Политика и контекст управления рисками

написано Александр Астахов | 10 июня, 2023

Политика управления рисками – внутренний нормативный документ организации, регламентирующий вопросы управления рисками и базирующийся на политике СУИБ, стандартах и нормативных документах. Она определяет контекст для управления рисками; используемую терминологию СУИР как систему взаимосвязанных процессов, выполняемых в определенной последовательности и взаимодействующих друг с другом определенным образом; информационные потоки СУИР, включая предоставление отчетности, коммуникацию рисков и получение обратной связи; а также ответственность за управление рисками.

Содержание политики управления рисками:

- *терминология;*
- *контекст управления рисками;*
- *процессы управления рисками;*
- *отчетность;*
- *коммуникация рисков.*

Систематическое управление рисками в организации должно начинаться с определения контекста для управления рисками, который согласно ISO 27005 включает в себя следующее:

- *Цель управления рисками*. Общая цель – это поддержка СУИБ, однако для каких-то частных задач могут ставиться и более узкие цели, например планирование непрерывности бизнеса, реагирование на инциденты и т.п.
- *Критерии управления рисками,* включающие в себя: критерии

оценки ущерба, критерии оценки рисков и критерии принятия рисков.
- *Область и границы управления рисками*, которые обычно совпадают с областью действия и границами СУИБ.
- *Организационную структуру*, определяющую функциональные роли по управлению рисками, обязанности и распределение ответственности.

Контекст управления рисками:

- *цель;*
- *критерии;*
- *область и границы;*
- *организационная структура.*

Область действия СУИР (область управления рисками) в идеале должна совпадать с областью действия СУИБ и охватывать всю организацию. Однако оценить сразу все риски для всех активов и внедрить СУИР сразу во всей организации довольно сложно. Поэтому чаще всего применяется стратегия поэтапного внедрения. В этом случае область действия СУИР может охватывать только часть организации.

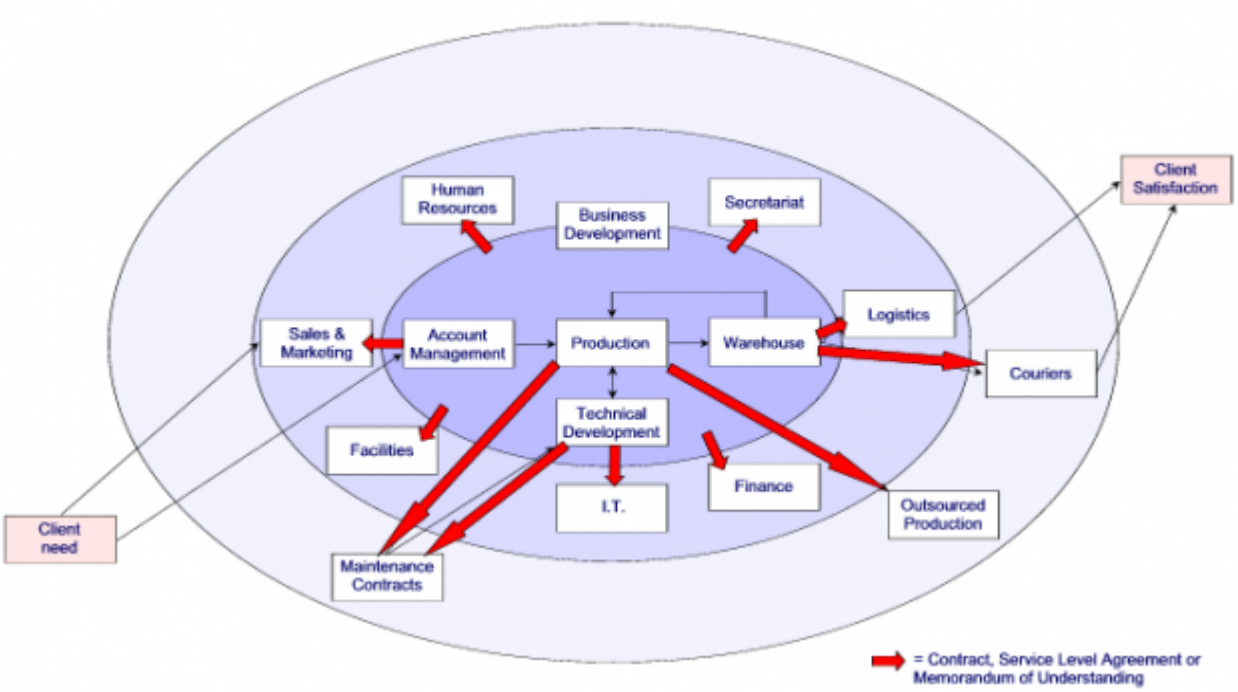
Область управления рисками определяется в тех же терминах, что и область действия СУИБ, а именно:

- бизнес-процессы;
- площадки;
- подразделения;
- сотрудники;
- приложения и сервисы;
- программно-аппаратные платформы;
- информационные активы.

Поводом для исключения из области действия определенных процессов, площадок, подразделений и других видов активов, помимо соображений поэтапного внедрения СУИР, может также служить децентрализованная структура организации, фактически имеющая несколько отдельных систем управления, требующих разных подходов к управлению рисками. Бизнес организации может быть диверсифицирован и включать в себя различные, не связанные друг с другом бизнес-процессы, каждый из которых требует особого подхода к управлению рисками. Организация может иметь также территориально распределенную структуру, включающую в себя офисы, филиалы, представительства или заводы в разных странах и в разных юрисдикциях. Для таких организаций одной СУИР может оказаться недостаточно.

Для определения границ управления рисками нужно описать интерфейсы организации и ее информационных систем с внешними системами, а также ее контракты с внешними сторонами, определив помимо контактной информации и способов связи, также процедуры взаимодействия, контрактные обязательства и другие вопросы, касающиеся любых внешних взаимодействий.

Область управления рисками, так же как и область действия СУИБ, может быть представлена схематично, например, как показано на рисунке.



На данной схеме внутренняя область включает в себя структурные подразделения организации в области действия СУИР. Эта область находится внутри более широкой области, включающей в себя все структурные подразделения организации. Эти подразделения (структурные единицы) непосредственным образом входят в зону контроля руководства организации. Внешняя область, помимо самой организации, включает в себя также внешние стороны, которые связаны с организацией договорными отношениями и от которых зависит ее деятельность.

Взаимодействие между подразделения в области действия СУИР регламентируется внутренними процедурами и регламентами; взаимодействие с внешними сторонами, не входящими в область действия СУИР, регламентируется договорами и соглашениями об уровне сервиса (SLA).

Для получения полной картины требуется несколько срезов, как минимум, по процессам, по организационной структуре и по информационным системам, а возможно, и по другим элементам области действия СУИР, включая информационные активы, сервисы и отдельных сотрудников.

Как можно более полное и точное определение области действия СУИР является крайне важным для управления рисками, как с

точки зрения идентификации и ограничения количества рассматриваемых рисков, так и с точки зрения передачи определенных рисков внешним сторонам, путем заключения с ними соответствующих договорных отношений, определяющих их ответственность за обеспечение информационной безопасности.