Чек-лист подготовки к внедрению

Supplier Analysis — управление рисками поставщиков и третьих лиц

Вопросы собраны от правил, уже встроенных в продукт: что он проверяет при создании записей, какие роли участвуют в согласовании и какие справочники загружаются при разворачивании модуля. Каждый пункт можно закрыть решением до начала работ — тогда первые третьи лица, поставщики и контроли заводятся без доработок на ходу.

1. Роли и согласование

- ☐ Назначен TPM-исполнитель и хотя бы один TPM-проверяющий — карточки третьих лиц, поставщиков и контролей заводит и согласовывает не один человек.

  Роли модуля с полным доступом ко всем объектам и 47 справочникам — security/Permissions.csv (role_id=3,4); RoleType.java:517-518

- ☐ Назначен ИБ-администратор — он управляет собственным контуром ролей, прав и аудита модуля через отдельную консоль /sasecurity, не пересекающуюся с общей схемой безопасности платформы.

  SaController.java:9-12; схема security_sa — 05-security.xml:8-142

- ☐ Для каждого вида контроля, которому нужна двойная проверка, определён второй проверяющий (checker2Role) — без него согласование останавливается на первом проверяющем автоматически, доработка не потребуется.

  hasChecker2 = !Strings.isBlank(controlKind.getChecker2Role()) — SaControlTransitionContext.java:5-17, ControlViewModel.java:129

- ☐ Назначены читатели с широким доступом для регуляторной отчётности (роли SA ICRM и Аудитор) — им не нужен доступ на изменение, только на просмотр по всем статусам.

  security/Roles.csv (role_id=5,8)

2. Третьи лица и поставщики

- ☐ Для каждого будущего контрагента заранее известны ИНН и, если применимо, КПП — модуль не даст завести дубль третьего лица с тем же ИНН и предупредит о дубле по КПП.

  ThirdPartyAddFormViewModel.java:60-78

- ☐ Понятно, что поставщик — это не контрагент сам по себе, а отношение «банк — третье лицо» по конкретной услуге: без привязанного третьего лица карточку поставщика создать нельзя.

  SupplierAddFormViewModel.java:51-57

- ☐ Собран состав атрибутов для первой партии поставщиков: тип и критичность отношения, аутсорсинг, ИТ-услуга, регион и страна, категория и подкатегория, доля процесса, признаки AML/SOX/Red Flag, использование четвёртых сторон.

  SaSupplier.java:12-91 (группы полей «отношения», «география и оргструктура», «признаки комплаенса», «четвёртые стороны»)

- ☐ Учтено, что новая карточка поставщика всегда получает статус «Новый» принудительно, а часть полей (15 расчётных индикаторов) обычным сохранением не перезаписывается — их обновляет только выделенный сервисный метод.

  SupplierAddFormViewModel.java:57; SaSupplierService.java:28-42,92-104

3. Контроли due diligence и мониторинга

- [ ] Понятна разница между двумя группами контролей: due diligence — предконтрактная проверка, ongoing monitoring — постконтрактный мониторинг. У каждой своя статусная модель.

  SaControlKindGroup.java:5-12

- [ ] Просмотрен справочник видов контроля (54 позиции с кодом методики, привязкой к виду риска и ролями maker/checker1/checker2) — понятно, какие виды контроля закрывают какой риск поставщика.

  ControlKind.csv — 54 строки, src/main/resources/db/suppliers/v1.0.0/csv/ControlKind.csv

- [ ] Для каждого вида контроля выбрана периодичность мониторинга из пяти доступных: ежегодно, раз в полгода, ежеквартально, ежемесячно, еженедельно.

  control_frequency.csv — 5 строк

- [ ] Учтено, что при переходе контроля или Gap в финальный статус фактическая дата завершения проставляется автоматически — вручную её вносить не нужно и незачем предусматривать это в регламенте.

  ControlViewModel.java:273-275; GapViewModel.java:166

4. Риски поставщика

- [ ] Просмотрен справочник из 13 видов риска: зависимость от субподрядчиков, существенность продукта/услуги, финансовое влияние, финансовые операции, риск мошенничества, геополитический риск, доступ к информации, соответствие нормативным требованиям, характер взаимодействия с клиентами, риск OSP, физический доступ и доступ к сетям, репутационное влияние, технологический риск.

  RiskKind.csv — 13 строк

- [ ] Определено, для каких видов риска у поставщика включается активный расчёт, а какие остаются неактивными — риск можно активировать и деактивировать точечно по каждому поставщику.

  SaSupplierRisk.isActive — SaSupplierRisk.java:12-22

5. Gap и связь с ISM

- [ ] Согласован порядок работы с Gap — несоответствием, которое выявляет контроль: кто назначает отдел и сотрудника, кто ставит плановую дату устранения.

  SaGap.java:11-24

- [ ] Понятно, что привязка и отвязка Issue и CAP модуля ISM к Gap протоколируется отдельным журналом операций (добавление/удаление) — история решений видна целиком, без ручных пометок.

  GapCapIssueListViewModel.java:62-133; SaGapItemsChangeLogService.java:29

6. Данные и согласие

- [ ] Согласован процесс получения согласия на обработку персональных данных контактных лиц поставщиков и третьих лиц — без отметки о согласии заявка с сайта не принимается.

  152-ФЗ «О персональных данных»; форма — legal/soglasie-na-obrabotku-personalnyh-dannyh.html

- [ ] Учтено, что пользовательский ввод в формах третьего лица, поставщика и Gap автоматически очищается от потенциально опасной разметки перед сохранением — дополнительная фильтрация на стороне регламента не нужна.

  ThirdPartyAddFormViewModel.java:47-52; GapViewModel.java:104-112

Отдельно от чек-листа — темы для разговора на демонстрации: поддерживаемые версии СУБД и браузеров, сроки и состав пилота, модель лицензирования, параметры поддержки. В срезе кода модуля этих данных нет, поэтому в чек-лист они не включены.