

д.э.н., профессор Алиев М.К.

магистрант Ибрагимова З. А.

Казахский университет экономики, финансов и международной торговли, Республика Казахстан, г. Астана

Организация внутреннего аудита на примере аудита информационных систем в соответствии с МСА

Сегодня внутренние аудиторы постоянно сталкиваются с нарастающим и непрерывным развитием новых технологий, которые безудержно проникают как в корпорации и организации, так и в нашу личную жизнь. “Большие данные”, облачные вычисления, использование мобильных устройств, социальные сети – вот несколько последних трендов в технологиях, которые размывают границы и трансформируют саму суть бизнеса. Технологии становятся глубоко интегрированными во все большее количество элементов корпоративных бизнес-процессов, пронизывая их снизу вверх и сверху вниз. И хотя они ускоряют и упрощают обмен информацией и активами, они влекут за собой новые риски, связанные с таким ускорением и упрощением. Реализация этих рисков ведет к потере активов, к утечке конфиденциальной информации, к остановке бизнеса из-за неработоспособности компьютерных систем.

Однако экспертиза в технологиях – давнишняя слабая сторона для профессии внутреннего аудитора, которая иллюстрируется в различных обзорах “состояния профессии” (“2013 State of the internal audit profession study” by PwC, “2013 Internal audit capabilities and needs survey report” by Protivity). Многие внутренние аудиторы не используют эффективно технологии для анализа данных и автоматизации процедур тестирования, также как и не включают в поле своего зрения риски и возможности, которые

привносят новые технологии. Зачастую незнание технологий вызывает у руководителя внутреннего аудита неуверенность в технических вопросах, и даже боязнь, и, соответственно, в годовом плане аудита рискам ИТ отводится минимальный приоритет.

Как же внутренние аудиторы могут предоставить надежные гарантии и ценные советы правлению и менеджменту в условиях глубокого проникновения высоких технологий, если им недостает технологических фокуса, знаний и умений? Внутренние аудиторы не могут позволить себе стоять в стороне в век постоянных технологических инноваций. Будущее создается и перестраивается каждый день, и внутренние аудиторы должны держаться “на гребне волны”, чтобы приносить пользу своим акционерам.

Этот вызов времени стоит особенно остро перед руководителем подразделения внутреннего аудита организации, требуя от него ясных и адекватных ответов на два ключевых вопроса, поднимаемые повсеместным проникновением технологий: насколько информационные технологии безопасны, и используются ли они эффективно и в соответствии с целями организации, внутренними политиками, процедурами и законодательством? Чтобы ответить на них, руководитель внутреннего аудита не обязательно должен быть глубоким экспертом в информационных технологиях, но если он действительно считает себя компетентным менеджером, он должен уверенно ориентироваться в них. Иначе говоря, руководитель подразделения внутреннего аудита должен уметь инициировать разумную и уверенную дискуссию о технологических рисках в своем общении с правлением и аудиторским комитетом. Чтобы вести такую дискуссию, необходимо уметь задавать правильные вопросы правильным людям и внимательно прислушиваться к вопросам, которые поднимает правление и аудиторский комитет. При этом важно совмещать детальное понимание специфики работы и операций бизнеса, видение зон, наиболее подверженных риску, с базовым пониманием основных принципов информационных технологий. Фокус должен быть на ключевых, с точки зрения текущих бизнес-рисков,

компонентах информационных технологий и элементах системы внутреннего контроля, в которых эти компоненты используются.

Нахождение оптимального баланса между глубокой ИТ-экспертизой и умениями внутреннего аудитора по пониманию риска является ключевым элементом успеха руководителя подразделения внутреннего аудита. При этом руководителю нет необходимости глубоко и в деталях вникать в особенности работы отдельной системы или элемента ИТ-инфраструктуры, изучать его конфигурацию, но важно уметь консультировать, давать совет, выражать свое объективное мнение о том, выполняют ли ИТ свою миссию и стратегические цели, идут ли они в ногу с бизнесом.

То, что должен знать внутренний аудитор об ИТ, часто обусловлено озабоченностью правления и аудиторского комитета вопросами, которые можно сгруппировать в следующие шесть категорий:

Информационная безопасность. Это самый общеизвестный аспект рисков в ИТ, который возникает в головах правления и менеджмента, когда речь идет об информации и технологиях. Здесь руководителю внутреннего аудита нужно дать четкий ответ, какие риски информационной безопасности существуют (например, остановка основной системы из-за вирусной атаки, несанкционированное вмешательство изнутри или извне в работу финансовых систем, повлекшее искажение отчетности или кражу денежных средств, кража секретной информации) и как они обрабатываются. Он должен понимать, как организовано управление информационной безопасностью, какие проекты были и будут реализованы, понимать оценку рисков, которую должно делать подразделение информационной безопасности или ИТ, знать о текущих проблемах, инцидентах, вопросах, поднятых внутренними и внешними аудиторами, проверяющими органами, консультантами.

Интеграция ИТ в бизнес-процессы. Аудиторский комитет или правление часто интересуется оценкой контролей в ключевых бизнес-процессах, включая используемые технологии, и здесь важно понимать поток транзакций и

операций, информационный поток, обслуживающий ключевые процессы и уметь наложить на этот поток необходимые контрольные механизмы, автоматизированные и ручные. Ведь в современном мире бизнес-процессы уже напрямую зависят от технологий, являются единым целым с ними. И проблемы в ИТ выливаются в проблемы в бизнесе компании. Поточковые диаграммы, диаграммы бизнес-процессов являются ключевым инструментом для получения правильных ответов в этом случае.

Управление ИТ-проектами. ИТ-проекты зачастую имеют значительные финансовые и ресурсные бюджеты, что особенно заботит правление, и понимание рисков в текущих проектах является важной частью работы главы внутреннего аудита, так как от проектов напрямую зависит реализация бизнес- и ИТ-стратегии организации. Обоснование проекта с точки зрения стратегии компании, адекватный устав проекта и организация проектной работы, полная вовлеченность бизнеса и четкая постановка требований с его стороны, полноценное документирование системы и надежное тестирование решения – вот ключевые факторы успеха в проектной работе, и руководитель подразделения внутреннего аудита должен их ясно понимать.

Взаимосвязи с бизнес-партнерами и поставщиками. Это особенно важно, когда партнеры оказывают услуги на условиях аутсорсинга и имеют прямой доступ в сеть организации к ключевым ее техническим элементам, обслуживают и развивают их. Здесь аудитор должен понимать степень ответственности поставщиков, разбираться в соглашениях об уровне сервиса, проработанность соглашений о неразглашении информации, включать в план аудиторских проверок аудиты системы внутреннего контроля критически важных поставщиков услуг, переданных на аутсорсинг.

Вопросы корпоративного управления ИТ. Корпоративное управление охватывает большое количество вопросов, таких как постановка целей, их взаимоувязка с бизнес-целями, измерение результатов, делегирование полномочий, выстраивание структур, подотчетность и обеспечение того, чтобы люди делали правильные вещи. Правление спрашивает много

вопросов из этого набора, например такой ключевой “Уверены ли мы что деятельность ИТ эффективно поддерживает достижение бизнес-целей?”

Каким же образом руководитель подразделения внутреннего аудита может разобраться во всем этом широком и технически специфичном спектре вопросов? Это действительно не просто для человека, никогда не имевшего ранее дело с техническими аспектами. Но понимание это действительно необходимо, и здесь только от желания аудитора и его настойчивости зависит, сможет ли он разобраться в этих вопросах. Необходимо поставить себе такую задачу и систематически уделять часть своего рабочего времени изучению технологий и технологических рисков. Возможным путем решения этого вопроса может быть привлечение в штат аудитора ИТ, или обучение ИТ-специалиста внутри подразделения аудита, совместно с которым руководитель будет разбирать весь спектр ИТ-рисков и особенностей технологий, при этом обсуждать не технические детали отдельных элементов инфраструктуры, а ключевые и принципиальные вопросы технологий, ее архитектурные аспекты в тесной привязке к обслуживаемым процессам.

Другим способом может быть привлечение экспертов из подразделений информационных технологий на регулярной основе для получения технических консультаций. Однако, здесь руководитель аудита должен быть уверенным, что он может доверять такому ИТ-эксперту, что его консультации свободны от конфликта интересов.

Кроме того, хорошим ресурсом ИТ-экспертизы может быть подразделение информационной безопасности, с которым имеет смысл наладить конструктивное сотрудничество, так как одна из его функций – это также контроль информационных технологий, и, значит, это подразделение во многих вопросах играет на стороне аудита.

Технологии не останавливают свое развитие, генерируя новые риски и вызовы, также будут развиваться и требования к знаниям аудиторов. Руководитель подразделения внутреннего аудита все больше и больше

должен развивать свои знания и компетенции в области информационных технологий. Прогрессирующие технологии будут требовать от него все лучшего, все большего, хотя и не обязательно глубоко детализированного, понимания технологических рисков. Никто не ожидает от руководителя внутреннего аудита, что он подчинит сломанный компьютер, или оценит правильность конфигурационного параметра отдельного сервера. Но каждый, кто полагается на его слово, ждет от него хорошего владения вопросами информационных технологий, ключевых ИТ-рисков, или знания где найти необходимую информацию.

Список использованной литературы:

1. Профессиональные стандарты внутреннего аудита. Кодекс этики// The Institute of Internal Auditors, Altamonte Spring, FL USA
2. Э. Аренс, Дж. Лоббек «Аудит»
3. Б.Т. Жарылгасова, А.Е. Суглобов «Международные стандарты аудита».
4. Международные стандарты аудита/Под ред. Ж.А. Кеворковой. – М.: Юрайт. — 464 с. – ISBN 978-5-9916-3086-3.
5. Стандарты и руководства разработанные международными организациями ISACA, Институтом Внутренних Аудиторов (IIA), ISO/IEC, IAASB (the International Auditing and Assurance Standards Board), PCAOB
6. Gehan, Mousa Corporate Environmental Reporting & the Auditor's Role / Gehan Mousa. - М.: LAP Lambert Academic Publishing, 2012. - 144 с.