Чек-лист внедрения ISM

Что нужно решить до старта, какие роли завести и какие справочники подготовить — на реальных правилах и порогах продукта. Модуль ISM ведёт реестр недостатков (Issue), корректирующих планов (CAP) с вехами и оформленных исключений (Exception) с очередью согласования.

---

1. Роли, которые нужно назначить до старта

Продукт поставляется с готовым набором ролей — до запуска нужно решить, кто из сотрудников какую роль получит. Три роли отмечены в продукте как уникальные: их нельзя назначить одному сотруднику вместе с другими.

- **Владелец процесса (Quality Coordinator / IS Quality Coordinator).** — ведёт реестр Issue и CAP по своему направлению.
- **Senior ISO.** — обязательный согласующий для недостатков источников Information Security и Vulnerability Assessment — без него такой недостаток не проходит активацию.
- **Internal Audit.** — проводит независимую валидацию (IA Validation) перед закрытием недостатка или корректирующего плана.
- **Issue Source Editor, IS/VA Editor, ORM Editor, Regulatory Event Editor.** — заводят недостатки по своим источникам выявления.
- **Security admin (ИБ администратор).** — уникальная роль: единственная без доступа к самому реестру ISM — администрирует права, не ведёт недостатки.
- **Auditor, Security Auditor.** — уникальные роли независимого контроля; несовместимы с назначением других ролей тому же сотруднику.

2. Справочники, которые нужно подготовить

Права на редактирование выдаются на 30 справочников продукта. Часть из них стоит адаптировать под структуру вашей организации до начала работы — ниже основные:

- Источник выявления недостатка (иерархический справочник) и линия защиты (1/2/3/внешняя)
- Коренная причина, бизнес-процесс, тип недостатка
- Рейтинг существенности, рейтинг присущего и остаточного риска
- Уровень репутационного риска, уровень влияния на клиента, вероятность (Likelihood)
- Потенциальные финансовые и операционные потери
- Категория критичности ИТ-ресурса, реестр компенсирующих контролей
- Статусы и фазы CAP, статус вехи

3. Пороговые значения, уже заложенные в продукте

Эти значения не настраиваются на демонстрации «под впечатление» — они встроены в расчётные правила, которые ежедневно пересчитывают сроки и просрочки по Issue, CAP и Exception. Их стоит сверить с внутренним регламентом организации заранее:

- **Контрольные точки пересчёта.** — 14, 30, 45, 60 и 90 дней — интервалы, по которым считаются просрочки и счётчики обратного отсчёта.

- **Compensating CAP.** — если целевая дата CAP превышает дату активации Issue на 305 дней и более, продукт требует CAP типа Compensating.
- **Срок действия Exception.** — до 365 дней для исключений уровня 3–5, до 180 дней для уровня 1–2 — при продлении новая дата обязана укладываться в этот диапазон.
- **Отвязка Exception от Issue.** — при отлинковке плановая дата устранения Issue автоматически сдвигается на 45 дней от даты отлинковки.
- **Long Dated.** — полгода (180 дней) и два года (730 дней) — пороги признака долгосрочного недостатка.

4. Правила, которые стоит обсудить с командой до запуска

Часть правил жёстко зашита в продукт и не отключается настройками — их стоит объяснить будущим пользователям заранее, чтобы на первой неделе они не выглядели багом:

- **Разделение полномочий (Segregation of Duties).** — сотрудник, отправивший Issue или CAP на активацию, не может сам провести проверку качества данных (Data Quality Review) по этой же записи.
- **Severity Rating уровня 1.** — не может иметь сценарий «Принять риск» — только «Устранить».
- **Business Process для активации Issue.** — обязан быть 3-го уровня иерархии справочника или ниже.
- **Required approver-ISO.** — обязателен для активации недостатков источников Information Security и Vulnerability Assessment — без назначенного согласующего переход недоступен.
- **Закрытие Issue и CAP.** — проходит через проверку качества данных и (где требуется) независимую валидацию внутренним аудитом — минуя эти шаги закрыть запись нельзя.
