COSO ERM 2017: двадцать принципов на одной странице

Краткое изложение принципов редакции 2017 года своими словами, с тем, что проверить в компании. Официальный текст COSO на английском. Разбор модели и самооценка в Excel: risk-place.ru/coso-erm/

Руководство и культура		
1	**Надзор со стороны совета директоров**	Совет видит главные риски и задает вопросы о них, а не только утверждает отчеты.
2	**Организационная структура**	Понятно, кто владеет риском, кто задает правила и кто проверяет.
3	**Требуемая культура**	О рисках говорят открыто, плохие новости доходят до руководства вовремя.
4	**Приверженность ценностям**	Поведение руководителей совпадает с декларациями, нарушения имеют последствия.
5	**Способные сотрудники**	Компания привлекает, развивает и удерживает людей, которые умеют работать с рисками.
Стратегия и постановка целей		
6	**Анализ бизнес-контекста**	При выборе стратегии учитываются внешняя среда, клиенты, конкуренты и регулирование.
7	**Определение риск-аппетита**	Совет утверждает, какой риск компания готова принять, в измеримых показателях.
8	**Оценка альтернативных стратегий**	Стратегии сравнивают по риску, а не только по доходности.
9	**Формулирование целей**	Цели подразделений выведены из стратегии и согласованы с риск-аппетитом.
Результативность		
10	**Выявление рисков**	Риски ищут регулярно и по всей компании, включая новые и редкие.
11	**Оценка серьезности**	Риски оценены по единой шкале, по возможности в деньгах.
12	**Приоритизация**	Понятно, какими рисками заниматься в первую очередь и почему.
13	**Реагирование**	У значимых рисков есть мера, владелец, срок и бюджет.
14	**Портфельный взгляд**	Руководство видит риски вместе и понимает их совокупный эффект.
Анализ и пересмотр		
15	**Существенные изменения**	Компания замечает изменения, которые меняют профиль риска, и пересматривает оценки.
16	**Риски и результативность**	Связь между рисками и достижением целей анализируется по факту.
17	**Совершенствование**	Система управления рисками улучшается по итогам аудита и инцидентов.
Информация, коммуникация и отчетность		
18	**Информация и технологии**	Данные о рисках достоверны, своевременны и собираются без ручного хаоса.
19	**Информирование о рисках**	Сотрудники знают свои риски и куда сообщать о проблемах.
20	**Отчетность**	Совет и руководство получают отчет о рисках, культуре и результатах на одной-двух страницах.

Как пользоваться: по каждому принципу ответьте «выполняется», «частично» или «нет». Три-пять «нет» в одном компоненте показывают, с чего начинать. Подготовлено risk-place.ru, свободное использование внутри организации.