|  |  |
| --- | --- |
| **Общие сведения** | |
| Наименование организации, для которой будет готовиться отчет об аудите | (в скобках приведены примеры заполнения) |
| Контактное лицо, заполнявшее анкету: |  |
| Какая организация предъявляет требования по подтверждению соответствия? | (платежные системы Visa, MasterCard, банк-эквайер, прочие контрагенты) |
| Укажите дату завершения предыдущего аудита по требованиям PCI DSS | (1 декабря 2022) |
| Укажите версию, по которой проводился предыдущий аудит по требованиям PCI DSS | (версия 3.2.1) |
| Требуется ли выполнение дополнительных работ помимо сертификационного QSA-аудита для вашей компании? | (Консультирование, тестирование на проникновение, разработка/доработка нормативных документов, ASV-сканирование) |
| **Описание области оценки** | |
| Укажите количество и адреса площадок, где располагаются ресурсы обрабатывающие данные карт и персонал (ЦОДы, помещения Компании) | (офис по адресу …,  2 арендованных помещения в ЦОД по адресам … ) |
| Пользуется ли ваша Компания услугами облачных сервис-провайдеров | (например, модели IaaS или PaaS в ХХХХХ) |
| Какие виды деятельности по обработке данных платежных карт Вы осуществляете? | (Выпуск и обслуживание платежных карт, POS-эквайринг, ATM-эквайринг, e-Commerce эквайринг, любое другое понятное описание) |
| Документирована ли область применения PCI DSS? | (Да/Нет/ Частично ) |
| Документированы ли политики ИБ, регламенты процедуры в соответствии с требованиями PCI DSS? | (Да/Нет/Частично ) |
| Выделены ли ресурсы сети, обрабатывающие платежные карты, в отдельные сетевые сегменты от ресурсов, выполняющих другой функционал? | (Да/Нет) |
| Обрабатываются ли данные платежных карт в ИС за пределами процессинга?  Если обрабатываются - включались ли данные ИС в область оценки? | Не обрабатываются |
| Примерный размер сети компании (количество серверов, рабочих станций и сетевого оборудования): | (менее 10 серверов, 10 – 30, 30 – 50, 50 – 100, более 100) |
| Примерный размер терминальной сети | (100 банкоматов,  2000 платежных терминалов  300 информационно-платежных киосков) |
| Какие виды ОС, СУБД, сетевого оборудования используются в среде обработки данных платежных карт? | (Windows 2016/2022, CentOS, RHEL, Oracle 19c, MS SQL 2016, Cisco IOS) |
| Используются ли в среде обработки данных платежных карт средства виртуализации? Какие? | (Да, VMware ESXi 6.7) |
| Какие виды прикладного ПО используются для обработки данных платежных карт?  Используется ли программное обеспечение собственной разработки? | (Way4 Cards, SmartVisa SVFE, Compass Plus TWO/TWCMS/TWA, Tieto RTPS, TSYS Prime/Online, собственная разработка) |
| Используются ли для предоставления доступа к среде данных платежных карт терминальные серверы? | (Да, Citrix XenApp, Windows Terminal Services) |
| Укажите количество внешних IP-адресов, расчтета ASV-сканирования | (10 IP-адресов) |
| Укажите дату проведения последнего тестирования на проникновение | (1 ноября 2020) |
| Укажите дату проведения последнего анализа рисков информационной безопасности | (15 ноября 2020) |
| Приведите перечень используемых средств защиты (желательно с указанием вендора) | (МЭ – FortiGate, SIEM – ELK, Антивирус – KES, сканер уязвимостей – Xspider, …) |