Техническое задание на проведение соответствия информационной инфраструктуры АО БАНК «СНГБ» требованиям действующего стандарта PCI DSS и PCI 3DS

Срок предоставления ТКП	**17.02.2020**
Адрес направления ТКП	**obit@sngb.ru**, дополнительный **fiv@sngb.ru**
Контакты	+7 (3462) 39-88-88 доб. 2181

Обязательно получите подтверждение о принятии Вашего ТКП представителем Банка в работу.

1. ЦЕЛИ ОКАЗАНИЯ УСЛУГ

1.1. Подтверждение соответствия информационной инфраструктуры Заказчика, используемой для обработки, хранения и передачи данных платёжных карт, (далее Инфраструктуры) требованиям действующего международного стандарта безопасности данных индустрии платежных карт PCI DSS[1] и требованиям действующего стандарта Payment Card Industry 3-D Secure (PCI 3DS.[2])

№ этапа	Наименование услуг	Сроки оказания услуг, рабочие дни	Отчётные документы
1.	Оценка соответствия информационной инфраструктуры требованиям действующего стандарта PCI DSS и PCI 3DS	02.03.2020 - 06.03.2020	Предварительный отчёт о соответствии; План устранения выявленных несоответствий (Action Plan), рекомендации по приведению системных компонентов Заказчика в соответствие требованиям PCI DSS и PCI 3DS и выполнению мероприятий, предусмотренных Action Plan; Детальный перечень мероприятий, которые рекомендуется провести для выполнения требований действующего стандарта PCI DSS и PCI 3DS до выполнения уровня Compliance у Клиента. Проекты документов с целью устранения выявленных замечаний. Предоставляется Заказчику в течении 7 рабочих дней после завершения этапа 1.
2.	Проведение тестирования на проникновение из сети Интернет и внутренней сети для выполнения пп. 11.3.1 и 11.3.2 требований стандарта PCI DSS и PCI 3DS (проводится посредством удаленного доступа по VPN) с последующей перепроверкой устранения выявленных уязвимостей и несоответствий. в соответствии с п.2.9	16.03.2020 - 20.03.2020	Экспертное заключение о проведенном тестировании на проникновение с подробными рекомендациями по устранению выявленных уязвимостей и несоответствий. (удаленная проверка); Экспертное заключение по результатам перепроверки выявленных уязвимостей и несоответствий. (удаленная проверка);

[1] Payment Card Industry Data Security Standard / Стандарт безопасности данных индустрии платежных карт
[2] Payment Card Industry 3-D Secure (PCI 3DS)

	технического задания. **Тестирование проводится по методологии Penetration Testing Guidance «Payment Card Industry Data Security Standard»**		Экспертное заключение предоставляется Заказчику в течении 7 рабочих дней после завершения работ по этапу 2;
3.	Сертификационный аудит на соответствие требованиям действующего стандарта PCI DSS и PCI 3DS	11.05.2020-22.05.2020	Свидетельство о Соответствии (Attestation of Compliance) согласно требований PCI DSS и PCI 3DS; Отчёт о Соответствии (Report on Compliance) согласно требований PCI DSS и PCI 3DS; Сертификат Исполнителя, подтверждающий соответствие инфраструктуры Заказчика требованиям действующего стандарта PCI DSS и PCI 3DS; Отчетные документы предоставляются Заказчику в течении 10 рабочих дней после завершения этапа 3, но не поздней **18.06.2020г**.
4.	Консультационное сопровождение по вопросам PCI DSS и PCI 3DS в течении 1 года от QSA - аудитора	1 год с момента заключения договора	Телефон, электронная почта.
5.	Передача AOC и ROC (по запросу) в ПС (НСПК, VISA, MC).	До 18.06.2020	AOC, ROC (в случае необходимости) передан в международные платежные системы. *Текущий AOC подписан 18.06.2019*
6.	Дополнительная проверка с последующей перепроверкой устранения выявленных уязвимостей и несоответствий сегментации сети п.11.3.4 (1 раз в шесть месяцев) требований стандарта PCI DSS и PCI 3DS, в соответствии с п.2.9. технического задания. **Тестирование проводится по методологии Penetration Testing Guidance «Payment Card Industry Data Security Standard»**	***Первая проверка*** 01.04.2020 – 10.04.2020 ***Вторая проверка*** 24.09.2020 - 28.09.2020	Подробный отчет с рекомендациями по устранению несоответствий по итогам дополнительной проверки сегментации сети (удаленная проверка). Подробный отчет по результатам перепроверке выявленных уязвимостей и несоответствий сегментации сети. Подробный отчет предоставляется Заказчику в течении 7 рабочих дней после завершения работ по этапу 6.
7.	Доступа к сертифицированному ASV-сканеру для проведения работ по соответствую требования стандартов PCI DSS и PCI 3DS (https://www.pcisecuritystandards	1 год с момента заключения договора	Неограниченное количество технических сканирований. Не менее 4 сертифицированных. С предоставлением подробного отчета по устранению уязвимостей. Подробный отчет предоставляется Заказчику в течении 3 рабочих дней после завершения работ по этапу 7.

	.org/assessors_and_solutions/approved_scanning_vendors)		По устранению уязвимостей Заказчик взаимодействует с Исполнителем (а не с разработчиком ASV-сканера). Поддержка от Исполнителя по работе с ASV-сканером в течении 1 года с момента заключения договора.

2. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ

2.1. Аудит по соответствию информационной инфраструктуры Заказчика требованиям действующего стандарта PCI DSS и PCI 3DS;

2.2. Срок исполнения всех обязательств: **не позднее 18.06.2020г, за исключением этапа 6** проверка сегментации сети «Вторая проверка»;

2.3. Исполнитель не имеет права привлекать внешних исполнителей.

2.4. Обязательное наличие лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации №79.

2.5. Опыт работы с банками не менее 3 (трех) лет, просим участников подтвердить рекомендательными письмами, по направлению PCI DSS и PCI 3DS.

2.6. Условия по оплате, с указанием отдельно стоимости НДС: 100% оплата поэтапная по факту выполнения работ каждого этапа. Стоимость командировочных расходов указывается отдельной позицией. Необходимо предоставить стоимость по каждому этапу с указанием объема и формы предоставления услуги.

2.7. Обязательное указание в ТКП[3] сроков и стоимости по каждому этапу работ;

2.8. Отсутствие Исполнителя в санкционном списке: https://sanctionssearch.ofac.treas.gov/.

2.9. В случае выявления в ходе оказания услуг на этапе 2 и 6, Исполнитель осуществляет повторную проверку на наличие уязвимостей после их устранения Заказчиком.

2.10. По окончании Этапа 3 Заказчику предоставляется сертификат Исполнителя, подтверждающий соответствие Инфраструктуры Заказчика требованиям действующего стандарта PCI DSS и PCI 3DS.

2.11. Предоставление консультаций специалистам Клиента по любым вопросам обеспечения и оценки выполнения требований PCI DSS и PCI 3DS, в т.ч. по эксплуатации технических средств защиты информации по телефону и электронной почте, в течение одного года с даты начала действия Договора производится без дополнительной оплаты.

2.12. Исполнитель гарантирует выполнение взятых на себя обязательств по Договору в случае попадания в санкционные списки.

2.13. Сертифицированный ASV-сканер должен быть включен в перечень «Approved Scanning Vendors» для выполнения требований стандартов PCI DSS и PCI 3DS:

- https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors

2.14. Исполнитель должен находится в перечне «Qualified Security Assessor Company» по адресу:

- https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors.

2.15. Аудит по соответствию информационной инфраструктуры Заказчика требованиям действующего стандарта PCI DSS и PCI 3DS проходит только в очной форме, пункт 2 и 6 возможны в заочной.

2.16. Исполнитель должен иметь возможность работать в системе электронного документа «Диадок» или совместимой с ней.

2.17. В коммерческое предложение Исполнитель включает контактные данные QSA-аудитора, который будет выполнять аудит на соответствие требованиям действующего стандарта PCI DSS и PCI 3DS.

2.18. Исполнитель обязан предоставить действующий аттестат QSA-аудитора.

2.19. Исполнитель передает AOC и ROC (по запросу) в ПС (НСПК, VISA, MC).

[3] Технико-коммерческое предложение

2.20. Обязательное указание в ТКП сроков и стоимости по каждому этапу работ.

2.21. В коммерческом предложении Исполнитель указывает сроки, стоимость по каждому этапу работ PCI 3DS и PCI DSS.

3. ГРАНИЦЫ ОКАЗАНИЯ УСЛУГ

№	Вопрос	Ответ
1.	Наименование организации	АО БАНК «СНГБ»
2.	Веб-сайт организации	https://www.sngb.ru
3.	Физический адрес организации (головного офиса)	ХМАО-Югра, г. Сургут, ул. Григория Кукуевицкого, д. 19
4.	Физический адрес дата – центра, в котором расположена информационная инфраструктура, и административных помещений, из которых осуществляется управление ею	ХМАО-Югра, г. Сургут, ул. Губкина, 15а ХМАО-Югра, г. Сургут, ул. Григория Кукуевицкого, д. 19

4. РЕЗУЛЬТАТ ОКАЗАНИЯ УСЛУГ

4.1. ЭТАП №1

4.1.1. Предварительный отчёт о соответствии;

4.1.2. План устранения выявленных несоответствий (Action Plan), рекомендации по приведению системных компонентов Заказчика в соответствие требованиям действующего стандарта PCI DSS и PCI 3DS и выполнению мероприятий, предусмотренных Action Plan:

4.1.2.1.1. Детальный перечень мероприятий, которые рекомендуется провести для выполнения требований действующих стандартов PCI DSS и PCI 3DS до выполнения уровня Compliance у Клиента.

4.1.3. Проекты документов с целью устранения выявленных замечаний.

4.1.4. Отчетная документация по этапу 1 предоставляется Заказчику в течении 7 рабочих дней после завершения этапа 1.

4.2. ЭТАП №2

4.2.1. Экспертное заключение о проведенном тестировании на проникновение с рекомендациями по устранению выявленных уязвимостей.

4.2.2. Экспертное заключение по результатам перепроверки выявленных уязвимостей и несоответствий. (удаленная проверка);

4.2.3. Отчетная документация по этапу 2 предоставляется Заказчику в течении 7 рабочих дней после завершения этапа 2.

4.3. ЭТАП №3

4.3.1. Свидетельство о Соответствии (Attestation of Compliance) согласно требований PCI DSS и PCI 3DS;

4.3.2. Отчёт о Соответствии (Report on Compliance) согласно требований PCI DSS и PCI 3DS;

4.3.3. Сертификат Исполнителя, подтверждающий соответствие Инфраструктуры Заказчика требованиям действующего стандарта PCI DS и PCI 3DS.

4.3.4. Отчетная документация по этапу 3 предоставляется Заказчику в течении 10 рабочих дней после завершения этапа 3, но не поздней 18.06.2019г.

4.4. ЭТАП №4

4.4.1. Консультационное сопровождение по вопросам PCI DSS и PCI 3DS в течении 1 года от QSA – аудитора, телеконференции, электронная почта.

4.5. ЭТАП №5

4.5.1. Свидетельство о Соответствии (Attestation of Compliance), Отчёт о Соответствии (Report on Compliance) и другие необходимые документы по требованиям PCI DSS и PCI 3DS переданы Исполнителем в платежные системы.

4.6. ЭТАП №6

4.6.1. Подробный отчет с рекомендациями по устранению несоответствий по итогам дополнительной проверки сегментации сети.

4.6.2. Подробный отчет по результатам перепроверке выявленных уязвимостей и несоответствий сегментации сети.

4.6.3. Отчетная документация по этапу 6 предоставляется Заказчику в течении 7 рабочих дней после завершения этапа 6.

4.7. ЭТАП №7

4.7.1. Доступ к сертифицированному по требованиям PCI DSS и PCI 3DS ASV-сканеру (https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors)

4.7.1.1. Неограниченное количество технических сканирований;

4.7.1.2. Не менее 4 сертифицированных;

4.7.1.3. Необходимое количество IP-адресов для ASV-сканера: 25штук;

4.7.1.4. Подробный отчета по устранению выявленных уязвимостей.

4.7.2. Отчетная документация по этапу 7 предоставляется Заказчику в течении 3 рабочих дней после завершения этапа 7.