Техническое задание

на проект

Проведение работ по разработке и подготовке к сертификации системы управления информационной безопасностью, соответствующей требованиям ISO/IEC 27001:2022 для Акционерного коммерческого банка «Банк развития бизнеса»

Ташкент – 2025 год

1. ТРЕБОВАНИЯ К УСЛУГАМ

1.1. Полное наименование предмета работ

Разработка и подготовка к сертификации системы управления информационной безопасностью (СУИБ), соответствующей требованиям международного стандарта ISO/IEC 27001:2022, для **Заказчика**

1.2. Границы проведения работ

В границы работ должен входят головной офис Банка: адрес и кол-во сотрудников
Язык подготовки документации проекта – русский. Работы проводятся удаленно.

1.3. Перечень документов, на основании которых должны быть оказаны услуги

Предлагаемые работы по разработке и подготовке к сертификации системы управления информационной безопасностью, соответствующей требованиям ISO/IEC 27001:2022 должны выполняться в соответствии со следующей нормативной документацией:

- ISO/IEC 27001:2022

2. Требования к Исполнителю

2.1. Исполнитель должен иметь опыт работы на рынке услуг информационной безопасности не менее 10 (десяти) лет.

2.2. Исполнитель должен иметь в штате не менее 10 сотрудников, имеющих высшее образование в области защиты информации.

2.3. В команде Исполнителя должны быть специалисты, обладающие следующими сертификатами:

- не менее **1 CISSP**
- не менее **1 CISA**;
- не менее **1 CISM**;
- не менее **1 BSI ISO/IEC 27001 Lead Auditor**;
- не менее **5 ISO/IEC 27001 Lead Implementer**;
- не менее **3 Certified Ethical Hacker (CEH)**;
- не менее **1 PCI Secure SLC или Secure Software Assessor**.

3. Этапы проведения работ по разработке и подготовке к сертификации системы управления информационной безопасностью, соответствующей требованиям ISO/IEC 27001:2022

3.1. Обследование текущего состояния ИБ и определение границ области действия СУИБ

3.1.1. Анализ бизнес-процессов и выбор области действия СУИБ

Целью данного этапа является определение области действия СУИБ.

На данном этапе проводятся следующие работы:

- анализ организационной структуры компании;
- проведение интервью руководства Заказчика;
- выявление критичных бизнес-процессов и целевой информации;
- определение подразделений, участвующих в критичных бизнес-процессах;
- определение основных активов (ИС, информация, ключевые сотрудники), используемых в рамках критичных бизнес-процессов;
- формирование предложения по возможной области действия СУИБ (далее - ОД СУИБ) с указанием обоснования выбора ОД СУИБ,
- разработка и согласование документа «Область действия СУИБ», соответствующего требованиям ISO/IEC 27001:2022;

- утверждение документа «Область действия СУИБ» Заказчиком.

Результатом этапа является документ «Область действия СУИБ».

3.1.2. Обследование на соответствие требованиям ISO/IEC 27001:2022

Целью данного этапа должно являться получение актуальной и достоверной информации об архитектуре создаваемого процессингового центра, потоках данных платежных карт, текущем уровне обеспечения информационной безопасности, планов по развитию и модернизации процессинга, а также другой информации, необходимой для оценки соответствия требованиям Стандарта PCI DSS и разработки Плана мероприятий с рекомендациями по подготовке к успешному сертификационному аудиту.

При выполнении данных работ Исполнителем должен производиться сбор следующих сведений:

- об организационной структуре;
- о структуре комплекса используемых программно-технических средств;
- о топологии сети и применяемых методах сегментации (в т.ч. характеристики используемых каналов и точек подключения к сетям связи и сети Интернет, беспроводные точки доступа);
- о процедурах обеспечения безопасности в локальной сети;
- о механизмах защиты данных платежных карт;
- о процедурах управления уязвимостями;
- о реализации системы управления доступом;
- о процедурах мониторинга и контроля доступа (на уровне сети и приложений);
- о политике информационной безопасности.

Сбор всех необходимых сведений Исполнителем должен производиться путем изучения предоставленной Заказчиком документации, проведения интервью с персоналом Заказчика, анализа конфигурационных файлов программных и программно-технических системных компонентов, демонстрирования сотрудниками Заказчика выполняемых ими процедур.

3.2. Проведение анализа и оценки рисков ИБ

Целью этапа является идентификация информационных рисков Заказчика в рамках ОД СУИБ, реализация которых может нанести ощутимый ущерб, выработка мероприятий по их обработке. Данный этап подразумевает проведение следующих работ:

- разработка (или корректировка существующей) методики анализа рисков ИБ, учитывающей специфику бизнес-процессов Заказчика, и требования стандартов ISO/IEC 27001:2022, ISO/IEC 31000;
- выбор критериев принятия рисков, включая порядок определения приемлемого уровня риска;
- оценка потенциального ущерба для бизнеса, который возможен в результате нарушения безопасности информационных активов;
- оценка потенциальной возможности нарушения безопасности информационных активов;
- определение уровней (величин) рисков ИБ в соответствии с «Методикой анализа рисков информационной безопасности»;
- сопоставление оцененных уровней рисков с выбранными на предыдущих подэтапах критериями для принятия рисков или обработки рисков;
- разработка «Плана управления рисками ИБ», описывающего решения по принятию или обработке рисков, с указанием выбранных мер и мероприятий по обработке, включая механизмы управления из Приложения А ISO/IEC 27001;
- разработка документа «Положение о применимости механизмов контролей СУИБ».

Результатом этапа являются разработанные проекты документов: «Методика анализа рисков информационной безопасности», «Отчет по результатам анализа рисков ИБ», «План управления рисками ИБ», «Положение о применимости механизмов контролей СУИБ».

3.3. Создание СУИБ, соответствующей требованиям ISO/IEC 27001:2022

Целью этапа является создание целостной структуры процессов управления и обеспечения ИБ, учитывающих специфику Заказчика и существующие системы менеджмента.

На данном этапе производится определение ролевой структуры СУИБ, ответственных сотрудников, распределение обязанностей и формальное описание ролей в части СУИБ.

Разработка (корректировка) процессов и документации СУИБ производится специалистами Исполнителя с привлечением специалистов Заказчика в части согласования разработанных документов.

На данном этапе разрабатываются документы, необходимые по требованиям ISO/IEC 27001:2022. Потребность в документах определяется на Этапе 1 при проведении обследования.

Результатом этапа является комплект документации СУИБ.

3.4. Внедрение процессов СУИБ

Внедрение процессов СУИБ производится за счет реализации следующих работ специалистами Исполнителя при активном содействии сотрудников Заказчика:

- консультации по выполнению персоналом Заказчика, вовлеченным в процесс функционирования СУИБ, своих ролевых обязанностей, в соответствии с разработанными процессами управления и обеспечения ИБ, изданной организационно-распорядительной документацией;
- проведение инструктажей для сотрудников заказчика по разработанным процессам;
- контроль и первичный запуск всех процессов СУИБ.
- помощь в документировании свидетельств функционирования процессов СУИБ (записей) в соответствии с требованиями разработанных процессов управления и обеспечения ИБ.

Результатом данного этапа являются:

- Набор записей по основной части ISO/IEC 27001, выработанных по результатам выполнения 1 цикла PDCA разработанных процессов управления ИБ;
- Работающая СУИБ, соответствующая требованиям ISO/IEC 27001:2022.

3.5. Оказание консультационной поддержки на сертификационном аудите

На этапе сертификационного аудита СУИБ Заказчика, **проводимого независимым органом по сертификации**, Исполнителем производятся следующие работы

- оказание финальных консультаций перед проведением этапа сертификации ключевых сотрудников, входящих в ОД СУИБ;
- оказание содействия в разработке плана корректирующих/предупреждающих действий по результатам проведения второй стадии сертификационного аудита.

Результатом данного этапа является план корректирующих и предупреждающих действий по выявленным в ходе аудита несоответствиям, направляемый в орган по сертификации.

3.6. Проведение сертификационного аудита органом по сертификации

Целью этапа является подтверждение соответствия созданной и внедрённой системы управления информационной безопасностью (СУИБ) требованиям ISO/IEC 27001:2022.

Работы на этом этапе проводятся независимым аккредитованным органом по сертификации.

В рамках данного этапа орган по сертификации выполняет:

- проведение аудита в два этапа (Stage 1 – документарная проверка, Stage 2 – аудит функционирования процессов);
- оформление отчётов по результатам каждого этапа;
- выдачу сертификата соответствия ISO/IEC 27001:2022 сроком на 1 (один) год;
- регистрацию сертификата в установленном порядке.

Результатом этапа является действующий сертификат ISO/IEC 27001:2022 сроком действия 1 (один) год.

Надзорные аудиты в рамках данного Технического задания не проводятся.