Чек-лист внедрения модуля MCA

Что нужно решить и подготовить до и во время внедрения самооценки контролей. Шаги идут в порядке, в котором модуль ожидает данные: сначала роли и доступ, потом справочники, потом карточки и их активация.

---

1. Роли и доступ

☐ Назначить ИБ-администратора MCA (роль securityAdmin) — управляет ролями и учётными записями модуля.

☐ Назначить Создателей MCA (mcaCreator) — заводят процессы, риски, контроли и мониторинги.

☐ Назначить Проверяющих MCA (mcaChecker) — согласовывают карточки и изменения; получают рассылку о необходимости оценки адекватности.

Согласовать собственные изменения нельзя — система заблокирует такую попытку: автор изменения и проверяющий обязаны быть разными сотрудниками.

☐ Назначить Владельцев мониторинга (mcaMonitoringOwner) — вносят результаты мониторингов, за которые отвечают.

☐ Назначить Аудиторов MCA (mcaAuditor) — доступ на чтение по всем карточкам и справочникам, без права изменять или согласовывать.

2. Справочники и таксономии

☐ Проверить таксономию процессов — она наследуется из модуля СУОН (критические процессы), отдельно в MCA не вводится.

☐ Проверить таксономию рисков — общий справочник видов риска платформы.

☐ Проверить таксономию контролей — поставляется сидом на 86 записей (класс контроля → тип → подтип); при необходимости дополнить видами, которых нет в поставке.

☐ Проверить таксономию мониторингов — три вида: инспекция, повторное проведение, метрика.

3. Анкеты самооценки

☐ Заполнить анкету присущего риска (MCA_1) по каждому риску: вероятность и пять видов последствий (финансовые, регуляторные, репутационные, недобросовестное поведение, нарушение работы бизнеса).

Итоговый присущий риск считается автоматически — как самый жёсткий уровень из пяти последствий по матрице «потери × вероятность».

☐ Заполнить анкету адекватности контроля (MCA_2) по каждому контролю — восемь вопросов о дизайне контроля.

Ответ «Нет» на обязательный вопрос блокирует активацию контроля; ответ «Не применимо» требует текстового комментария.

☐ Заполнить анкету адекватности мониторинга (MCA_3) по каждому мониторингу — восемь вопросов о методологии.

4. Активация карточек

☐ Активировать мониторинги — обязательные поля: название, описание, частота, цель, уровень автоматизации, место процедуры, пороговое значение и его тип, покрытие, подтверждение выполнения, ответственный.

☐ Активировать контроли — только после того, как под контролем есть хотя бы один активный мониторинг.

☐ Активировать риски — только после того, как у риска есть хотя бы один активный контроль и заполнены присущий и остаточный риск.

5. Пороги контроля (настройка mca.config)

Параметр	Значение по умолчанию	Назначение
Период привязки события операционного риска, дней (sorPeriod)	90	Событие операционного риска, привязанное к контролю позже э
Порог общей суммы валовых потерь, руб (totalLoss)	300 000	Если сумма потерь по привязанным событиям операционного рис
Период подачи первичного результата, дней (firstResult)	60	Отображается на экране конфигурации; в расчёт эффективности
Срок внесения результатов, дней (resultSubmit)	20	Отображается на экране конфигурации; в расчёт эффективности

Решить, остаются ли значения по умолчанию или их нужно изменить под вашу организацию, до того как контроли начнут получать расчётные оценки эффективности.

6. Пересчёт и уведомления

☐ Убедиться, что после сохранения и согласования запускается автоматический пересчёт: результат мониторинга → эффективность контроля → уровень риска.

☐ Настроить время ежедневной проверки сроков оценки адекватности (по умолчанию — 08:00): в этот момент проверяющим уходит уведомление по всем контролям и мониторингам, у которых подошёл срок повторной проверки.

7. Согласование

☐ Проверить, что согласование изменений активных карточек работает как ожидается: изменение критичного поля не применяется сразу, а ждёт решения проверяющего.

☐ Проверить каскадное согласование на дереве: согласование процесса последовательно проходит по его рискам, контролям и мониторингам.