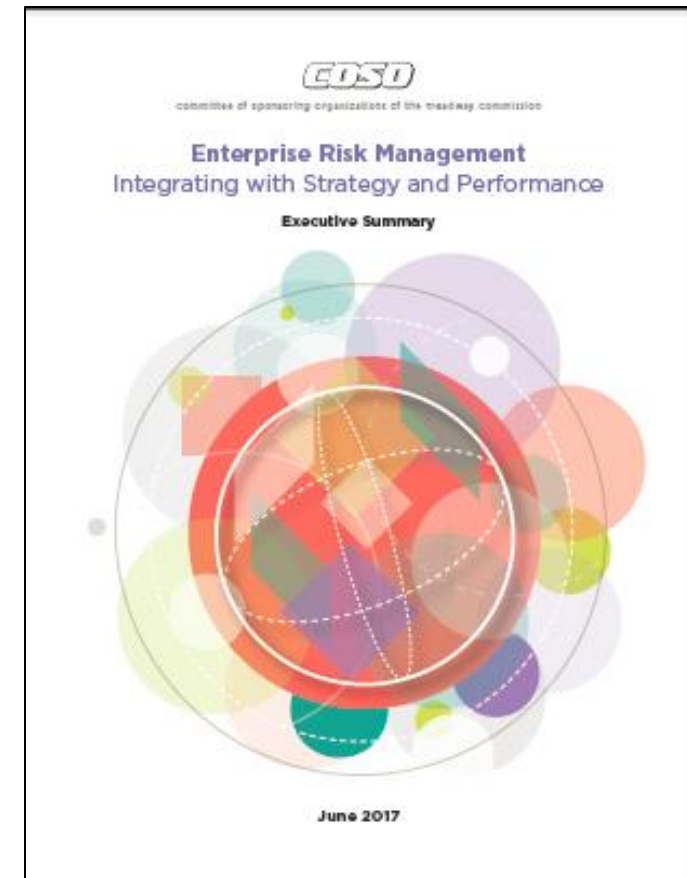


**Управление рисками**  
Правила игры меняются

«Делойт», 30 января 2018 года

# Концептуальные основы управления рисками COSO ERM

- Концептуальные основы управления рисками: Интеграция со стратегией управлением деятельностью (COSO ERM), разработаны Комитетом организаций-спонсоров Комиссии Тредвея.
- COSO ERM содержит 202 страницы и доступна в английской версии на сайтах следующих организаций: The Institute of Internal Auditors, AICPA
- Стоимость варьируется, в зависимости от наличия членства в организациях и версии (электронная, бумажная) от 129.99\$ до 169.99\$.
- COSO ERM не является стандартом и концептуально представляет лучшие практики в управлении рисками.
- В силу ограниченной доступности новой версии COSO ERM команда по управлению рисками Делойт представляет ее краткий обзор и свое видение практических аспектов применения в Российской практике.



# Предпосылки для обновления COSO ERM

В практической плоскости сформированная традиционная модель управления рисками была больше сконцентрирована на процессах управления рисками, которые осуществлялись обособлено от процессов планирования и принятия управленческих решений. Увеличение волатильности бизнес среды и требования по оптимизации эффективности деятельности способствовали тому, что акционеры и менеджмент стали задаваться вопросом в целесообразности системы управления рисками в процессе создания стоимости.

## COSO ERM 2004






Предыдущая версия концептуальных основ управления рисками COSO ERM 2004 получила широкое распространение и была принята многими организациями в качестве отправной точки для внедрения интегрированной системы управления рисками.

## COSO ERM 2017

В новой редакции COSO ERM: Интеграция со стратегией и управлением деятельностью, авторы постарались отразить новые тенденции в практике и видении управления рисками, а также дать ответы на возникшие вопросы.

# COSO ERM 2004 - Прояснение недоразумений

Предыдущая версия концепции COSO ERM представила компоненты интегрированной системы управления рисками, которые были больше сфокусированы на этапах процесса управления рисками и в меньшей степени на практических аспектах их внедрения и интеграции с бизнесом. В связи с этим в практике риск-менеджмента возникли недоразумения, которые авторы концепции решили прояснить в самом начале:

-  Управление рисками организаций не является функцией или отделом. Это культура, компетенции и практики, которые организации интегрируют с процессом разработки стратегии и ее реализации с целью управления рисками при создании, сохранении и реализации стоимости.
-  Управление рисками организаций не ограничивается реестром рисков.
-  Управление рисками организаций связано не только с внутренним контролем. Оно также взаимосвязано со стратегией, корпоративным управлением, коммуникацией с заинтересованными сторонами и управлением эффективностью деятельности.
-  Управление рисками организаций не является чек-листом. Оно включает принципы, в соответствии с которыми могут быть выстроены бизнес-процессы и является системой мониторинга, обучения и улучшения эффективности деятельности.
-  Управление рисками организаций применимо для всех организаций вне зависимости от их размера.

# Что нового в концепции?



1. Новая структура концептуальных основ: 5 компонентов и 20 принципов, покрывающих процессы стратегического планирования и управления эффективностью организации.



2. Акцент на интеграции управления рисками с процессами стратегического планирования и управления эффективностью предприятий.



3. Больше значения придается корпоративному управлению и культуре.



4. Учет возрастающей роли технологий в процессах управления рисками.

# COSO ERM 2017 – Структура концепции



## Управление и культура

1. Осуществление советом директоров надзорной функции за управлением рисками
2. Создание операционных структур
3. Определение желаемой культуры
4. Демонстрация приверженности основным ценностям
5. Привлечение, развитие и удержание квалифицированных специалистов



## Стратегия и постановка целей

6. Анализ условий ведения деятельности
7. Определение риск-аппетита
8. Оценка стратегических альтернатив
9. Формулировка бизнес-целей



## Эффективность деятельности

10. Выявление рисков
11. Оценка влияния рисков
12. Приоритизация рисков
13. Реагирование на риск
14. Комплексный взгляд на риски



## Мониторинг и внедрение изменений

15. Оценка существенных изменений
16. Анализ рисков и эффективности деятельности
17. Повышение эффективности системы управления рисками



## Информация, коммуникация и отчетность

18. Использование информации и технологий
19. Распространение информации о рисках
20. Отчетность о рисках, корпоративной культуре и эффективности деятельности

# Ключевые понятия и определения



## Риск

**Риск** – вероятность возникновения событий, которые могут оказать влияние на достижение стратегических и бизнес целей.



## Риск-менеджмент

**Риск-менеджмент** – культура, компетенции и практики, интегрированные с процессом определения стратегии и управления эффективностью, на которые организация полагается в создании, сохранении и реализации стоимости.

# COSO ERM 2017 – Управление и культура

## Принципы

1

Осуществление советом директоров надзорной функции за управлением рисками

## Основные тезисы

- Совет директоров несет ключевую ответственность за осуществление надзора за управлением рисками.
- Осуществление надзора за управлением рисками требует от Совета директоров глубокого понимания стратегии, отрасли и информированности по текущим вопросам.
- Совет директоров должен оценивать эффективность управления рисками с точки зрения его вклада в создание стоимости.

2

Создание операционных структур

- Операционная структура организации определяется исходя из ее стратегии и целей.
- Сбор информации по рискам может быть делегирован комитетам при Совете директоров.
- Риск-офицер осуществляет роль методологической поддержки и координации деятельности по управлению рисками.

3

Определение желаемой культуры

- Корпоративная культура оказывает влияние на то, каким образом риски выявляются, оцениваются и управляются в организации с момента определения стратегии до ее реализации.
- В риск-ориентированной корпоративной культуре принимаемые решения и поведение четко очерчены риск-аппетитом организации.



# COSO ERM 2017 – Управление и культура

## Принципы

4

Демонстрация приверженности основным ценностям

## Основные тезисы

- Понимание ключевых ценностей организации закладывает фундамент для интегрированной системы управления рисками.
- Совет директоров назначает генерального директора ответственным за управление рисками для обеспечения достижения стратегических и бизнес целей.
- Генеральный директор и прочие представители топ-менеджмента несут ответственность за все аспекты развития культуры и системы управления рисками.

5

Привлечение, развитие и удержание квалифицированных специалистов

- Руководство, при надзоре со стороны Совета директоров, определяет потребность в человеческом капитале, необходимом для достижения стратегических и бизнес целей.
- Система поощрения должна быть привязана к достижению стратегических и бизнес целей организации, что также требует соответствующую оценку, приоритизацию рисков и план мероприятий по их управлению.

# Практические соображения

## > 1

---

Во многих компаниях Совет директоров формально выполняет надзорные функции в части управления рисками, но не проявляет реального интереса в развитии риск-менеджмента и его интеграции с бизнесом. Перед риск-менеджерами по-прежнему стоит задача повышения интереса к управлению рисками со стороны Совета директоров и руководства посредством разработки и внедрению подходов, при которых взаимосвязь между управлением рисками и созданием стоимости будет более очевидной и просчитанной.

## > 2

---

Существуют практики, при которых риск-офицер рассматривается как сотрудник, который несет ответственность за риски. Концепция однозначно подчеркивает, что роль риск-офицера заключается в методологической поддержке и координации деятельности по управлению рисками. Тем не менее, необходимо понимать ситуации, при которых роль риск-офицера может быть более расширенной.

## > 3

---

Во многих компаниях организационная структура и кадровая политика сформированы исторически и не всегда отражают стратегические инициативы. Реструктуризация может потребовать существенных ресурсов и столкнуться с сопротивлением со стороны руководства.

# COSO ERM 2017 – Стратегия и постановка целей

## Принципы

6

Анализ условий ведения бизнеса

## Основные тезисы

- Организация рассматривает условия (внешние/внутренние) ведения бизнеса в процессе разработки стратегии для реализации своей миссии, видения и ключевых ценностей.
- Влияние условий ведения бизнеса на профиль риска может рассматриваться в перспективе прошлых, текущих и будущих событий.

7

Определение риск-аппетита

- Решения связанные с выбором стратегии и определением риск-аппетита не связаны линейными отношениями, когда одно предшествует другому.
- Подходы к определению риск-аппетита определяются организациями исходя из специфики их деятельности.
- Лучшим подходом считается определение риск-аппетита в контексте риск профиля и емкости риска.

# COSO ERM 2017 – Стратегия и постановка целей

## Принципы

8

Оценка стратегических альтернатив

### Основные тезисы

- Организация должна проводить анализ альтернативных стратегий и оценивать риски и возможности каждой из альтернатив.
- Руководство и Совет директоров должны учитывать профиль риска и риск-аппетит при выборе стратегии.

9

Формулировка бизнес целей

- Цели определяются на различных уровнях, но должны быть привязаны к стратегии организации.
- Толерантность отражает приемлемое отклонение от поставленных целей. Соответственно, толерантность определяется в отношении целей и эффективности, а не конкретных рисков.
- Степень эффективности достижения целей определяется границами толерантности.

# Практические соображения

## > 4

---

Риск-аппетит становится неотъемлемой частью интеграции управления рисками со стратегическим планированием. Так как концепция оставляет разработку подходов к определению риск-аппетита на усмотрение организаций, перед заинтересованными сторонами стоит задача по внедрению риск-аппетита, который будет использоваться как работающий инструмент при принятии решений, а не оставаться в качестве формального упражнения.

## > 5

---

Во многих бизнес-практиках концепция толерантности к рискам уже применяется в процессах планирования и осуществления хозяйственной деятельности. Появляется задача по взаимоувязке толерантности к рискам с риск-аппетитом организации.

# COSO ERM 2017 – Эффективность деятельности

## Принципы

10

### Выявление рисков

## Основные тезисы

- Организация выявляет риски, связанные с достижением стратегических и бизнес целей.
- Первоначально организация формирует общую базу данных по рискам (risk inventory) и в последующем определяет, какие риски являются актуальными.
- Риски могут быть структурированы в отдельные категории, которые организация определяет по своему усмотрению
- Риски определяются на всех уровнях бизнес-процессов и функций.

11

### Оценка рисков

- Риски оцениваются по воздействию и вероятности. Воздействие риска измеряется в отношении цели, на которую риск оказывает влияние. Вероятность риска может быть выражена экспертной оценкой, количественной оценкой и частотой реализации риска.
- Описание риска включает описание риск-факторов и его последствий.
- Подходы к оценке рисков могут быть количественными и качественными.
- В процессе оценки рисков руководство принимает во внимание присущий риск, целевой остаточный риск, фактический остаточный риск.
- Карта рисков (heat map) используется как инструмент графической визуализации существенности рисков.
- При оценке рисков руководство должно принимать во внимание и снижать эффект предвзятости.

# COSO ERM 2017 – Эффективность деятельности

## Принципы

12

### Приоритизация рисков

## Основные тезисы

- Организация приоритизирует риски с целью определения адекватной стратегии по реагированию на риски и распределению ресурсов по их управлению.
- При приоритизации рисков необходимо учитывать риск-аппетит. Повышенный приоритет получают риски, воздействие которых может привести к превышению риск-аппетита.
- Приоритетность рисков определяется по установленным критериям (примеры критериев: адаптивность к риску, сложность риска, скорость воздействия риска, устойчивость влияния риска, восстановление после реализации риска).

13

### Реагирование на риск

- Выделяются 5 стратегий реагирования на риск (принятие риска, избегание риска, добор риска, снижение риска, передача риска).
- Вышеуказанные стратегии применяются в рамках существующих условий деятельности, принятых целей и риск-аппетита. В случаях, когда уровень риска оказывается слишком высоким, а стратегии по реагированию на риски неприемлемыми, организация может пересмотреть свои стратегические и операционные цели.
- Выбор стратегии реагирования на риски с учетом условий ведения бизнеса, соотношения выгоды и затрат, обязательств и ожиданий, приоритизации рисков, риск-аппетита и существенности риска.

# COSO ERM 2017 – Эффективность деятельности

## Принципы

14

Комплексный взгляд на риски

## Основные тезисы

- Комплексный взгляд на риски позволяет организации определить насколько остаточный профиль риска соответствует установленному риск-аппетиту.
- Выделяются несколько подходов к портфельному анализу рисков в зависимости от степени интеграции управления рисками с бизнесом:
  - Минимальная интеграция (фокус на существенных рисках) – организация выявляет и оценивает дискретные риски. Ключевой фокус на существенных рисковом событиях, а не целях.
  - Ограниченная интеграция (фокус на категориях рисков) – организация формирует базу данных по рискам, структурированных по категориям. Портфель рисков представляет перечень рисков сгруппированных по категориям.
  - Частичная интеграция (фокус на профиле риска) – организация переносит фокус на бизнес-цели и риски, связанные с их достижением.
  - Полная интеграция (комплексный взгляд на риски) – организация фокусируется на стратегии и бизнес-целях. Риски определяются на всех уровнях принятия решений.



# Практические соображения

## 6

Создание и ведение базы данных по рискам может потребовать много ресурсов. Не всегда оказывается возможным обосновать целесообразность этого процесса в точки зрения создания стоимости.

## 7

Концепция по-прежнему устанавливает основные метрики для оценки рисков (вероятность/воздействие). Тем не менее, не упоминается, что для определенных рисков более целесообразным является определение вероятностного распределения воздействия.

## 8

Карта рисков остается основным инструментом графической визуализации профиля рисков. При этом не упоминается применение альтернативных инструментов (например, диаграмма Торнадо).

## 9

Во многих бизнес-практиках концепция толерантности к рискам уже применяется в процессах планирования и осуществления хозяйственной деятельности. Появляется задача по взаимосвязки толерантности к рискам с риск-аппетитом организации.

# COSO ERM 2017 – Мониторинг и внедрение изменений

## Принципы

15

Оценка существенных изменений

## Основные тезисы

- Организация, как правило, рассматривает потенциальные изменения в процессе определения стратегии и установки бизнес-целей, но, тем не менее, ей необходимо осуществлять мониторинг изменений в текущей деятельности и оценивать влияние изменений на стратегию и профиль риска.

16

Анализ рисков и эффективности деятельности

- Анализ рисков и эффективности деятельности должен быть интегрирован в деятельность организации. Ключевыми вопросами являются:
  - Достигла ли организация своих целей с ожидаемой эффективностью?
  - Какие риски реализовываются и могут повлиять на эффективность деятельности?
  - Является ли достаточным уровень риска для достижения целей компании?
  - Правильно ли был оценен риск?
- В случае существенных отклонений от заданных целей, организация может пересмотреть бизнес-цели, стратегию, корпоративную культуру, целевые показатели эффективности деятельности, оценку рисков, стратегии реагирования на риски, риск-аппетит.

17

Повышение эффективности управления рисками

- Организация должна стремиться к постоянному повышению эффективности управления рисками на всех уровнях управления.

# COSO ERM 2017 – Информация, коммуникация и отчетность

## Принципы

18

Использование информации и технологий

## Основные тезисы

- Построение информационной инфраструктуры должно учитывать обеспечение гибкости в принятии решений.
- Необходимо принимать во внимание развитие технологий по анализу данных (искусственный интеллект, дата майнинг), которые позволяет охватывать большие объемы данных и принимать более информированные решения.

19

Распространение информации по рискам

- Коммуникация информации по рискам должна стать неотъемлемой частью коммуникации стратегии и бизнес-целей.
- Необходимо определить роли и обязанности между Советом директоров и руководством в части подготовки и использования информации по рискам.
- Обсуждение риск-аппетита между Советом директоров и руководством должно проходить на постоянной основе.

20

Отчетность о рисках, корпоративной культуре и эффективности деятельности

- Отчетность по рискам может подготавливаться на всех уровнях управления.
- На уровне Совета директоров отчетность должна быть сфокусирована на взаимосвязи между стратегией, бизнес-целей, рисками и эффективностью деятельности.
- Частота и качество отчетности определяется руководством исходя из специфики и бизнес-необходимости.

# Ключевые выводы

## ➤ Вывод 1

---

Новая версия COSO ERM является однозначным улучшением предыдущей версии, устанавливая новые перспективы развития в области управления рисками.

## ➤ Вывод 2

---

Некоторые новые положения концепции затрагивают достаточно очевидные и базовые аспекты корпоративного управления, но тем не менее остаются актуальными для Российской практики по управлению рисками.

## ➤ Вывод 3

---

Области, которые потребуют наибольшего внимания с точки зрения дальнейшего развития включают развитие риск-ориентированной культуры, практическое применение риск-аппетита и внедрение управление рисками в процессы стратегического планирования и управления эффективностью организации.

## ➤ Вывод 4

---

Концепция по-прежнему не в достаточной мере покрывает подходы к количественной оценке рисков и альтернативные инструменты визуализации рисков.

## ➤ Вывод 5

---

Не достаточно детально раскрыта тема взаимоувязки управления рисками с процессом создания стоимости.



## deloitte.ru

### О «Делойте»

Наименование «Делойт» относится к одному либо любому количеству юридических лиц, включая их аффилированные лица, совместно входящих в «Делойт Туш Томацу Лимитед», частную компанию с ответственностью участников в гарантированных ими пределах, зарегистрированную в соответствии с законодательством Великобритании (далее — ДТТЛ). Каждое такое юридическое лицо является самостоятельным и независимым юридическим лицом. ДТТЛ (также именуемая «международная сеть «Делойт»») не предоставляет услуги клиентам напрямую. Подробная информация о юридической структуре ДТТЛ и входящих в нее юридических лиц представлена на сайте [www.deloitte.com/about](http://www.deloitte.com/about).

«Делойт» предоставляет услуги в области аудита, консалтинга, финансового консультирования, управления рисками, налогообложения и иные услуги государственным и частным компаниям, работающим в различных отраслях экономики. «Делойт» — международная сеть компаний, в число клиентов которой входят около четырехсот из пятисот крупнейших компаний мира по версии журнала Fortune. «Делойт» имеет многолетний опыт практической работы при обслуживании клиентов в любых сферах деятельности более чем в 150 странах мира и использует свои обширные отраслевые знания и опыт оказания высококачественных услуг для решения самых сложных бизнес-задач клиентов. Более 264 тысяч специалистов «Делойта» по всему миру привержены идеям достижения результатов, которыми мы можем гордиться. Для получения более подробной информации заходите на нашу страницу в [Facebook](#), [LinkedIn](#) или [Twitter](#).

Настоящее сообщение содержит информацию только общего характера. При этом ни компания «Делойт Туш Томацу Лимитед», ни входящие в нее юридические лица, ни их аффилированные лица (далее — «сеть «Делойт»») не представляют посредством данного сообщения каких-либо консультаций или услуг профессионального характера. Прежде чем принять какое-либо решение или предпринять какие-либо действия, которые могут отразиться на вашем финансовом положении или состоянии дел, проконсультируйтесь с квалифицированным специалистом. Ни одно из юридических лиц, входящих в сеть «Делойт», не несет ответственности за какие-либо убытки, понесенные любым лицом, использующим настоящее сообщение.