ЧЕК-ЛИСТ · 37 ПУНКТОВ

Готовность данных к внедрению

ISRA Ланселот: Оценка Риска Информационной Безопасности. Каждый пункт — правило, которое модуль применяет к данным. Пройдите список до пилота: он показывает, какие сведения придётся собрать и какие решения принять до первой загрузки.

Код правила справа от пункта — идентификатор из разбора исходного кода продукта. Пунктами без кода отмечены требования к организационной подготовке.

Оргструктура и бизнес-единицы

- [ ] Для каждого подразделения, которое войдёт в охват, определено, нужна ли ему собственная бизнес-единица: на одно подразделение может существовать только одна неархивная бизнес-единица. `BR-BU-01`
- [ ] Проверено, не покрыто ли подразделение бизнес-единицей вышестоящего уровня — иначе при заведении система предупредит о дублировании покрытия. `BR-BU-02`
- [ ] На каждую бизнес-единицу готовы четыре обязательных значения: наименование, подразделение оргструктуры, офицер ИБ, старший офицер ИБ. `BR-BU-04`
- [ ] Выгрузка оргструктуры получена в виде дерева: у каждого узла есть родитель, иначе обход вверх по иерархии работать не будет. `BR-BU-03`
- [ ] Учтено, что новый контроль бизнес-единицы нельзя создать, пока не завершён предыдущий. `BR-BU-05`

Информационные системы

- [ ] На каждую систему готовы наименование, тип и статус; для систем в статусе «Активно» определена бизнес-единица, к которой они относятся. `BR-APP-01`
- [ ] Решено, какие системы проверяются периодически: для одной системы не может быть двух одновременных контролей типа TimeTrigger. `BR-APPCTRL-01`
- [ ] Для проектных контролей есть идентификатор проекта и наименование проекта — без них проектный контроль не создаётся. `BR-APPCTRL-02`
- [ ] Определено, нужны ли дочерние контроли: они наследуют систему и тип родителя. `BR-APPCTRL-03`

Библиотека вопросов и анкеты

- [ ] Библиотека вопросов подготовлена с датами открытия и закрытия: активными считаются вопросы с незаполненной датой закрытия. `BR-QUEST-02`
- [ ] Проверено, что дата закрытия вопроса не раньше даты создания и не в прошлом. `BR-QUESTDIR-01`
- [ ] Вопросы разложены по областям влияния — от этого зависит, какой набор попадёт в анкету после одобрения проектной анкеты. `BR-QUEST-01`
- [ ] Определено, в каких случаях нужен полный набор вопросов: признак «весь TimeTrigger» разворачивает анкету целиком. `BR-QUEST-01`
- [ ] Согласовано, кто и на каком статусе правит анкету: ответы редактируются только в статусах «Заполнение» и «Шаблон (с дополнением)». `BR-QUEST-03`

Несоответствия и проблемы

- [ ] Принято, что отрицательный ответ в завершённой анкете становится кандидатом в несоответствие (NCI) автоматически. `BR-NCI-01`
- [ ] Определён владелец разбора NCI: по умолчанию новый NCI получает статус «Необработан». `BR-NCI-02`
- [ ] Учтено ограничение: в одной проблеме нельзя смешивать анкетные NCI и ручные дефициты, а один NCI нельзя связать с двумя проблемами. `BR-NCI-03`
- [ ] Согласовано, откуда берётся признак закрытия проблемы: внутренний статус «Завершено» либо внешний статус closed / cancelled. `BR-ISSUE-01`
- [ ] Готовы регламентные формулировки обоснования: если итоговая вероятность отличается от расчётной, обоснование обязательно. `BR-ISSUE-02`

Оценка риска

- [ ] Шкалы влияния и вероятности сопоставлены с весами продукта: влияние High=5, Medium=3, Low=1; вероятность Very High=1,0, High=0,9, Medium=0,3, Low=0,1. `BR-RISK-01`
- [ ] Принято, что по каждой оси берётся максимум из четырёх факторов влияния, а присущий риск — произведение этого максимума на вес итоговой вероятности. `BR-RISK-02`
- [ ] Пороги рейтинга согласованы с методикой организации: от 1,5 — High, выше 0,49 — Medium, иначе Low. `BR-RISK-04`
- [ ] Пороги уровня критичности согласованы: сумма остаточных рисков трёх осей до 0,9 — Level 5, меньше 3,0 — Level 4, до 9,0 — Level 3, до 15,0 — Level 2, выше — Level 1. `BR-RISK-05`
- [ ] Определено, что итоговая вероятность оценки берётся как максимальная среди связанных проблем. `BR-RISK-03`
- [ ] Учтено, что оценку нельзя создать без выбранной проблемы и заполненных факторов влияния, а ручная корректировка требует обоснования. `BR-RISK-08`
- [ ] Три параметра расчёта вероятности угрозы заполняются в организации: источник угрозы, требуемый доступ, уровень подготовленности нарушителя. `BR-THREAT-01`
- [ ] Учтено, что значения вероятности и влияния принимаются на двух языках — русском и английском. `BR-RISK-07`

Классификатор ИТ-риска приложения

- [ ] Для каждой системы известны класс информации и категория персональных данных — от них зависит рейтинг конфиденциальности. `BR-ITRC-01`
- [ ] Собраны признаки целостности: финансовая отчётность, надзорные требования, высокий финансовый риск, массовый доступ, доступ к критичным функциям, мониторинг критичной информации. `BR-ITRC-02`
- [ ] Определена бизнес-критичность каждой системы — вместе с надзорным признаком она задаёт рейтинг доступности по справочной матрице. `BR-ITRC-03`
- [ ] Учтено, что сводный рейтинг не считается, пока не заполнены все три оси: конфиденциальность, целостность, доступность. `BR-ITRC-04`
- [ ] Согласован порядок ручного переопределения: обоснование обязательно, при возврате на доработку обязателен комментарий. `BR-ITRC-06`

Документы, роли и аудит

- [ ] Для сопроводительных документов есть наименование и ссылка, а объект сохраняется до того, как к нему добавляют документ. `BR-DOC-01`
- [ ] Составлен перечень ролей и того, что каждой роли можно читать, писать, добавлять, удалять и выполнять: права выдаются роли на пару «объект безопасности — тип объекта». –
- [ ] Определено, кто инициирует, а кто подтверждает переходы статусов: подтверждать переход не может тот же сотрудник, который его начал. –
- [ ] Выбран механизм аутентификации из поддерживаемых ядром: LDAP, Kerberos+LDAP, SSO, SAML, база данных или файл пользователей. –
- [ ] Назначен получатель журнала безопасности и истории согласований — перечень действий по контролю фиксируется целиком. –

Чего в этом списке нет намеренно

Сроков, трудозатрат и стоимости: они зависят от числа подразделений и систем в охвате, состояния оргструктуры и готовности библиотеки вопросов. Оценку по вашим цифрам считает калькулятор на странице контактов.

ООО «Ланселот-ИТ» · РФ, г. Москва, ул. Профсоюзная 45 · +7 (499) 380-74-23 · info@lancelot-it.ru
ОГРН 1145022003070 · ИНН 5022045340 · КПП 502201001