基于 PCI DSS 的

云用户数据安全标准白皮书（简版）

2019 年 7 月

深圳腾讯计算机系统有限公司

腾讯云计算（北京）有限责任公司

艾特赛克（北京）信息技术有限公司

中国云安全与新兴技术安全创新联盟

联合出品

腾讯云

【服务声明】

2019 年 7 月

本文档仅供参考。对于本文档中所描述的信息和内容，腾讯云计算（北京）有限责任公司（以下简称腾讯云）和艾特赛克（北京）信息技术有限公司（以下简称 atsec 中国）不作明示、默示的保证。本文档基于现状编写。在本文档中的信息和意见，包括网址和其他互联网网站参考，均可能会改变，恕不另行通知。您将承担直接引用它的风险。

本文档未授予您任何腾讯产品的任何知识产权的法律权利。您可以复制和使用本文档中的内容作为您内部以参考为目的的使用。

序言

本白皮书基于国际范围内得到最广泛认可和运用的数据安全标准 PCI DSS，提出了数据安全合规建设的方法论，同时也尽可能详细的将合规要求落到实处，特别是 “云服务提供商与云用户的 PCI DSS 合规要求责任分析”，详细的诠释了云服务提供商和云用户在基于 PCI DSS 实施数据安全合规时逐条阐述了各自的责任和具体工作。

数据安全合规并不是一次性工作，产业的技术不断演进发展，同时各个系统组件也会出现新的脆弱性和攻击模型。我们会长期致力于该白皮书以及相关技术的更新，不断监控标准以及技术的更新，从而更好的为产业合规做出我们的贡献。

感谢如下人员在本白皮书编制工作的努力。

主要作者：腾讯 王永霞；atsec 中国 谢继来

参与者：腾讯 代威、周弈良、蒋增增、彭思祥、刘双立; atsec 中国 高向东、白海蔚

感谢腾讯公司领导丁珂、黎巍、杨鹏、董志强的大力支持；

感谢 atsec 中国 PCI 实验室主任刘岩的大力支持。

目录

引言

随着云计算产业的快速发展，云计算在降低成本，简化 IT 运维和管理，集成的安全性，易于部署，简化合规流程等方面的优势越来越明显，产业互联网企业越来越多着手通过使用云计算提供的便捷服务来实现业务目标。PCI DSS 虽然是支付卡行业的数据安全国际标准，但是该标准围绕数据安全的核心要求，提出了一整套完整的规范要求，也称“要求最严格的数据安全标准”。发布十余年以来，该标准得到了全球范围统一且作为在数据安全合规领域的最早的规范要求获得了广泛的认可和实施，推动了数据安全防护水平。

由于云用户和云服务提供商在合规过程中存在责任相互交叠的部分，并且事实上目前并没有一份详细的针对云环境下每个数据安全标准点的责任细分。基于这些问题，本白皮书希望帮助厘清云用户和云服务提供商的安全责任，从而清晰、高效地协助云用户达到基于 PCI DSS 的数据安全标准要求。本文介绍针对的仅是公有云，其他类型的云没有在本文的介绍范围之内。

凭借腾讯集团多年的安全经验和积累，腾讯云为云平台搭建了强大的纵深安全防御体系，数据安全一直是其中至关重要的一环。腾讯云于 2017 年 12 月发布《腾讯云数据安全白皮书》，郑重发布了云端数据保护承诺，以及数据保护六大原则。腾讯云在保障底层云平台安全的同时，通过提供全方位多样化的数据安全功能、工具和控制赋能和助力产业互利网安全，携手客户一起为云端数据构建更好更完善的安全保障体系。

第一章 基于 PCI DSS 的云用户数据安全标准简介

1.1 支付卡产业数据安全标准(PCI DSS)的成立背景

2006 年 VISA 和 MasterCard 联合美国运通、JCB 及 Discover 网络公司，成立了支付卡行业数据安全标准委员会 PCI SSC（Payment Card Industry Security Standards Council)。

为了建立统一的业界标准，最大程度地降低支付卡风险，标准委员会联合制定了旨在严格控制数据存储、传输和处理以保障支付卡用户在线交易安全的数据安全标准，即 PCI DSS 安全认证标准。

支付卡行业数据安全标准(PCI DSS) 旨在促进并增强持卡人的数据安全，便于统一的数据安全标准要求在全球范围内广泛应用，PCI DSS 是目前全球最严格、覆盖安全要求最全面的数据安全认证标准。

1.2 PCI DSS 基本概要内容

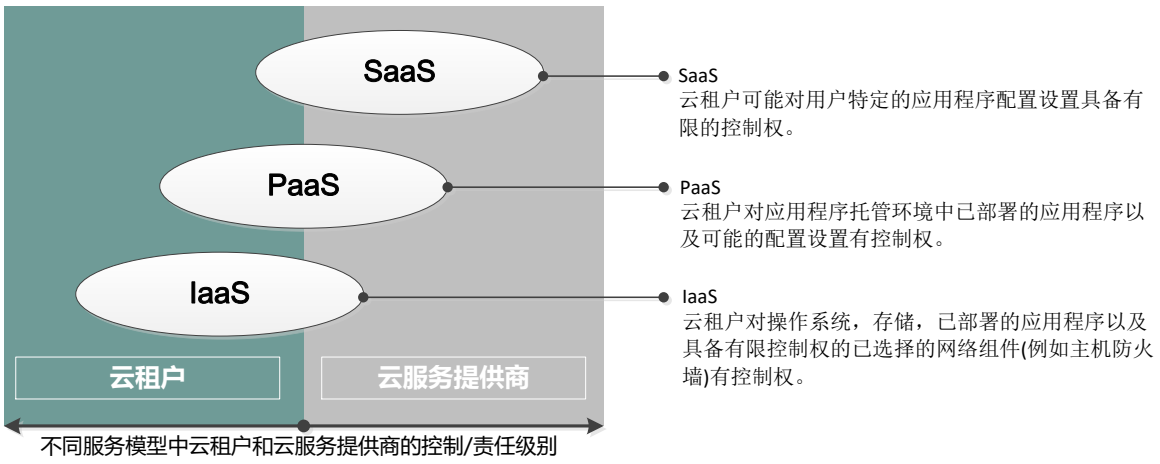
PCI DSS 安全要求适用于所涉及的 “系统组件”，即处理持卡人数据的环境或与之相关的任何网络组件、服务器或应用程序。

PCI DSS 包括 6 个控制域，12 个控制目标。对涉及持卡人数据的存储、处理、传输等过程进行安全保护，以防止持卡人数据被泄露。

涉及 PCI DSS 合规的机构，需要每年对持卡人数据环境范围内存储、处理或传输持卡人数据的所有系统组件执行合规性验证。

1.3 云用户和云服务商基于 PCI DSS 标准责任分摊的框架模型

1.3.1 总体责任分摊框架



1.3.2 逻辑分层责任分摊框架

	云用户
	共享
	云服务商

责任	服务模型		
	IaaS	PaaS	SaaS
安全治理，风险和合规	云用户	云用户	云用户
数据安全	云用户	云用户	云用户
应用安全	云用户	云用户	共享
平台安全	云用户	共享	云服务商
架构安全	共享	云服务商	云服务商
物理安全	云服务商	云服务商	云服务商

图：“云用户和云服务提供商责任分摊的框架模型”

引自《PCI 标委会云计算指南 版本 3（2018 年 4 月)》

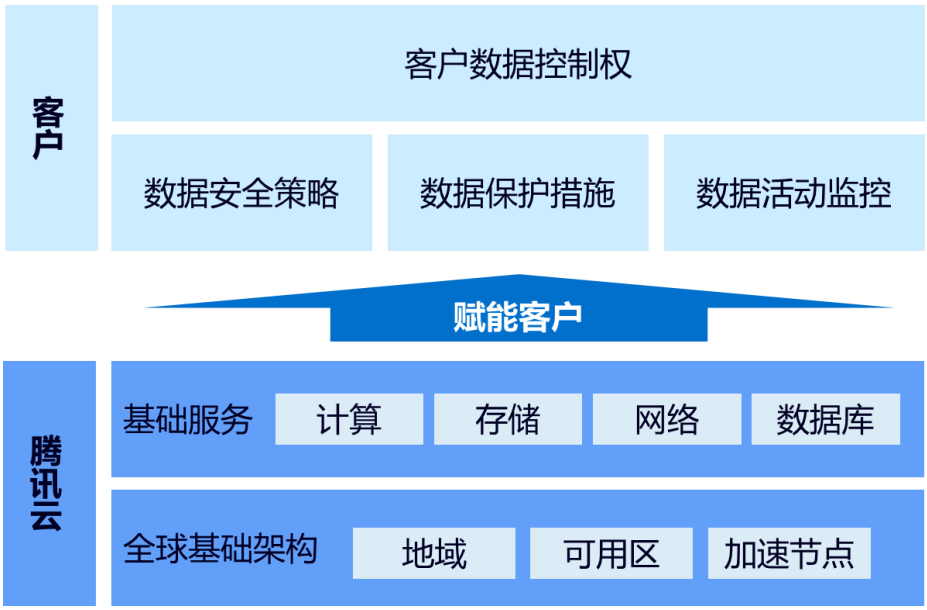
1.4 对应 PCI DSS 标准的责任分摊框架

	云用户
	共享
	云服务商

PCI DSS 标准要求 版本 3.2.1	管理控制的责任分配示例		
	IaaS	PaaS	SaaS
要求 1：安装并维护防火墙配置以保护持卡人数据	共享	共享	云服务商
要求 2：不要使用供应商提供的默认系统密码和其他安全参数	共享	共享	云服务商
要求 3：保护存储的持卡人数据	共享	共享	云服务商
要求 4：加密持卡人数据在开放式公共网络中的传输	云用户	共享	云服务商
要求 5：为所有系统提供恶意软件防护并定期更新杀毒软件或程序	云用户	共享	云服务商
要求 6：开发并维护安全的系统和应用程序	共享	共享	共享
要求 7：按业务知情需要限制对持卡人数据的访问	共享	共享	共享
要求 8：识别并验证对系统组件的访问	共享	共享	共享
要求 9：限制对持卡人数据的物理访问	云服务商	云服务商	云服务商
要求 10：跟踪并监控对网络资源和持卡人数据的所有访问	共享	共享	云服务商
要求 11：定期测试安全系统和流程	共享	共享	云服务商
要求 12：维护针对所有工作人员的信息安全政策	共享	共享	共享
附录 A1：针对共享托管服务提供商的 PCI DSS 附加要求	云服务商	云服务商	云服务商

1.5 腾讯云端数据保护责任模型

腾讯云在 2017 年 12 月正式发布的《腾讯云数据安全白皮书》中，明确提出了云端数据保护责任模型。腾讯云负责云平台的安全，并协助客户保障其云端数据的安全。为了更好地保护客户托管于云端的数据资产，腾讯云从平台层和赋能层两个层面为云服务客户提供双重保障。平台层提供的保障全面覆盖数据安全事前防范、事中保护和事后追溯三个阶段，而赋能层则围绕数据全生命周期给出一站式的解决方案供客户选用，以帮助客户最大程度地降低在流程、技术以及合规方面的数据安全风险。



图：云端数据保护责任模型

第二章 云服务提供商与云用户数据安全合规要求简析

通过云服务提供商和云用户在 PCI DSS 合规过程中的详细责任分析，云用户将会清晰了解如何更好地利用云服务提供商所提供的合规产品帮助云用户高效、快速地达到 PCI DSS 的标准要求，同时云服务提供商也能依据责任分摊模型，更高效地改善云产品并提高服务水平。

PCI DSS 标准要求 版本 3.2.1	云服务提供商的合规责任分析	云用户的合规责任分析
建立并维护安全的网络和系统		
要求 1： 安装并维护防火墙配置以保护持卡人数据	云服务提供商负责提供可用于不同云用户独立使用的网络逻辑访问控制的解决方案。	云用户负责针对云资源实例所需要开放的端口配置网络访问控制规则，同时需要依据云用户自己的网络变更流程进行核准并测试这些网络访问控制规则及连通性。
要求 2： 不要使用供应商提供的默认系统密码和其他安全参数	云服务提供商负责针对范围内的云主机及网络，系统组件等实施安全加固。	云用户负责修改云供应商提供的云服务器和私有网络实例及实例上的软件的默认值，以及制定安全加固手册并予以实施。
保护持卡人数据		
要求 3： 保护存储的持卡人数据	云服务提供商不直接存储，处理或传输持卡人数据或敏感认证	云用户负责维护适当的持卡人数据的保留和处理策略及流

	数据。	程，以达到 PCI 数据安全标准要求。
要求 4： 加密持卡人数据在开放式公共网络中的传输	云服务提供商不直接存储，处理或传输持卡人数据或敏感认证数据，可提供云用户相关服务，并负责维护适用的符合 PCI DSS 标准要求的策略。	云用户负责维护适用于其持卡人数据环境的策略和流程 PCI DSS 标准要求的策略，并选择云服务提供商提供的符合 PCI DSS 要求的产品以达到标准要求。
维护漏洞管理计划		
要求 5： 为所有系统提供恶意软件防护并定期更新杀毒软件或程序	云服务提供商负责平台中底层的系统组件的防病毒，防止被病毒和蠕虫等恶意软件影响。	云用户负责管理所租用的云服务器和办公电脑中的防病毒并符合 PCI DSS 标准要求的全部内容；可选择云服务提供商提供的符合 PCI DSS 要求的防病毒产品以达到标准要求。
要求 6： 开发并维护安全的系统和应用程序	云服务提供商负责针对平台系统和组件的安全漏洞制定评级标准和修复方案。	云用户负责针对云服务器等实例管理和实施必要的的安全补丁；审核云服务提供商推送的安全漏洞告警并根据指引实施适用于客户环境的任何建议；按 PCI DSS 标准要求制定软件

		开发标准，并实施到开发和部署到云服务的过程中；使用云服务提供商提供的已经合规的页面，软件或者 API 接口。
实施强效访问控制措施		
要求 7： 按业务知情需要限制对持卡人数据的访问	云服务提供商负责提供各种基于账号和权限来访问服务和资源的控制机制。	云用户负责对其持卡人数据环境中包含的所有云服务提供商可被管理的服务及服务器的账号和权限的访问控制管理；可使用云服务提供商提供的基于账号和权限的访问控制机制来管理所使用的云服务和资源。
要求 8： 识别并验证对系统组件的访问	云服务提供商负责提供各种基于账号和权限来访问服务和资源的控制机制。	云用户负责维护适用于其持卡人数据环境的策略和流程 PCI DSS 标准要求的策略；例如，负责控制用户帐户的分配，创建，删除，修改和注销。这包括对认证范围中包含的所有云服务提供商的服务和资源的访问控制。
要求 9： 限制对持卡人数据的物	云服务提供商负责维护认证范	云用户负责选择符合 PCI DSS

理访问	围内的数据中心的物理安全和媒介物理安全，包括但不限于门禁，监控，机柜，访客流程以及支持 PCI DSS 评估所包含的机房管理服务等。	要求的云服务提供商直接达到标准要求；负责云服务提供商的环境之外的支付卡数据读取设备的防篡改，资产管理，定期安全检查及培训。
定期监控并测试网络		
要求 10： 跟踪并监控对网络资源和持卡人数据的所有访问	针对云用户不能直接管理查询审计日志的系统组件(如管理控制台等)：云服务提供商负责提供给云用户符合 PCI DSS 标准要求的审计日志收集，查询和下载界面/接口或可以通过申请获得必要的审计日志，以及及时响应和处理底层及云用户不可管理的关键安全控制系统的安全故障并制定故障响应流程和恢复功能等。	云用户负责其使用的云服务器和私有网络实例的审计日志的收集和监控，并将日志关联到个人账户；负责收集所有对持卡人数据访问的审计日志且至少保存 1 年，使用云服务提供商提供的符合 PCI DSS 要求的操作日志管理产品以达到标准要求；按 PCI DSS 标准要求及时响应和处理可管理的关键安全控制系统的安全故障并制定故障响应流程和恢复功能。
要求 11： 定期测试安全系统和流程	云服务提供商负责底层系统及云用户不可管理的系统组件的	云用户负责其使用的云服务器，数据库实例和应用程序等

	内部、外部漏洞扫描和渗透测试，并按标准要求解决发现的高风险漏洞。	的季度内部及外部漏洞扫描，以及（至少年度）渗透测试，并按标准要求解决发现的高风险漏洞；实施完整性监控和响应流程解决方案。
维护信息安全政策		
要求 12：维护针对所有工作人员的信息安全政策。	云服务提供商负责维护适用的符合 PCI DSS 标准要求的策略. 云服务提供商负责提供对接云用户的接口人或团队，负责说明云服务提供商的 PCI DSS 合规情况。适当时，协助向云用户提供云平台的 PCI DSS 合规证明及协助处理云用户的安全事件。	云用户负责维护适用于其持卡人数据环境的策略和流程，并与 PCI DSS 标准要求 12 的全部内容保持一致。 云用户负责提供对接云服务提供商的接口人或团队从而获得合规方面的协助或者最佳实践指导。
附录 A： PCI DSS 附加要求		
附录 A1：针对共享托管服务提供商的 PCI DSS 附加要求	云服务提供商负责按 PCI DSS 标准附录 A 的要求实现每个云用户的逻辑隔离，访问控制及针对每个云用户的日志记录和保存。	云用户不适用。

附录 A2：针对使用 SSL/早期 TLS 用于刷卡 POS POI 终端连接的实体的 PCI DSS 附加要求	云服务提供商不适用。 云服务提供商并未提供用于支付卡数据读取的设备。	云用户负责云服务提供商的环境之外的支付卡数据读取设备的 SSL/TLS 的漏洞评估和风险减轻转移计划。
A.2.3 此要求只针对服务提供商：所有服务提供商必须提供安全的服务。	云服务提供商负责对云用户共同使用的互联网开放的服务提供安全的传输加密协议。	云用户负责其对互联网开放的服务只提供安全的传输加密协议。

第三章 腾讯云数据安全合规产品简介

腾讯云提供了下列符合 PCI DSS 标准要求的产品，云用户可通过选择合适的产品缩短 PCI DSS 合规时间周期同时可降低运维复杂度和成本。

序号	产品名称（中英文对照）	产品简介
PA-01	云支付 (Cloud Pay) Cpay	提供开放、可靠的移动支付收单和服务商、商户管理服务，支持刷卡支付、扫码支付、一码多付多种支付方式。
PA-02	私有网络 (Virtual Private Cloud) VPC	提供网络服务，不同私有网络间完全逻辑隔离，可以通过软件定义网络的方式管理云用户的私有网络 VPC。
PA-03	负载均衡 (Cloud Load Balance) CLB	提供安全快捷的流量分发服务，经由 CLB 可以自动分配到云中的多台云服务器上，扩展系统的服务能力并消除单点故障。
PA-04	专线接入 (Direct Connect) DC	提供一种便捷地连接企业数据中心与腾讯云的方法，云用户可通过专线接入，建立与公网完全隔离的私有连接服务。
PA-05	NAT 网关 NAT Gateway	提供 IP 地址转换的网络云服务。
PA-06	VPN 连接 VPN Connections	提供本地数据中心与腾讯云上资源连通的传输服务。
PA-07	云联网 (cloud connect network) CCN	提供全网互联服务，助力云用户实现各地域的云上、云下多点互联。

PA-08	云服务器（Cloud Virtual Machine) CVM	提供安全可靠的弹性计算服务，可以实时扩展或缩减计算资源。
PA-09	专用宿主机（CVM Dedicated Host) CDH	提供用户独享的物理服务器资源，满足云用户资源独享、资源物理隔离、安全、合规需求。
PA-10	独享加密机服务（Exclusive Encryption Service) EES	提供独享的硬件加密机服务。
PA-11	密钥管理服务（key management service) KMS	提供安全管理类服务，使用经过第三方认证的硬件安全模块 HSM (hardware security module)来生成和保护密钥。
PA-12	访问管理（Cloud Access Management) CAM	提供账号和权限管理体系，用于帮助客户安全且精细化管理腾讯云产品和资源的访问。
PA-13	多因子认证（Multi-factor Authentication) MFA	提供除了用户名和密码之外针对账号额外的验证方法，使得账号登录过程更安全。
PA-14	云审计 CloudAudit	提供记录日志、持续监控的服务，同时保留通过腾讯云管理控制台、API 服务、命令行工具和其他腾讯云服务执行的操作等账号活动日志。
PA-15	云监控（Cloud Monitor) CM	提供立体化云产品数据监控、智能化数据分析、实时化异常告警和个性化数据报表配置。
PA-16	云拨测（Cloud Automated Testing) CAT	提供自定义可用率指标等阈值告警功能，云用户可以通过配置告警实现异常实时通知。
PA-17	数盾数据安全审计 Cloud Data Shield-Audit	提供基于人工智能的数据库安全审计系统。

PA-18	敏感数据处理 Cloud Data Shield-Mask	提供敏感数据脱敏与水印标记工具，可为数据系统中的敏感信息进行脱敏处理并在泄漏时提供追溯依据。
PA-19	数盾数据安全网关 Cloud Shield-Data Data Access Security Broker	提供运维人员操作审计，对异常行为进行告警，防止内部数据泄密。
PA-20	数据安全治理中心 Data Security Governance Center	提供敏感数据资产治理，包括数据分类，异常用户行为分析，DLP 等功
PA-21	大禹 DDoS 防护 Dayu Anti-DDos Service	提供 BGP 高防包、BGP 高防 IP、棋牌盾等多种 DDoS 解决方案。
PA-22	腾讯云 Web 应用防火墙 (Web Application Firewall) WAF	提供给腾讯云内及云外用户应对 Web 攻击、入侵、漏洞利用、挂马、篡改、后门、爬虫、域名劫持等网站及 Web 业务安全防护问题的解决方案。
PA-23	主机安全（云镜） Host Security	提供黑客入侵检测和漏洞风险预警等安全防护服务，主要包括密码破解拦截、异常登录提醒、木马文件查杀、高危漏洞检测等安全功能。

第四章　云用户的 PCI DSS 合规测评建议

通过前述介绍，云服务提供商和云用户各自承担了标准要求中对应的责任，根据《PCI 标委会云计算指南》的指导建议，获得了 PCI DSS 合规的云服务提供商，在云用户的合规评估过程中针对云服务提供商的相应责任的评估审核可**按云服务提供商的合规结果直接引用。**而对于云用户采用了非合规的云服务提供商用于 PCI DSS 评估的情况下，非合规的云服务提供商在支持每个云用户的评估过程还需针对云服务提供商的责任提供完整的评估支持材料，从而可能使得评估过程更复杂和冗长。因此我们强烈推荐**云用户采用 PCI DSS 合规的云服务提供商**来帮助机构便捷、高效地达到合规要求。

云用户的 PCI DSS 合规建议根据本文第三章中的分析实施必要的措施及进行评估，通常的 PCI DSS 流程如下:

参考文献

- Payment Card Industry (PCI) Data Security Standard, version 3.2.1 (May 2018)

  支付卡行业(PCI)数据安全标准 3.2.1 版本（2018 年 5 月）

- 支付卡行业(PCI)数据安全标准要求和安全评估程序 3.2 版本（2016 年 4 月）

- Payment Card Industry (PCI) Data Security Standard Approved Scanning Vendors Program Guide 3.1 (July 2018)

  支付卡行业数据安全标准 ASV 指导 3.1 （2018 年 7 月）

- PCI SSC Cloud Computing Guidelines Version 3(April 2018)

  PCI 标委会云计算指南 版本 3（2018 年 4 月）

- Penetration Testing Guidance 1.1 (Sept 2017)

  渗透测试指导 1.1（2017 年 9 月）

附录：

腾讯云计算（北京）有限责任公司所提供的腾讯金融云自 2017 年 8 月 10 日通过了 PCI DSS 认证，并每年维护此资质，属于 PCI DSS 标准合规的云服务提供商。