ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на проведение аудита ИТ-инфраструктуры включая информационные системы Агентства по защите депозитов Кыргызской Республики

Бишкек 2023 г.

Информационная безопасность и программно-технологическое обеспечение.

Цели и задачи Агентства в области информационных технологий направлены на его инновационное развитие для совершенствования всех направлений деятельности в части безопасности, сохранности и дальнейшего развития программно-технологического обеспечения.

В Агентстве структура архитектуры IT состоит из комплекса технических средств (КТС), специального и пользовательского программного обеспечения, интернета, электронной почты, сети передачи данных (СКС), Система электронного документооборота «Infodocs» (далее – СЭД).

I. Состав комплекса технических средств:

1. Сервер Агентства:
   - Сервер приложений;
   - Сервер баз данных;
   - Виртуализация серверных оборудований
   - Сетевые оборудования
   - Источники бесперебойного питания.
2. Персональные компьютеры (ПК):
   - Стационарные пользовательские ПК – 19 единиц;
   - Переносные ПК – ноутбуки - 8 единиц.
3. Аппаратно-программное оборудование (маршрутизатор cisco) для организации обмена информацией Агентства с Национальным банком;
   - Периферийное офисное оборудование: принтеры, сканеры.

II. Программное обеспечение

1. На виртуальном сервере приложений установлена Программное обеспечение «Информационно-аналитическая система по процессу выплаты компенсаций по вкладам» (далее - ИАС).
2. На персональных компьютерах сотрудников Агентства ПК установлены операционные системы Windows 7,10, офисные приложения (Word, Excel и т. д.).
3. Бухгалтерский учёт и отчётность финансово-хозяйственной деятельности Агентства осуществляются средствами программного продукта 1С_8.3. Информационная база данных хранится на сервере Агентства, доступ к базе данных осуществляется только регламентированным сотрудником по ключу доступа. Предусмотрено сопровождение программного продукта 1С_8.3, которое осуществляется разработчиком.
4. Для работы на рынке НБКР с ценными бумагами в онлайн режиме по каналам связи используется аппаратно-программный маршрутизатор (cisco).
5. Система электронного документооборота «Infodocs» представляет собой информационную систему, предназначенную для автоматизации документооборота в государственных органах по переводу документов в электронный формат.

III. Информационное взаимодействие и обмен данными

1. Обмен данными и доступ к данным на сервере осуществляется по проводной локальной сети. Доступ к Интернет, эл. почте сотрудников Агентства – по проводной и беспроводной (Wi-Fi) локальной сети.

2. Доступ к базе данных программного комплекса 1С_8.3 разрешен только регламентированным пользователям.
3. Взаимодействие Агентства с НБКР производится по выделенному каналу связи.

IV. Безопасность и защита информации

1. Защита от вирусных заражений обеспечивается антивирусной программой, обновление антивирусной базы осуществляется в автоматическом режиме.
2. В целях предотвращения несанкционированного доступа к пользовательским данным каждому пользователю присвоено уникальное имя (Login) и пароль, на сервере защита данных осуществляется средствами и политиками безопасности сервера (Active Directory).
3. Защита данных и персональных компьютеров при несанкционированных отключениях электричества приобретено для каждого персонального компьютера источники бесперебойного питания.

Программное обеспечение «Информационно-аналитическая система по процессу выплаты компенсаций по вкладам» (ИАС), для автоматизации бизнес-процессов АЗД по:

- сбору отчетности от коммерческих банков и расчету обязательных взносов, штрафов и пени;
- выплате гарантированных сумм вкладчикам банков-банкротов (при наступлении гарантийного случая);
- формированию архива электронных документов по принятым решениям АЗД, в том числе для хранения истории работы с банком агентом.

ИАС не охватывает административно-хозяйствующие операции, такие как расчет заработной платы, кадровый учет, бюджетирование, учет размещения денежных средств ФЗД в ГЦБ и др.

Для бухгалтерского учёта и отчётности внутрихозяйственной деятельности Агентства эксплуатируется имеющийся программный продукт на платформе 1С.

Агентство считает необходимым проведение независимой аудиторской компанией аудита текущего состояния информационной системы Агентства, системы защиты информации и оценки уязвимости информационно-аналитической системы, включая все программно - аппаратные средства Агентства.

Цель аудита:

Оценка зрелости ИТ процессов, эффективности использования информационных технологий, уровня обеспечения информационной безопасности (ИБ) и непрерывности, а также соответствие лучшим мировым практикам таким как COBIT 2019, ISO/IEC 20000-1:2018, ISO/IEC 27001:2022 и ISO 22301:2019.

В связи с вышеуказанным перед внешним IT аудитом ставятся следующие задачи:

• Анализ внутренних нормативных документов по обеспечению информационной безопасности на предмет их достаточности и соответствия требованиям законодательства Кыргызской Республики;

• Изучение стратегических документов Агентства, стратегию развития, политики и процедуры по управлению рисками информационных систем в целях оценки их адекватности, достаточности и актуальности с учетом международных стандартов и лучших практик ИТ и ИБ;

• Оценить существующие ИТ процессы и определить их соответствие требованиям лучших мировых практик COBIT 2019.

• Оценка систем управления качеством ИТ-процессов и систему управления операционными рисками;

• Оценка системы обеспечения непрерывности деятельности информационных систем и планов восстановления информационных систем в случае чрезвычайных ситуаций в соответствии с международными стандартами по управлению непрерывностью деятельности (ISO 22301:2019);

• Проверить соответствие системы управления информационной безопасностью требованиям стандарта ISO/IEC 27001:2022.

• Анализ возможностей серверного и сетевого оборудования на соответствие масштабам Агентства, объему проводимых операций;

• Оценка уровня обеспечения безопасности сети, операционных систем, приложений и баз данных, персонала и физической безопасности (проведение тестирования на проникновение и анализ уязвимостей информационной инфраструктуры);

• Рассмотрение степени защищенности информационных систем от воздействия внешних и внутренних факторов;

• Оценка системы управления доступом и распределения ролей в автоматизированной системе;

• Оценка уровня осведомленности персонала Агентства в области информационной безопасности;

• Оценка квалификации сотрудников Службы по информационным технологиям;

• Рассмотрение вопросов соблюдения требований законодательства в отношении прав интеллектуальной собственности и использования лицензионных программных продуктов.

• Оценка используемых программных обеспечений в Агентстве и определить меры для их оптимизации;

• Оценка процесса идентификации и категоризации информационных активов, включая их степень защиты;

• Оценка качества ИТ контролей и оценку контрольных механизмов внесения изменений в информационную систему Агентства и процесс администрирования;

• Оценка текущего уровня защищенности информационных систем, анализ рисков и выявить возможные уязвимости, проблемы в системе защиты информации;

• Оценка соответствия требованиям по эксплуатации информационных систем;

• Анализ эффективности дизайна и уровня автоматизации средств внутреннего контроля, в том числе общих компьютерных контролей над процессами поддержки пользователей, внесения изменений;

• Анализ эффективности ИТ структуры Агентства;

• Анализ управления следующими ИТ процессами:

a) Управление событиями информационной безопасности;
b) Управление уязвимостями;
c) Управление инцидентами информационной безопасности;
d) Безопасность персонала.

• Оценка ИАС Агентства:

– выявление критичных мест архитектуры;
– рассмотрение механизма аутентификации и разграничения прав доступа;
– анализ программных средств (ОС, СУБД и т.д.);
– оценка уровня автоматизации бизнес-процессов;
– оценка контроля работоспособности (функционирования, эффективности) реализованных в ИАС защитных мер;

Планируемые действия:

– Проведение аудита всех ИТ процессов организации, включая процессы управления ИТ, разработки и поддержки систем, обеспечения ИБ и непрерывности.
– Изучение документов, связанных с ИТ, включая политики и процедуры, утвержденные руководителем организации.

– Проведение интервью с сотрудниками, ответственными за ИТ процессы и ИБ.
– Проверка действующих систем и средств обеспечения ИБ, их настройки и состояние.
– Анализ результатов тестирования на проникновение и оценка результатов.
– Сравнение текущей системы ИБ с требованиями стандартов ISO/IEC.

Результаты аудита должны быть предоставлены в следующем виде:

• Отчет о текущем состоянии ИТ Агентства, с предоставлением списка уязвимостей согласно международных классификаций;

Отчет должен содержать подробную и достоверную информацию о состоянии ИТ в процессах и инфраструктуре с применением аналитических инструментов.

• Заключение об уровне зрелости информационных систем в плане дизайна, архитектуры, конструктивных решений и оптимального использования ресурсов (лицензирование, программное обеспечение, в том числе ИАС, компьютерное оборудование);

• Заключение о эффективности процессов управления рисками и планирования инвестиций в ИТ Агентства и предложения по оптимизации процессов.

• Рекомендации по оптимизации и повышению эффективности ИТ и ИБ.

Отчет должен основываться как минимум на следующих стандартах и методологиях:

- ISO/IEC 27001;
- ISO 22031;
- COBIT 2019;
- ITIL;
- Требования по обеспечению информационной безопасности в КР.

Требования к аудиторской организации

- аудиторская компания должна иметь признанную в Кыргызской Республике международную репутацию, имеющий сертификат о международном признании не менее пяти последних лет в Кыргызской Республике, необходимо подать конкурсную заявку с приложением копий сертификатов или свидетельства о международном признании не менее пяти последних лет;
- иметь опыт проведения ИТ аудита финансово-кредитных учреждений в соответствии с международными стандартами ИТ аудита (COBIT, ITIL, ISO 2000*, ISO 22301) **не менее трех лет**.
- иметь не менее трех отчетов по ИТ аудиту финансово-кредитных учреждений КР.

Требования к руководителю проектной команды:

- должен обладать квалификационными международными сертификатами в области ИТ аудита и информационной безопасности (CISA (Certified Information System Auditor), CISM (Certified Information Security Manager), Lead auditor of information Security Management Systems ISO/TEC 27001:2013);
- иметь стаж проведения ИТ-аудитов финансово-кредитных организаций **не менее трех лет.**

Общие требования к проектной команде:

- иметь не менее одного аудитора обладающими сертификатами CISA (Certified Information System Auditor)

Участник конкурса должен предоставить свидетельства (доказательства) наличия условий, отмеченных в Требованиях данного раздела, а также:

а) список финансово-кредитных учреждений и других организаций, внешний ИТ аудит которых осуществляла аудиторская организация за последние **три года**;

б) предложения, включающие планируемый масштаб аудиторской проверки, период и ИТ области, которые будут изучены в ходе аудиторской проверки, план и график проведения внешнего ИТ аудита Агентства, а также отчеты, которые планируется подготовить.

в) состав команды аудиторов, с указанием руководителя, наличие сертификатов членов команды, опыта их работы в подобных проектах, степень участия и направление работы в данном проекте. Заявленные лица должны непосредственно (физически) участвовать в процессе аудиторской проверки (т.е. удаленный/дистанционный аудит не допускается).

г) стоимость услуг по аудиту информационных технологий, должна указываться с выделением предусмотренных налогов. Оплата производиться по факту оказанных услуг и подписания акта.

Сроки предоставления отчетов и услуг:

Предоставление аудиторского заключения по результатам работ не более 1 месяца после начала процедур по аудиту.

Стоимость услуг и условия оплаты услуг:

1. Стоимость услуг должна быть выражена только в сомах Кыргызской Республики и не должна превышать сумму указанную в конкурсе включая налоги и другие расходы.
2. Оплата производится в течение 10 рабочих дней после предоставления аудиторского заключения.

Результаты выполненных работ принимаются Заказчиком с подписанием Акта сдачи-приемки работ.

Исполнитель обязуется представить результаты отчета на заседание Совета директоров Агентства.

Конфиденциальность

Условия и предмет заключённого договора являются конфиденциальной информацией во взаимоотношениях между Аудитором и Заказчиком, при этом Аудитор должен быть полностью независим от своего клиента, а также от любой третьей заинтересованной стороны. Аудитор не будет, без предварительного письменного согласия Заказчика, а также в случаях, предусмотренных законодательством Кыргызкой Республики, разглашать какую-либо информацию, являющуюся собственностью или представляющую собой конфиденциальные данные и относящуюся к аудиту.

Заместитель исполнительного директора **Н. Байбосунов**

Главный аудитор СВА **Е. Токтабеков**

Риск менеджер **А. Бейшеналы**

Системный администратор **Б. Рыскелдиев**

Администратор по ИТ **М. Омуралиев**