Матрица разграничения зон ответственности с клиентами облачной платформы Evolution Public при выполнении требований стандарта безопасности PCI DSS 4.0.1

Москва 2026

Содержание

Перечень сокращений и терминов

API – от англ. Application Programming Interface – интерфейс программирования приложения

CDE – от англ. Cardholder Data Environment - среда данных держателей карт

IaaS – от англ. Infrastructure as a Service – инфраструктура как услуга

PaaS – от англ. Platform as a Service – платформа как услуга

PCI DSS – от англ. Payment Card Industry Data Security Standard - стандарт безопасности данных индустрии платежных карт

API – набор правил и протоколов, который позволяет разным программным приложениям обмениваться данными и взаимодействовать друг с другом, работая как посредник или переводчик между ними без необходимости знать внутреннюю реализацию каждого сервиса.

CDE - критически важная информация (PAN, имя, срок действия), обрабатываемая, хранящаяся или передаваемая в рамках систем, соответствующих стандарту PCI DSS.

IaaS – модель облачных вычислений, где поставщик предоставляет клиентам доступ к базовым IT-ресурсам (виртуальным серверам, хранилищам, сетям) через интернет по подписке, оплачиваемой по факту использования, что позволяет компаниям арендовать и масштабировать IT-инфраструктуру без покупки физического оборудования, сохраняя при этом контроль над операционными системами и приложениями.

PaaS – модель облачных вычислений, предоставляющая разработчикам готовую среду для создания, тестирования, развертывания и управления приложениями, включая операционные системы, базы данных, серверы и инструменты, при этом провайдер управляет всей базовой инфраструктурой, позволяя разработчикам сосредоточиться на коде. Это избавляет от забот о покупке, настройке и поддержке оборудования, снижая затраты и ускоряя разработку.

PCI DSS - международный стандарт безопасности данных платежных карт, обязательный для всех организаций, которые хранят, обрабатывают или передают данные держателей карт (Visa, Mastercard, МИР, и др.).

QSA-аудитор (Qualified Security Assessor) - аккредитованный Советом по стандартам безопасности PCI эксперт, уполномоченный проводить независимую проверку соответствия инфраструктуры организации стандарту безопасности данных индустрии платежных карт PCI DSS

Предупреждение об исключительных правах и конфиденциальной информации

Исключительные права на все результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана (интеллектуальная собственность), используемые при разработке, поддержке и эксплуатации облачной платформы Cloud.ru Evolution Public (далее - платформа Evolution), включая, но не ограничиваясь, программы для электронной вычислительной машины, базы данных, изображения, тексты, другие произведения, а также изобретения, полезные модели, товарные знаки, знаки обслуживания, коммерческие обозначения и фирменные наименования, принадлежат ООО «Облачные технологии».

Использование результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации в целях, не связанных с разработкой, поддержкой и эксплуатацией платформы Evolution, не допускается без получения предварительного согласия правообладателя.

Отношения ООО «Облачные технологии» с лицами, привлекаемыми для разработки, поддержки и эксплуатации платформы Evolution, регулируются законодательством Российской Федерации и заключаемыми в соответствии с ним трудовыми и/или гражданско-правовыми договорами (соглашениями). Нарушение требований об охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, а равно как и конфиденциальной информации, влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Контактная информация ООО «Облачные технологии»

Контакты технической поддержки:

Тел. 8-800-444-24-99

E-mail: support@cloud.ru

Контакты офиса:

Тел. 8 495 260-10-82

Адрес: 117312, Москва, ул. Вавилова, д. 23, стр. 1 комната № 1.207

Введение

Платформа Evolution является собственной разработкой ООО «Облачные технологии» и представляет собой платформу виртуализации, состоящую из множества компонент и подсистем, позволяющую использовать набор сервисов по моделям Infrastructure as a Service (далее – IaaS) и Platform as a Service (далее – PaaS) в целях выполнения задач коммерческого публичного и частного облака.

Для создания и управления облачными ресурсами пользователь использует Личный кабинет как единую точку доступа к сервисам, контролю затрат, управлению доступами и поддержке.

Клиенты, которые хотят соответствовать стандарту безопасности данных индустрии платежных карт (далее - PCI DSS) на базе компонентов платформы Evolution, должны использовать настоящий документ.

Документ описывает разделение ответственности за выполнение требований PCI DSS. Часть требований выполняет платформа Evolution, часть должен выполнить Клиент, часть требований является обоюдной ответственностью сторон. Разделение ответственности за выполнение большинства требований каждого раздела PCI DSS в зависимости от используемой модели облачных сервисов.

Рекомендуемая последовательность действий Клиента для соответствия требованиям PCI DSS:

- изучить настоящий документ, четко понимать свою зону ответственности.
- построить инфраструктуру, обрабатывающую данные платежных карт (CDE) на платформе Evolution.
- выполнить требования PCI DSS в зоне ответственности Клиента.
- выбрать QSA-аудитора и провести аудит инфраструктуры, развернутой на платформе Evolution, на соответствие требованиям PCI DSS.

1 Сервисы платформы Evolution

Таблица 1 содержит перечень сервисов платформы Evolution и их краткое описание.

Таблица 1 - Перечень сервисов платформы Evolution

Наименование сервиса	Назначение
API Gateway	Высокопроизводительный, доступный и безопасный сервис размещения (API), который помогает создавать, разворачивать программные интерфейсы приложения в любом масштабе и управлять ими
Application Load Balancer (L7 load balancers)	Сервис, позволяющий управлять сетевыми балансировщиками нагрузки
Cloud DNS (Domain name management)	Управляемый сервис обслуживания DNS-зон, который позволяет создавать и управлять доменными зонами и их ресурсными записями без необходимости развертывания собственных DNS-серверов
Cloud DirectConnect	Сервис, который позволяет создать выделенный канал связи с гарантированной пропускной способностью
Compute Cloud (Virtual machines)	Сервис, который управляет виртуализацией, взаимодействует с другими службами для создания экземпляров виртуальных машин. Инкапсулирует клиентские виртуальные машины для рабочей нагрузки, а также виртуальных машин для работы Managed Kubernetes
SDS (Software-defined storage – block storage)	Сервис создания логического уровня управления ресурсами хранения. Позволяет программно объединять диски в единое хранилище, которое оптимизировано для хранения больших объемов данных, обеспечивает их репликацию и высокую доступность
Network Load Balancer (L3-L4 load balancers)	Сервис, который реализует работу сетей и распределение нагрузки
Object Storage (S3)	Сервис объектного хранилища
Virtual Private Cloud (Cloud network management)	Сервис сетевой изоляции виртуальных частных облаков "доменов" внутри пользовательской инфраструктуры
Bare Metal	Сервис аренды физических серверов для систем, которым требуется доступ к аппаратной части
ContainerApps	Сервис для запуска контейнерных приложений в облаке, без знаний Kubernetes и создания виртуальных машин

Artifact Registry	Сервис для версионирования, хранения и распространения Docker-образов
Managed Kubernetes	Сервис управления кластерами Kubernetes. Позволяет автоматически развертывать контейнеризированные приложения и создавать кластеры Kubernetes
Managed Service for PostgreSQL	Сервис для создания кластеров реляционной СУБД PostgreSQL® и управления ими
Pangolin	Сервис для развертывания и управления кластерами Pangolin
Corax	Сервис для развертывания и управления кластерами Corax* в инфраструктуре платформы Evolution. *Corax - программный брокер сообщений, представляющий собой распределенную, отказоустойчивую, реплицированную и легко масштабируемую систему передачи сообщений. Работает по принципу «публикация-подписка».
ClickHouse	Сервис для создания и управления кластерами ClickHouse
MySQL	Сервис для развертывания и управления MySQL
MongoDB	Сервис для создания и управления кластерами MongoDB
Apache Kafka	Сервис для создания и управления кластерами Kafka
ArenaDataDB	Сервис предназначен для хранения и обработки больших объемов структурированных и полуструктурированных данных
AIRFlow	Сервис для оркестрации и мониторинга задач (ETL, ML, обработка данных и др.), который позволяет автоматизировать, планировать и отслеживать сложные пайплайны
BI	Сервис для визуализации и анализа данных из различных источников
Spark	Сервис, который позволяет развернуть кластерное вычислительное решение на основе Apache Spark для распределенной обработки данных.
Trino	Сервис, который предоставляет массивно-параллельный аналитический SQL-движок для обработки больших объемов данных из разных источников
Redis	Сервис для создания и управления кластерами Redis

2 Верхнеуровневое распределение ответственности

Таблица 2 содержит верхнеуровневую (обобщенную) информацию о разделении ответственности в зависимости от используемой модели облачных сервисов.

Таблица 2 - Верхнеуровневое распределение ответственности в зависимости от используемой модели облачных сервисов

Набор требований PCI DSS		**Разделение ответственности**	
		IaaS	**PaaS**
1	Install and Maintain Network Security Controls	Обоюдная	Обоюдная
2	Apply Secure Configurations to All System Components	Обоюдная	Обоюдная
3	Protect Stored Account Data	Обоюдная	Обоюдная
4	Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	Обоюдная	Обоюдная
5	Protect All Systems and Networks from Malicious Software	Обоюдная	Обоюдная
6	Develop and Maintain Secure Systems and Software	Обоюдная	Обоюдная
7	Restrict Access to System Components and Cardholder Data by Business Need to Know	Обоюдная	Обоюдная
8	Identify Users and Authenticate Access to System Components	Обоюдная	Обоюдная
9	Restrict Physical Access to Cardholder Data	Обоюдная	Обоюдная
10	Log and Monitor All Access to System Components and Cardholder Data	Обоюдная	Обоюдная
11	Test Security of Systems and Networks Regularly	Обоюдная	Обоюдная
12	Support Information Security with Organizational Policies and Programs	Обоюдная	Обоюдная
A1	Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers	Платформа Evolution	Платформа Evolution
A2	Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for CardPresent POS POI Terminal Connections	Клиент	Клиент
A3	Appendix A3: Designated Entities Supplemental Validation (DESV)	Обоюдная (в случае применимости)	Обоюдная (в случае применимости)

3 Соотношение предоставляемых платформой Evolution сервисов с моделью облачных сервисов

Таблица 3 содержит перечень сервисов и их отношение к модели предоставления сервиса.

Таблица 3 - Соотношение предоставляемых платформой Evolution сервисов с моделью облачных сервисов

Наименование сервиса	Используемая модель предоставления сервиса
API Gateway	IaaS
Application Load Balancer (L7 load balancers)	IaaS
Cloud DNS (Domain name management)	IaaS
Cloud DirectConnect	IaaS
Compute Cloud (Virtual machines)	IaaS
SDS (Software-defined storage – block storage)	IaaS
Network Load Balancer (L3-L4 load balancers)	IaaS
Object Storage (S3)	IaaS
Virtual Private Cloud (Cloud network management)	IaaS
Bare Metal	IaaS
ContainerApps	PaaS
Artifact Registry	PaaS
Managed Kubernetes	PaaS
Managed Service for PostgreSQL	PaaS
Pangolin	PaaS
Corax	PaaS
ClickHouse	PaaS
MySQL	PaaS
MongoDB	PaaS
Apache Kafka	PaaS
ArenaDataDB	PaaS
AIRFlow	PaaS
BI	PaaS
Spark	PaaS
Trino	PaaS
Redis	PaaS

4 Детальная матрица разграничения зон ответственности

Текущий раздел содержит подробные данные о разграничении зон ответственности.

4.1 Build and Maintain a Secure Network and Systems

Requirement 1: Install and Maintain Network Security Controls

PCI DSS Requirements	Платформа Evolution	Клиент
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood		
1.1.1 All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Платформа Evolution, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за документирование и выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.
1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части распределения ролей, обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения ролей, обязанностей и ответственности за обеспечение ИБ для компонентов, развернутых на платформе Evolution.
1.2 Network security controls (NSCs) are configured and maintained		
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	Платформа Evolution отвечает за обеспечение безопасности согласно требованиям PCI DSS для	Клиент отвечает за реализацию процессов и процедур в соответствии с требованиями PCI

1.2.2 All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.	сервисов в области оценки, в том числе безопасное хранение конфигураций сетевых устройств.	DSS для компонентов, развернутых на платформе Evolution, а именно: • внедрение процедур и подготовку необходимой внутренней документации в части управления межсетевыми экранами (МЭ) и сетевым оборудованием; • конфигурацию настроек сетевых компонентов Evolution; • управление виртуальными сетями; • управление МЭ; • безопасное хранение конфигураций сетевых устройств • используемый набор сервисов, протоколов и портов; • управление группами безопасности.
1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.		
1.2.4 An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment.		
1.2.5 All services, protocols, and ports allowed are identified, approved, and have a defined business need.		
1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.		
1.2.7 Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.		
1.2.8 Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations.		
1.3 Network access to and from the cardholder data environment is restricted		
1.3.1 Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	Платформа Evolution обеспечивает для сервисов в области оценки межсетевое экранирование и	Клиент отвечает за реализацию ограничений сетевого трафика в соответствии с требованиями PCI

1.3.2 Outbound traffic from the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	процессы управления им в соответствии с требованиями PCI DSS. В инфраструктуре платформы Evolution используется межсетевое экранирование (МЭ) на разных уровнях.	DSS для компонентов, развернутых на платформе Evolution: • архитектуру проекта и конфигурацию настроек сетевых компонентов Evolution; • управление клиентскими виртуальными сетями; • управление МЭ и маршрутизаторами; • управление группами безопасности.
1.3.3 NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE.		
1.4 Network connections between trusted and untrusted networks are controlled		
1.4.1 NSCs are implemented between trusted and untrusted networks.	Платформа Evolution обеспечивает для сервисов в области оценки межсетевое экранирование и процессы управления им в соответствии с требованиями PCI DSS. В инфраструктуре платформы Evolution реализован контроль исходящего и входящего трафика средствами МЭ с контролем состояния соединений, а также реализованы меры антиспуфинга.	Клиент отвечает за реализацию ограничений сетевого трафика в соответствии с требованиями PCI DSS для компонентов, развернутых на платформе Evolution, включая конфигурирование клиентских сетей таким образом, чтобы серверы баз данных, в которых могут храниться данные платежных карт, размещались во внутренних сегментах виртуальных сред, недоступных напрямую из недоверенных сетей.
1.4.2 Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied.		
1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.		
1.4.4 System components that store cardholder data are not directly accessible from untrusted networks		
1.4.5 The disclosure of internal IP addresses and routing information is limited to only authorized parties.		

1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated		
1.5.1 Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	Платформа Evolution отвечает за безопасность рабочих станций своих пользователей, имеющих доступ к компонентам платформы Evolution.	Клиент отвечает за установку средств защиты информации и управление ими для всех рабочих мест пользователей, которые имеют доступ к компонентам платформы Evolution, задействованным в обработке данных платежных карт.

Requirement 2: Apply Secure Configurations to All System Components

PCI DSS Requirements	Платформа Evolution	Клиент
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood		
2.1.1 All security policies and operational procedures that are identified in Requirement 2 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Платформа Evolution, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.
2.1.2 Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развернутых на платформе Evolution.

2.2 System components are configured and managed securely		
2.2.1 Configuration standards are developed, implemented, and maintained to: • Cover all system components.	Платформа Evolution отвечает за выполнение требований PCI DSS для компонентов, обеспечивающих	Клиент отвечает за настройки безопасности для компонентов, развернутых на платформе Evolution:
• Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.	Функционирование сервисов в области оценки.	• операционных систем; • баз данных (за исключением PAAS-сервисов); • прикладного ПО; • других компонентов и сервисов, включенных Клиентом в область оценки. Клиент отвечает за разделение ресурсов, реализующих функции различных уровней защиты, для компонентов, развернутых на платформе Evolution.
2.2.2 Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled.		
2.2.3 Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component, OR • Primary functions with differing security levels that exist on the same system component are isolated from each other, OR • Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.		

2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.		
2.2.5 If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.		
2.2.6 System security parameters are configured to prevent misuse.		
2.2.7 All non-console administrative access is encrypted using strong cryptography.	Платформа Evolution обеспечивает шифрование любого неконсольного административного доступа для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за внедрение безопасных протоколов и стойкой криптографии для доступа к компонентам, развернутым на платформе Evolution.
2.3 Wireless environments are configured and managed securely		
2.3.1 For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults. • Any other security-related wireless vendor defaults.	Требование неприменимо. Платформа Evolution не использует беспроводные сети для передачи данных пользователей.	Клиент отвечает за настройку параметров безопасности используемых беспроводных сред.
2.3.2 For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: • Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. • Whenever a key is suspected of or known to be compromised.		

4.2 Protect Account Data

Requirement 3: Protect Stored Account Data

PCI DSS Requirements	Платформа Evolution	Клиент
3.1 Processes and mechanisms for protecting stored account data are defined and understood		
3.1.1 All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Платформа Evolution, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.
3.1.2 Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развернутых на платформе Evolution.
3.2 Storage of account data is kept to a minimum		
3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.	Требование неприменимо. Платформа Evolution самостоятельно не обрабатывает данные платежных карт.	Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе данных платежных карт.

• Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.		
3.3 Sensitive authentication data (SAD) is not stored after authorization		
3.3.1 SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.	Требование неприменимо. Платформа Evolution самостоятельно не обрабатывает данные платежных карт.	Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе данных платежных карт.
3.3.2 SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.		
3.3.3 Additional requirement for issuers and companies that support issuing services and store sensitive authentication data: Any storage of sensitive authentication data is: • Limited to that which is needed for a legitimate issuing business need and is secured. • Encrypted using strong cryptography. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.		
3.4 Access to displays of full PAN and ability to copy PAN is restricted		
3.4.1 PAN is masked when displayed (the BIN and last four	Требование неприменимо. Платформа	Клиент отвечает за процессы

digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.	Evolution самостоятельно не обрабатывает данные платежных карт.	обработки, хранения и уничтожения своих данных, в том числе данных платежных карт.
3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.		
3.5 Primary account number (PAN) is secured wherever it is stored		
3.5.1 PAN is rendered unreadable anywhere it is stored by using any of the following approaches: • One-way hashes based on strong cryptography of the entire PAN. • Truncation (hashing cannot be used to replace the truncated segment of PAN). – If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN. • Index tokens. • Strong cryptography with associated key- management processes and procedures.	Требование неприменимо. Платформа Evolution самостоятельно не обрабатывает данные платежных карт.	Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе данных платежных карт.
3.6 Cryptographic keys used to protect stored account data are secured		
3.6.1 Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: • Access to keys is restricted to the fewest number of custodians necessary.	Платформа Evolution предоставляет сервис управления ключевой информацией. Документация сервиса описывает, способы его применения. Платформа Evolution не осуществляет	Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе использование шифрования. Клиент отвечает за процедуры

• Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms.	самостоятельные операции: • Генерации ключевой информации; • Управления доступом к ключевой информации; • Удаления или вывода из обращения ключевой информации; • Шифрования данных в системах клиентов.	управления ключами шифрования данных. Клиент может использовать сервис управления ключевой информацией, и самостоятельно осуществляет его настройку.
3.6.1.1 Additional requirement for service providers only: A documented description of the cryptographic architecture is maintained that includes: • Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. • Preventing the use of the same cryptographic keys in production and test environments. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. • Description of the key usage for each key. • Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4.		
3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented		
3.7.1 Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	Платформа Evolution предоставляет сервис управления ключевой информацией. Документация сервиса описывает, способы его применения. Платформа Evolution не осуществляет	Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе использование шифрования. Клиент отвечает за процедуры
3.7.2 Key-management policies and procedures are implemented to include secure distribution of cryptographic		

keys used to protect stored account data.	самостоятельные операции: • Генерации ключевой информации; • Управления доступом к ключевой информации; • Удаления или вывода из обращения ключевой информации; • Шифрования данных в системах клиентов.	управления ключами шифрования данных. Клиент может использовать сервис управления ключевой информацией, и самостоятельно осуществляет его настройку.
3.7.3 Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.		
3.7.4 Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following: • A defined cryptoperiod for each key type in use. • A process for key changes at the end of the defined cryptoperiod.		
3.7.5 Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: • The key has reached the end of its defined cryptoperiod. • The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. • The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations.		
3.7.6 Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented include		

managing these operations using split knowledge and dual control.		
3.7.7 Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.		
3.7.8 Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key- custodian responsibilities.		
3.7.9 Additional requirement for service providers only: Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider's customers.		

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

PCI DSS Requirements	Платформа Evolution	Клиент
4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented		
4.1.1 All security policies and operational procedures that are identified in Requirement 4 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Платформа Evolution, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.
4.1.2 Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части	Клиент отвечает за выполнение требований PCI

	распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развернутых на платформе Evolution.
4.2 PAN is protected with strong cryptography during transmission		
4.2.1 Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. This bullet is a best practice until its effective date; refer to applicability notes below for details. • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. • The encryption strength is appropriate for the encryption methodology in use.	Платформа Evolution использует безопасные криптографические протоколы, обеспечивающие защиту данных при передаче.	Клиент отвечает за процессы безопасной передачи данных платежных карт, включая использование безопасных протоколов и шифрования.
4.2.2 PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.	Требование неприменимо. Платформа Evolution самостоятельно не обрабатывает данные платежных карт и не передает данные пользователей в открытом виде.	Клиент отвечает за приведение карточных данных в нечитаемый вид в случае использования технологий обмена мгновенными сообщениями.

4.3 Maintain a Vulnerability Management Program

Requirement 5: Protect All Systems and Networks from Malicious Software

PCI DSS Requirements	Платформа Evolution	Клиент
5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.		
5.1.1 All security policies and operational procedures that are identified in Requirement 5 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Платформа Evolution, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.
5.1.2 Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развернутых на платформе Evolution.
5.2 Malicious software (malware) is prevented, or detected and addressed		
5.2.1 An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.	Платформа Evolution отвечает за функционирование антивирусного программного обеспечения для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за процессы защиты от вредоносного ПО для компонентов, развернутых на платформе Evolution и подверженных вирусному заражению.
5.2.2 The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.		
5.2.3 Any system components that are not at risk for malware are		

evaluated periodically to include the following: • A documented list of all system components not at risk for malware. • Identification and evaluation of evolving malware threats for those system components. • Confirmation whether such system components continue to not require anti-malware protection.		
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored		
5.3.1 The anti-malware solution(s) is kept current via automatic updates.	Платформа Evolution отвечает за функционирование антивирусного программного обеспечения для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за процессы защиты от вредоносного ПО для компонентов, развернутых на платформе Evolution и подверженных вирусному заражению.
5.3.2 The anti-malware solution(s): • Performs periodic scans and active or real-time scans. OR • Performs continuous behavioral analysis of systems or processes.		
5.3.3 For removable electronic media, the anti- malware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted, OR • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.	Требование неприменимо. Платформа Evolution не передает данные с использованием съемных носителей.	Клиент отвечает за выполнение необходимых процедур для защиты компонентов, в том числе съемных носителей, обрабатывающих данные платежных карт, от вредоносного ПО.
5.3.4 Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	Платформа Evolution отвечает за функционирование антивирусного программного обеспечения для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за процессы защиты от вредоносного ПО для компонентов, развернутых на платформе Evolution и подверженных вирусному заражению.
5.3.5 Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.		

5.4 Anti-phishing mechanisms protect users against phishing attacks.		
5.4.1 Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.	Платформа Evolution отвечает за функционирование механизмов защиты от фишинговых атак для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за процессы защиты от фишинговых атак для компонентов, развернутых на платформе Evolution.

Requirement 6: Develop and Maintain Secure Systems and Software

PCI DSS Requirements	Платформа Evolution	Клиент
6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood		
6.1.1 All security policies and operational procedures that are identified in Requirement 6 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Платформа Evolution, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.
6.1.2 Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развернутых на платформе Evolution.
6.2 Bespoke and custom software are developed securely		
6.2.1 Bespoke and custom software are developed securely, as follows:	Требование неприменимо.	Клиент отвечает за выполнение

• Based on industry standards and/or best practices for secure development. • In accordance with PCI DSS (for example, secure authentication and logging). • Incorporating consideration of information security issues during each stage of the software development lifecycle.	Платформа Evolution не осуществляет разработку ПО, взаимодействующего с карточными данными.	требований PCI DSS для процессов разработки своего ПО.
6.2.2 Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: • On software security relevant to their job function and development languages. • Including secure software design and secure coding techniques. • Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.		
6.2.3 Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: • Code reviews ensure code is developed according to secure coding guidelines. • Code reviews look for both existing and emerging software vulnerabilities. • Appropriate corrections are implemented prior to release.		
6.2.4 Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: • Injection attacks, including SQL, LDAP , XPath, or other command, parameter, object, fault, or injection-type flaws. • Attacks on data and data structures, including attempts to manipulate		

buffers, pointers, input data, or shared data. • Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. • Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client- side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). • Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. • Attacks via any “high-risk” vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.		
6.3 Security vulnerabilities are identified and addressed		
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Платформа Evolution отвечает за процессы управления уязвимостями для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за процессы управления уязвимостями для компонентов, развернутых на платформе Evolution.
6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is		

maintained to facilitate vulnerability and patch management.		
6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).		
6.4 Public-facing web applications are protected against attacks		
6.4.1 For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections OR • Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent web- based attacks. – Actively running and up to date as applicable.	Платформа Evolution отвечает за соблюдение требования PCI DSS в части защиты общедоступных веб-приложений для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за конфигурацию и защиту собственных общедоступных веб-приложений, развернутых на платформе Evolution.

– Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated.		
6.4.2 For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated.		
6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written justification as to why each is necessary.	Требование неприменимо. Платформа Evolution не работает с карточными данными.	Клиент отвечает за конфигурацию и защиту собственных платежных страниц, развернутых на платформе Evolution.
6.5 Changes to all system components are managed securely		
6.5.1 Changes to all system components in the production environment are made according to established procedures that include: • Reason for, and description of, the change. • Documentation of security impact. • Documented change approval by authorized parties. • Testing to verify that the change does not adversely impact system security. • For bespoke and custom software changes, all updates are tested for	Платформа Evolution отвечает за выполнение требований PCI DSS для процедур контроля изменений компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в отношении всех изменений в компонентах, развернутых на платформе Evolution.

compliance with Requirement 6.2.4 before being deployed into production. • Procedures to address failures and return to a secure state.		
6.5.2 Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.		
6.5.3 Pre-production environments are separated from production environments and the separation is enforced with access controls.		
6.5.4 Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.		
6.5.5 Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.		
6.5.6 Test data and test accounts are removed from system components before the system goes into production.		

4.4 Implement Strong Access Control Measures

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know

PCI DSS Requirements	Платформа Evolution	Клиент
7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood		
7.1.1 All security policies and operational procedures that are identified in Requirement 7 are: • Documented. • Kept up to date.	Платформа Evolution, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.

• In use. • Known to all affected parties.		
7.1.2 Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развернутых на платформе Evolution.
7.2 Access to system components and data is appropriately defined and assigned		
7.2.1 An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части контроля и управления доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за процессы контроля и управления доступом к компонентам, развернутым на платформе Evolution.
7.2.2 Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities.		
7.2.3 Required privileges are approved by authorized personnel.		
7.2.4 All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months. • To ensure user accounts and access remain appropriate based on		

job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.		
7.2.5 All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.		
7.2.6 All user access to query repositories of stored cardholder data is restricted as follows: • Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. • Only the responsible administrator(s) can directly access or query repositories of stored CHD.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части аутентификации и управления доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части использования механизмов аутентификации и управления доступом для компонентов, развернутых на платформе Evolution.
7.3 Access to system components and data is managed via an access control system(s)		
7.3.1 An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части контроля и управления доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за процессы контроля и управления доступом к компонентам, развернутым на платформе Evolution.
7.3.2 The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.		
7.3.3 The access control system(s) is set to "deny all" by default.		

Requirement 8: Identify Users and Authenticate Access to System Components

PCI DSS Requirements	Платформа Evolution	Клиент
8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood		

8.1.1 All security policies and operational procedures that are identified in Requirement 8 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Платформа Evolution, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.
8.1.2 Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развернутых на платформе Evolution.
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle		
8.2.1 All users are assigned a unique ID before access to system components or cardholder data is allowed.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части контроля, аутентификации и управления доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за процессы контроля, механизмов аутентификации и управления доступом к компонентам, развернутым на платформе Evolution.
8.2.2 Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: • Account use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.		

8.2.3 Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.	Требование неприменимо. По умолчанию сотрудники Evolution не имеют доступа к ресурсам Клиентов, расположенным на платформе Evolution.	Клиент в случае, если является поставщиком услуг, отвечает за использование уникальных аутентификационных данных в системах, развернутых на платформе Evolution
8.2.4 Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: • Authorized with the appropriate approval. • Implemented with only the privileges specified on the documented approval.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части контроля и управления доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за процессы контроля и управления доступом к компонентам, развернутым на платформе Evolution.
8.2.5 Access for terminated users is immediately revoked.		
8.2.6 Inactive user accounts are removed or disabled within 90 days of inactivity.		
8.2.7 Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: • Enabled only during the time period needed and disabled when not in use. • Use is monitored for unexpected activity.		
8.2.8 If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.		
8.3 Strong authentication for users and administrators is established and managed		
8.3.1 All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части аутентификации и управления доступом для компонентов, обеспечивающих	Клиент отвечает за выполнение требований PCI DSS в части использования механизмов аутентификации и управления доступом для компонентов,

• Something you are, such as a biometric element.	функционирование сервисов в области оценки.	развернутых на платформе Evolution.
8.3.2 Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.		
8.3.3 User identity is verified before modifying any authentication factor.		
8.3.4 Invalid authentication attempts are limited by: • Locking out the user ID after not more than 10 attempts. • Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.		
8.3.5 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: • Set to a unique value for first-time use and upon reset. • Forced to be changed immediately after the first use.		
8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). • Contain both numeric and alphabetic characters.		
8.3.7 Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.		
8.3.8 Authentication policies and procedures are documented and communicated to all users including: • Guidance on selecting strong authentication factors. • Guidance for how users should protect their authentication factors. • Instructions not to reuse previously used passwords/passphrases. • Instructions to change passwords/passphrases if there is any		

suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.		
8.3.9 If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.		
8.3.10 Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single- factor authentication implementation), then guidance is provided to customer users including: • Guidance for customers to change their user passwords/passphrases periodically. • Guidance as to when, and under what circumstances, passwords/passphrases are to be changed.	Требование неприменимо. Платформа Evolution не осуществляет действий с карточными данными	Клиент в случае, если является поставщиком услуг, отвечает за формирование и предоставление инструкций клиентов по работе с аутентификационными данными, которые используются в его системах, развернутых на платформе Evolution
8.3.10.1 Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.		
8.3.11 Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: • Factors are assigned to an individual user and not shared among	Платформа Evolution отвечает за соблюдение требований PCI DSS в части аутентификации и	Клиент отвечает за выполнение требований PCI DSS в части использования механизмов

multiple users. • Physical and/or logical controls ensure only the intended user can use that factor to gain access.	управления доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	аутентификации и управления доступом для компонентов, развернутых на платформе Evolution.
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE		
8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части многофакторной аутентификации и управления доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части использования многофакторной аутентификации для компонентов, развернутых на платформе Evolution.
8.4.2 MFA is implemented for all access into the CDE.		
8.4.3 MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: • All remote access by all personnel, both users and administrators, originating from outside the entity's network. • All remote access by third parties and vendors.		
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse		
8.5.1 MFA systems are implemented as follows: • The MFA system is not susceptible to replay attacks. • MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. • At least two different types of authentication factors are used. • Success of all authentication factors is required before access is granted.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части многофакторной аутентификации и управления доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части использования многофакторной аутентификации для компонентов, развернутых на платформе Evolution.
8.6 Use of application and system accounts and associated authentication factors is strictly managed		
8.6.1 If accounts used by systems or applications can be used for interactive login, they are managed as follows:	Платформа Evolution отвечает за соблюдение требований PCI DSS в	Клиент отвечает за выполнение требований PCI DSS в части

• Interactive use is prevented unless needed for an exceptional circumstance. • Interactive use is limited to the time needed for the exceptional circumstance. • Business justification for interactive use is documented. • Interactive use is explicitly approved by management. • Individual user identity is confirmed before access to account is granted. • Every action taken is attributable to an individual user.	части многофакторной аутентификации и управления доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	использования многофакторной аутентификации для компонентов, развернутых на платформе Evolution.
8.6.2 Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code.		
8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows: • Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise. • Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases.		

Requirement 9: Restrict Physical Access to Cardholder Data

PCI DSS Requirements	Платформа Evolution	Клиент
9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood		
9.1.1 All security policies and operational procedures that are identified in Requirement 9 are: • Documented.	Платформа Evolution, для сервисов в области оценки, обеспечивает выполнение всех необходимых	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих

• Kept up to date. • In use. • Known to all affected parties.	требований и процедур согласно требованиям PCI DSS.	данные платежных карт.
9.1.2 Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развернутых на платформе Evolution.
9.2 Physical access controls manage entry into facilities and systems containing cardholder data		
9.2.1 Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	Платформа Evolution обеспечивает физическую безопасность дата-центров, в которых расположены компоненты, необходимые для функционирования сервисов в области оценки.	Требование неприменимо, кроме случаев расположения системы, относящейся к области действия стандарта PCI DSS в том числе вне инфраструктуры платформы Evolution.
9.2.2 Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.		
9.2.3 Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.		
9.2.4 Access to consoles in sensitive areas is restricted via locking when not in use.		
9.3 Physical access for personnel and visitors is authorized and managed		
9.3.1 Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including: • Identifying personnel. • Managing changes to an individual’s physical access requirements. • Revoking or terminating personnel identification. • Limiting access to the identification process or system to authorized	Платформа Evolution обеспечивает физическую безопасность дата-центров, в которых расположены компоненты, необходимые для функционирования сервисов в области оценки.	Требование неприменимо, кроме случаев расположения системы, относящейся к области действия стандарта PCI DSS в том числе вне инфраструктуры платформы Evolution.

personnel.		
9.3.2 Procedures are implemented for authorizing and managing visitor access to the CDE, including: • Visitors are authorized before entering. • Visitors are escorted at all times. • Visitors are clearly identified and given a badge or other identification that expires. • Visitor badges or other identification visibly distinguishes visitors from personnel.		
9.3.3 Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.		
9.3.4 A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive areas, including: • The visitor's name and the organization represented. • The date and time of the visit. • The name of the personnel authorizing physical access. • Retaining the log for at least three months, unless otherwise restricted by law.		
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed		
9.4.1 All media with cardholder data is physically secured.	Платформа Evolution обеспечивает выполнение требований PCI DSS в части физической безопасности дата-центров и носителей информации, содержащих данные Клиентов, для компонентов, обеспечивающих	Клиент отвечает за защиту физических носителей данных, контроль хранения/уничтожения и управление доступом к носителям данных, если такие применяются в процессах обработки данных платежных карт.
9.4.2 All media with cardholder data is classified in accordance with the sensitivity of the data.		
9.4.3 Media with cardholder data sent outside the facility is secured as follows: • Media sent outside the facility is logged. • Media is sent by secured courier or other delivery method that can		

be accurately tracked. • Offsite tracking logs include details about media location.	функционирование сервисов в области оценки.	
9.4.4 Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).		
9.4.5 Inventory logs of all electronic media with cardholder data are maintained.		
9.4.6 Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. • Materials are stored in secure storage containers prior to destruction.		
9.4.7 Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: • The electronic media is destroyed. • The cardholder data is rendered unrecoverable so that it cannot be reconstructed.		
9.5 Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution		
9.5.1 POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: • Maintaining a list of POI devices. • Periodically inspecting POI devices to look for tampering or unauthorized substitution. • Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Требование неприменимо.	Клиент отвечает за защиту устройств, считывающих данные с платежных карт путем прямого физического взаимодействия с картой.

4.5 Regularly Monitor and Test Networks

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

PCI DSS Requirements	Платформа Evolution	Клиент
10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and understood		
10.1.1 All security policies and operational procedures that are identified in Requirement 10 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Платформа Evolution, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.
10.1.2 Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развернутых на платформе Evolution.
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events		
10.2.1 Audit logs are enabled and active for all system components and cardholder data.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части регистрации необходимых типов событий для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части регистрации необходимых типов событий для компонентов, развернутых на платформе Evolution
10.2.2 Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication.		

• Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol).		
10.3 Audit logs are protected from destruction and unauthorized modifications		
10.3.1 Read access to audit logs files is limited to those with a job-related need.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части защиты журналов регистрации событий для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части защиты журналов регистрации событий для компонентов, развернутых на платформе Evolution.
10.3.2 Audit log files are protected to prevent modifications by individuals.		
10.3.3 Audit log files, including those for external- facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.		
10.3.4 File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.		
10.4 Audit logs are reviewed to identify anomalies or suspicious activity		
10.4.1 The following audit logs are reviewed at least once daily: • All security events. • Logs of all system components that store, process, or transmit CHD and/or SAD. • Logs of all critical system components. Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).	Платформа Evolution отвечает за соблюдение требований PCI DSS в части проверки и анализа зарегистрированных событий для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части проверки и анализа зарегистрированных событий для компонентов, развернутых на платформе Evolution.
10.4.2 Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.		
10.4.3 Exceptions and anomalies identified during the review process		

are addressed.		
10.5 Audit log history is retained and available for analysis		
10.5.1 Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части хранения зарегистрированных событий для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части хранения зарегистрированных событий для компонентов, развернутых на платформе Evolution.
10.6 Time-synchronization mechanisms support consistent time settings across all systems		
10.6.1 System clocks and time are synchronized using time-synchronization technology.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части синхронизации времени для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части синхронизации времени для компонентов, развернутых на платформе Evolution.
10.6.2 Systems are configured to the correct and consistent time as follows: • One or more designated time servers are in use. • Only the designated central time server(s) receives time from external sources. • Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). • The designated time server(s) accept time updates only from specific industry-accepted external sources. • Where there is more than one designated time server, the time servers peer with one another to keep accurate time. • Internal systems receive time information only from designated central time server(s).		
10.6.3 Time synchronization settings and data are protected as follows: • Access to time data is restricted to only personnel with a business		

need. • Any changes to time settings on critical systems are logged, monitored, and reviewed.		
10.7 Failures of critical security control systems are detected, reported, and responded to promptly		
10.7.1 Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).	Платформа Evolution отвечает за соблюдение требований PCI DSS в части фиксации и выявления отказов систем контроля безопасности для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент, являющийся поставщиком услуг, обеспечивает соблюдение требований PCI DSS в части фиксации и выявления отказов систем контроля безопасности для компонентов, развернутых на платформе Evolution
10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • Change-detection mechanisms. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms.		Клиент отвечает за выполнение требований PCI DSS в части фиксации и выявления отказов систем контроля безопасности для компонентов, развернутых на платформе Evolution.

• Segmentation controls (if used). • Audit log review mechanisms. • Automated security testing tools (if used).		
10.7.3 Failures of any critical security controls systems are responded to promptly, including but not limited to: • Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure and documenting required remediation. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls.		

Requirement 11: Test Security of Systems and Networks Regularly

PCI DSS Requirements	Платформа Evolution	Клиент
11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood		
11.1.1 All security policies and operational procedures that are identified in Requirement 11 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Платформа Evolution, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.

11.1.2 Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развернутых на платформе Evolution.
11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed		
11.2.1 Authorized and unauthorized wireless access points are managed as follows: • The presence of wireless (Wi-Fi) access points is tested for, • All authorized and unauthorized wireless access points are detected and identified, • Testing, detection, and identification occurs at least once every three months. • If automated monitoring is used, personnel are notified via generated alerts.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части обнаружения и идентификации авторизованных и неавторизованных беспроводных точек доступа для компонентов, обеспечивающих функционирование сервисов в области оценки.	Требование неприменимо, кроме случаев расположения системы, относящейся к области действия стандарта PCI DSS в том числе вне инфраструктуры платформы Evolution.
11.2.2 An inventory of authorized wireless access points is maintained, including a documented business justification.		
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed		
11.3.1 Internal vulnerability scans are performed as follows: • At least once every three months. • High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are performed that confirm all high- risk and critical	Платформа Evolution отвечает за соблюдение требований PCI DSS в части регулярного проведения внешних ASV-сканирований, внутренних сканирований	Клиент отвечает за выполнение требований PCI DSS в части регулярного проведения внешних ASV-сканирований, внутренних сканирований безопасности, а

vulnerabilities (as noted above) have been resolved. • Scan tool is kept up to date with latest vulnerability information. • Scans are performed by qualified personnel and organizational independence of the tester exists.	безопасности, а также устранения найденных уязвимостей для компонентов, обеспечивающих функционирование сервисов в области оценки.	также устранения найденных уязвимостей для компонентов, развернутых на платформе Evolution.
11.3.2 External vulnerability scans are performed as follows: • At least once every three months. • By a PCI SSC Approved Scanning Vendor (ASV). • Vulnerabilities are resolved and ASV Program • Guide requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.		
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected		
11.4.1 A penetration testing methodology is defined, documented, and implemented by the entity, and includes: • Industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scope- reduction controls. • Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. • Network-layer penetration tests that encompass all components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части регулярного проведения внешних и внутренних тестирований на проникновение, а также устранения найденных недостатков для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части регулярного проведения внешних и внутренних тестирований на проникновение, а также устранения найденных недостатков для компонентов, развернутых на платформе Evolution.

• Retention of penetration testing results and remediation activities results for at least 12 months.		
11.4.2 Internal penetration testing is performed: • Per the entity's defined methodology, • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third-party • Organizational independence of the tester exists (not required to be a QSA or ASV).		
11.4.3 External penetration testing is performed: • Per the entity's defined methodology • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third party • Organizational independence of the tester exists (not required to be a QSA or ASV).		
11.4.4 Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: • In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1. • Penetration testing is repeated to verify the corrections.		
11.4.5 If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every 12 months and after any changes to segmentation controls/methods • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology.		

• Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).		
11.4.6 Additional requirement for service providers only: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every six months and after any changes to segmentation controls/methods. • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. Organizational independence of the tester exists (not required to be a QSA or ASV).		Клиент, являющийся поставщиком услуг, отвечает за выполнение требований PCI DSS в части проведения теста на проникновение для механизмов сегментации, а также устранения найденных недостатков для компонентов, развернутых на платформе Evolution.
11.4.7 Additional requirement for multi-tenant service providers only: Multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4.	В случае необходимости, платформа Evolution оказывает поддержку клиентам при проведении внешнего теста на проникновение.	Требование неприменимо

11.5 Network intrusions and unexpected file changes are detected and responded to		
11.5.1 Intrusion-detection and/or intrusion- prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части использования методов и систем обнаружения/предотвращения вторжений для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части использования методов и систем обнаружения/предотвращения вторжений для компонентов, развернутых на платформе Evolution.
11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.		
11.6 Unauthorized changes on payment pages are detected and responded to		
11.6.1 A change- and tamper-detection mechanism is deployed as follows: • To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. • The mechanism is configured to evaluate the received HTTP header and payment page. • The mechanism functions are performed as follows: – At least once every seven days OR – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	Требование неприменимо. Платформа Evolution не работает с карточными данными.	Клиент отвечает за выполнение требований PCI DSS в части использования механизмов контроля целостности файлов платежных страниц для компонентов, развернутых на платформе Evolution.

4.6 Maintain an Information Security Policy

Requirement 12: Support Information Security with Organizational Policies and Programs

PCI DSS Requirements	Платформа Evolution	Клиент
12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current		
12.1.1 An overall information security policy is: • Established. • Published. • Maintained. • Disseminated to all relevant personnel, as well as to relevant vendors and business partners.	Платформа Evolution отвечает за выполнение требований PCI DSS в части разработки, соблюдения политики безопасности и других процедур обеспечения ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части разработки, соблюдения политики безопасности и других процедур обеспечения ИБ для компонентов, развернутых на платформе Evolution.
12.1.2 The information security policy is: • Reviewed at least once every 12 months. • Updated as needed to reflect changes to business objectives or risks to the environment.		
12.1.3 The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развернутых на платформе Evolution.
12.1.4 Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management.		
12.2 Acceptable use policies for end-user technologies are defined and implemented		
12.2.1 Acceptable use policies for end-user technologies are documented and implemented, including: • Explicit approval by authorized parties.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части использования критичных	Клиент отвечает за выполнение требований PCI DSS в части использования критичных

• Acceptable uses of the technology. • List of products approved by the company for employee use, including hardware and software.	технологий для компонентов, обеспечивающих функционирование сервисов в области оценки.	технологий для компонентов, развернутых на платформе Evolution.
12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed		
12.3.1 Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against. • Identification of factors that contribute to the likelihood and/or impact of a threat being realized. • Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. • Performance of updated risk analyses when needed, as determined by the annual review.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части процедур целевой оценки рисков для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части процедур целевой оценки рисков для компонентов, развернутых на платформе Evolution.
12.3.2 A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: • Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis).		

• Approval of documented evidence by senior management. • Performance of the targeted analysis of risk at least once every 12 months.		
12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.		
12.3.4 Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: • Analysis that the technologies continue to receive security fixes from vendors promptly. • Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance. • Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology. • Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans.		
12.4 PCI DSS compliance is managed		
12.4.1 Additional requirement for service providers only: Responsibility is established by executive management for the protection of cardholder data and a PCI DSS compliance program to	Платформа Evolution отвечает за выполнение программы соответствия требованиям PCI	Клинт, являющийся поставщиком услуг, отвечает за выполнение программы соответствия

include: • Overall accountability for maintaining PCI DSS compliance. • Defining a charter for a PCI DSS compliance program and communication to executive management.	DSS для компонентов, обеспечивающих функционирование сервисов в области оценки.	требованиям PCI DSS для компонентов, развернутых на платформе Evolution.
12.4.2 Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: • Daily log reviews. • Configuration reviews for network security controls. • Applying configuration standards to new systems. • Responding to security alerts. • Change-management processes.	Платформа Evolution отвечает за проведение периодических проверок выполнения требований PCI DSS для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клинт, являющийся поставщиком услуг, отвечает за проведение периодических проверок выполнения требований PCI DSS для компонентов, развернутых на платформе Evolution.
12.5 PCI DSS scope is documented and validated		
12.5.1 An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.	Платформа Evolution обеспечивает выполнение процедур учета для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за ведение журнала учета компонентов, развернутых на платформе Evolution и входящих в область оценки соответствия стандарту PCI DSS.
12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: • Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present,	Платформа Evolution отвечает за документирование и подтверждение области оценки компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за документирование и подтверждение области оценки компонентов, развернутых на платформе Evolution и входящих в область оценки соответствия

and e-commerce). • Updating all data-flow diagrams per Requirement 1.2.4. • Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. • Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. • Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. • Identifying all connections from third-party entities with access to the CDE. • Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.		стандарту PCI DSS.
12.5.2.1 Additional requirement for service providers only: PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2.	Платформа Evolution отвечает за документирование и подтверждение области оценки компонентов, обеспечивающих функционирование сервисов.	Клиент, являющийся поставщиком услуг, отвечает за документирование и подтверждение области оценки компонентов, развернутых на платформе Evolution.
12.5.3 Additional requirement for service providers only: Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management.	Платформа Evolution обеспечивает документирование и анализ влияния значительных изменений в организационной структуре для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент, являющийся поставщиком услуг, обеспечивает документирование и анализ влияния значительных изменений в организационной структуре для компонентов, развернутых на платформе Evolution.

12.6 Security awareness education is an ongoing activity		
12.6.1 A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части обучения сотрудников и повышения их осведомленности о безопасности для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части обучения сотрудников и повышения их осведомленности о безопасности для компонентов, развернутых на платформе Evolution.
12.6.2 The security awareness program is: • Reviewed at least once every 12 months, and • Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's CDE, or the information provided to personnel about their role in protecting cardholder data.		
12.6.3 Personnel receive security awareness training as follows: • Upon hire and at least once every 12 months. • Multiple methods of communication are used. • Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.		
12.7 Personnel are screened to reduce risks from insider threats		
12.7.1 Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части проверки потенциальных сотрудников до их приема на работу в сервисы, входящие в область оценки.	Клиент отвечает за выполнение требований PCI DSS в части проверки потенциальных сотрудников до их приема на работу для компонентов, развернутых на платформе Evolution.
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed		
12.8.1 A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части взаимодействия с сервис-провайдерами, которые могут	Клиент отвечает за выполнение требований PCI DSS в части взаимодействия с сервис-провайдерами, которые могут
12.8.2 Written agreements with TPSPs are maintained as follows:		

• Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.	повлиять на безопасность данных Клиентов.	повлиять на безопасность данных платежных карт.
12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.		
12.8.4 A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.		
12.8.5 Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.		
12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance		
12.9.1 Additional requirement for service providers only: TPSPs acknowledge in writing to customers that they are responsible for the security of account data the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's CDE.	Платформа Evolution заключает с Клиентами договор, в котором явно определена ответственность за безопасность данных.	Требование неприменимо, кроме случаев, когда клиент самостоятельно является поставщиком услуг.
12.9.2 Additional requirement for service providers only: TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request: • PCI DSS compliance status information for any service the TPSP performs on behalf of customers (Requirement 12.8.4). • Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5).		

12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately		
12.10.1 An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • Business recovery and continuity procedures. • Data backup processes. • Analysis of legal requirements for reporting compromises. • Coverage and responses of all critical system components. • Reference or inclusion of incident response procedures from the payment brands.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части реагирования на инциденты и тестирования планов реагирования на инциденты для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части реагирования на инциденты и тестирования планов реагирования на инциденты для компонентов, развернутых на платформе Evolution.
12.10.2 At least once every 12 months, the security incident response plan is: • Reviewed and the content is updated as needed. • Tested, including all elements listed in Requirement 12.10.1.		
12.10.3 Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.		
12.10.4 Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.		
12.10.5 The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to:		

• Intrusion-detection and intrusion-prevention systems. • Network security controls. • Change-detection mechanisms for critical files. • The change-and tamper-detection mechanism for payment pages. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. • Detection of unauthorized wireless access points.		
12.10.6 The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.		
12.10.7 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: • Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Identifying whether sensitive authentication data is stored with PAN. • Determining where the account data came from and how it ended up where it was not expected. • Remediating data leaks or process gaps that resulted in the account data being where it was not expected.	Требование неприменимо. Платформа Evolution не взаимодействует с номерами карт	Клиент отвечает за процедуры реагирования на инциденты, которые должны быть инициированы при обнаружении хранимого PAN в любом месте, где это не ожидается.

4.7 Additional PCI DSS Requirements

Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers

PCI DSS Requirements	Платформа Evolution	Клиент
A1.1 Multi-tenant service providers protect and separate all customer environments and data		
A1.1.1 Logical separation is implemented as follows: • The provider cannot access its customers' environments without	Платформа Evolution отвечает за соблюдение требований PCI DSS в	Требование неприменимо, кроме случаев, когда клиент

authorization. • Customers cannot access the provider's environment without authorization	части предоставления механизмов управления доступом, обеспечивающих изоляцию разных Клиентов, и разграничения сред разных Клиентов.	самостоятельно является "Multi-tenant service provider"
A1.1.2 Controls are implemented such that each customer only has permission to access its own cardholder data and CDE.		
A1.1.3 Controls are implemented such that each customer can only access resources allocated to them.		
A1.1.4 The effectiveness of logical separation controls used to separate customer environments is confirmed at least once every six months via penetration testing.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части регулярного проведения внешних и внутренних тестирований на проникновение, а также устранения найденных недостатков для компонентов, обеспечивающих функционирование сервисов в области оценки.	
A1.2 Multi-tenant service providers facilitate logging and incident response for all customers		
A1.2.1 Audit log capability is enabled for each customer's environment that is consistent with PCI DSS Requirement 10, including: • Logs are enabled for common third-party applications. • Logs are active by default. • Logs are available for review only by the owning customer. • Log locations are clearly communicated to the owning customer. • Log data and availability is consistent with PCI DSS Requirement 10.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части ведения журналов регистрации событий каждого Клиента, с возможностью их выгрузки для хранения в инфраструктуре Клиента	Требование неприменимо, кроме случаев, когда клиент самостоятельно является "Multi-tenant service provider"
A1.2.2 Processes or mechanisms are implemented to support and/or facilitate prompt forensic investigations in the event of a suspected or		

confirmed security incident for any customer.		
A1.2.3 Processes or mechanisms are implemented for reporting and addressing suspected or confirmed security incidents and vulnerabilities, including: • Customers can securely report security incidents and vulnerabilities to the provider. • The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities according to Requirement 6.3.1.	Платформа Evolution отвечает за соблюдение требований PCI DSS в части информирования Клиентов в случае обнаружения и расследования инцидентов ИБ.	Требование неприменимо, кроме случаев, когда клиент самостоятельно является “Multi-tenant service provider”

Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for CardPresent POS POI Terminal Connections

PCI DSS Requirements	Платформа Evolution	Клиент
A2.1 POI terminals using SSL and/or early TLS are confirmed as not susceptible to known SSL/TLS exploits		
A2.1.1 Where POS POI terminals at the merchant or payment acceptance location use SSL and/or early TLS, the entity confirms the devices are not susceptible to any known exploits for those protocols.	Требование неприменимо. Платформа Evolution не использует POS/POI-терминалы.	Клиент отвечает за выполнение требований PCI DSS в части использования безопасных версий используемых протоколов TLS.
A2.1.2 Additional requirement for service providers only: All service providers with existing connection points to POS POI terminals that use SSL and/or early TLS as defined in A2.1 have a formal Risk Mitigation and Migration Plan in place that includes: • Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, and type of environment. • Risk-assessment results and risk-reduction controls in place. • Description of processes to monitor for new vulnerabilities associated with SSL/early TLS. • Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments.		

• Overview of migration project plan to replace SSL/early TLS at a future date.		
A2.1.3 Additional requirement for service providers only: All service providers provide a secure service offering.		