Периодическая оценка рисков внутренним аудитом

I. Введение

Шаблон пособия по хорошей практике внутреннего аудита, разработанный Практикующим сообществом по внутреннему аудиту Pempal, определяет важность и воздействие, которое действенная стратегия аудита и план аудита могут оказать на достижение общих целей, выполнение задач и миссии группы внутреннего аудита. Планирование обеспечивает систематический подход к работе внутреннего аудита и требует знаний и компетентности в широком ряде областей, таких как оценка риска и внутренний контроль.

Этот Шаблон методологии оценки рисков более подробно рассматривает процесс оценки рисков, как описано в параграфе 3.1.2 Шаблона Пособия по хорошей практике внутреннего аудита
:

- Идентификация и определение соответствующих категорий рисков;
- Идентификация и определение критериев риска для воздействия и вероятности;
- Определение содержания качественной оценки рисков и объяснение логического обоснования присвоения высокого, среднего или низкого балла определенному риску. Этот шаблон основан на Стандарте ИВА 2010, который гласит:

«Руководитель внутреннего аудита обязан составить риск-ориентированный план, определяющий приоритеты внутреннего аудита в соответствии с целями организации», а 2010.A1 требует следующее –
«План работы внутреннего аудита должен основываться на формализованной оценке рисков, проводимой, по крайней мере, один раз в год. При составлении плана должно учитываться мнение высшего руководства и Совета».

При составлении проекта шаблона также использовались консультационные и руководящие примечания ИВА, а также и общепринятые примеры хорошей практики, используемые для таких упражнений.

Шаблон шаг за шагом следует за процессом оценки рисков и приводит практический пример для каждого шага. В приложения можно найти дополнительные примеры используемой терминологии.

II. Почему оценка рисков является важной частью Внутреннего аудита?

Руководитель группы внутреннего аудита отвечает за разработку стратегического и ежегодного плана внутреннего аудита. Эти планы разрабатываются в ходе процесса, который идентифицирует и определяет приоритетность возможных тем аудита. Вся популяция потенциальных тем (которые могут быть операционными процессами или группами) называется **пространством аудита**[i1]. Для каждой из этих значимых тем в пространстве аудита нужно будет оценить риски или возможности.

Каковы риски?

Риск – это возможность того, что произойдет событие и негативно повлияет на достижение цели.

Основные риски – это риски, которые, при правильном управлении, сделают организацию успешной в достижении ее целей, или, в случае неправильного управления, приведут к краху организации.

Кто отвечает за риски?

Старшее руководство организации несет ответственность за смягчение рисков эффективным с точки зрения затрат образом. Как **«собственник рисков»** оно должно создать систему управления рисками.

Управление рисками связано с предотвращением плохих ситуаций (смягчение риска), или неспособностью гарантировать то, что будут иметь место хорошие ситуации (рассмотрение возможностей). В то время как многие риски действительно представляют угрозу для организации, неспособность достичь положительных результатов также может создать препятствие для достижения цели и, таким образом, ее также следует рассматривать как риск.

Риски и способ, которым ими управляет организация, должны быть независимо оценены внутренним аудитом. Результаты этой оценки обеспечат соответствующий периодический аудиторский охват классифицированного по рискам пространства аудита.

Кроме того, внутренний аудит фиксирует вклад от старшего руководства, чтобы удостовериться в том, что определенные как приоритетные риски, соответствуют взглядам и ожиданиям руководства.

[1] Объяснение процесса определения Пространства аудита не охвачено в данном шаблоне, но это первый шаг в процессе аудита. В этом шаблоне это рассматривается как данное

Когда оцениваются риски?

В идеале периодическая оценка рисков должна происходить ближе к концу года, например, в ноябре или декабре. Однако в любое время, когда происходят значительные события, например, пересмотр бюджета или радикальное урезание затрат, меняется подверженность риску, и необходимо провести новую (частичную) оценку риска. Результаты этой обновленной оценки риска могут привести к изменениям в годовом плане внутреннего аудита.

III. Что собой представляет процесс оценки рисков?

Каждая организация сталкивается с различными типами рисков. Риск представляет собой диапазон возможных результатов, от наилучших до наихудших сценариев. Процесс оценки рисков состоит из **пяти шагов**.

Шаг 1. Существует большое количество рисков, с которыми сталкиваются организации по мере того, как они пытаются выполнить свои стратегии и достичь своих поставленных целей. Таким образом, имеет смысл начать с ***определения категорий рисков***.

Шаг 2. Далее, необходимо определить для каждой категории (подкатегории) риска, какие риски будут оцениваться. Эта часть процесса оценки рисков называется ***определением факторов риска.***

Шаг 3. Не каждый определенный риск представляет собой одинаковую степень опасности для организации. Поэтому в шаге 3 Внутренний аудит оценивает воздействие риска вероятность возникновения риска. Эта часть процесса оценки риска называется ***определением критериев риска*** в плане того, как риски будут оцениваться и измеряться.

Шаг 4. После того как значимые факторы риска и критерии риска определены, их необходимо оценить и присвоить им баллы (сделать качественную оценку). Этот шаг называют ***присвоением баллов рискам***.

Шаг 5.. Результаты оценки различных значимых рисков будут консолидированы в пространстве аудита. Этот шаг называется ***определением классифицированного по рискам пространства аудита,*** которое послужит основой для разработки многолетних и годовых планов внутреннего аудита.

ЯЧЕЙКА ВИЗУАЛИЗАЦИИ ШАГОВ

IV. Шаги оценки рисков в подробностях

1. Как прийти к категориям рисков?

Чтобы определить категории рисков, непременно нужно следовать методологии, чтобы составить карту и оценить различные риски.

Хорошим способом структурированного подхода к оценке рисков является отнесение рисков к определенной группе категорий рисков.

В государственном секторе имеет смысл идентифицировать следующие широкие категории:

- *Управление, стратегия и планирование*. Это категория рисков, связанная с тем, как организована организация, включая разработку ее целей, стратегию и планирование.
- *Операции*. Это риски, связанные с основными операциями организации. В качестве примера для Министерства образования эта категория будет включать риски, связанные с обслуживанием школ, наем хороших преподавателей, предоставление признанных дипломов, и т.д.
- *Инфраструктура*. Это риски, связанные с различными поддерживающими процессами в рамках организации. Примеры поддерживающих процессов – это кадровые ресурсы, информационные технологии, финансы и т.д.
- *Соответствие*. Это риски, связанные с юридическими и нормативными требованиями. Примеры этих рисков включают несоответствие законам о труде, налогово-бюджетным требованиям, регламентам, касающимся здравоохранения и безопасности, и т.д.
- *Отчетность*. Это риски, связанные с финансовой и операционной, обязательной или по запросу, отчетностью. Примерами являются заявления руководства, финансовая отчетность, пресс-релизы и т.д.

Поскольку некоторые категории могут стать очень большими, мы можем подразделить их на подкатегории. Например, мы можем разделить **категорию инфраструктуры** на следующие подкатегории:

- *Кадровые ресурсы*. Эта подкатегория может включать программу найма, зарплат, обучения, выхода на пенсию, производительность и компенсацию, и т.д.
- *Информационная технология*. Эта подкатегория может включать ИТ инфраструктуру, управление изменениями, бесперебойность деятельности, информационную безопасность, защиту данных от уничтожения и тайны, лицензирование программного обеспечения и т.д.

- *Юридические услуги*. Эта подкатегория будет включать юридические и нормативные вопросы, включая обслуживание контрактов.
- *Финансы*. Эта подкатегория будет включать все вопросы составления бюджетов, бухгалтерского учета и финансов.

ЯЧЕЙКА С ПРАКТИЧЕСКИМ ПРИМЕРОМ КАТЕГОРИИ РИСКА

2. Как прийти к факторам риска?.

Внутреннему аудиту потребуется разработать перечень всех потенциальных и значимых рисков на основании вклада от руководства, имеющейся в организации информации, информации от других лиц, дающих гарантии, или информации от коллег. На практике представители функции внутреннего аудита проведут интервью с ответственными лидерами различных подразделений организации («с владельцами рисков»), одновременно обращаясь и к научным публикациям, и к существующим профессиональным организациям, занимающимся управлением рисками, и к аудиторским организациям, и к анализу рисков, проведенному менеджерами по рискам, и т.д.

Примеры факторов риска следующие:

- Категория «Управление, стратегия и планирование».
    - Подкатегория «Организационная структура».
        - Риск 1: Неясный порядок подчиненности
        - Риск 2: Сложная организационная схема
        - Риск 3: Избыточный фокус на деление
        - Риск 4: …
- Категория «Инфраструктура».
    - Подкатегория «Информационная безопасность».
        - Риск 1: Неэффективные средства управления доступом
        - Риск 2: Уязвимость для злонамеренных действий
        - Риск 3: Отсутствие разделения обязанностей
        - Риск 4: …

ЯЧЕЙКА С ПРАКТИЧЕСКИМ ПРИМЕРОМ ФАКТОРОВ РИСКА

3. Каковы критерии риска в организациях государственного сектора? .

Каждая организация должна определить критерии, которые будут использоваться для оценки значимости риска. Критерии риска должны

отражать ценности, цели и ресурсы организации. Некоторые критерии могут быть продиктованы, или могут происходить из юридических и нормативных требований, или других требований, которым подчиняется организация. Критерии риска должны быть согласованы с политикой управления рисками организации, должны быть определены в начале любого процесса управления рисками, и их необходимо непрерывно пересматривать.

Риски измеряются в плане **воздействия и вероятности**. Воздействие определяет финансовые или нефинансовые последствия для организации в случае возникновения риска. Вероятность определяет шансы возникновения риска. Чем более уязвима организация к смягчению определенного риска, тем больше вероятность того, что риск может возникнуть.

Могут быть рассмотрены следующие **критерии на предмет воздействия**:

- *Финансовое воздействие*. Денежные последствия для организации, если возникает риск.
- *Воздействие на репутацию*. Последствия для репутации организации, министерства или даже на более высоком уровне – репутации всей страны – в глазах рейтинговых агентств, международных доноров, и т.д.
- *Нормативное воздействие*. Возникновение риска может привести в результате к замороженным бюджетам или программам, или даже к штрафам (например, средства ЕС).
- *Воздействие на миссию*. Возникновение риска может оказать воздействие на миссию организации.

Могут быть рассмотрены следующие **критерии для вероятности или уязвимости**:

- *Результативность системы внутреннего контроля*. Это можно оценить, исходя из предыдущего опыта внутреннего аудита, или существования / отсутствия серьезных проблем в недавнем прошлом.
- *Скорость реагирования.* Не все риски могут оказывать немедленное воздействие на организацию. Скорость реагирования определяет время, которое есть у организации, чтобы отреагировать на риск, когда он возникает. Чем больше у организации есть времени для устранения недостатков, тем менее уязвимой она является.
- *Сложность операций*. Сложные операции понимают лишь немногие люди в организации. Чем меньше людей понимают операции, тем больше шансы того, что могут не заметить какую-то неправильность.
- *Темпы изменений в организации*. Стабильные системы и процессы делают организацию менее уязвимой.
- *Потенциальные возможности людей и процессов*. Чем более структурированными и прозрачными являются процессы, тем менее

уязвимой является организация. Менее компетентные люди делают организацию более уязвимой.

Приведенные выше критерии являются просто примерами. Необходимо выбрать надлежащие критерии в зависимости от специфики организации. В результате можно выбрать меньше критериев или другие критерии.

При определении критериев риска, факторы, которые следует принимать во внимание, должны включать следующее:

- Природа и типы причин и последствий, которые могут возникнуть, и как они будут измеряться;
- как будет определяться вероятность;
- временные рамки вероятности и (или) последствия (последствий);
- как будет определяться уровень риска;
- взгляды вовлеченных лиц;
- уровень, на котором риск становится приемлемым или допустимым; и следует ли принимать во внимание сочетания множественных рисков, и если да, то как и какие сочетания следует учитывать.

ЯЧЕЙКА С ПРАКТИЧЕСКИМ ПРИМЕРОМ КРИТЕРИЕВ РИСКА

4. Как присваивать баллы рискам?

После того как идентифицированы значимые риски, их необходимо оценить и присвоить им баллы. Рекомендуется не присваивать баллы рискам чисто математическим способом. Более практичным представляется оценка и присвоение им баллам в соответствии с заранее определенной шкалой оценки рисков. В имеющейся литературе мы часто находим три уровня присвоения баллов, но это может привести к чрезмерным баллам в средней категории. Шкала оценки рисков в идеале должна состоять из **четырех уровней присвоения баллов**:

- Низкий риск. И воздействие, и вероятность оцениваются как низкие и не значимые.
- Средний низкий. Либо воздействие, либо вероятность оцениваются как потенциальная, но не слишком значимая угроза.
- Средний высокий. Либо воздействие, либо вероятность оцениваются как потенциальная и значимая угроза.
- Высокий. И воздействие, и вероятность оцениваются как высокие и значимые.

Люди оценивают риски различным образом. Некоторые люди намеренно избегают рисков, а другие, наоборот, склонны рисковать. Если один человек оценивает риск как высокий, а другой как низкий, результат никогда не может быть средним. Необходимо прийти к консенсусу. Таким образом, рекомендуется заранее договориться о том, как будут присваиваться баллы рискам, используя шкалу для оценки рисков.

ЯЧЕЙКА СО ШКАЛОЙ ДЛЯ ОЦЕНКИ РИСКОВ

Несколько примеров:

- Можно считать, что риск оказывает большое финансовое воздействие, если возникновение риска может генерировать убытки, которые будут на 3% превышать бюджет организации.
- Репутация организации может серьезно пострадать, если возникновение риска может привести к освещению в национальной и международной прессе.
- Можно считать, что организация очень уязвима, если возникновение риска затрагивает большое количество сделок и (или) процессов.
- Организация может показаться менее уязвимой, если управление процессами хорошо разработано и внедрено, и работает эффективно.

ЯЧЕЙКА С ПРАКТИЧЕСКИМ ПРИМЕРОМ ПРИСВОЕНИЯ БАЛЛОВ РИСКУ