Диагностика системы контроля над рисками мошенничества: роль внутреннего аудита

Василий Кудрин

17 декабря 2009

Внутренний аудит:
Фокус на риски мошенничества

Процент респондентов, считающих, что фокус ВА на риски мошенничества возрастет

Response	Chart	Frequency
Yes		52.1%
Yes, but only in certain business sectors/industries		25.8%
No		22.1%

**** Результаты исследования GAIN «Горячие темы для внутреннего аудита в 2009 г.»***

- **Рассмотрение факторов мошенничества при анализе каждого риска**
- **Анализ специфических областей, связанных с большим объемом раздельных обязанностей**
- **Дополнение процедур оценки рисков (и в дальнейшем процедур оценки контролей) мероприятиями по выявлению факторов мошенничества («возможность», «мотивация», «давление» обстоятельств)**
- **Фокус на связанные риски, например, контрактные**

Формирование эффективной системы контроля над рисками мошенничества

➔Для выработки наиболее эффективной системы противодействия мошенничеству {**3**} необходимо совместить {**1**} мероприятия по внедрению универсальных общекорпоративных средств противодействия мошенничеству с {**2**} проектом диагностики системы внутреннего контроля (2.2), сфокусированной на рисках мошенничества (2.1), которая включает как оценку общекорпоративной модели противодействия мошенничеству (*2.1.i*), так и оценку контроля внутри “рискованных” мега-процессов (*2.2.ii*).

1

Внедрение универсальных средств противодействия мошенничеству

… таких, как кодекс этики, «горячая» линия, интервью при увольнении, проактивные опросы сотрудников, практика независимых расследований

2

Оценка рисков (2.1) и диагностика (2.2) системы противодействия мошенничеству

Оценка рисков мошенничества в целом по компании и в ключевых мега-процессах. Общекорпоративная (2.2.i) и попроцессная (2.2.ii) оценка дизайна и операционной эффективности системы внутреннего контроля над рисками мошенничества.

3

Совершенствование корпоративной системы противодействия мошенничеству

Определение и приоритезация последовательных и согласованных улучшений:

- ➔Разработка и внедрение специфических планов действий по улучшению процессов контроля и мониторинга рисков мошенничества,
- ➔Развитие компетенций менеджеров по управлению рисками мошенничества, а также
- ➔Совершенствование общекорпоративных компонентов модели противодействия мошенничеству и обеспечение эффективной согласованности (координации) между ними.

Общекорпоративные универсальные средства: «быстрые победы» и «следующие шаги»

«Быстрые победы»:

- Кодекс этики
- Запуск «горячей линии» по этическим вопросам
- Практика независимых расследований
- Специальные интервью при увольнении сотрудников
- Система проактивных опросов сотрудников

«Следующие шаги»:

- Эффективная координация между разными службами
- Единые протоколы расследований
- Формирование практики аудита (диагностики) внутреннего контроля над рисками мошенничества

Оценка рисков мошенничества и диагностика системы управления рисками мошенничества

2.1. Оценка рисков мошенничества

Оценка и ранжирование рисков мошенничества, присущих компании и ее мега-процессам:

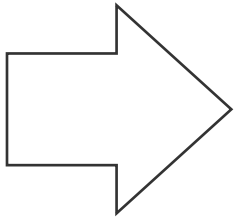
➔Проявление общекорпоративного риска мошенничества в разных мега-процессах компании

➔Выбор процессов, (потенциально) насыщенных мошенничеством

➔Оценка специфических рисков мошенничества в выбранных «рискованных» мега-процессах

2.2.*i*. Диагностика общекорпоративной модели противодействия мошенничеству

Оценка дизайна модели управления рисками мошенничества



2.2.*ii*. Оценка системы контроля над рисками мошенничества в мега-процессах

➔*Начинается с* оценки специфических рисков мошенничества в выбранных для целей диагностики “рискованных” мега-процессах

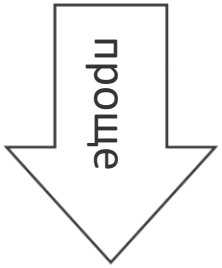
➔Оценка дизайна и операционной эффективности контролей (контрольных процедур) над рисками мошенничества в мега-процессах, а также основных процессах

➔Определение (ориентировочных) планов действий

В зависимости от уровня зрелости модели хронологическое “местоположение” стадии 2.2.i может меняться

Оценка рисков мошенничества: 1 шаг (до выбора мега-процессов для диагностики)

Формирование представления относительно (риска) мошенничестве



- **Скоординированная оценка присущих рисков общекорпоративного уровня**
- **Рассмотрение фактора мошенничества при оценке каждого риска (“возможность”, “мотивация”, “давление”)**

- **Отражение, или проявление риска в процессах или специальных проектах - «мэппинг» рисков на процессы/проекты**
- **Уровень отражаемости риска - «высокий», «средний», «низкий»**
- **Насыщенность процессов/проектов рисковыми событиями**
- **Организационная сложность процессов/проектов: «внутренняя сложность» и «объемность»**
- **Учет эффективности универсальных средств противодействия мошенничеству (стадии 1 и 2.2.i)**

- ➔ ***Подготовительная работа (подготовка типовой карты рисков, предварительные интервью, подтверждение описаний рисков)***
- ➔ ***Вступительная презентация и вспомогательные раздаточные материалы***
- ➔ ***Голосование с дальнейшим обсуждением***
- ➔ ***Ориентирование на мнения экспертов***
- ➔ ***Рассылка материалов и подтверждающие интервью***

Корпоративная модель внутреннего контроля над рисками мошенничества

➔ Компоненты защиты (обороны) против рисков мошенничества

Внутренняя Среда (Этика)	Система внутреннего контроля	Мониторинг СВК	Whistleblowing («информирование»)	Расследования
▪ Ценности Компании ▪ Тон со стороны Совета директоров и высшего руководства ▪ Этические нормы ▪ Кодекс корпоративных правил ▪ Система внедрения и поддержания Кодекса корпоративных правил и этических норм	▪ Оценка рисков хищений / мошенничества на уровне мега-процессов и ниже ▪ Система процедур и механизмов предотвращения мошенничества - Ответственность - Нормы и правила - Контрольные процедуры - Регулярные проверки по сигналам (признакам)	▪ Мониторинг СВК на уровне владельцев бизнес-процессов ▪ Мониторинг СВК со стороны вспомогательных функций ▪ Мониторинг (диагностика) СВК со стороны Службы безопасности ▪ Отдел внутреннего аудита ▪ Мониторинг IT-систем и IT-мониторинг	▪ Внедрение «горячих» линий ▪ Вопросы подотчетности и обеспечение защиты «горячих» линий ▪ Защита информаторов и фильтрация сигналов ▪ Система инициирования действий по сигналам «горячих» линий	▪ Исследование менеджментом (инцидентов) ▪ Расследования на уровне Дирекции по безопасности (подотчетной CEO) ▪ Отдел внутренних расследований ▪ Координация ▪ IT-расследования ▪ Отчетность и информирование

Уровни зрелости модели управления рисками мошенничества: критерии для оценки

Уровень зрелости	Определение
Ведущая практика	Процедуры управления рисками мошенничества внедрены, скоординированы и исполняются должным образом во всей компании. Применяемые практики признаются лучшими и рассматриваются другими компаниями в качестве ведущих примеров.
Хорошая практика	Процедуры управления рисками мошенничества внедрены, исполняются должным образом и хорошо понятны менеджменту и соответствующим сотрудникам компании. Некоторые небольшие улучшения приветствуются.
Нормальная практика	Процедуры управления рисками мошенничества внедрены, но не всегда исполняются должным образом или не полностью понятны менеджменту и соответствующим сотрудникам. Возможны некоторые умеренные улучшения.
Развивающаяся практика	Процедуры управления рисками мошенничества внедрены частично, не исполняются должным образом и их значение не очень понятно менеджменту и сотрудникам. Необходимы значимые улучшения.
Плохая практика	Имеется некоторый незначительный (ограниченный) набор процедур управления рисками мошенничества. Необходимы значимые улучшения.

Общекорпортивная диагностика:
уровни зрелости и пирамида издержек, связанных с мошенничеством

Результаты общекорпоративной диагностики

- Пример результатов общекорпоративной диагностики

Оценка системы контроля над рисками мошенничества в мега-процессе

Определение роли внутреннего аудита

1

Внедрение универсальных средств противодействия мошенничеству

… таких, как кодекс этики, «горячая» линия, интервью при увольнении, проактивные опросы сотрудников, практика независимых расследований

➔*Частично – возможная*

➔*Ключевая в части мониторинга эффективности внедрения*

2

Оценка рисков (2.1) и диагностика (2.2) системы противодействия мошенничеству

Оценка рисков мошенничества в целом по компании и в ключевых мега-процессах. Общекорпоративная (2.2.i) и попроцессная (2.2.ii) оценка дизайна и операционной эффективности системы внутреннего контроля над рисками мошенничества.

➔*Ключевая*

3

Совершенствование корпоративной системы противодействия мошенничеству

Определение и приоритезация последовательных и согласованных улучшений:

➔ Разработка и внедрение специфических планов действий по улучшению процессов контроля и мониторинга рисков мошенничества,

➔ Развитие компетенций менеджеров по управлению рисками мошенничества, а также

➔ Совершенствование общекорпоративных компонентов модели противодействия мошенничеству и обеспечение эффективной согласованности (координации) между ними.

➔*Вспомогательная*

➔*Возможная или ключевая в части мониторинга эффективности внедрения*

Ключевая роль внутреннего аудита в вопросах, связанных с рисками мошенничества

Определение внутреннего аудита

➔ **деятельность по предоставлению независимых и объективных гарантий и консультаций, направленных на совершенствование деятельности организации;**

➔ **помогает организации достичь поставленные цели, используя систематизированный и последовательный подход к оценке и повышению эффективности процессов управления рисками, контроля и корпоративного управления.**

Стандарт 1210 – Профессионализм

➔ **Внутренние аудиторы должны обладать знаниями, навыками и другими компетенциями, необходимыми для выполнения своих должностных обязанностей. Для выполнения стоящих перед подразделением внутреннего аудита задач, сотрудники подразделения должны коллективно обладать необходимыми знаниями, навыками и другими компетенциями или получить их.**

Практическое указание 1210-1 «Профессионализм» раскрывает, что к знаниям, навыкам и компетенциям, упоминаемым в Стандарте, относят в том числе …

➔ **знания, необходимые для идентификации признаков мошенничества.**

Стандарт 1210.A2

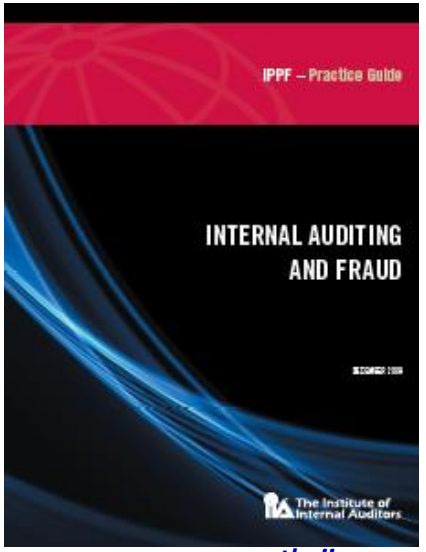
➔ **Внутренние аудиторы должны обладать достаточными знаниями, чтобы оценить риск мошенничества и то, каким образом организация управляет этим риском. В то же время не предполагается, что внутренние аудиторы обладают компетенцией специалиста, чья основная функция заключается в выявлении и расследовании фактов мошенничества.**

Роли внутреннего аудита в вопросах борьбы с мошенничеством

- Оценка систем защиты от мошенничества – КЛЮЧЕВАЯ
- Оценка рисков мошенничества – КЛЮЧЕВАЯ
- Выявление признаков мошенничества – КЛЮЧЕВАЯ
- Обслуживание «горячей линии» – СООТВЕТСТВУЮЩАЯ
- Выявление (detection) случаев мошенничества – ВОЗМОЖНАЯ
- Расследование (investigation) случаев мошенничества – ВОЗМОЖНАЯ
- Сообщение о результатах мошенничества – ВОЗМОЖНАЯ
- Участие в принятии решений по результатам расследований – ЗАПРЕТНАЯ
- Внедрение (по поручению менеджмента) «механизмов» защиты от мошенничества – ЗАПРЕТНАЯ

Практическое руководство The Institute of Internal Auditors: “Внутренний аудит и мошенничество”

- Осознаны ли в компании нормы, связанные с мошенничеством (как преступлением) в областях, в которых компания ведет бизнес?
- Имеется ли в компании общая политика в области борьбы с мошенничеством?
- Закрепляет ли такая политика обязанности в части расследования мошенничества?
- Предусматривает ли корпоративная программа противодействия мошенничеству координацию работы с внутренним аудитом ?
- Имеется ли в компании “горячая линия” по этическим вопросам?
- Включены ли в положение о внутреннего аудите роль и обязанности внутреннего аудита в области борьбы с мошенничеством?
- Обозначена ли в компании ответственность за выявление, предотвращение мошенничества, информирование о необходимости противостоять мошенничеству, разрешение ситуаций по расследованным случаям?



www.theiia.org

- Информирует ли руководство и Главный аудитор комитет по аудиту о событиях, связанных с мошенничеством?
- Занимается ли руководство компании информированием сотрудников о необходимости противостоять мошенничеству, организует ли соответствующие тренинги?
- Проводит ли руководство компании оценку рисков мошенничества и приглашается ли внутренний аудит к процессу оценку? Учитывается ли оценка в плане внутреннего аудита?
- Доступны ли для тех, кто ответственен за предотвращение, выявление и расследование мошенничества автоматизированное (компьютеризированные) средства?
- Имеет ли руководство компании и Главный аудитор доступ к необходимым методическим руководствам от профессиональных организаций по вопросам борьбы с мошенничеством? Имеются ли у менеджмента необходимые компетенции, необходимые для расследования мошенничества?

Вопросы / Контакты

Vasily.Kudrin@gmail.com

Василий Кудрин,
CIA, CFE, CCSA

Директор по корпоративному аудиту
X5 Retail Group N.V.

Директор, Совет Института внутренних аудиторов
Директор, Совет российского отделения ACFE (Association of Certified Fraud Examiners)