ТЕХНИКАЛЫҚ СИПАТТАМА

1257023 , Менеджмент жүйелерін аудит/сертификаттау бойынша қызметтер (PCI DSS 4.0.1.) сатып алу бойынша Ашық тендер тәсілімен

Лот № 1 (2129 У, 4541783) Аудит өткізу/менеджмент жүйелерін сертификаттау бойынша қызмет көрсету

Тапсырыс беруші: Акционерное общество «Казпочта»

Ұйымдастырушы: Акционерное общество «Казпочта»

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	2129 У
Атауы және қысқаша сипаттамасы	Аудит өткізу/менеджмент жүйелерін сертификаттау бойынша қызмет көрсету, Аудит өткізу /менеджмент жүйелерін сертификаттау бойынша қызмет көрсету
Қосымша сипаттама	Басқару жүйесінің аудиті/сертификаттау қызметтері (PCI DSS 4.0.1.)
Саны	1.000
Өлшем бірлігі	-
Жеткізу орны	ҚАЗАҚСТАН, Алматы қ., г. Алматы, ул. Богенбая батыра, 152
Жеткізу шарттары	-
Жеткізу мерзімі	Шартқа қол қойылған күннен бастап (қоса алғанда) 12.2026 дейін.
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 0%, Соңғы төлем - 100%

2. Сипаттамасы және талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары

Техникалық ерекшелік

процессингтік орталықтың сертификаттық және алдын ала аудитін жүргізуге төлем жүйелері индустриясының деректер қауіпсіздігі стандартының талаптарына

PCI DSS 4.0.1 карталарының

Жұмыстың немесе қызметтің атауы ТЖҚ БНА коды бойынша*	Процессингтік орталықтың PCI DSS 4.0.1 төлем карточкалары индустриясының деректер қауіпсіздігі стандартының талаптарына сертификаттау және алдын-ала тексеру. оның ішінде сыртқы және ішкі ену тестілеуі және осалдықтарды сыртқы ASV сканерлеу.
Талап етілетін техникалық сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы (ақаулы акт, жобалау-сметалық құжаттама). (Қызмет көрсету бойынша көрсетілетін қызметтердің тізбесі)	Қызмет көрсетудің мақсаты төлем карталарын ұстаушылар деректерінің қауіпсіздігін қамтамасыз ету жөніндегі қолданыстағы шаралардың (бұдан әрі - Тапсырыс беруші) PCI DSS 4.0.1 төлем карталары индустриясы деректерінің қауіпсіздігі стандартының (бұдан әрі - Стандарт) талаптарына сәйкестігін аудит (бағалау) болып табылады.

өнім берушіге (мердігерге) қойылатын талаптар	1. Өнім беруші Тапсырыс берушімен қызмет көрсету барысында алынған ақпаратты жарияламау туралы келісімге қол қоюға міндетті. 2. Жабдықтаушы компанияның Қазақстан Республикасының аумағында PCI DSS стандартының талаптарына сәйкестігі бойынша консультациялық қызметтер көрсетуге құқық беретін QSA (Qualified Security Assessor) мәртебесінің болуы; 3. Жеткізуші қамтамасыз ететін құралдарды пайдалана отырып, құжаттар мен аудиторлық материалдармен алмасудың қауіпсіз арнасын қамтамасыз етуі керек берілетін ақпараттың құпиялылығы мен тұтастығы. Айырбастаудың нақты тәсілі Тапсырыс Берушімен келісіледі; 4. PCI DSS стандарттарының талаптарына қатысты мәселелер бойынша халықаралық төлем жүйелерімен өзара әрекеттесу кезінде қолдау және кеңес беру.

1. Міндеттер

Осы мақсатқа жету үшін Жеткізуші келесі міндеттер тізімін орындауы керек:

- Енуге сыртқы тестілеуді өткізу;
- Енуге ішкі тестілеуді өткізу;
- Өткізу сегменттеу механизмдерін тестілеу
- Осалдықтарды сыртқы сканерлеуді жүргізу (ASV-сканерлеу);
- Тапсырыс берушінің рәсімдері мен құжаттамасының Стандарт талаптарына сәйкестігін талдау. Сәйкестік дәрежесі Стандарттың әрбір талабы бойынша анықталады;
- Қалыптасуы ұсынымдар бойынша жетілдіруге рәсімдерді және құжаттамалар Тапсырыс берушінің.
- Жобаларды қажетті құжаттамамен қамтамасыз ету;
- Тапсырыс берушінің сәйкестігін алдын ала талдау кезінде Стандарттар талаптарына сәйкессіздік анықталған жағдайда, Тапсырыс берушіге оларды жоюға көмек көрсетіңіз;
- Қызметті орындау нәтижелері бойынша есеп дайындау және келісу;
- Сұраныс бойынша Заказшы 31 желтоқсанға дейін 2026 жылғы сыртқы тестілеуді, ішкі тестілеуді және сыртқы тестілеуді өткізіңіз ASV сканерле у.

2. Жобаның шеңбері

Бағалау объектілері төлем карталарын ұстаушылардың ақпараттық ортасында қамтылған және/немесе қосылған Тапсырыс Берушінің барлық жүйелік компоненттері болып табылады. Мұндай жүйелік компоненттердің сипаттамасы, мысалдарды қоса, Стандартта, "PCI DSS талаптарының ауқымы" бөлімінде келтірілген.

3. Қызметке қойылатын талаптар

Қызмет көрсету шеңберінде келесі міндеттер орындалуы тиіс:

1. Тапсырыс берушімен қызмет көрсетудің екіжақты жоспар—кестесін әзірлеу және келісу:

• Тапсырыс беруші тарапынан мүдделі тұлғалардың қатысуымен кіріспе кездесу өткізу;

• Жобаның шекараларын анықтау;

• Жобаға қатысатын Тапсырыс берушінің негізгі персоналын анықтау;

• Ақпаратты ұсынуға сұрау салуды дайындау;

• Қызмет көрсету үшін қажетті ақпаратты анықтау;

• Тапсырыс берушінің Стандарт талаптарына сәйкестігін сертификаттау аудиті бойынша қызмет көрсетуді дайындау.

2. Стандарттар талаптарына сәйкестіктің ағымдағы деңгейін алдын ала бағалауды жүргізу және процедураларды, құжаттаманы жетілдіру және қауіпсіздік құралдарын орнату бойынша ұсыныстарды қалыптастыру.

3. PCI DSS стандартының талаптарының қолданылу аясы шеңберінде енуге сыртқы тестілеуді жүргізу.

4. Қажетті нормативтік құжаттаманың жобаларын ұсыну

5. PCI DSS стандартының қолданыстағы талаптары шеңберінде ішкі ену тестілеуін өткізу.

6. Осалдықтарды сыртқы сканерлеу (ASV-сканерлеу) сервисін ұсыну.

7. Тапсырыс берушінің рәсімдері мен құжаттамасының Стандарттар талаптарына сәйкестігін талдау. Сәйкестік дәрежесі Стандарттың әрбір талабы бойынша анықталады.

8. Жергілікті жерде қауіпсіздік аудитін жүргізу. АЖ Стандарт талаптарына сәйкестігін талдау.

9. Процедураларды, ұйымдастырушылық шаралар кешенін және бағдарламалық-техникалық құралдарды жетілдіру бойынша ұсыныстарды қалыптастыру, олардың орындалуы АЖ Стандарт талаптарына сәйкестігін қамтамасыз етуі тиіс.

10. Тапсырыс берушіге анықталған сәйкессіздіктер болған жағдайда оларды жоюға көмек көрсету. Сондай-ақ, әрбір анықталған сәйкессіздік үшін Стандарт талаптарына сәйкессіздікке байланысты тәуекелдерді анықтау және сәйкессіздікті жою бойынша практикалық ұсыныстарды әзірлеу.

11. Сәйкессіздіктерді жою бойынша ұсыныстарды Тапсырыс берушімен келісу. Егер Тапсырыс беруші ұсынылған ұсыныстарды 1 жыл ішінде орындалмайтын деп тапса, Тапсырыс берушімен Стандарт талаптарына сәйкес келмеуіне байланысты тәуекелдерді азайту бойынша өтемақы шараларын әзірлеп, келісу қажет.

12. Халықаралық төлем жүйелерінің талаптарына сәйкес қорытынды тексерулердің нәтижелері туралы есеп дайындау және келісу.

4. Көрсетілетін қызмет нәтижелеріне қойылатын талаптар

Диагностика нәтижелері бойынша Жеткізуші Тапсырыс берушіге келесілерді ұсынуы керек:

- Қызмет көрсетудің бекітілген екі жақты жоспар-кестесі;
- Бекітілген және әзірленген құжаттар, олардың болуы қажеттілігі анықталған жағдайда;
- Процедураларды, құжаттаманы жетілдіру және қорғаныс құралдарын орнату бойынша ұсыныстар (алдын ала бағалау нәтижелері бойынша);
- Анықталған сәйкессіздіктердің нәтижелері бойынша дайындалған тәуекелдер тізілімі, тәуекелдер картасы және тәуекелдерді азайту жоспары;
- Енуге сыртқы тестілеу нәтижелері бойынша есеп;
- Енуге арналған ішкі тестілеудің нәтижелері туралы есеп;
- Сегменттеу тетіктерін қосымша ішкі тестілеудің нәтижелері туралы есеп;
- PCI SSC кеңесінің ресми нысаны бойынша PCI DSS стандартының талаптарына сәйкестік туралы есеп (RoC);
- PCI SSC кеңесінің ресми нысаны бойынша PCI DSS стандартының талаптарына сәйкестік сертификаты (AOC);
- PCI DSS 4.0.1 сәйкестік сертификаты

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1257023 , Услуги по проведению аудита/сертификации систем менеджмента (PCI DSS 4.0.1.) способом Открытый тендер

Лот № 1 (2129 У, 4541783) Услуги по проведению аудита/сертификации систем менеджмента

Заказчик: Акционерное общество «Казпочта»

Организатор: Акционерное общество «Казпочта»

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	2129 У
Наименование и краткая характеристика	Услуги по проведению аудита/сертификации систем менеджмента, Услуги по проведению аудита/сертификации систем менеджмента
Дополнительная характеристика	Kazpost Digital_272111505_Услуги по проведению аудита/сертификации систем менеджмента (PCI DSS 4.0.1.)
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, г.Алматы, г. Алматы, ул. Богенбая батыра, 152
Условия поставки	-
Срок поставки	С даты подписания договора по (включительно) 12.2026
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

2. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики

Техническая спецификация

на проведение сертификационного и предварительного аудита процессингового центра требованиям стандарта безопасности данных индустрии платежных

карт PCI DSS 4.0.1

Наименование работы или услуги по коду ЕНС ТРУ*	Сертификационный и предварительный аудит процессингового центра требованиям стандарта безопасности данных индустрии платежных карт PCI DSS 4.0.1. включая проведение внешнего и внутреннего тестирования на проникновение, и внешнего ASV-сканирования уязвимостей.
Описание требуемых технических характеристик, параметров и иных исходных данных (дефектный акт, проектно-сметная документация). (Перечень услуг по обслуживанию)	Целью оказания услуги является аудит (оценка) соответствия существующих мер по обеспечению безопасности данных держателей платежных карт (далее - Заказчик) требованиям стандарта безопасности данных индустрии платежных карт PCI DSS 4.0.1 (далее - Стандарт).

Требование к поставщику (подрядчику)	1. Поставщик обязан подписать соглашение о неразглашении информации, полученной в ходе оказания услуги с Заказчиком. 2. Наличие у компании-поставщика статуса QSA (Qualified Security Assessor), дающий право на оказание консультационных услуг по соответствию требованиям стандарта PCI DSS на территории Республики Казахстан; 3. Поставщик должен обеспечить защищенный канал обмена документами и материалами аудита с использованием средств, обеспечивающих конфиденциальность и целостность передаваемой информации. Конкретный способ обмена согласовывается с Заказчиком; 4. Сопровождение и консультирование при взаимодействии с международными платежными системами по вопросам, касающихся требований стандартов PCI DSS.

1. Задачи

Для достижения поставленной цели Поставщик должен реализовать следующий перечень задач:

- Проведение внешнего тестирования на проникновение;
- Проведение внутреннего тестирования на проникновение;
- Проведение тестирования механизмов сегментаций
- Проведение внешнего сканирования уязвимостей (ASV-сканирование);
- Анализ процедур и документации Заказчика на соответствие требованиям Стандарта. Степень соответствии определяется по каждому требованию Стандарта;
- Формирование рекомендаций по совершенствованию процедур и документации Заказчика.
- Предоставление проектов необходимой документации;
- В случае выявления несоответствия требованиям Стандартов при предварительном анализе соответствия Заказчика, оказать содействие Заказчику по их устранению;
- Подготовить и согласовать отчет по результатам выполнения услуги;
- По запросу Заказчика до 31 декабря 2026 года провести внешнее тестирование, внутреннее тестирование и внешнее ASV сканирование.

2. Рамки проекта

Объектами оценки являются все системные компоненты Заказчика, содержащиеся и/или подключенные к информационной среде держателей платежных карт. Описание таких системных компонентов, включая примеры, приведены в Стандарте, секция «Scope of PCI DSS Requirements».

3. Требования к услуге

В рамках оказания услуги должны быть выполнены следующие задачи:

1. Разработать и согласовать с Заказчиком двухсторонний план — график оказания услуги:

• Проведение вводной встречи с участием заинтересованных лиц со стороны Заказчика;

• Определение границ Проекта;

• Определение ключевого персонала Заказчика, задействованного в Проекте;

• Подготовка запроса на предоставление информации;

• Определение необходимой информации для оказания услуги;

• Подготовка оказания услуги по сертификационному аудиту Заказчика на соответствие требованиям Стандарта.

2. Провести предварительную оценку текущего уровня соответствия требованиям Стандартов и сформировать рекомендации по совершенствованию процедур, документации и настройке средств защиты.

3. Провести внешнее тестирование на проникновение в рамках области действия требований стандарта PCI DSS.

4. Предоставить проекты необходимой нормативной документации

5. Провести внутреннее тестирования на проникновение в рамках области действия требований стандарта PCI DSS.

6. Предоставить сервис внешнего сканирования уязвимостей (ASV-сканирование).

7. Анализ процедур и документации Заказчика на соответствие требованиям Стандартов. Степень соответствия определяется по каждому требованию Стандарта.

8. Проведение аудита безопасности на месте. Анализ ИС на соответствие требованиям Стандарта.

9. Формирование рекомендаций по совершенствованию процедур, комплекса организационных мер и программно-технических средств, выполнение которых должно обеспечить соответствие ИС требованиям Стандарта.

10. Оказание содействия Заказчику по устранению выявленных несоответствий, в случае их наличия. Также для каждого выявленного

несоответствия определить риски, связанные с несоответствием требованию Стандарта, и разработать практические рекомендации по устранению несоответствия.

11. Согласовать рекомендации по устранению несоответствий с Заказчиком. В случае, если предложенные рекомендации будут признаны Заказчиком невыполнимыми в течение 1 года, разработать и согласовать с Заказчиком компенсационные меры по снижению рисков, связанных с несоответствием требованию Стандарта.

12. Подготовить и согласовать отчет по результатам проведения итоговых аудитов согласно требованиям международных платежных систем.

4. Требования к результатам услуги

По результатам диагностики Поставщик должен предоставить Заказчику следующее:

- Утверждённый двухсторонний план-график оказания услуги;
- Утверждённые и разработанные документы, в случае выявления необходимости их наличия;
- Рекомендации по совершенствованию процедур, документации и настройке средств защиты (по результатам предварительной оценки);
- Реестр рисков, карта рисков и план минимизации рисков, подготовленных по результатам выявленных несоответствий;
- Отчет по результатам внешнего тестирования на проникновение;
- Отчет по результатам внутреннего тестирования на проникновение;
- Отчет по результатам дополнительного внутреннего тестирования механизмов сегментации;
- Отчет о соответствии (RoC) требованиям Стандарта PCI DSS по официальной форме Совета PCI SSC;
- Аттестат соответствия (AOC) требованиям Стандарта PCI DSS по официальной форме Совета PCI SSC;
- Сертификат соответствия PCI DSS 4.0.1