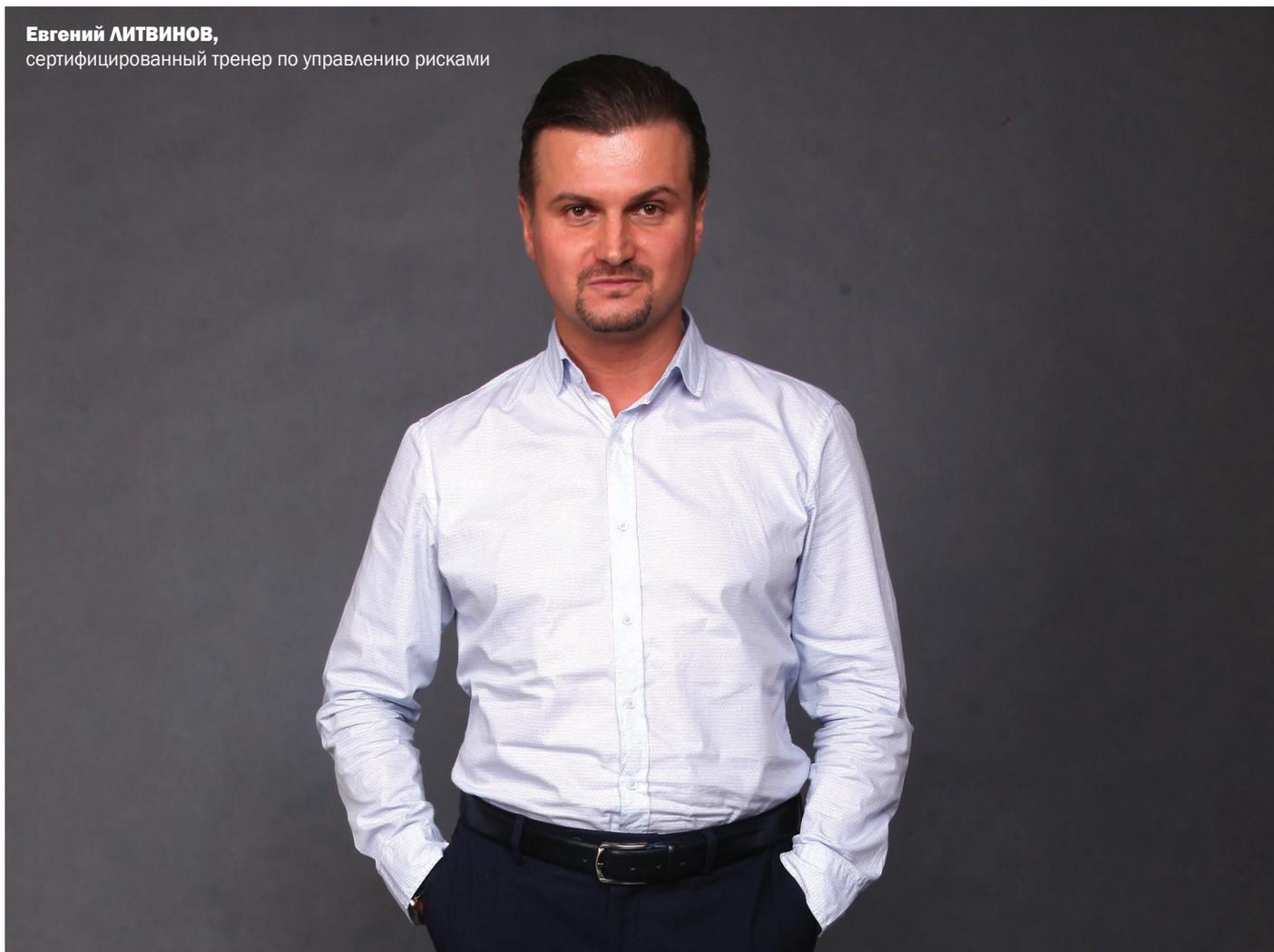


Евгений ЛИТВИНОВ,
сертифицированный тренер по управлению рисками



ПРОЦЕСС УПРАВЛЕНИЯ РИСКАМИ: ТРЕБОВАНИЯ СТАНДАРТОВ И РЕАЛЬНОСТЬ

Интеграция процесса риск-менеджмента в бизнес-процессы компании – задача непростая, но именно от ее реализации зависят качество и эффективность управления рисками в организации. Такого мнения придерживается CEO международной тренинговой компании TQM-pro, сертифицированный тренер по управлению рисками Евгений ЛИТВИНОВ. Опираясь на новые требования стандартов, эксперт прокомментировал каждый этап управления рисками и дал коллегам полезные практические рекомендации в рамках Risk Awareness Week-2020.

СТАНДАРТЫ ПО РИСК-МЕНЕДЖМЕНТУ

Первый национальный стандарт по риск-менеджменту – AS/NZS 4360:2004 – был выпущен в 1995 году в Австралии. Затем в 1997 году вышел канадский стандарт CSA Q 850:1997 «Риск-менеджмент. Руководство», в 2001-м – японский JIS Q 2001:2001 «Рекомендации по разработке и внедрению RM», в 2002-м в Великобритании появился IRM 2002 «Стандарт управления рисками». В 2002-м в Европе вышел стандарт FERMA «Управление рисками», а в 2004-м в США – COSO-2004 «Интегрированная модель управления рисками организации», Комитет спонсорских организаций Комиссии Тредвея. Наконец, в 2009 году вышла первая версия международного стандарта ISO 31000.

На данный момент стандарты по риск-менеджменту можно разделить на три основные модели:

- Международный стандарт ISO 31000:2018 «Управление рисками. Руководство»;
- Американская модель COSO ERM-2017 (ERM – Enterprise Risk Management);
- Европейский стандарт FERMA-2002 (Федерация Европейских Ассоциаций риск-менеджеров)

Несмотря на разницу в подходах, стилистике, да и просто в объеме этих документов (например, COSO ERM – это 200 страниц, ISO 31000 – менее 20 страниц), каждый из данных стандартов придерживается определения, что риск – это влияние неопределенности на достижение поставленных целей. При этом важно правильно идентифицировать риски, не путать риск и последствия.

Часто в ходе проведения проектов и тренингов в тех или иных компаниях я вижу, что специалисты этих компаний (риск-менеджеры в том числе) неправильно идентифицируют риски, называют риском недостижение целевых показателей или последствия риска. Чтобы это продемонстрировать, приведу пример. Неискушенный риск-менеджер или менеджер проекта нередко видит осуществление проекта таким образом, что все будет гладко, ровно и без проблем. На самом деле выполнение проекта выглядит по-другому.

Риск – это влияние неопределенности на достижение целей



Не стоит забывать о трех основных критериях оценки (целевых показателях) любого проекта:

- бюджет
- сроки
- качество.

Превышение бюджета проекта и срыв сроков реализации проекта будут являться последствиями реализа-

COSO ERM – это 200 страниц, ISO 31000 – менее 20 страниц, каждый из данных стандартов придерживается определения, что риск – это влияние неопределенности на достижение поставленных целей. При этом важно правильно идентифицировать риски, не путать риск и последствия

ции тех или иных рисков, поскольку риск – это, напомним, влияние неопределенности на достижение поставленных целей. Соответственно, риски в каждом случае будут разные, например:

- отсутствие или некачественные критерии по переходу с одной части проекта на другую: с этапа пред-ТЭО (технико-экономические обоснования) на ТЭО, с этапа ПСД (проектно-сметная документация) на СМР (строительно-монтажные работы);
- низкое качество самих ПСД и СМР;
- некачественный контроль за приемкой ПСД и осуществлением СМР.

Учитывая это, важно четко поставить цели и только после этого заниматься рисками.

Вернемся к моделям, описывающим риск-менеджмент. По сути, три указанные модели (COSO ERM, FERMA и ISO 31000), какими бы разными они ни были, связывают понятие «риск» с установленными целями.

Предлагаю рассмотреть алгоритмы, которые описывают управление рисками в этих трех моделях. **Европейский стандарт FERMA** отталкивается от стратегических целей. Далее происходит анализ рисков (идентификация и описание рисков), оценка рисков и принятие решения об их обработке.

COSO ERM-2004 рассматривает четыре категории бизнес-целей (стратегические, операционные, цели подготовки отчетности, цели соблюдения законодательства или комплаенс) и выстраивание Системы управления рисками для достижения этих целей. В 2017 году COSO отошел от прежней концепции («магический куб» в COSO больше не упоминается) и сделал акцент на интеграцию процесса риск-менеджмента в существующие процессы.

ISO 31000 представляет собой целое семейство стандартов, которое начинается, собственно, с самого ISO 31000:2018 «Управление рисками. Руководство» – это на данный момент вторая редакция стандарта. Также есть ISO 31010:2019 «Управление рисками. Методы оценки рисков», где отражены более 30 способов идентификации, анализа и оценки рисков. В отдельном документе – ISO Guide 73:2009 «Управление рисками. Словарь» содержатся термины и определения. Можно отметить и ISO 31004:2013 «Управление рисками. Руководство по внедрению».

Модель управления рисками по ISO 31000 также отталкивается от контекста компании и целей, затем происходит идентификация, анализ, оценка и обработка рисков.



Обобщенная модель управления рисками трех стандартов – COSO, FERMA и ISO 31000 выглядит следующим образом: установление контекста компании, определение целей, процессов и KPI. Затем происходит идентификация, анализ и оценивание рисков, после этого – обработка рисков. В рамках каждого этапа процесса риск-менеджмента необходимы консультации и коммуникации по рискам, а также мониторинг и анализ рисков.

Остановимся на ISO 31000:2018, потому что он единственный из трех моделей по управлению рисками имеет статус международного стандарта. Для начала разберемся, почему он так называется. 31000 – это идентификационный номер стандарта (не порядковый), через двоеточие – год выпуска документа. ISO – это аббревиатура, под которой имеется в виду International Organization for Standardization – Международная Организация по Стандартизации. Она учреждена 14 октября 1946 года в Лондоне 25 странами, в том числе СССР. На данный момент штаб-квартира ISO находится в Женеве (Швейцария) и включает в себя более 180 стран мира, в том числе страны СНГ – Россию и Казахстан. По состоянию на 2020 год в ISO зарегистрировано более 19,5 тысячи международных стандартов. Стандарт ISO 31000 переведен и принят в качестве национального стандарта, например в России – это ГОСТ Р ИСО 31000, в Республике Казахстан – СТ РК ИСО 31000.

ИНТЕГРАЦИЯ ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ

Итак, три модели по управлению рисками: ISO 31000:2018, FERMA и COSO ERM:2017. На своих тренингах я всегда спрашиваю у слушателей, сколько раз, по их мнению, в данных моделях упоминается словосочетание «система управления рисками», и даю варианты ответов: до 10, до 20 или более 30 раз? На самом деле правильный ответ – ноль раз. В данных документах такого словосочетания (система управления рисками) нет, но есть термин «процесс управления рисками». Более того, в них прописаны четкие требования, что процесс управления рисками должен быть интегрирован (встроен) в существующие процессы. Главное – он должен быть интегрирован в один из самых критичных процессов – в процесс принятия решений, то есть решения должны приниматься с учетом рисков.

В качестве подтверждения, что в ISO 31000, FERMA и COSO ERM звучит именно словосочетание «процесс риск-менеджмента» и требуется его интеграция в существующие процессы, приведу краткую выдержку из этих трех моделей.

COSO ERM-2017, п.4 «**Интеграция процесса** управления рисками в организации»:

Процесс управления рисками в организации **успешно интегрирован**, когда:

- при оценке вариантов в **процессе определения стратегии** прямо **учитывается риск**;
- менеджмент ведет активную работу **с рисками** в целях **достижения KPI**.

FERMA, п.8.6 «Ресурсы и реализация Программы управления рисками»:

Процесс риск-менеджмента должен быть **интегрирован** в организацию **через: стратегическое управление и бюджетный процесс**.

ISO 31000:2018, п.6 «**Процесс** риск-менеджмента»:

Процесс риск-менеджмента **должен быть** неотъемлемой **частью процессов** управления и должен быть **интегрирован в процессы** организации.

Он должен применяться на:

- стратегическом,
- операционном,
- программном и проектном уровнях.

Между тем, самым популярным стандартом в мире, по которому сертифицированы более полутора миллионов предприятий, является ISO 9001:2015. Начиная с 2015 года данный стандарт ввел термин риск-ориентированного мышления, и в пунктах 4.4.1 и 6.1 четко говорится, что **в процессах** должны быть определены **риски**, а мероприятия в ответ на них должны быть **интегрированы в процессы** компании.

В топ-4 международных стандартов ISO (это «дженгельменский набор» для каждого уважающего себя крупного промышленного предприятия) входят: ISO 9001 (качество), ISO 14001 (экология), ISO 45001 (охрана здоровья и обеспечение безопасности труда) и ISO 50001 (энергоменеджмент). В последних версиях этих стандартов есть пункт 6, который практически идентично описывает действия по реагированию на риски и возможности. Он требует идентифицировать риски в своих процессах, запланировать действия по реагированию на эти риски и интегрировать эти действия в существующие процессы.

Мы должны заниматься рисками не как отдельными сущностями (в отрыве от целей и процессов), а идентифицировать риски в своих процессах, отталкиваясь от стратегических целей, КПД (ключевых показателей деятельности) и KPI-процессов.

ющие процессы, а также оценивать результативность этих действий.

При этом важно отметить, что в данных стандартах не прописаны такие действия, как анализ и оценивание рисков, то есть методик как это делать, там нет. Здесь на помощь приходит ISO 31010, который содержит свыше 30 способов по анализу, оценке, идентификации риска. Соответственно, мы можем применить эти инструменты, чтобы сделать интегрированную систему менеджмента в компании риск-ориентированной.

Несмотря на то что во второй версии модели COSO ERM 2017 года выпуска четко говорится, что риск-менеджмент – это процесс (в отличие от первой версии COSO ERM:2004, где использовался термин «система управления рисками»), а в первой и второй редакциях ISO 31000 прописано, что риск-менеджмент – это процесс, который должен быть интегрирован в существующие процессы, во многих компаниях СНГ присутствуют положения о КСУР (корпоративной системе управления рисками), есть регламенты КСУР и отчеты о КСУР (то есть создается некая отдельная, обособленная «вселенная рисков» в виде системы управления рисками). В соответствии с этими документами происходит идентификация, анализ и оценка рисков, итоги которой фиксируются в регистре и карте рисков. Далее происходит обработка рисков, итоги которой вносятся в План мероприятий, входящий в Регистр рисков. В итоге все это отображается в отчетах по рискам, которые раз в квартал выносятся на совет директоров либо на наблюдательный совет, в зависимости от структуры корпоративного управления. Вопрос – а где же интеграция риск-менеджмента в процессы в данной концепции? То есть, чтобы сделать систему менеджмента риск-ориентированной, мы должны внедрить, встроить, интегрировать риск-менеджмент в существующие процессы. Как это сделать, пояснение – ниже (см. слайд).



Важный момент: мы должны заниматься рисками не как отдельными сущностями (в отрыве от целей и процессов), а идентифицировать риски в своих процессах, отталкиваясь от стратегических целей, КПД (ключевых показателей деятельности) и KPI-процессов. Так как риск – это влияние неопределенности на достижение поставленных целей.

Мы должны идентифицировать риски в процессах, проанализировать, оценить и обработать риски. Критичный аспект – планируемые мероприятия по обработке рисков необходимо встроить в существующие ВНД (внутренние нормативные документы), которые описывают данный процесс (или процесс принятия решений, например – положение о совете директоров). Наилучшая практика – когда мероприятия по обработке

рисков будут отражены в критических документах: положениях о структурных подразделениях, положениях о функционировании коллегиальных органов (Бюджетный/Инвестиционный комитет), должностных инструкциях ключевых сотрудников, в ВНД, описывающих функционирование процессов. «Вишенка на торте» – ключевые рискованные показатели должны быть отражены в управленческой отчетности, а проводимые внутренние аудиты – риск-ориентированными, вот тогда считается, что процесс управления рисками успешно интегрирован в существующие процессы. При этом по факту компания может иметь только один документ в рамках риск-менеджмента – так называемую Политику по управлению рисками, прочих отдельных документов стандарты ISO 31000 и ISO 9001 в части риск-менеджмента не требуют. Имейте это в виду при коммуникации с органами по сертификации.

Отчеты по рискам, регистр и карты рисков мы условно называем «риск-менеджмент-1» (PM1), его потребителями в основном являются внешние стейкхолдеры (банки, страховые агентства, контрагенты, советы директоров, акционеры), «риск-менеджмент-2» (PM2) – это управление рисками, а скорее даже анализ рисков в интересах руководителей, принимающих решения внутри компании.

У риск-менеджеров нет выбора между PM1 и PM2. Оба должны быть реализованы в компании. Это, скорее, выбор приоритетов.

Эффективное распределение времени:

- 20% времени или меньше на PM1;
- 80% или больше на PM2.

Примеры PM1 и PM2:

Регламент по управлению рисками:

- PM1 – политика / положение о Корпоративной системе управления рисками (на основе ISO 31000 / COSO ERM);
- PM2 – элементы управления рисками включены в действующие ВНД в виде соответствующих методик / чек-листов, разработанных по итогам анализа рисков.

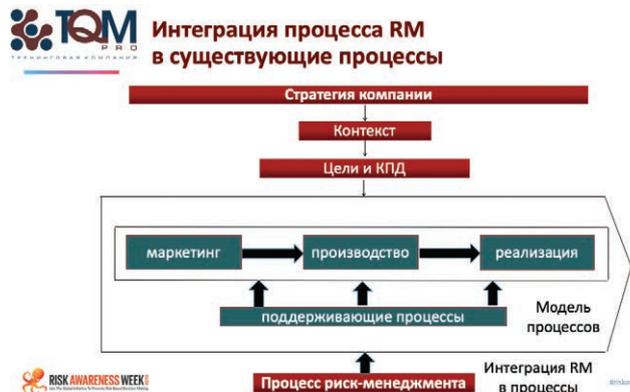
Реестр рисков:

- PM1 – имеется единый реестр рисков, который обновляется раз в год и связан с циклом бюджетирования;
- PM2 – риски анализируются при необходимости принятия решения.

Отчеты о рисках:

- PM1 – ежеквартальный отчет о рисках;
- PM2 – информация о рисках (в виде ключевых рискованных показателей) включена в управленческую отчетность компании и в процесс принятия решений.

Рассмотрим, как провести интеграцию процесса PM (риск-менеджмента) в существующие процессы. На основании стратегии компании делаем контекст, уста-



СОВЕТЫ ПРОФЕССИОНАЛА

навливаем цели и ключевые показатели деятельности. Безусловно, вышеперечисленные действия также необходимо осуществлять с учетом рисков, однако в рамках данного кейса мы разберем порядок интеграции РМ именно в бизнес-процессы компании.

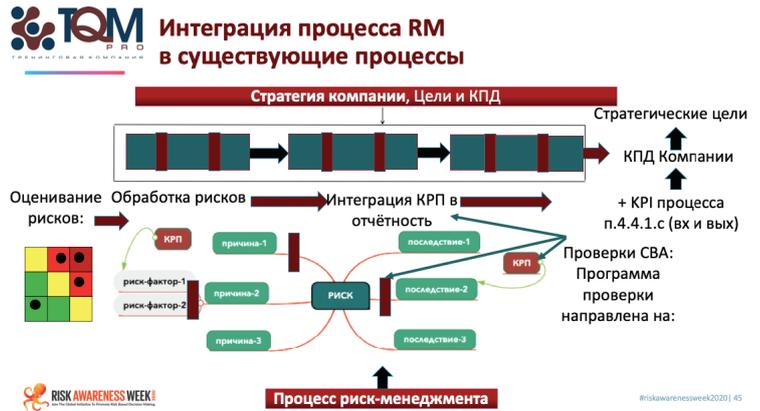
Поэтому, прежде всего, строим модель процессов и интегрируем в нее процесс риск-менеджмента (см. слайд).

Это происходит следующим образом: берем в помощь ISO 31010, где есть метод идентификации и анализа рисков, который называется «процессный подход». То есть мы берем каждый из критичных для нас процессов, разбиваем его на этапы и устанавливаем критерии процесса. Не забываем, что в ISO 9001 в пункте 4.4.1.с указано два требуемых критерия: входной (критерий для управления) и выходной (критерий для результативности процесса). Данные критерии устанавливаются на основе КПД компании, которые формируются на основании стратегических целей.

Очень важно в процессах определить два вида критериев. Как правило, в 80% случаев в рамках тренингов, семинаров и проектов я вижу, что в компаниях определен только один вид критериев – входные, а выходные либо не полностью, либо в неполном объеме, либо они не сбалансированы. Рекомендую обратить на этот аспект внимание, поскольку это прямое требование стандарта ISO 9001, и его выполнение даст вам правильный подход к управлению рисками, так как критерии процесса – это цели, а риск – это влияние неопределенности на достижение целей.

Таким образом, взяв ключевой процесс, мы разбиваем его на этапы и определяем «входные» и «выходные» критерии процесса (это прямое требование п.4.4.1.с ISO 9001). После этого включается процесс риск-менеджмента, и мы начинаем идентификацию рисков. То есть выписываем события, которые могут положительно или отрицательно повлиять на поставленные KPI процесса («входные» и «выходные» критерии процесса). Затем происходит анализ рисков. Существует много способов анализа. В данном кейсе я демонстрирую метод «галстук-бабочка» из ISO 31010. После анализа рисков наступает этап оценивания рисков. Его можно проводить качественно, количественно или же комбинированным способом. В рамках разбираемого кейса я не буду спорить о преимуществах и недостатках того или иного способа; важно понимать, что оценка рисков осуществляется, чтобы в том числе определить приоритет обработки рисков.

ся метод «галстук-бабочка». Мы ставим дополнительные контрольные точки – фильтры с тем, чтобы снизить вероятность реализации причины, которая привела к тому или иному риску. Таким образом, в процессе закрываем пробелы нашими мероприятиями. Это и есть интеграция процесса риск-менеджмента в существующие процессы (в упрощенном виде).



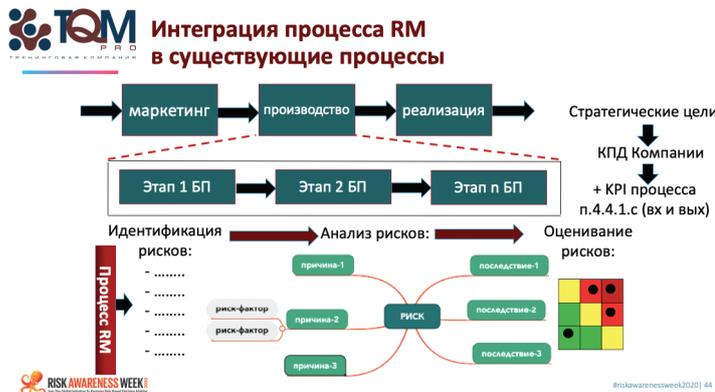
Сделав апгрейд управленческой отчетности и интегрировав в нее КРП (ключевые рисковые показатели), переходим к мониторингу и анализу рисков, что можно сделать, например, силами службы внутреннего аудита (СВА). То есть в программу СВА добавляем проверку выполнения тех процедур, которые мы встроили в наши процессы. Это и есть риск-ориентированный аудит. Также проверяем полноту интеграции КРП в управленческую отчетность и логику оформления самих КРП. Эта схема дает представление о выполнении критериев процесса, что позволяет достигать KPI и КПД компании, а впоследствии – стратегических целей компании.

На тренингах, как правило, мы определяем стратегию компании, формируем контекст, тем самым выполняя пункт 4.1 ISO 9, 14, 45, 50; формируем КПД и риск-ориентированные цели, выполняя пункт 6.2 ISO 9, 14, 45, 50. После этого формируем модель процессов, необходимых для достижения поставленных целей и стратегии компании, выполняя пункт 4.4. ISO 9, 14, 45, 50.

Часто во время тренингов и проектов я вижу, что компании идентифицируют слишком большое количество процессов. На моей практике было и 15, и 20, и даже 50 процессов. Это не очень эффективно, хотя сам стандарт ISO 9001 нас не ограничивает. Если исходить из такого термина, как «нормы управляемости», то я придерживаюсь мнения, что верхнеуровневых процессов должно быть 5–7, максимум 10.

Итак, мы сформировали необходимые процессы (для достижения стратегических целей – по итогам анализа контекста). Для примера возьмем такие процессы, как маркетинг, проектирование, закупки, производство, складирование, реализация и некие поддерживающие процессы. В них нужно интегрировать процесс риск-менеджмента, тем самым выполняя пункт 6.1 ISO 9, 14, 45, 50.

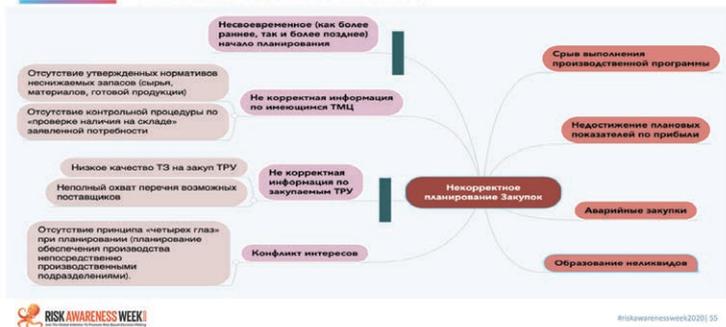
Необходимо пояснить взаимосвязь стратегии, целей и рисков, которая заложена в стандартах ISO. Исходя из стратегии, формируется контекст (пункт 4.1), по итогам контекстного анализа формируются процессы (пункт 4.4.1) – те виды деятельности, где у нас проблемы, где мы зарабатываем деньги и хотим добавить улучшений. В процессах мы устанавливаем критерии (KPI) двух видов (пункт 4.4.1с) на входе и выходе. Соответственно, достигая поставленных критериев, мы достигаем стратегической цели компании.



По итогам оценки рисков мы выявляем риски, которые нужно обработать в первую очередь, и переходим к обработке рисков. В данном случае также использует-



Анализ риска – текущие контрольные процедуры



Смоделируем ситуацию, что у нас есть некий «Регламент закупок», который закрывает причины по планированию, там установлен срок начала планирования закупочной кампании, а также некие требования по формированию технического задания на закупку товаров, работ и услуг. Проведем анализ рисков, приступаем к их оцениванию. Представим, что первый риск – некорректное планирование закупок в приоритете, соответственно, его будем обрабатывать в первую очередь. Стандарт предусматривает четыре способа обработки риска:

- устранение,
- изменение (снижение или повышение риска),
- передача,
- принятие.

Можно выбрать один или несколько вариантов. В рамках данного кейса выбираем вариант снижения риска путем разработки дополнительных контрольных процедур либо усиление существующих (то есть усиливаем «существующие фильтры»). У нас есть «Регламент закупок», где установлен единый срок проведения или начала планирования закупок. Соответственно, проводим анализ горизонта планирования закупок и вносим в «Регламент закупок» разные сроки планирования по различным группам ТРУ.

Одной из обозначенных нами причин некорректного планирования закупок является некорректная информация по имеющимся ТМЦ, что может произойти в связи с отсутствием утвержденных нормативов неснижаемых запасов, отсутствием контрольной процедуры по проверке наличия на складе заявленной потребности ТМЦ. Исходя из этого, делаем здесь дополнительную контрольную точку (в виде приложения к «Регламенту закупок») в виде разработанных нормативов неснижаемых запасов (сырья, материалов, продукции) и включаем в «Регламент закупок» контрольную точку по проверке наличия на складе заявленной потребности. Отражаем в должностных инструкциях соответствующих лиц ответственность за это действие.

Другая причина – некорректная информация по покупаемым ТРУ. В риск-факторах стоит низкое качество на закупку ТРУ и неполный охват перечня возможных поставщиков. Мы можем разработать типовые формы на технические задания и провести обучение по составлению ТЗ, можем включить в «Регламент закупок» требования о наличии минимум двух-трех потенциальных поставщиков, а также наличие регулярно обновляемого пула поставщиков по большинству позиций закупок.

Наконец, последняя причина – конфликт интересов. Здесь можем сделать следующее: отразить в «Регламенте закупок», что потребность формируется планово-экономическим отделом и согласуется с директором по снабжению и производственными подразделениями;

отразить в «Регламенте закупок» необходимость расчета экономической эффективности аутсорсинга (передача чего-либо на аутсорсинг рассматривается на тендерном комитете).

Благодаря обработке рисков нам удалось восполнить имеющиеся пробелы и интегрировать процесс управления рисками в процесс закупок. То есть мы усилили «Регламент закупок», не разработав ни одного нового документа.

После обработки рисков необходим мониторинг, и мы приступаем к интеграции ключевых рисков показателей (КРП) в управленческую отчетность. КРП – это индикаторы, которые позволяют оценить приближение риска по тем или иным направлениям, чтобы у нас было время на воздействие и чтобы сам риск не реализовался. Соответственно, эти КРП необходимо определить и встроить в существующую управленческую отчетность, не создавая при этом нового документа (например, отчетов по рискам).



Обработка риска: Снижение риска



КРП может быть двух видов – прогнозным и итоговым. Возьмем, например, риск «технологические отказы». Под прогнозным КРП мы понимаем уровень выполнения физических объемов ППР и капитального ремонта до 95%, а итоговый КРП – это количество аварийных остановов в межремонтный цикл (от 1 до 3 раз считаем допустимым). Суть в том, что если итоговый КРП превышен, а прогнозный был соблюден, это является лакмусовой бумажкой, что нужно провести более глубокий анализ, используя метод «галстук-бабочка», «5 почему», деревья решений, сценарный анализ, имитационное моделирование методом Монте-Карло. Таким образом, сможем разобраться в причинах: почему итоговый КРП превышен, а прогнозный был в норме.

По данному кейсу мы должны разработать прогнозный и итоговые КРП. Они могут выглядеть следующим образом: допустим, дата закупочной кампании по группам ТРУ; по факту отсутствия утвержденных нормативов (напомним, ранее мы разработали норматив, теперь нужно убедиться, что он пересматривается в установленные промежутки времени, анализируется обоснованность расчета данных нормативов со стороны уполномоченного подразделения – допустим, силами службы внутренних аудиторов или привлеченными экспертами); отсутствия контрольной процедуры по проверке наличия на складе заявленной потребности (мы добавили контрольную точку в «Регламент закупок», соответственно, устанавливаем ключевой рискованный показатель – данные о проверке наличия на складе).

По факту низкого качества технического задания на закупку ТРУ мы определяем, что должна быть свое-

временная актуализация и пополнение альбома типовых форм ТЗ плюс своевременное обучение персонала. По факту неполного охвата перечня возможных поставщиков включаем в КРП наличие регулярно обновляемого пула поставщиков по большинству позиций закупа не менее какой-то позиции X.

В конфликте интересов может быть много риск-факторов, мы в рамках данного кейса рассматриваем один – отсутствие принципа «четырех глаз» при планировании. КРП здесь будет следующий – выборочный анализ правильности выбора закупочной процедуры в установленные периоды.

Теперь поговорим об итоговых КРП. Они могут быть такие: аварийные закупки допускаются не более трех раз в квартал (при этом необходим анализ фактов срыва графиков производства из-за отсутствия ТМЦ). По обоснованию неликвидов итоговый КРП устанавливаем, условно, не более 2%

Этот пример показывает, как можно установить итоговый и прогнозный КРП по риску «некорректное планирование закупок» (см. слайд). Мы усилили существующий «Регламент закупок» и сделали апгрейд управленческой отчетности подразделения, которое осуществляет закупки.

После установки КРП требуется мониторинг, его можно выполнять силами службы внутреннего аудита. Соответственно, мы должны сделать риск-ориентированную программу внутреннего аудита. Для этого на риск-фактор «конфликт интересов» мы можем сделать про-

Действия по тестированию:

- ✓ Анализ причин отсутствия номенклатуры, по которой произошла аварийная закупка, в том числе в первоначальной потребности.

По факту отсутствия утвержденных нормативов программа проверки: убедиться в обоснованности нормативов запаса сырья и материалов.

Признак эффективного дизайна:

- ✓ Нормативы разработаны планово-экономическим отделом и согласованы с директором по производству и директором по снабжению;
- ✓ Регулярный пересмотр нормативов.

Действия по тестированию:

- ✓ Анализ обоснованности установления норматива для сырья и материалов с оборачиваемостью свыше 0,5 года;
- ✓ Анализ факторов срывов графиков производства из-за отсутствия сырья и материалов/аварийных закупок.

КУЛЬТУРА УПРАВЛЕНИЯ РИСКАМИ

Мы последовательно прошли по этапам процесса управления рисками: идентификация, анализ, оценка, обработка и мониторинг.

При этом вы должны помнить, что на каждом из этапов процесса управления рисками вас ожидают ментальные ловушки (когнитивные искажения), которых более 200. Например, на этапе идентификации рисков существуют в том числе такие ментальные ловушки, как чрезмерный оптимизм, риски-невидимки, ранее принятые решения, ментальные якоря. На этапе анализа и оценивания рисков – иллюзия контроля, большая выгода, формулировка риска. На этапе обработки риска – снижение сегодняшних рисков, но ухудшение будущих или бездействие.

Важно понимать, знать ментальные ловушки и владеть инструментами противодействия им. Но при этом также важна и культура управления рисками. Я всегда говорю, что управление рисками это на 10% – процесс и на 90% – культура.

В рамках проводимых тренингов и проектов, в ходе групповых работ и мозговых штурмов, мы детально (и, что очень важно – конкретно на примере бизнес-процессов компании-Заказчика) разбираем каждый из этапов процесса управления рисками, определяем ключевые риски рассматриваемого бизнес-процесса компании-Заказчика, формируем мероприятия по управлению рисками (которые встраиваем в существующие внутренние нормативные документы, описывающие данный бизнес-процесс), определяем КРП (прогнозные и итоговые) и способы их интеграции в существующую управленческую отчетность и, наконец, разрабатываем риск-ориентированную программу внутреннего аудита и мероприятия по усилению Системы внутреннего контроля.

При этом даются инструменты противодействия когнитивным искажениям (ментальным ловушкам), а также методы повышения культуры управления рисками и принятия качественных, риск-ориентированных решений.

Уважаемые коллеги, берите за основу ISO 31000, повышайте культуру управления рисками, изучайте ментальные ловушки и способы принятия качественных решений, и тогда интеграция процесса риск-менеджмента в ваши бизнес-процессы у вас пройдет успешно, а значит, ваша компания достигнет поставленных целей, поскольку ключевые решения у вас будут приниматься с учетом рисков.



грамму проверки – убедиться в применении принципа «четырех глаз» при формировании потребности на период.

Признак эффективного дизайна:

- ✓ потребность формируется планово-экономическим отделом и согласуется с директором по снабжению и производственными подразделениями.

Действия по тестированию:

- ✓ анализ корректности расчетов по выборке за какой-нибудь период.

В рамках аварийных закупок нужно прежде всего убедиться в их обоснованности.

Признак эффективного дизайна:

- ✓ Аварийные закупки осуществляются только при согласовании по принципу «четыре глаза» (закупку не могут инициировать только снабженцы или только производственники);
- ✓ Проводится регулярный анализ причин аварийных закупок, в том числе применяются административные меры.