документа.

Должность	ФИО	Подпись
Менеджер по информационной безопасности	All Si	
Генеральный директор	High Vision	

Этот документ рассматривается и утверждается руководством через Руководящий комитет ISMS, который отвечает за официальное разрешение на его публикацию. Любые запросы на внесение изменений в этот документ могут быть отправлены только в отдел качества и внутреннего аудита для дальнейшей обработки.

Информация о документе

Владелец:	Менеджер по информационной безопасности	Дата выпуска:	01 декабря 2020
Email:	SiAll@AlphaBetaPrinting.com	Дата последнего обновления:	
		Дата следующего обновления:	

Хронология документа

Версия	Автор	Дата	Изменения
0.1	Менеджер по качеству	01/09/2020	Первоначальный проект опубликован для рассмотрения и комментариев
0.2	Менеджер по качеству	01/10/2020	Второй проект опубликован для рассмотрения и комментариев
1.0	Менеджер по качеству	30/10/2012	Опубликован для внедрения

Содержание

1	Введение.....	3
1.1	Область применения	3
1.2	Владелец.....	3
1.3	Аспекты информационной безопасности, охраны здоровья и безопасности	3
2.	Основы политики	4
2	Процесс	5
3	Записи	14
4	KPI показатели	14

1 Введение

В этом документе описываются роли и обязанности, а также способ проведения внутренних аудитов в соответствии с требованиями стандарта ISO 27001:2013.

Целью проведения внутренних аудитов является изучение и оценка эффективности процессов организации, определение областей для улучшения бизнеса и обеспечение соответствия нормативным актам, стандартам и рабочей политике и практикам компании, включая соответствие требованиям стандарта ISO 27001:2013.

Этот процесс применяется ко всем аудитам, проводимым внутри организации, внешними компаниями, текущими и потенциальными поставщиками.

1.1 Область применения

Этот документ применим ко всем подразделениям организации.

1.2 Владелец

Владельцем этого документа является менеджер по качеству. Любые изменения в документ могут быть внесены только менеджером по качеству после контроля процесса документов и записей.

1.3 Аспекты информационной безопасности, охраны здоровья и безопасности

Информационная безопасность: Проявляйте заботу о защите конфиденциальности и целостности данных, собранных и управляемых во время выполнения этого процесса.

Здоровье и безопасность: Соблюдайте все соответствующие правила и рекомендации по охране труда при проведении аудита в областях, которые представляют (или могут представлять) опасность для здоровья. Может потребоваться использование средств индивидуальной защиты (СИЗ) (например, использование защитной обуви при проверке цехов).

2. Основы политики

Система менеджмента была разработана в соответствии с требованиями стандарта ISO 27001:2013.

Процедуры информационной безопасности определены в Руководстве вместе с философией, видением и миссией организации.

Поскольку размер и требования организации постоянно развиваются, важно проводить аудит на плановой основе внедренной системы менеджмента организации, чтобы гарантировать ее постоянную пригодность и эффективность в удовлетворении требований и нужд организации.

2 Процесс

S/N	Роль	Ответственность	Комментарий
1	Внутренний аудитор	<p>Планировать аудиты на основе годового плана аудита и/или любых других исходных данных.</p> <p>Внутренний аудитор готовит Годовой план аудита, используя соответствующую форму, охватывающую тип аудитов, а также частоту и методы аудита. Годовой план аудита учитывает статус и важность процессов и областей, подлежащих аудиту, отчет об оценке рисков, а также результаты предыдущих аудитов.</p> <p>Все отделы и процессы организации, входящие в сферу охвата, должны проходить аудит один раз в год. Как упоминалось выше, принимая во внимание оценку рисков, новизну процессов, несоответствия, внесенные изменения и т.д., отдельные аудиты могут проводиться с определенной периодичностью.</p>	<p>Любой тип аудита может быть проведен в результате:</p> <ul style="list-style-type: none"> Годового план аудита Результатов проверок внешних органов Действий, согласованных во время совещаний руководства и/или любого другого совещания Результатов опросов, анкет поставщиков и любых других ключевых показателей эффективности Запросов от отделов организации Результатов оценки поставщиков и официальные лица Любого внутреннего запроса на аудит текущего или потенциального поставщика
2	Внутренний аудитор	<p>Внутренний аудитор представляет план менеджеру по информационной безопасности на утверждение.</p> <p>Менеджер по информационной безопасности представляет Годовой план аудита Руководящему комитету для окончательного утверждения.</p> <p>После утверждения годового плана аудита Внутренний аудитор доводит план до сведения заинтересованных сторон (проверяемых).</p>	

S/N	Роль	Ответственность	Комментарий
3	Внутренний аудитор	<p>Уведомить руководство областей, подлежащих аудиту, относительно:</p> <p>а) цели и объем аудита</p> <p>б) времени аудита и</p> <p>с) Предлагаемого графика мероприятий на месте и времени, необходимого конкретным командам.</p> <p>Необходимо достичь общего консенсуса между руководством проверяемой области и внутренним аудитором, чтобы определить соответствующих представителей, доступных для проведения аудита.</p> <p>Кроме того, следует предпринять дальнейшие действия для того, чтобы сообщить о предстоящем аудите заинтересованным подразделениям компании и собрать любую другую соответствующую информацию.</p>	Обсуждение предстоящего аудита должно проводиться с соответствующим руководством.
4	Внутренний аудитор	<p>Создать аудиторскую группу, выбрав членов с соответствующим опытом в области/системе, подлежащей оценке.</p> <p>Минимальные компетенции (образование, профессиональная подготовка, опыт, навыки) для роли внутреннего аудитора Системы управления информационной безопасностью определены в должностной инструкции внутреннего аудитора.</p> <p>Более того, для всех членов команды отбор должен соответствовать следующим требованиям независимости:</p> <ul style="list-style-type: none"> - Ни один внутренний аудитор не должен проверять свою собственную работу. - Ни один внутренний аудитор не должен проверять своего непосредственного руководителя. - Ни один внутренний аудитор не должен проверять членов своей ближайшей семьи. 	Проинформировать других внутренних аудиторов

S/N	Роль	Ответственность	Комментарий
5	Внутренний аудитор	<p>Просмотреть качественные результаты, прежде чем оценивать какую-либо область / процесс / поставщика.</p> <p>Качественными результатами могут быть: отзывы клиентов, измерения производительности поставщиков, инциденты информационной безопасности, связанные показатели, журналы, статистика контроля качества, временные планы проектов, результаты тестов, официальные данные предыдущих аудитов и т.д.</p>	<p>Команда аудиторов должна проанализировать все данные и/или ключевые показатели эффективности, относящиеся к сфере аудита:</p> <ul style="list-style-type: none"> • Обзор соответствующей существующей документации (документы процесса, процедуры, результаты предыдущих аудитов, самоаудит и т.д.) • Качественные результаты по показателям качества: отзывы клиентов, измерения производительности поставщиков, инциденты информационной безопасности, связанные показатели, журналы, статистика контроля качества, временные планы проектов, результаты тестов и т.д. <ul style="list-style-type: none"> ▪ Результаты KPI ▪ Инциденты , связанные с безопасностью , произошедшие с момента последнего аудита ▪ Кадровые проблемы , связанные с безопасностью , возникшие после последнего аудита ▪ Результаты любой оценки рисков , проведенной с момента последнего аудита , и обсуждение предлагаемых мер контроля ▪ Назначение людей или процессов для управления рисками (например, страхование). ▪ Предлагаемые изменения в Политике безопасности ▪ Отчеты о ходе выполнения ранее принятых мер

S/N	Роль	Ответственность	Комментарий
6	Внутренний аудитор	В случае аудита процесса, если процесс, подлежащий оценке, еще не нанесен на карту и не утвержден с помощью корпоративного документооборота, проект блок-схемы может быть разработан на основе соответствующей документации и / или любой другой доступной информации. На основе этого проекта может быть подготовлен конкретный контрольный чек-лист список интервью.	Для первоначального аудита процесса команде аудиторов рекомендуется подготовить настольную схему технологического процесса, которая может помочь им получить целостное и интегрированное представление о процессе.
7	Внутренний аудитор	Для каждого конкретного отдельного аудита определить области для оценки и при необходимости подготовьте контрольный чек-лист.	Внутренний аудитор (ы) собирает и изучает результаты предыдущих аудитов и возможные нерешенные вопросы. Кроме того, команда готовит любые дополнительные документы, которые будут необходимы для проведения аудита (например, чек-лист для аудитов QMS и ISMS).
8	Внутренний аудитор	Провести обзор соответствующей существующей документации (документы процесса, процедуры, результаты предыдущих аудитов, самоаудит и т.д.)	
9	Внутренний аудитор	Подготовить программу аудита , включающую: <ul style="list-style-type: none"> • задачи и объем аудита • время аудита, • цель аудита • список участников • Расписание интервью, если это необходимо. Повестка дня аудита рассылается не менее чем за 5 рабочих дней всем вовлеченным сторонам для окончательного подтверждения аудита.	
10	Внутренний аудитор	Аудит начинается с ознакомительного совещания с руководством функции/отдела, подлежащего оценке, чтобы четко объяснить цель и процесс аудита.	В ходе этой встречи должны быть рассмотрены следующие вопросы: <ol style="list-style-type: none"> 1) Цель аудита 2) Объем аудита 3) Ожидаемые результаты аудита 4) Процесс, которому следует следовать во время аудита 5) Предыдущие результаты аудита

S/N	Роль	Ответственность	Комментарий
11	Внутренний аудитор	<p>Провести аудит в заранее установленные сроки.</p> <p>Процесс аудита включает в себя:</p> <ul style="list-style-type: none"> • Интервью с соответствующими сотрудниками • Пошаговое руководство по оцениваемой области. • Сбор и анализ соответствующей документации и/ или доказательств. • Наблюдение за системами и процессами. • Внутренний аудитор ISMS проводит аудит и завершает предварительно определенный аудиторский отчет. В ходе аудита Внутренний аудитор пытается выявить достаточные доказательства, чтобы убедиться в том, что: • Документированные процедуры соблюдаются (т.е. в рамках ISMS) и соответствуют их желаемым целям • Согласованные действия по результатам предыдущих аудитов были реализованы • ISMS соответствуют стандарту • Политика безопасности является точным отражением бизнес - требований • Что процессы измеряются с точки зрения их эффективности. • KPI достигнуты, а если нет, то предпринимаются соответствующие корректирующие действия. • Используется соответствующая методология оценки рисков • Технические средства контроля установлены, правильно настроены и работают по назначению и эффективно • Остаточные риски были оценены правильно и приемлемы для руководства компании 	<p>Аудиты проводятся группой аудиторов путем проведения ряда интервью.</p> <p>Во время интервью аудиторы должны:</p> <ul style="list-style-type: none"> • Собрать всю необходимую информацию по обсуждаемым вопросам. • Определить сильные стороны и области, требующие улучшения • В случае аудита процесса собрать всю необходимую информацию и данные для проверки или обновления существующей карты процесса или разработки новой.

S/N	Роль	Ответственность	Комментарий
12	Внутренний аудитор	<p>По завершении аудита проводится заключительное совещание с привлеченным руководством проверяемой области. Во время заключительного совещания должны быть рассмотрены и согласованы следующие вопросы:</p> <ol style="list-style-type: none"> 1) Результаты аудита 2) Результаты аудита и области для улучшения согласовываются с руководством проверяемой области. 3) План действий с предлагаемыми корректирующими или предупреждающими действиями, согласованный с местным руководством. <p>Для аудитов, которые длятся более 1 дня, в конце каждого дня требуется итоговое совещание с руководством, чтобы информировать и согласовать выводы.</p>	<p>Вся аудиторская группа должна присутствовать (если это практически возможно) на заключительном совещании.</p>

S/N	Роль	Ответственность	Комментарий
13	Внутренний аудитор	<p>Подготовить аудиторский отчет в согласованное время.</p> <p>Аудиторский отчет включает в себя выводы аудита и корректирующие действия и/или возможности для улучшения, согласованные во время заключительного совещания, а также любую другую полезную информацию, которую аудиторская группа хотела бы сообщить.</p>	<p>Любой вывод аудита должен быть помечен в соответствии с его уровнем приоритета:</p> <ul style="list-style-type: none"> Результаты аудита, которые характеризуются как приоритет 1, являются серьезными несоответствиями и должны быть запланированы для устранения в течение 2 недель, а последующий аудит должен быть запланирован в конце этого периода. Обратите внимание, что, если это считается критичным, может потребоваться немедленное решение по некоторым выводам аудита. Результаты аудита, которые характеризуются как приоритет 2, являются незначительными несоответствиями и должны быть запланированы для устранения в течение 3 месяцев, а последующий аудит должен быть запланирован в конце этого периода Результаты аудита, которые характеризуются как наблюдения, должны быть запланированы для разрешения в течение 6 месяцев, и их прогресс должен отслеживаться во всех следующих периодических аудитах до разрешения Результаты аудита и соответствующее им несоответствие должны быть доведены до сведения менеджера по информационной безопасности в конце каждого аудита
Internal Use			каждого аудита

S/N	Роль	Ответственность	Комментарий
14	Внутренний аудитор	В случае аудита процесса должна быть определена и разработана вся необходимая документация, включая соответствующую технологическую схему.	
15	Внутренний аудитор	<p>Распространить аудиторский отчет среди руководства оцениваемой области и других заинтересованных получателей.</p> <p>Отчет должен быть отправлен в течение 5 рабочих дней после заключительного заседания.</p> <p>В исключительных случаях и в случае, если во время внутреннего аудита заключительное заседание не может быть проведено, проект отчета, включающий рекомендации и предлагаемые действия, направляется для официальных комментариев и принятия ответа руководства.</p>	Если это применимо, к отчету может быть приложена обновленная карта процесса.
16	Внутренний аудитор	<p>Записать согласованные области для улучшений и предлагаемые корректирующие действия.</p> <p>Выявленные проблемы, предлагаемые действия, ответственный персонал, целевая дата, а также статус проблемы сохраняются в конкретных планах действий для каждого отдела и/или для каждого процесса</p>	В соответствии с результатами аудита и уровнем несоответствия должен быть разработан план действий (указанный в журнале корректирующих/предупреждающих действий).
17	Внутренний аудитор	<p>Отслеживать последующие меры по поднятым областям для улучшений / нерешенным (ожидающим рассмотрения) выводам.</p> <p>На основе плана действий менеджер по информационной безопасности координирует действия по выполнению корректирующих действий и соответствующим образом обновляет журнал корректирующих/предупреждающих действий.</p> <p>Менеджер по информационной безопасности должен оценить эффективность реализованных действий (задокументированных в журнале корректирующих/предупреждающих действий) и, если он сочтет необходимым, он может запросить повторный аудит. Объем последующих аудитов ограничен несоответствием, и используются те же механизмы аудита, которые привели к выводу.</p>	<p>Совещания по обзору проекта или команды и/или любое другое совещание могут быть запланированы на ежегодной основе. Во время этих встреч (среди прочего) может быть проведена последующая работа с областями для улучшений.</p> <p>Также, если будет сочтено необходимым, может быть осуществлен специальный контроль за ходом выполнения.</p>

S/N	Роль	Ответственность	Комментарий
18	Руководящий комитет	Рассмотрение руководством	Результаты внутренних аудитов должны быть рассмотрены в ходе ежегодного рассмотрения руководством

3 Записи

S/N	Наименование	Тип	Время хранения	Ответственный	Место	Классификация
1.	Аудиторские записи, включая повестку дня, подтверждения, аудиторский отчет, открытые вопросы, примечания, вопросник по аудиту процесса и т.д.	Электронные или физические	3 года	Внутренний аудитор	Соответствующая область	Конфиденциально

4 KPI показатели

Наименование KPI	Периодичность	Ответственный	Место	Target
Аудиты MS, проведенные в соответствии с планом	Ежегодно	Менеджер по качеству	Электронный файл	100% как запланировано
% несоответствий—устраненных в течение обозначенного времени	Ежеквартально	Менеджер по качеству	Электронный файл	80% в обозначенное время