ОБЪЯВЛЕНИЕ

На тендер по выбору компании(организации) по оказанию консалтинговых услуг и услуг по тестированию инфраструктуры и информационных систем ЗАО «АРМБИЗНЕСБАНК» на защищенность от проникновений (Penetration test), а также проверке и сертификации Банка на соответствие требованиям по защите данных держателей пластиковых карт, организации и защите транзакций по пластиковым картам

ЗАО «АРМБИЗНЕСБАНК» (в дальнейшем Банк) объявляет тендер на приобретение следующих услуг.

I. Перечень приобретаемых услуг:

1. Услуги по проведению тестов на заищенность от проникновения (Penetration test) инфраструктуры и информационных систем Банка, а также консалтинговые услуги по устранению выявленных во время тестов уязвимостей информационных систем (см. Приложение № 1);
2. Консалтинговые услуги по приведению в соответствие, сертификации и аудиторскому обслуживанию по стандарту Payment Card Industry Data Security Standard (PCI DSS) (по деиствующей версии) информационных технологий и систем Банка (см. Приложение № 2);
3. Услуги по оценке соответствия требованиям стандарта PCI PIN security Recuairements (по деиствующей версии).

Все три пункта требуемых услуг считяются одним Проектом (в дальнейшем Проект) (см. Приложение № 3).

II. Целями оказания услуг являются:

1. Проверка защищенности и оценка устойчивости информационных систем Банка от попыток проникновений (В том числе и целевых таргетированных атак APT) злоумышленников извне и изнутри информационных систем Банка.
2. Обеспечение выполнения требований стандарта Payment Card Industry Data Security Standard (PCI DSS) (по деиствующей версии) в информационной системе Банка и демонстрация их выполнения в международных платежных системах.
3. Оценка соответствия процедур управления ключами шифрования ПИН-кодов с требованиями стандарта безопасности PCI PIN Security Requirements.

III. Требования к потенциальному поставщику.

1. Быть специализированной компанией занимающийся вопросами кибербезопасности или в своем составе иметь специализированное подразделение предоставляющие услуги по вопросам кибербезопасности;
2. Иметь минимум 3-х летний опыт работы в области кибербезопасности;

3. Компания должна иметь действующие статусы:
   3.1. Аккредетацию в «CREST International», дающее право проводить работы в Республике Армения, или в регионе где находится Республика Армения (подтвержденный на официальном сайте ассоциации «CREST International» http://www.crest-approved.org/).
   3.2. QSA – Qualified Security Assessor;
   3.3. PA-QSA - Payment Application Qualified Security Assessor;
   3.4. ASV - ApprovedScanningVendor;
   3.5. QSA (P2PE), PA-QSA (P2PE) - Qualified Security Assessors Point to Point Encryption; «PCI security Standarts Counsil», иметь статус QSA (Qualifaed Security Assesor);
   подтвержденные на официальном сайте ассоциации PCI SSC https://www.pcisecuritystandards.org.
4. Компания должна иметь опыт проведения тестирования на проникновение (Penetration test) как минимум в 5 (пяти) банках вне территории Армении;
5. Компания должна обладать практическим опытом выполнения работ по стандарту PCI DSS не менее 3 (трех) лет, иметь в своем активе не менее 5 (пяти) успешно завершенных проектов по стандарту PCI DSS вне территории Армении (положительно завершенные сертификации по стандарту PCI DSS).
6. Иметь опыт работы на территории Армении;
7. Компания должна иметь действующую страховку на свою деятельность в области информационной безопасности и быть готова предоставить гарантии о компенсации возможного ущерба причиненного Банку в результате действий тестирущей компании и/или его сотрудников;
8. Заключить договор о неразглашении информации.
9. Переписка, консультирование и общение должны осуществляться на русском языке.
10. Результаты всего проекта или отдельных его этапов должны быть представлены на русском и/или английском языках (по согласованию сторон).
11. Персонал компании (Исполнитель) задействованный в Проекте должен соответствовать следующим квалификационным требованиям:
    11.1.1. Персонал проводящий тестирование должен быть соответствующим образом сертифицирован.
    11.1.2. Состав группы исполнителей по каждому направлению должен быть указан в тендерном предложении (не менее 3-х человек).
    11.1.3. Должен быть назначен Руководитель (Менеджер) группы исполнителей, обладающий опытом участия в не менее чем двух успешно завершенных аналогичных проектах в качестве руководителя проекта или направления в области аудита ИТ и ИБ (подтверждением является официальное письмо от Исполнителя, заверенное подписью первого руководителя Исполнителя и скрепленное печатью).
    11.1.4. Члены группы должны иметь высокий уровень профессиональной квалификации. На каждого члена группы Исполнителя предоставляется его резюме, заверенное подписью первого руководителя Исполнителя и скрепленное печатью. В резюме необходимо указать общие профессиональные сведения, опыт работы, опыт

участия в аналогичных проектах с указанием роли в проектной группе, наименование или обобщенное описание компании-клиента.

11.1.5. Минимум два члена группы должны иметь опыт по оказанию услуг в области аудита ИТ и ИБ не менее 6 лет. Описание опыта оказания аналогичных услуг приводится в резюме согласно таблице ниже:

№	Наименование компании, которой были предоставлены услуги	Краткое описание оказанных услуг	Результат по оказанным услугам	Период времени, в который были предоставлены услуги

11.1.6. Состав членов группы исполнителя в ходе оказания услуг может изменяться только по согласованию с Банком.

11.1.7. Умение сотрудников компании, задействованных в работах, изъясняться на русском языке дополнтельный бонус.

IV. Условия Проведения тендера

Заказчик услуг (Организатор закупок) - ЗАО «АРМБИЗНЕСБАНК».

Срок оказания услуг- 12(двенадцать) месяцев с момента заключения договора.

Срок действия тендерного предложения участника - не менее 60 (шестьдесят) календарных дней.

Конкретные данные об инфраструктуре Заказчика для формирования коммерческого предложения Банк предоставит после получения заявки на участие;

Заявки потенциальных поставщиков на участие в тендере принимаются на электронный адрес: gurgen.baghdasaryan@armbusinessbank.am; до 17:00 (по местному времени) 22 октября 2018 года включительно.

Контактное лицо –Начальник Информационно-аналитического отдела Гурген Багдасарян, тел. +374 10 592045.e-mail: gurgen.baghdasaryan@armbusinessbank.am.

Отказ от закупок

Заказчик вправе на любом этапе закупок отказаться от осуществления закупок без возмещения убытков потенциальным поставщикам, в случаях сокращения расходов на приобретение товаров, работ и услуг, предусмотренных в плане закупок, обоснованного уменьшения потребности или обоснованной нецелесообразности приобретения товаров, работ и услуг.

В этом случае Заказчик обязуется в течение 3 (трех) рабочих дней со дня принятия решения об отказе от осуществления закупок известить об этом лиц, участвующих в проводимых закупках, и опубликовать соответствующее объявление на веб-сайте Заказчика;

V. Требования к тендерному предложению.

1. В технической спецификации, приложенной к тендерному предложению исполнителя, должно быть приведено описание:

1.1. подхода исполнителя к реализации Проекта;

1.2. структуры и состава группы исполнителей в соответствии с квалификационными требованиями;

1.3. плана-графика реализации Проекта с указанием стоимости и длительности каждой части(этапа) проекта.

2. Пакет документов присылается в запечатанных конвертах, по почте, на адрес: ***0010 Республика Армения, г. Ереван, ул. Налбандяна дом 48. Получатель: "Тендерная комиссия" ЗАО "АРМБИЗНЕСБАНК".***

3. Пакеты с документами принимаются до 17:00 (по местному времени) 05 ноября 2018 года включительно

Приложение № 1
к Тендерной документации

Техническая спецификация закупаемых услуг

Услуги по проведению Внутреннего и внешнего теста на проникновение (Penetration test) с применением социального инжиниринга, консултирование по устранению выявленных уязвимостей в
информационных системах ЗАО «АРМБИЗНЕСБАНКА»

12. ЗАДАЧИ ОКАЗАНИЯ УСЛУГ

Задача теста на проникновение (Penetration test) моделируя действия нарушителя определить реальный уровень защищенности информационной системы Банка при помощи общедоступных (общеизвестных) методов получения несанкционированного доступа, реализации активных или пассивных действий злоумышленника минимум должен состоять:

13. ОПИСАНИЕ ГРАНИЦ ОКАЗАНИЯ УСЛУГ

Тестированию подлежат все информационные системы Банка, в том числе информационные системы задействованные в обработке данных держателей карт.

14. ПОРЯДОК ОКАЗАНИЯ УСЛУГ

14.1. Тест на проникновение извне выполняется в отношении ресурсов Банка доступных из сети Интернет. Моделирование действий нарушителя подразумевает получение доступа к информационной системе злоумышленником, не обладающим полной информацией о системе (black box) и состоит из следующих этапов:

- 14.1.1. инвентаризация доступных злоумышленнику информационных ресурсов и сервисов – зондирующие атаки,
- 14.1.2. выявление уязвимостей;
- 14.1.3. разработка векторов моделируемой атаки;
- 14.1.4. моделирование атаки(тест на проникновение).

14.2. Тест на проникновение изнутри выполняется в отношении всех информационных ресурсов доступных из внутренней сети Банка. Моделирование действий нарушителя подразумевает получение доступа к информационной системе злоумышленником, обладающим некоторой информацией о системе(white box) и состоит из следующих этапов:

- 14.2.1. Обзор конфигураций брандмауэров;
- 14.2.2. Обзор конфигураций маршрутизаторов;
- 14.2.3. Обзор VPN;
- 14.2.4. Тестирование инфраструктуры изнутри(без аутентификации);

14.3. Обзор защищенности от таргетированных атак(APT) с последующим согласованием вектора атаки(минимум 2 раза в год);

14.4. Тест на проникновение с применением методов Социального инжиниринга(как минимум фишинг сценарий);

14.5. Сканирование внутренней сети банка(минимум одно сканирование и одно ресканирование в течении 3-х месяцев).

14.6. Перед началом работ Компания предоставляет и согласует с Банком план-график работ, включая список документов, необходимых для анализа, а также перечень должностных лиц, с которыми предполагается провести собеседование и способ его проведения.

15. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

По итогам проведенных работ Исполнителем предоставляются следующие документы в электронном виде(.pdf) и на бумажных носителях.

15.1. Полный технический отчет по внешнему тесту, обобщенный отчет для руководства(Executive review). Рекомендации по устранению выявленных уязвимостей.

15.2. Полный технический отчет по внутреннему тесту, обобщенный отчет для руководства(Executive review). Рекомендации по устранению выявленных уязвимостей.

15.3. Полный технический отчет по результатам теста на проникновение с применением методов Социального инжиниринга, обобщенный отчет для руководства(Executive review). Рекомендации по устранению выявленных уязвимостей.

15.4. Полный отчет по результатам проверки на защишенност от APT в период проверки. Рекомендации по устранению выявленных уязвимостей.

15.5. Полный технический отчет после каждого сканирования. Рекомендации по устранению выявленных уязвимостей.

Приложение № 2
к Тендерной документации

Техническая спецификация закупаемых услуг
консалтинговых услуг по приведению в соответствие,
сертификации и аудиторскому обслуживанию по стандарту
PCI DSS информационных технологий и систем ЗАО «АРМБИЗНЕСБАНКА»

16. ЗАДАЧИ ОКАЗАНИЯ УСЛУГ

В ходе оказания услуги произвдится оценка соответствия требованиям стандарта Payment Card Indastry Data Seurity Standard (PCI DSS)(по действующей версии) информационных технологий и систем и как минимум должен состоять:

16.1. Исследование и анализ инфраструктуры;

16.2. Определение(уточнение) области применения стандарта;

16.3. Составление и согласование плана-графика работ;

16.4. Оценка текущего уровня соответствия стандарту(Предварительный аудит на соответствие требованиям стандарта) PCI DSS, для разработки рекомендаций по приведению в соответствие требованиям стандарта и включает два этапа:

16.4.1. Сбор и исследование нормативных и распорядительных документов на соответствие требованиям стандарта PCI DSS(оценка соответствия на организационном уровне);

16.4.2. Анализ технических, программных и аппаратно-программных комплексов защиты информации(технологическая оценка), влючая:

16.4.2.1. Физическую защиту помещений;

16.4.2.2. программно-аппаратные средства защиты каналов передачи данных;

16.4.2.3. программно-аппаратные комплексы защиты сетевого уровня;

16.4.2.4. программные средства защиты на прикладном уровне;

16.4.2.5. программные средства защиты информации на серверах и рабочих станциях.

16.4.2.6. Результаты выполненных работ по итогам уже проведенных ранее IT–аудитов.

16.4.3. По результатам предаудита банку предоставляется итоговый подробный отчет отражающий ситуацию в период проведения аудита и план действий(Action plan) в котором указаны основные мероприятия, запланированные для устранения несоответствий, лица, ответственные за реализацию мероприятий и планируемые сроки;

16.4.4. Action plan может предоставляться в международные платежные системы либо другие заинтересованные организации только с согласия Банка.

16.4.5. Тест на проникновение с использованием IP внешнего периметра(black box);

16.4.6. Тест на проникновение из внутреннего периметра (тест проводится в банке) (white box);

16.4.7. Сканирование внутренней компютерной сети банка(минимум одно сканирование и одно ресканирование в течении 3-х месяцев). Кроме того обеспечение сканирования при каждом измененин в инфраструктуре банка. После каздого сканирования банку предоставлять полный отчет о результатах и рекомендации по устранению выявленных недостатков;

16.4.8. Предоставляет рекомендации по приведению в соответствие PCI DSS, а именно:

16.4.8.1. по изменению конфигураций и настроек внешних и встроенных средств защиты информации;

16.4.8.2. по изменению или дополнению документов существующей политики информационной безопасности;

16.4.8.3. по внедрению дополнительных средств защиты информации;

16.4.8.4. другие рекомендации, выполнение которых обеспечит выполнение требований Стандарта.

16.4.8.5. рекомендаций по внедрению компенсационных мер. В случае если Заказчику не представляется возможным выполнить некоторые требования Стандарта из-за сложившихся бизнес-процессов, чрезвычайной дороговизны технических решений, их несовместимости с имеющимися ИС или по иным причинам.

16.4.9. консултации по устранению выявленных недостатков и несоответствий. Составление плана действий по устранению несоответствий.

16.5. Сертфикационный аудит на соответствие требованиям PCI DSS проводится по всему объему требований стандарта, По результататам предоставляется отчет;

16.5.1. Определяется(уточняется) область применения стандарта;

16.5.2. По результатам сертификационного аудита банку предоставляется итоговый подробный отчет отражающий ситуацию в период проведения аудита;

17. ПОРЯДОК ОКАЗАНИЯ УСЛУГ

В соответствии с задачами, определенными выше, Услуги должны быть выполнены в 3 (три) этапа:

17.1. Предварительная оценка соответствия требованиям стандарта PCI DSS (Этап 1);

17.2. Составление плана-графика мероприятий и рекомендаций по устранению выявленных несоответствий, консультации в ходе выполнения работ по устранению несоответствий (Этап 2).

17.3. Предварительная оценка соответствия требованиям стандарта PCI PIN Security Requirements 2.0(Этап 1);

17.4. Контроль устранения несоответствий и подготовка итоговых отчетных документов(Этап 2).

17.5. Сертификационный аудит соответствия требованиям стандарта PCI DSS, подготовка итоговых отчетных документов и отправка в международные организации(Этап 3).

18. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

По итогам выполнения работ по оценке соответствия требованиям PCI DSS, Исполнителем должны быть разработаны следующие документы в электронном виде (pdf) и на бумажном носителе:

18.1. Полный отчет о предварительном обследовании по требованиям стандарта PCI DSS и отражающий степень соответствия требованиям стандарта и план действий(Action plan) по устранению несоответствий требованиям стандарта;

18.2. По результатам сертификационного аудита банку предоставляется итоговый подробный отчет отражающий ситуацию в период проведения аудита;

18.3. Заключение о результатах аудита.

18.4. Документ подтверждающий сертификацию соответствия стандарту PCI DSS

Приложение № 3
к Тендерной документации

Техническая спецификация закупаемых услуг
По оказанию услуг по оценке соответствия требованиям стандарта PCI PIN security Recuairements

19. ЗАДАЧИ ОКАЗАНИЯ УСЛУГ

В ходе оказания услуги произвдится оценка соответствия процедур управления ключами шифрования ПИН-кодов с требованиями стандарта безопасности PCI PIN Security Requirements. как минимум должен состоять:

19.1. Подготовка к обследованию и предварительный анализ;
19.2. Проведение оценки соответствия на площадке Заказчика;
19.3. Подготовка предварительного отчета об обследовании с рекомендациями по устранению выявленных несоответствий;
19.4. Консультации по устранению несоответствий с требованиями стандарта безопасности PCI PIN Security Requirements
19.5. Проведение оценки на соответствие требованиям PCI PIN secur Security Requirements. Предоставление Банку полного отчета по итогам оценки и предоставление сведений о результатах оценки в Visa.

20. ОПИСАНИЕ ГРАНИЦ ОКАЗАНИЯ УСЛУГ

20.1. Оценке соответствия по требованиям стандарта PIN Security Requirements подлежит деятельность Заказчика, связанная с созданием, хранением, загрузкой, удалением криптографических ключей шифрования, обеспечением безопасности криптографических ключей, физической и логической инфраструктуры, в которой ключи обрабатываются.
20.2. Оценка проводится согласно применимым требованиям стандарта PCI PIN Security Requirements версии 2.0 и документа PIN Security Requirements and Testing Procedures, опубликованных на официальном сайте PCI SSC - https://www.pcisecuritystandards.org.

21. ПОРЯДОК ОКАЗАНИЯ УСЛУГ

В соответствии с задачами, определенными выше, Услуги должны быть выполнены в 2 (два) этапа:

21.1. Предварительная оценка соответствия требованиям стандарта PCI PIN Security Requirements 2.0(Этап 1);
21.2. Контроль устранения несоответствий и подготовка итоговых отчетных документов(Этап 2).

22. ТРЕБОВАНИЯ К СОДЕРЖАНИЮ И ОБЪЕМУ ОКАЗЫВАЕМЫХ УСЛУГ

22.1. В рамках этапа 1 Исполнитель:

22.1.1. проводит подготовку к обследованию и предварительный сбор и анализ сведений о деятельности Заказчика, включая:

- запрос сведений, предварительный анализ документации и определение области оценки,
- предоставление и согласование с Заказчиком плана обследования на месте;

22.1.2. проводит оценку соответствия требованиям PCI PIN Security Requirements на месте, включая:

- проведение интервью согласно плану обследования и сбор свидетельств аудита на территории Заказчика;
- проведение встречи с ключевыми сотрудниками для обсуждения предварительных результатов обследования;

22.1.3. разрабатывает отчет об обследовании, включающий общую информацию об обследуемой организации, описание оцениваемой деятельности по управлению ключами шифрования ПИН, перечень выявленных несоответствий стандарту и рекомендации аудитора по их устранению;

22.2. В рамках этапа 2 Исполнитель:

22.2.1. согласует с Заказчиком план устранения выявленных несоответствий, включая планируемые сроки устранения;

22.2.2. осуществляет контроль устранения несоответствий путем оценки предоставленных Заказчиком свидетельств;

22.2.3. дорабатывает отчет об обследовании по результатам устранения несоответствий;

22.2.4. Предоставляет Банку окончательный вариант итогового отчета(Visa Attestation of Compliance).

22.2.5. по факту выполнения всех требований стандарта оформляет Visa Attestation of Compliance (VAOC), предоставляет и согласовывает с Visa Inc. результаты прохождения процедуры оценки.

23. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

По итогам выполнения работ по оценке соответствия требованиям PCI PIN Security Requirements, Исполнителем должны быть разработаны следующие документы в электронном виде (pdf) и на бумажном носителе:

23.1. Отчет об обследовании по требованиям стандарта PCI PIN Security Requirements (PIN Security Assessment Report);

23.2. Заключение о результатах аудита - Visa Attestation of Compliance.