

alpha

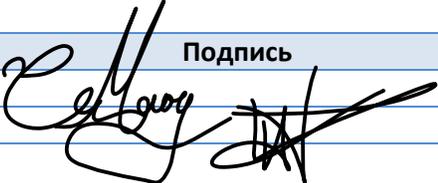
BETA

Процесс Управления рисками

Version 1.0, 01.12.2020

Одобрение документа

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

Должность	ФИО	Подпись
Менеджер по качеству	Mary Check	
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 документа:	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 информационной безопасности	01/09/2020	Первоначальный проект опубликован для рассмотрения и комментариев
0.2	Менеджер по информационной безопасности	01/10/2020	Второй проект опубликован для рассмотрения и комментариев
1.0	Менеджер по информационной безопасности	01/12/2020	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 Ссылки на документы.....	3
3 Процесс управления рисками.....	3
3.1 Область применения, Контекст и Критерии	4
3.1.1 Область применения.....	4
3.1.2 Критерии	4
3.2 Оценка Риска	7
3.3 Обработка Риска.....	8
4 Записи	9
5 KPI	9

1. Введение

Целью этого документа является определение методологии управления рисками информационной безопасности в типографии Alphabeta и предоставление всей информации, необходимой для различных ролей в организации для реализации этого процесса.

1.1 Область применения

Этот документ применим ко всем подразделениям организации.

1.2 Владелец

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

1.3 Аспекты информационной безопасности, охраны здоровья и безопасности

К данному документу не применяются никакие требования по охране труда и технике безопасности.

Что касается требований информационной безопасности, следует проявлять осторожность в отношении защиты Конфиденциальности, Целостности и Доступности всех документов и соответствующих записей, созданных в рамках реализации процедур обеспечения качества и информационной безопасности. Эта защита должна применяться с помощью надлежащих механизмов контроля доступа, как описано в документах “Управление доступом” и “Политике допустимого использования”.

2 Ссылки на документы

- ISO/IEC 27005:2018 INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — Information Security Risk Management
- ISO 31000:2018 RISK MANAGEMENT — GUIDELINES

3 Процесс управления рисками

Управление рисками носит повторяющийся характер и помогает организациям в определении стратегии, достижении целей и принятии обоснованных решений.

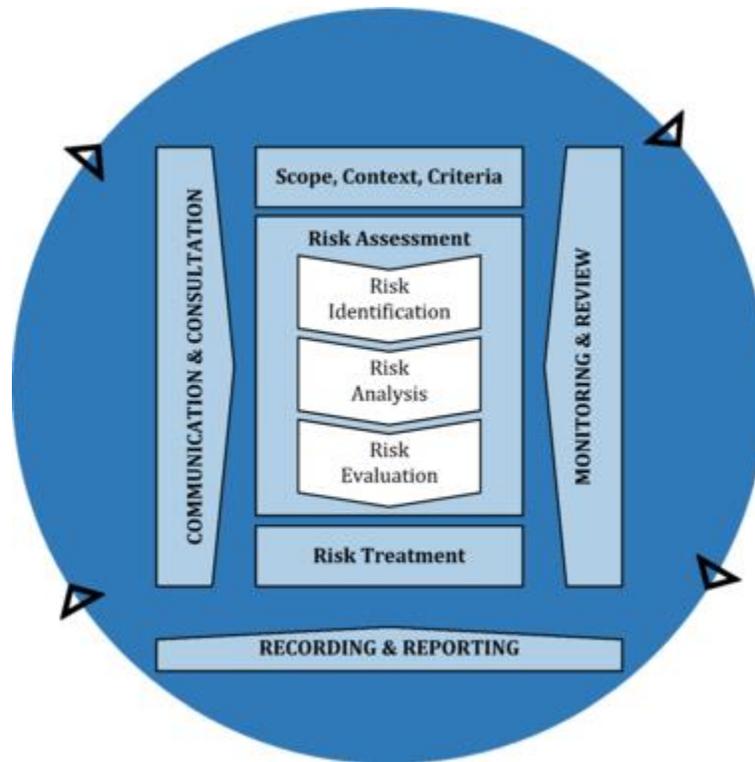
Управление рисками является частью управления и лидерства и имеет основополагающее значение для процесса управления организацией на всех уровнях. Это способствует совершенствованию системы управления.

Управление рисками является частью всех видов деятельности, связанных с организацией, и включает взаимодействие с заинтересованными сторонами.

Управление рисками учитывает внешний и внутренний контекст организации, включая поведение людей и культурные факторы.

[Источник ISO 31000:2018]

Процесс управления рисками включает систематическое применение политики, процедур и практик к деятельности по коммуникации и консультированию, установлению контекста и оценки, обработке, мониторингу, обзору, регистрации и представлению отчетности о риске. Этот процесс проиллюстрирован на следующем рисунке:



3.1 Область применения, Контекст и Критерии

3.1.1 Область применения

Данный риск информационной безопасности применим ко всей организации по конкретному предмету информационной безопасности. Этот процесс также используется в масштабе различных проектов организации с целью выявления рисков информационной безопасности также в ходе реализации проекта.

3.1.2 Критерии

Типография Alphabeta определила следующие критерии для использования в Процессе управления рисками, приведенные в данном документе.

Критерии Оценки Риска

Введение

Организация должна, как часть процесса управления рисками, указать величину и тип риска, который она может принимать или не принимать, в зависимости от целей. Таким образом, определение критериев для оценки значимости риска и поддержки процессов принятия решений является обязательным и отражено ниже.

Значимость риска (R) оценивается по следующей формуле с использованием терминов Вероятность (L) и Последствия (C).

$$R = L \times C$$

(определения из ISO 31000):

Вероятность - это шанс наступления события.

В терминологии управления рисками слово “вероятность” используется для обозначения вероятности того, что что-то произойдет, независимо от того, определено ли оно, измерено или определено объективно или субъективно, качественно или количественно, и описано с использованием общих терминов или математически (например, вероятность или частота за данный период времени).

Английский термин “likelihood” не имеет прямого эквивалента в некоторых языках; вместо этого часто используется эквивалент термина “probability”. Однако в английском языке “probability” часто узко интерпретируется как математический термин. Поэтому в терминологии управления рисками термин “likelihood” в широком значении, какое термин “probability” имеет во многих языках, отличных от английского.

Последствие - это результат события, влияющего на цели.

Следствие может быть определенным или неопределенным и может оказывать положительное или отрицательное прямое или косвенное воздействие на цели.

Последствия могут быть выражены качественно или количественно.

Любое последствие может усиливаться за счет каскадных и кумулятивных эффектов.

Шкалы

Для критериев, упомянутых выше, используются следующие шкалы:

Вероятность

Числовое значение	Качественное ранжирование	Описание
5	(Почти) возможно	Мы обязательно столкнемся с дальнейшими инцидентами подобного рода - на самом деле они, вероятно, происходят прямо сейчас! С точки зрения частоты, такие случаи являются обычным явлением.
4	Весьма вероятно	Вероятно, в скором времени мы столкнемся с инцидентами подобного рода. С точки зрения частоты такие инциденты могут происходить примерно раз в месяц.
3	Вероятно	Вполне возможно, что мы столкнемся с инцидентами такого рода. С точки зрения частоты такие инциденты могут происходить примерно раз в год.
2	Маловероятно	Инциденты такого рода редки, но есть реальный шанс, что мы можем столкнуться с ними в какой-то момент в будущем. С точки зрения частоты, такие инциденты, как известно, происходят в отрасли (один раз в пять лет).
1	Слабо вероятно (редко)	Хотя они возможны, мы сомневаемся, что когда-либо столкнемся с инцидентами подобного рода. Что касается частоты, то о подобных инцидентах в отрасли никогда не сообщалось.

Последствие

Числовое значение	Качественное ранжирование	Описание
5	Катастрофическое	Полный сбой в работе, непоправимый урон организации, информация, доверенная клиентами компании, была украдена или утеряна, организация не соблюдает важные законодательные или нормативные акты.
4	Значительное	Серьезная потеря работоспособности, наносящая значительный ущерб и чрезвычайно дорогостоящая, но жизнеспособная, информация, доверенная клиентами компании, была уничтожена, к некоторой информации получили доступ неавторизованные стороны, имеет место

		частичное несоблюдение организацией важного законодательства или нормативного акта.
3	Среднее	Существенное операционное воздействие, очень дорогостоящее, информация, доверенная клиентами компании, была недоступна в течение длительного периода времени, организации будет трудно доказать свое соответствие важному законодательству или нормативным актам
2	Минимальное	Заметное, но ограниченное операционное воздействие, некоторые затраты, информация, доверенная клиентами компании, недоступна в течение короткого периода времени, организация минимально не соответствует законодательству или нормативным актам
1	Незначительное	Минимальное, если такое имеется, операционное воздействие, незначительные затраты, некоторая информация организации (внутренняя, не связанная с клиентом) была утеряна или стала недоступной.

Критерий приемлемости риска

На основании формулы и критериев, приведенных выше, для оценки риска ($R = L \times C$) используется следующая таблица:

Вероятность ⇨ Последствие ⇩	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Организация установила значение 10 в качестве уровня приемлемости риска. Это означает, что риски, превышающие 10 (не включая 10), неприемлемы для организации и должны обрабатываться посредством обработки рисков.

3.2 Оценка Риска

Оценка риска - это общий процесс идентификации риска, анализа риска и сравнительной оценки риска.

Оценка рисков проводится систематически, итеративно и совместно, опираясь на знания и мнения заинтересованных сторон. Для нее используется актуальная доступная информация, дополняемая при необходимости дальнейшими запросами.

Оценка риска состоит из следующих этапов:

- Идентификация риска: Цель идентификации рисков состоит в том, чтобы найти, распознать и описать риски, которые могут помочь или помешать организации достичь своих целей. Соответствующая, уместная и актуальная информация важна для выявления рисков.
- Анализ риска: Целью анализа рисков является понимание природы риска и его характеристик, включая, при необходимости, уровень риска. Анализ рисков включает в себя детальное рассмотрение неопределенностей, источников риска, последствий, вероятности, событий, сценариев, средств контроля и их эффективности. Событие может иметь множество причин и последствий и может влиять на множество целей.
- Сравнительная оценка риска: Цель сравнительной оценки риска - поддержать принимаемые решения. Оценка риска включает сравнение результатов анализа риска с установленными критериями риска, чтобы определить, где требуются дополнительные действия.

Организация создала команду по управлению рисками, которой поручено идентифицировать, анализировать и оценивать риски. Команда будет взаимодействовать с остальными командами, чтобы получить необходимые знания.

Владелец любого риска в организации – Генеральный директор.

3.3 Обработка Риска

Целью обработки рисков является выбор и внедрение вариантов обработки риска.

Обработка рисков включает в себя итеративный процесс:

- формулирования и выбора вариантов обработки рисков;
- планирования и внедрения обработки рисков;
- оценку эффективности обработки;
- принятия решения о том, является ли оставшийся риск приемлемым;
- если это неприемлемо, продолжаем обработку.

Когда план обработки рисков в области информационной безопасности сформулирован, организация получает разрешение от владельцев рисков. Такое разрешение основано на определенных критериях принятия риска или обоснованной уступке, если есть какие-либо отклонения от них. Организация регистрирует принятие владельцем риска остаточного риска и одобрение руководством плана.

Это проводится путем внесения изменений в план обработки рисков, описанный выше, с помощью столбцов, указывающих эффективность контроля, остаточный риск и одобрение владельца риска..

4 Записи

S/N	Наименование	Тип	Время хранения	Ответственный	Место хранения	Классификация
1.	Файл управление рисками	электронный	3 года	Информ. риск менеджер	Соответствующие области сети	Конфиденциально

5 KPI

KPI Наименование	Периодичность	Ответственный	Место хранения	Цель
Количество эффективно выполненных планов по обработке рисков	Ежегодно	Информ. риск менеджер	Электронно	100%
Количество планов по обработке рисков, выполненных в заранее намеченные сроки	Ежегодно	Информ. риск менеджер	Электронно	100%