Банк России

ОПЕРАЦИОННЫЕ РИСКИ

2022 г.

Требования к управлению операционным риском в отношении торгово-клиринговой инфраструктуры (ТКИ)

Действующее регулирование

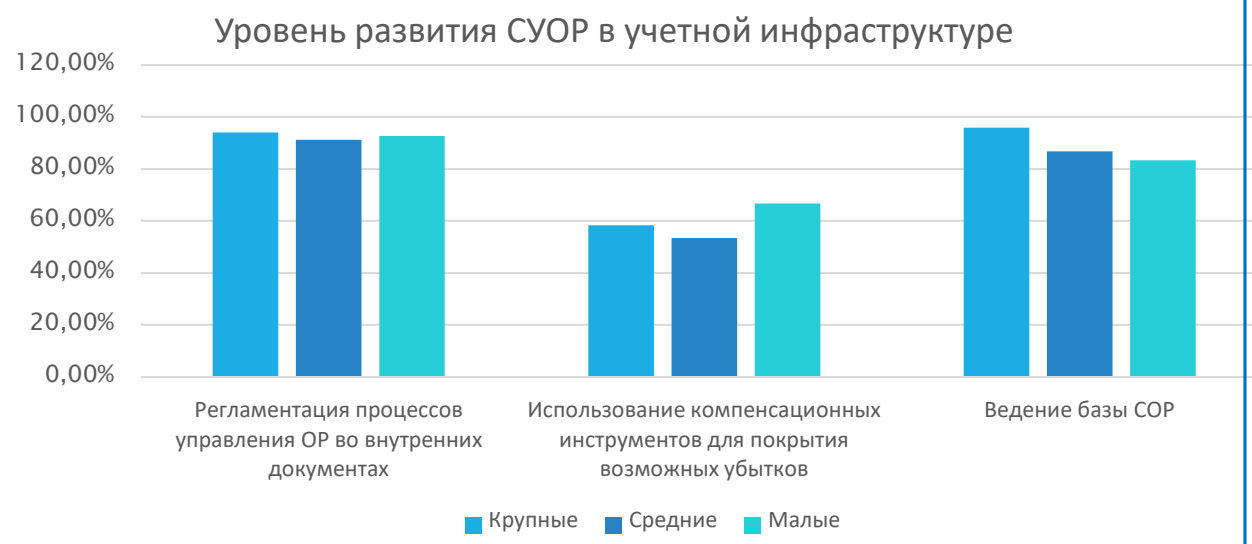
Организаторы торговли	4791-У
Клиринговые организации	463-П
Центральные контрагенты	575-П 4258-У
Центральный депозитарий	4905-У

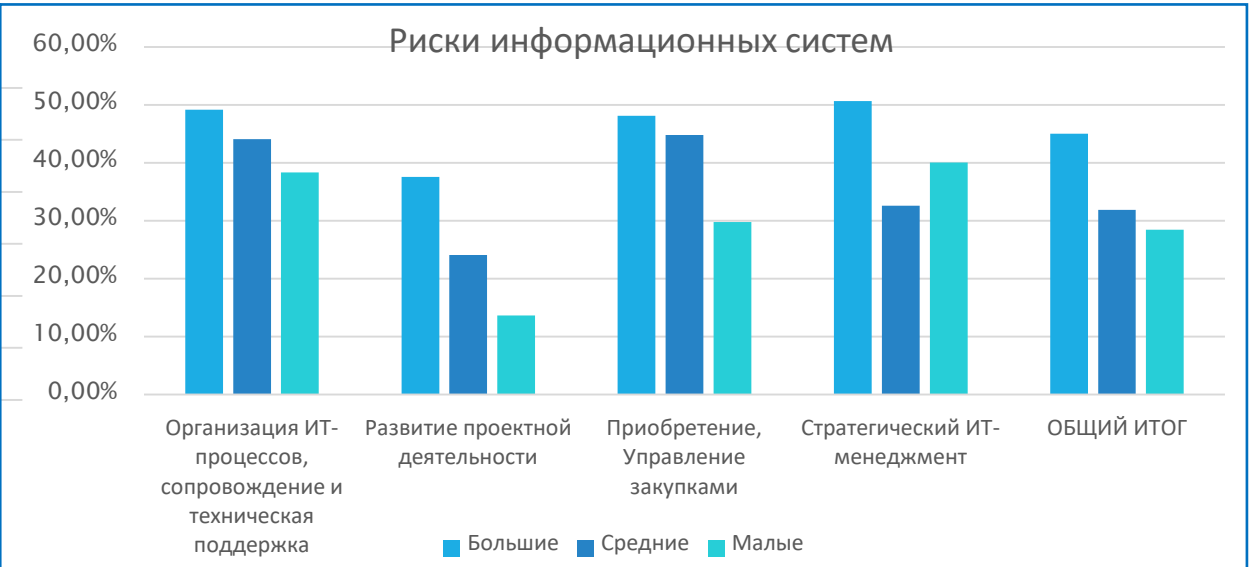
- Определение целевых показателей операционной надежности;
- Ведение базы событий ОР;
- Определение мер по защите информации, контроль прав доступа, аудит основных процессов эксплуатации систем;
- Выявление и контроль потенциальных источников ОР;
- Идентификация угроз работоспособности технических средств, определение требований к программно-техническим средствам (ПТС), проведение нагрузочного тестирования;
- Разработка, модификация и тестирование ПТС;
- Обеспечение непрерывности деятельности (наличие плана ОНиВД), определения перечня критически важных процессов (КВП), выявление чрезвычайных обстоятельств, способных привести к приостановлению КВП;
- Возобновление КВП **в течение 2 часов;**
- Функционирование резервного комплекса;
- Обслуживание основного и резервного комплекса как минимум двумя независимыми поставщиками телекоммуникационных услуг.

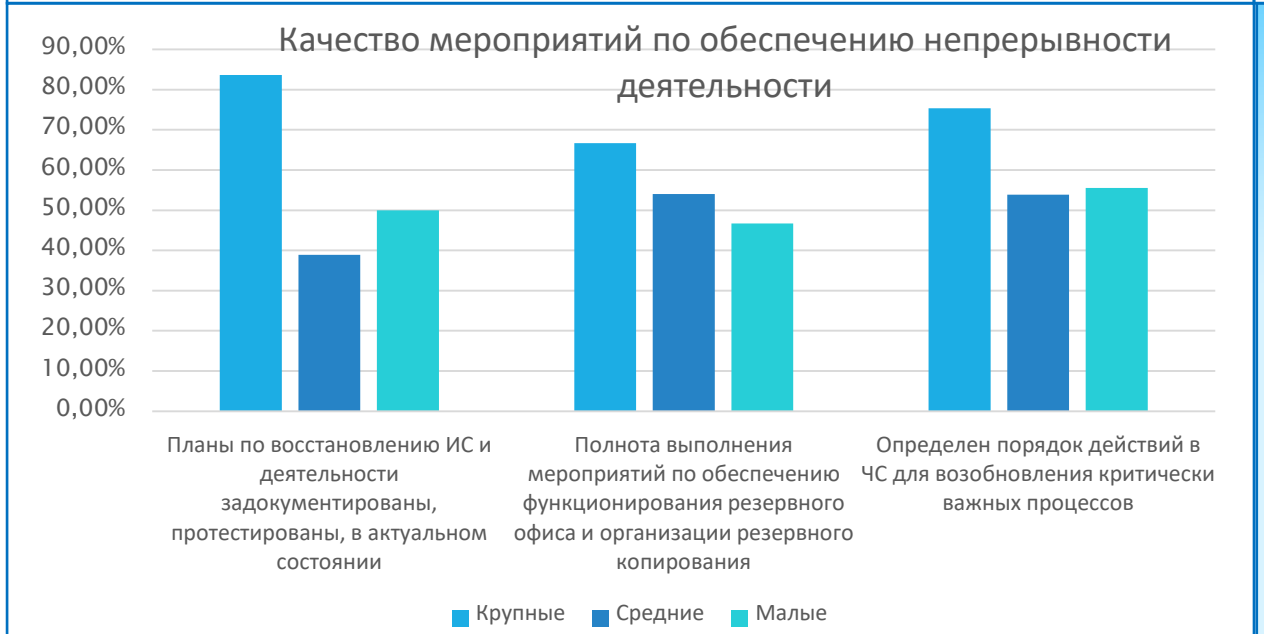
Планируемые нововведения

1. Единый понятий аппарат
2. Типовые процедуры управления операционным риском
3. Универсальный классификатор событий и видов операционного риска
4. Общие контрольные показатели уровня операционного риска
5. Единый подход к ведению Реестра рисков и Базы событий операционного риска

Организация УОР в учетной инфраструктуре (итоги самооценки 2021, 45 НФО)







ВЫВОДЫ

1. Организация СУОР в учетной инфраструктуре находится на достаточно высоком уровне (согласно самооценке в части регламентации и наличия базовых процессов около 90% респондентов ответили положительно).
2. В части обеспечения непрерывности ОУИ придерживаются рекомендаций Банка России (28-МР).
3. Чем крупнее организация, тем выше уровень зрелости ИТ-процессов и более качественно ведётся управление риском информ систем (РИС).
4. Подходы ОУИ к организации проектной деятельности, релизной политике, закупкам и ИТ-стратегии зависят от уровня автоматизации процессов, от масштабов деятельности, привлечения сторонних вендеров и от наличия связей с крупными финансовыми группами.
5. Формализация ИТ-процессов у средних и малых организаций учетной инфраструктуры находится на низком уровне.

Организация СУОР в части ИТ-систем. Выводы

Результаты проверок

Развитие проектной деятельности
(Характерно для большинства организаций):
- ✓ Отсутствует у большинства организаций
- ✓ 7 из 8 организаций используют ПО вендера

Организация непрерывности деятельности
(Характерно для большинства организаций):
- ✓ Мероприятия описаны во внутренних документах в различном объеме по причине отсутствия требований, закрепленных на уровне НА.
- ✓ Наиболее полно набор мероприятий описан в крупных организациях.

Риски информационных систем
(Характерно для крупных организаций):
- ✓ Риски в части ИТ выделяются, идентифицируются, в основном описаны.
- ✓ Выделяется отдельное должностное лицо, ответственное за ИТ риски.
- ✓ Разработана релизная политика.

Выводы

МЕТОДОЛОГИЯ разработана. Риски ИТ-систем чаще всего включаются в состав операционного риска.

ПРОЦЕДУРЫ:
1.Процедуры управления ИТ-рисками осуществляются в соответствии с внутренними документами
2. Все компании осуществляют ведение базы событий операционного риска
3.Комплекс мероприятий по управлению рисками ИТ-систем достаточен для поддержания устойчивого состояния компании

ОРГАНИЗАЦИОННАЯ СТРУКТУРА. Организация управления рисками ИТ-систем осуществляется должностным лицом по управлению рисками Общества.