Утверждено приказом Генерального директора

ЗАО «Центральный депозитарий» № 78 от «18» сентября 2026 г.

Техническое задание на проведение IT-аудита ЗАО «Центральный депозитарий»

1. Общие положения

Заказчик: ЗАО «Центральный депозитарий».

Основание: Приказ Генерального директора № 74 от «09» сентября 2026 г.

Цель аудита: получить независимую оценку того, насколько информационные системы, IT-процессы и защита информации депозитария надежны, безопасны и соответствуют требованиям законодательства КР и признанным стандартам.

Задачи аудита:

1. Оценить состояние IT-инфраструктуры и информационных систем, которые обеспечивают учет прав на ценные бумаги.
2. Проверить защищенность информации, включая данные депонентов и персональные данные.
3. Оценить готовность к сбоям: резервное копирование, восстановление, непрерывность деятельности.
4. Проверить соответствие внутренних документов и фактической практики требованиям законодательства и стандартов.
5. Выявить риски и слабые места и дать практические рекомендации по их устранению с указанием приоритета.

2. Объект и область аудита

Проверяемый период: последние 12 месяцев.

Место проведения: офис Заказчика.

В область аудита входят:

Объект	Что именно проверяется
Депозитарная учетная система	Ведение счетов депо, учет прав на ценные бумаги, операции, сверки, отчеты
Связь с внешними участниками	Обмен данными с фондовой биржей, расчетным банком, брокерами, реестродержателями, регулятором
Клиентские сервисы	Личный кабинет депонентов, порталы и интерфейсы для участников
IT-инфраструктура	Серверы, сети, СУБД, рабочие места, облачные сервисы, ЦОД и резервная площадка

Объект	Что именно проверяется
Процессы IT	Управление доступом, изменениями, инцидентами, резервным копированием, подрядчиками
Информационная безопасность	Политики, средства защиты, мониторинг, защита персональных данных
Непрерывность деятельности	План обеспечения непрерывности (BCP) и план восстановления (DRP), их тестирование

3. Вопросы для проверки

Аудитор проверяет каждое направление: есть ли документ, выполняется ли он на практике, работают ли контроли.

3.1. Управление IT и информационной безопасностью

- Есть ли утвержденная IT-стратегия, политика ИБ и распределение ответственности (кто отвечает за IT, кто за ИБ)
- Независима ли служба ИБ от IT-подразделения
- Как оцениваются и учитываются IT-риски, есть ли реестр рисков
- Как руководство получает отчеты по IT и ИБ

3.2. Депозитарная учетная система

- Готовность системы обслуживать сектор ГЦБ и корп бумаг
- Соответствие системы текущим задачам
- Полнота и точность учета: сверка остатков по счетам депо с реестродержателями и расчетной организацией
- Контроль целостности данных: невозможность изменить записи без следа
- Журналы операций (audit trail): что пишется, как долго хранится, кто может изменить
- Разделение полномочий: ввод, контроль и подтверждение операций разными сотрудниками
- Корректность отчетов для депонентов и регулятора

3.3. Управление доступом

- Порядок выдачи, изменения и отзыва прав (в том числе при увольнении)
- Принцип минимальных прав, периодический пересмотр доступов
- Контроль привилегированных учетных записей (администраторы, DBA)
- Парольная политика и многофакторная аутентификация, особенно для удаленного доступа

3.4. Защита информации и сети

- Сегментация сети, межсетевые экраны, защита периметра
- Антивирусная защита, обновления ОС и ПО, управление уязвимостями
- Шифрование данных при передаче и хранении
- Мониторинг событий безопасности, сбор и анализ логов
- Защита персональных данных депонентов

3.5. Изменения и разработка

- Порядок внесения изменений в ПО и инфраструктуру: заявка, тест, согласование, внедрение
- Разделение сред разработки, тестирования и рабочей среды
- Контроль исходного кода и версий

3.6. Эксплуатация и инциденты

- Регистрация и разбор инцидентов, сроки реакции
- Порядок уведомления руководства и регулятора об инцидентах
- Мониторинг доступности систем

3.7. Резервное копирование и непрерывность

- Регламент резервного копирования, хранение копий вне основной площадки
- Регулярные тесты восстановления из копий
- Наличие BCP и DRP, целевые сроки восстановления (RTO) и допустимая потеря данных (RPO)
- Когда и как проводилось последнее тестирование переключения на резервную площадку

3.8. Подрядчики и внешние сервисы

- Договоры с поставщиками ПО, хостинга и облачных сервисов: требования к безопасности и конфиденциальности
- Контроль доступа подрядчиков к системам
- Зависимость от одного поставщика и план на случай его отказа

3.9. Персонал

- Обучение сотрудников по ИБ, подписание обязательств о неразглашении
- Проверка осведомленности (например, учебная фишинговая рассылка)

4. Нормативная база и стандарты

Аудит проводится на соответствие законодательству КР и международным стандартам.

Законодательство КР:

- Закон КР «О рынке ценных бумаг»
- Закон КР «Об информации персонального характера»

- Нормативные правовые акты уполномоченного государственного органа по регулированию рынка ценных бумаг о депозитарной деятельности, информационной безопасности и управлении рисками
- Внутренние документы Заказчика: политика ИБ, регламенты IT, BCP/DRP, правила ведения депозитарного учета

Международные стандарты и практики:

- ISO/IEC 27001:2022 и ISO/IEC 27002:2022 - управление информационной безопасностью
- COBIT 2019 - управление и контроль IT
- ISO 22301:2019 - непрерывность деятельности
- Принципы для инфраструктур финансового рынка CPMI-IOSCO (PFMI), в первую очередь Принцип 17 «Операционный риск», и Руководство CPMI-IOSCO по киберустойчивости
- NIST Cybersecurity Framework 2.0 - как дополнительный ориентир

5. Требования к аудитору

- Опыт IT-аудита или аудита ИБ в финансовых организациях не менее 3 лет, желательно - в депозитариях, биржах, банках или брокерских компаниях
- Не менее 2 завершенных проектов IT-аудита в финансовом секторе за последние 3 года (с отзывами или рекомендациями)
- В команде есть специалисты с сертификатами CISA, CISSP, CISM или ISO/IEC 27001 Lead Auditor
- Независимость: Аудитор не оказывал Заказчику услуги по внедрению или сопровождению проверяемых систем за последние 2 года и не связан с поставщиками этих систем
- Готовность подписать соглашение о конфиденциальности (NDA) до начала работ
- Работа на русском языке, отчет на русском языке (при необходимости - дополнительно на английском)

6. Порядок проведения и сроки

Общий срок аудита - [3-6] недель с даты подписания договора.

Этап	Что делается	Срок	Результат
1. Подготовка	Установочная встреча, запрос документов, согласование плана и графика	1-2 недели	Утвержденный план аудита
2. Сбор и анализ	Изучение документов, интервью, изучение	1-2 недель	Рабочие материалы

Этап	Что делается	Срок	Результат
	депозитарной системы, осмотр ЦОД, проверка настроек, выборочное тестирование контролей		
3. Проект отчета	Обсуждение предварительных выводов с Заказчиком	1-2 недели	Проект отчета
4. Итоговый отчет	Учет комментариев Заказчика, презентация руководству	1 неделя	Итоговый отчет, акт приемки

Заказчик обязуется:

- Назначить ответственное лицо для взаимодействия с Аудитором
- Предоставить документы и доступ к системам в согласованные сроки (только на чтение, если иное не согласовано)
- Обеспечить участие сотрудников в интервью

Аудитор обязуется:

- Не вносить изменений в рабочие системы и данные Заказчика
- Проводить активные проверки
- Сразу сообщать Заказчику о критических уязвимостях, не дожидаясь итогового отчета
- Хранить полученную информацию в тайне и вернуть или уничтожить ее после завершения работ с подтверждением в письменной форме
- Не передавать информацию третьим лицам и не привлекать субподрядчиков без согласия Заказчика

7. Результаты аудита и приемка

Итоговый отчет должен содержать:

1. Краткое резюме для руководства (2-3 страницы): общая оценка, главные риски, что сделать в первую очередь.
2. Описание объема, методики и проверенных материалов.
3. Выводы по каждому направлению из раздела 3.

4. Перечень замечаний. По каждому: суть, риск для депозитария, уровень критичности (высокий / средний / низкий), ссылка на требование, рекомендация.
5. План устранения замечаний с рекомендуемыми сроками.

Форма передачи: на бумаге с подписью и печатью Аудитора в [2] экземплярах и в электронном виде (PDF). Файлы с описанием уязвимостей передаются в защищенном виде.

Приемка: Заказчик рассматривает проект отчета в течение [10] рабочих дней и направляет замечания. Работы считаются выполненными после подписания акта приемки итогового отчета.

Дополнительно: по запросу Заказчика Аудитор проводит повторную проверку устранения критических замечаний