A PCI Walk in the Clouds

Jilai Xie atsec China
Yongxia Wang Tencent Cloud
Yan Liu atsec China

Content

Traditional architecture VS cloud architecture

Cloud payment products (SAAS based) VS Cloud-based payment services (IAAS based)

Cloud Security Considerations

Practice Shared Responsibility

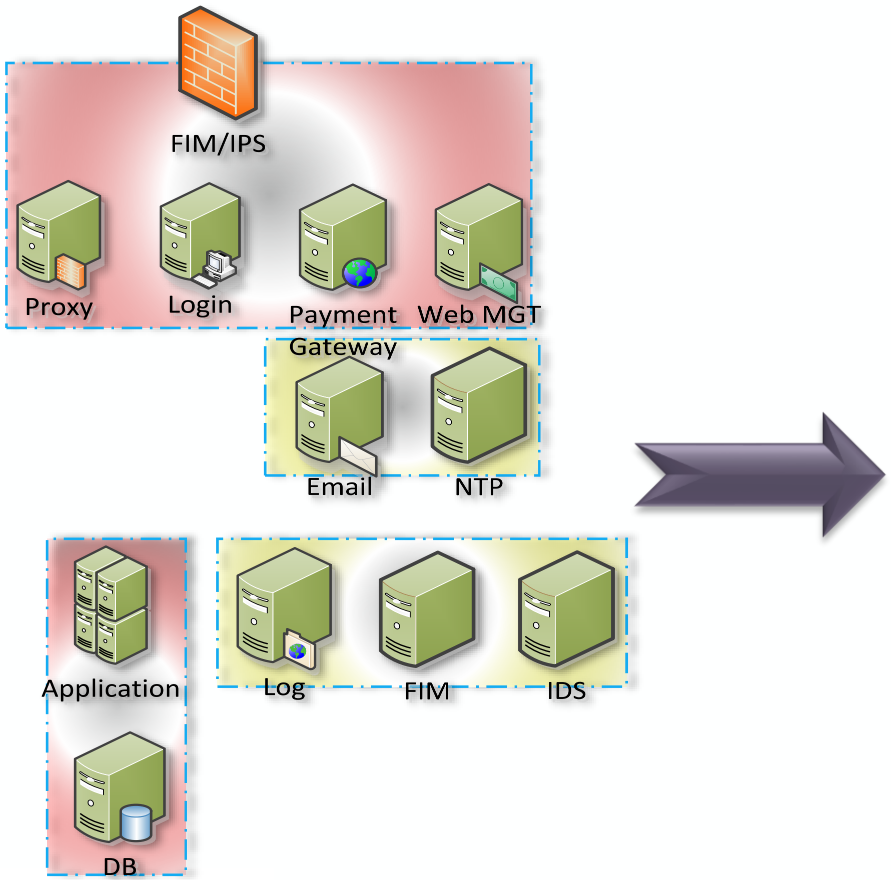
Case Study - Tencent Cloud

- Tencent Cloud Data Security Compliance Certifications

- Tencent Cloud Data Security Model

Traditional architecture VS cloud architecture

Migrating from traditional architecture to cloud architecture



Physical network layer | Virtual network layer

Customer network layer | Cloud MGT network layer | Cloud Platform network layer | ...

Firewall | Router/ Switch | SDN | WAF | Anti DDos | CDN | ...

Hosts | VMs | Containers | DB | API | Microservices | ...

CPU | MEM | NIC | Storage

KVM | ESXi | Hyper-V | Xen

Amazon Aurora | Postgre SQL | MySQL | Maria DB | Oracle | MS SQL Server

Mongo DB | Redis | Memcache | Blockchain | KMS/ HSM | ...

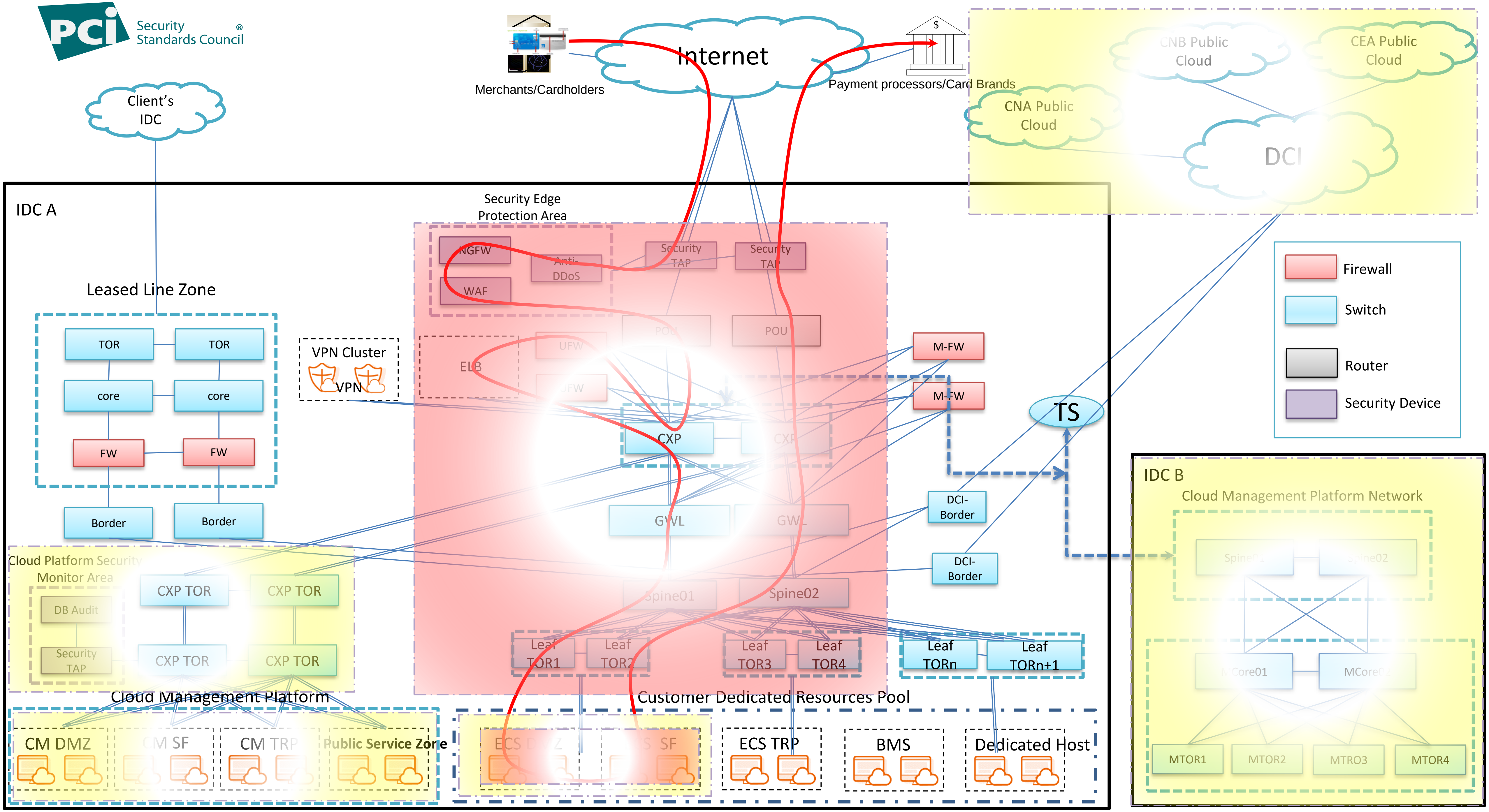
Traditional Architecture VS Cloud Architecture

Category	Advantage	Disadvantage
Traditional enterprise self-built IT environment	The simpler, more secure	The level of technology is uneven
	Segmentation control is easy	Weak capability against large-scale DDoS attacks
	Vulnerability has a small range of influence	Non-reusable assessment results
	Exclusive equipment and data encryption device/application	High initial investment and technical requirements
Iaas/SaaS cloud architecture	High level of security protection	More complex, higher risks
	Assessment results can be reused	Vulnerability has a huge range of influence
	Strong capability against large-scale DDoS attacks	Risk of sharing encryption mechanisms
	Low initial investment and technical requirements	Shared responsibility leads to mutual excuses

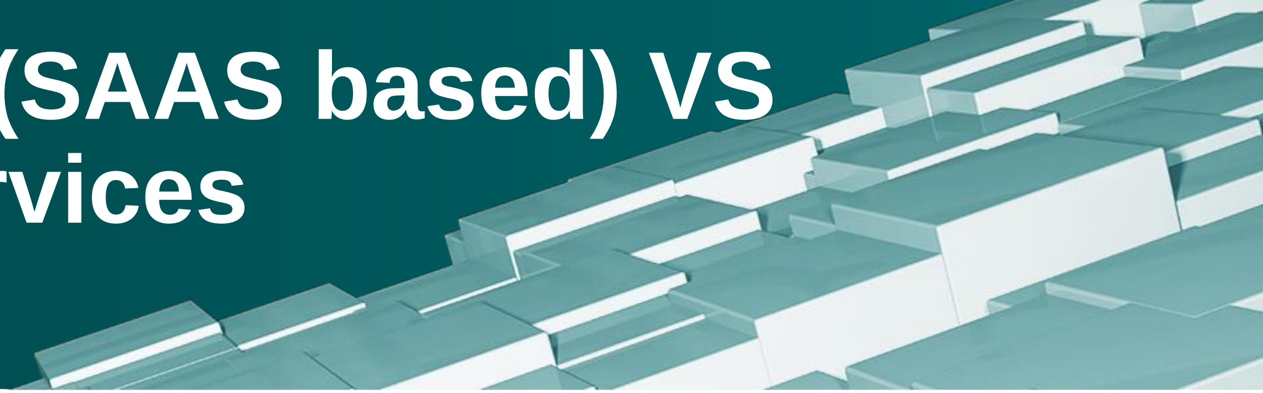
the information security provider

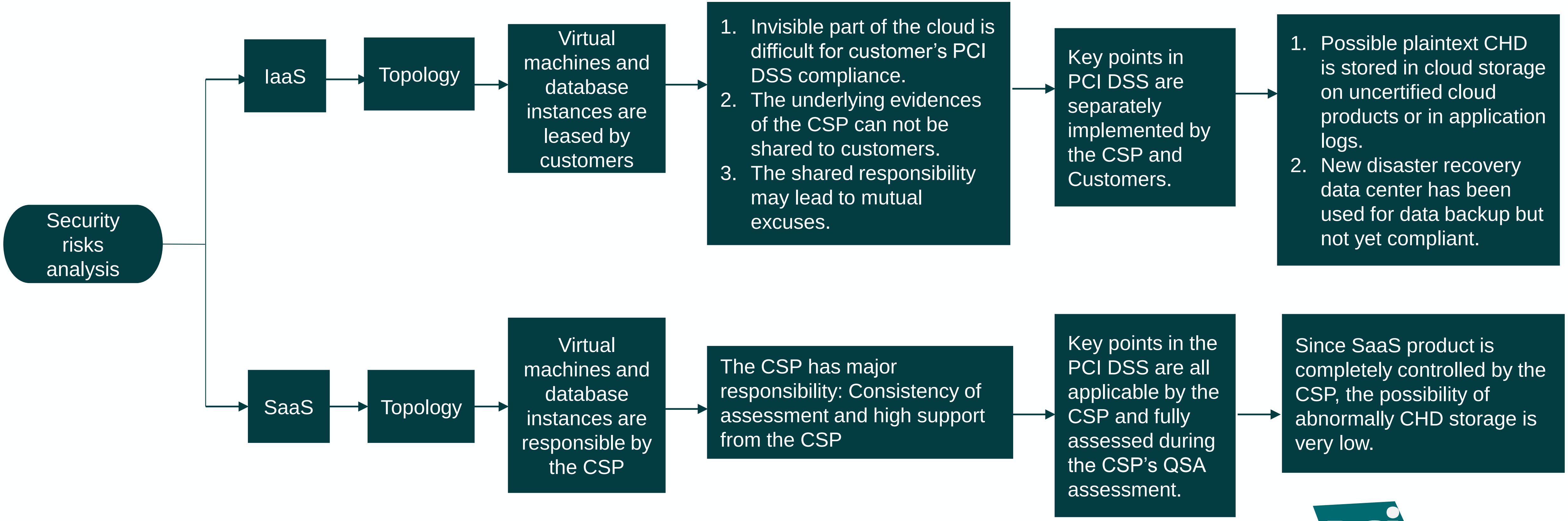
PCI Security Standards Council ®

PCI Security Standards Council ®



Cloud Payment Products (SAAS based) VS Cloud-based Payment Services (IAAS based)





Security risks analysis

IaaS

Topology

Virtual machines and database instances are leased by customers

1. Invisible part of the cloud is difficult for customer’s PCI DSS compliance.
2. The underlying evidences of the CSP can not be shared to customers.
3. The shared responsibility may lead to mutual excuses.

Key points in PCI DSS are separately implemented by the CSP and Customers.

1. Possible plaintext CHD is stored in cloud storage on uncertified cloud products or in application logs.
2. New disaster recovery data center has been used for data backup but not yet compliant.

SaaS

Topology

Virtual machines and database instances are responsible by the CSP

The CSP has major responsibility: Consistency of assessment and high support from the CSP

Key points in the PCI DSS are all applicable by the CSP and fully assessed during the CSP’s QSA assessment.

Since SaaS product is completely controlled by the CSP, the possibility of abnormally CHD storage is very low.

Cloud Security Considerations

Introspection

Challenges:

- **Introspection bypass the login access control so that no log information is generated in VM.**

Recommendations:

1. Strictly follow the change control process.

2. Separate the roles of use and audit.

3. Identify and alert high-risk operations or commands.

Cloud Security Considerations

Penetration test

Challenges:

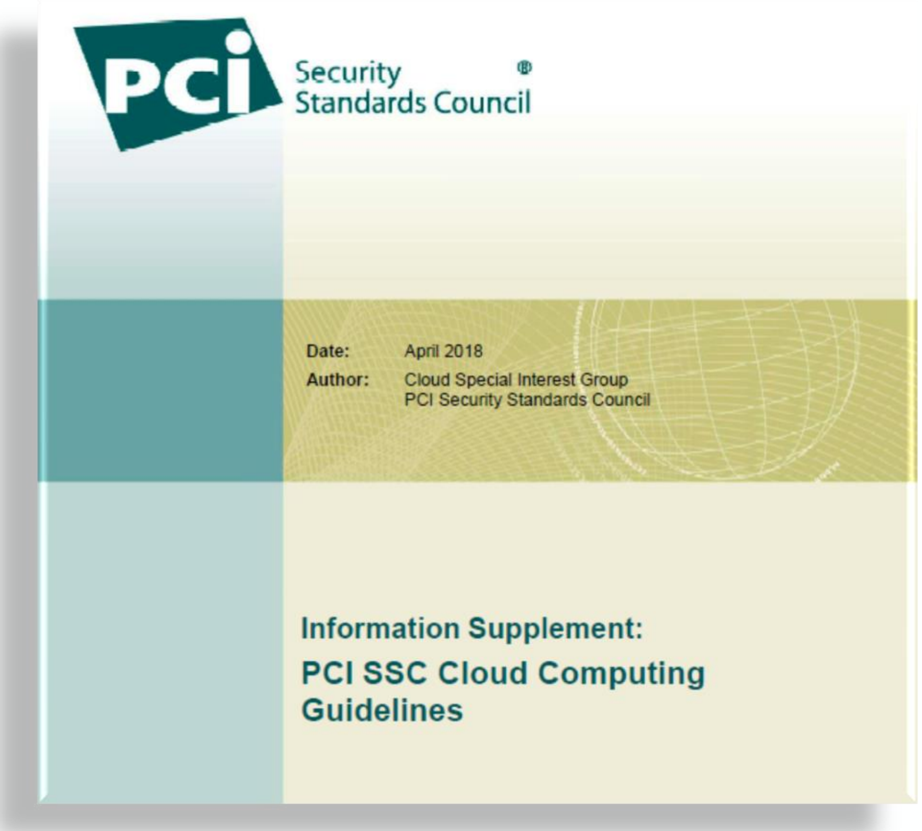
- **Segmentation to reduce the scope of PCI DSS assessment.**
- **Penetration testing to verify segmentation is challenge in cloud.**

Recommendations:

1. **Perform testing when each instance is created.**
2. **Perform testing when access policy change is made to the VPC or between VPCs or between customers and CMN.**
3. **The CSP is responsible for periodically testing the isolation of the underlying resources.**

For the above-mentioned testing, automatic methods are recommended and push alarms to the NOC.

Practice Shared Responsibility



Security Standards Council®

Date: April 2018

Author: Cloud Special Interest Group
PCI Security Standards Council

Information Supplement:

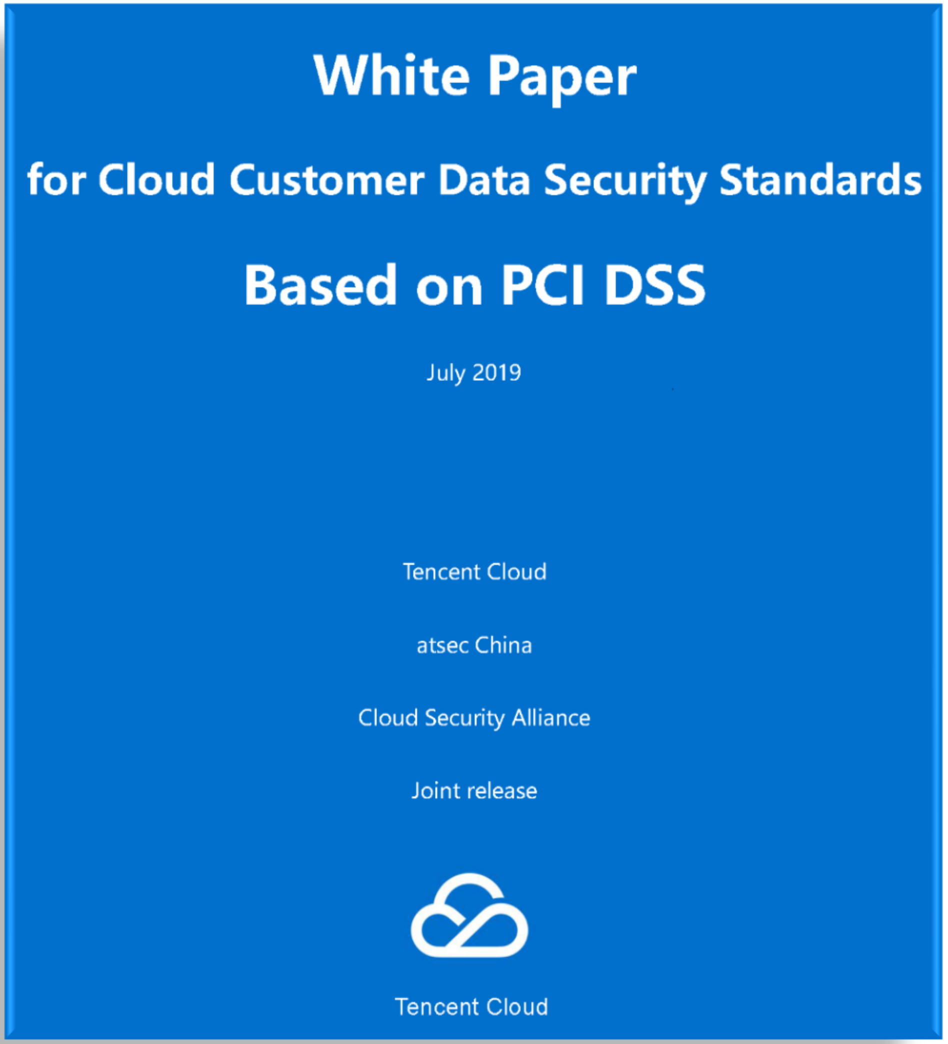
PCI SSC Cloud Computing Guidelines

Challenge:

- Shared compliance responsibility between CSP and Customer which could lead to mutual excuses.

Practice Shared Responsibility

White Paper for Cloud Customer Data Security Standards Based on PCI DSS



White Paper

for Cloud Customer Data Security Standards

Based on PCI DSS

July 2019

Tencent Cloud

atsec China

Cloud Security Alliance

Joint release

Tencent Cloud

1 Cloud Data Security Compliance based on PCI DSS

1.1 Background of the PCI DSS

1.2 PCI DSS Overview

1.3 Shared Responsibility Framework

1.3.1 Overview

1.3.2 Logical Tiered Framework

1.3.3 Corresponding to the PCI DSS requirements

2 Compliance Products provided by Tencent Cloud

3 Compliance responsibility Analysis for the CSP and Cloud Customers

4 Compliance and Assessment Suggestions for Cloud Customers

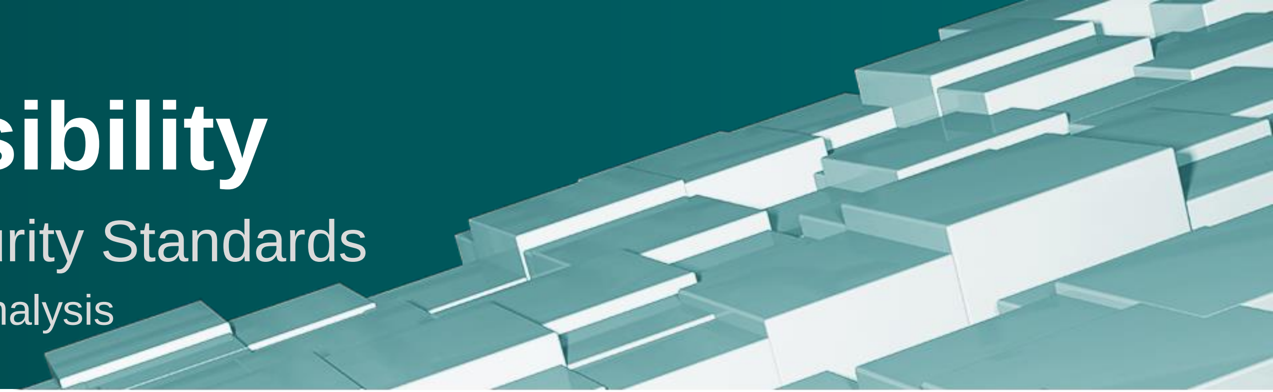
5 PCI DSS Compliance Case Study

References and Appendix

PCI Security Standards Council®

Practice Shared Responsibility

White Paper for Cloud Customer Data Security Standards Based on PCI DSS – Chapter three: responsibility analysis

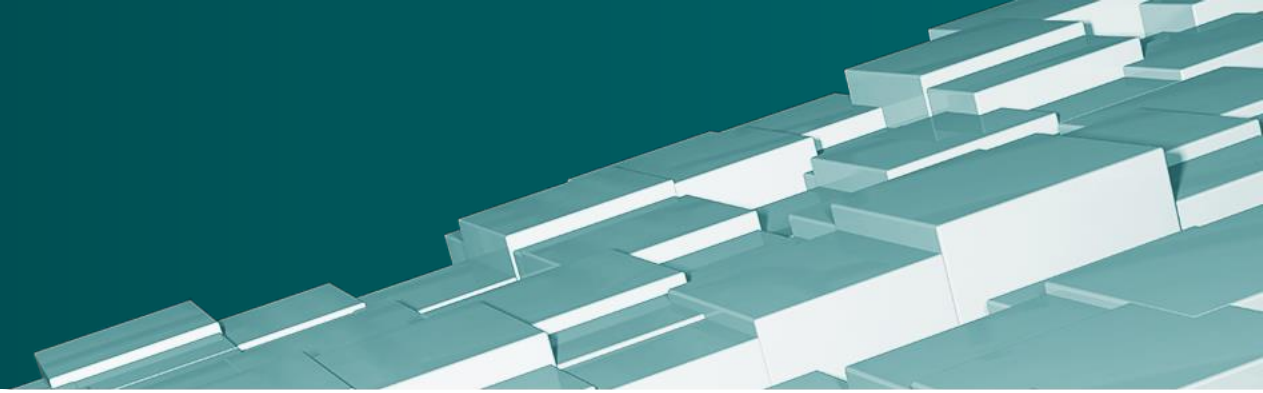


PCI DSS Requirements	Responsibilities of the CSP	Responsibilities of Cloud Customers
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	**IAAS** service mode do not directly store, process or transmit cardholder data or sensitive authentication data, hence this requirement does not directly apply to the CSP. **SAAS:** If the cloud service provider provides products (e.g. Cloud Payment product: Cpay) in order to help cloud customers to meet the requirement, the CSP is also responsible for maintaining the related evidences.	Cloud customers are responsible for maintaining cardholder data flow diagram for defined CDE and related networks.
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:	**IAAS** service mode do not directly store, process or transmit cardholder data or sensitive authentication data, hence the relevant requirements for cardholder data protection are not directly applicable for the CSP. **SAAS:** If the cloud service provider provides payment products (e.g. Cloud Payment product: Cpay) in order to meet the requirements, the CSP is also responsible for the PAN data protection.	The cloud customers are responsible for selecting and maintaining the appropriate solution(s) for cardholder data protection, key management and corresponding technology implementation in order to meet the requirements.

@sec the information security provider

PCI Security Standards Council ®

Content



Traditional architecture VS cloud architecture

Cloud payment products (SAAS based) VS Cloud-based payment services (IAAS based)

Cloud Security Considerations

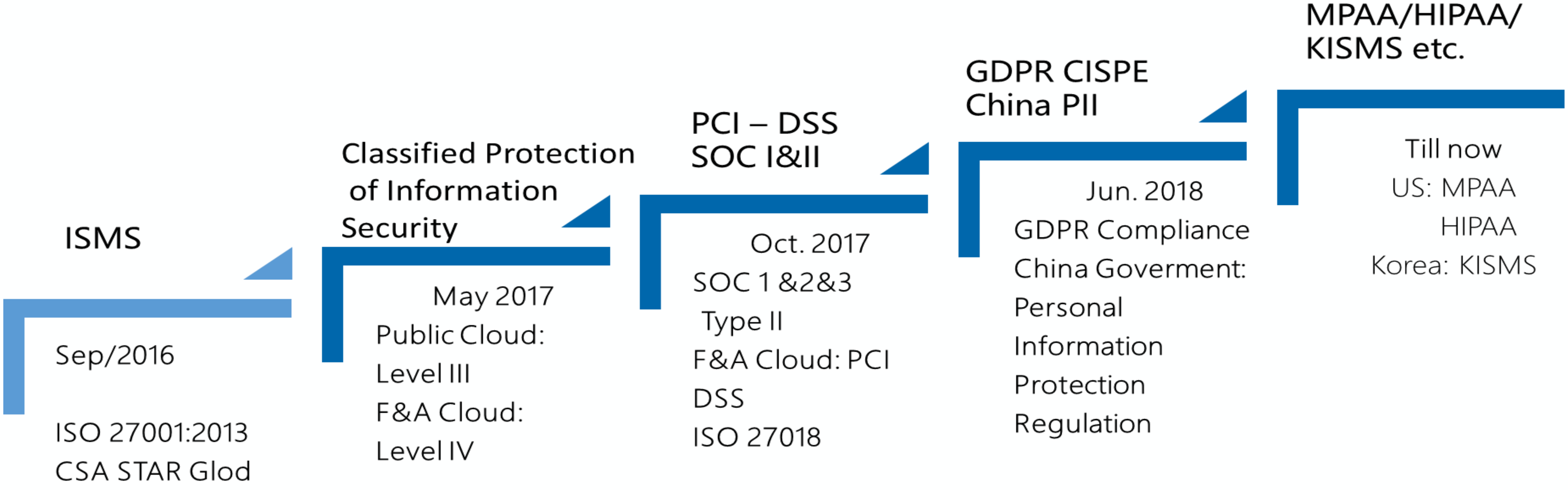
Practice Shared Responsibility

Case Study - Tencent Cloud

- Tencent Cloud Data Security Compliance Certifications
- Tencent Cloud Data Security Model

Case Study - Tencent Cloud

- Data Security Compliance Certifications



ISMS

Sep/2016

ISO 27001:2013
CSA STAR Glod

Classified Protection of Information Security

May 2017
Public Cloud:
Level III
F&A Cloud:
Level IV

PCI – DSS
SOC I&II

Oct. 2017
SOC 1 &2&3
Type II
F&A Cloud: PCI DSS
ISO 27018

GDPR CISPE
China PII

Jun. 2018
GDPR Compliance
China Goverment:
Personal
Information
Protection
Regulation

MPAA/HIPAA/
KISMS etc.

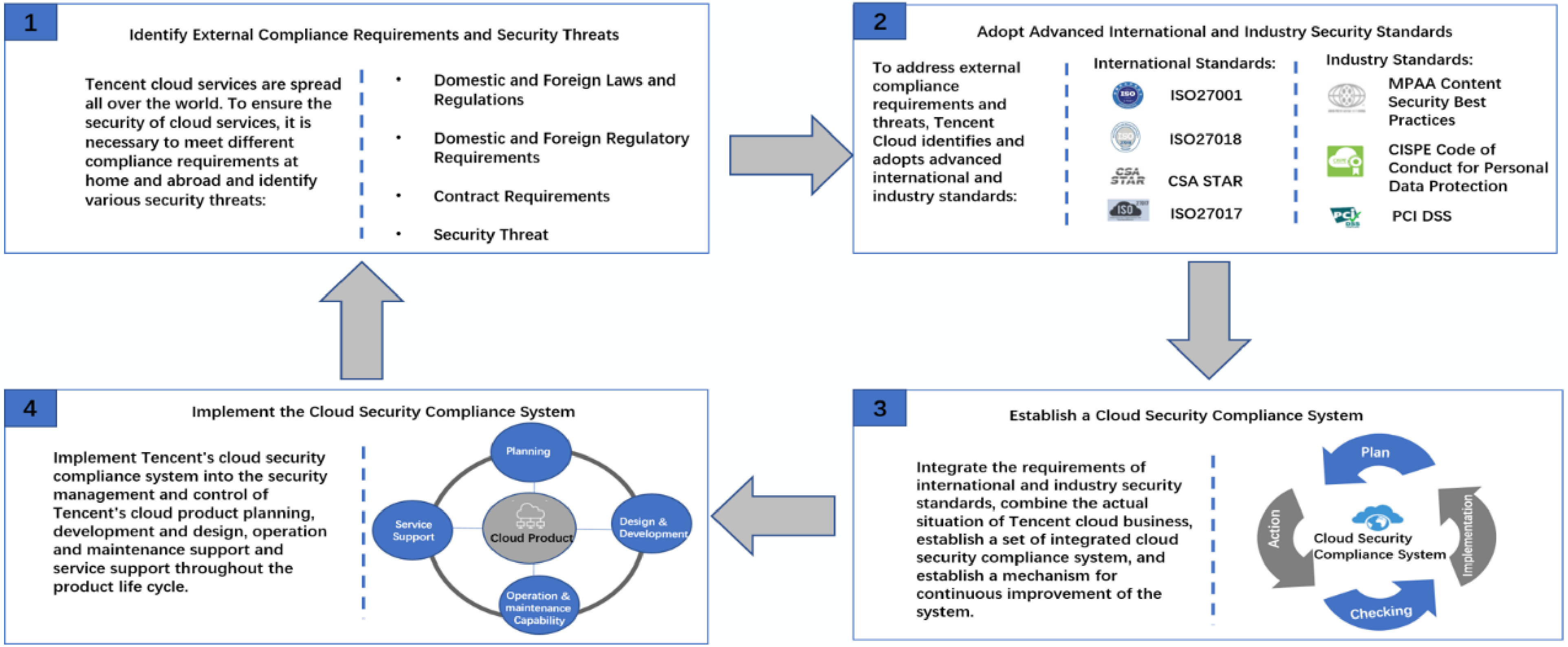
Till now
US: MPAA
HIPAA
Korea: KISMS

@SEC the information security provider

腾讯标准 Tencent Standard

PCI Security Standards Council ®

Case Study - Tencent Cloud
- Data Security Compliance Roadmap



1 Identify External Compliance Requirements and Security Threats

Tencent cloud services are spread all over the world. To ensure the security of cloud services, it is necessary to meet different compliance requirements at home and abroad and identify various security threats:

- Domestic and Foreign Laws and Regulations
- Domestic and Foreign Regulatory Requirements
- Contract Requirements
- Security Threat

2 Adopt Advanced International and Industry Security Standards

To address external compliance requirements and threats, Tencent Cloud identifies and adopts advanced international and industry standards:

International Standards:

- ISO27001
- ISO27018
- CSA STAR
- ISO27017

Industry Standards:

- MPAA Content Security Best Practices
- CISPE Code of Conduct for Personal Data Protection
- PCI DSS

3 Establish a Cloud Security Compliance System

Integrate the requirements of international and industry security standards, combine the actual situation of Tencent cloud business, establish a set of integrated cloud security compliance system, and establish a mechanism for continuous improvement of the system.

4 Implement the Cloud Security Compliance System

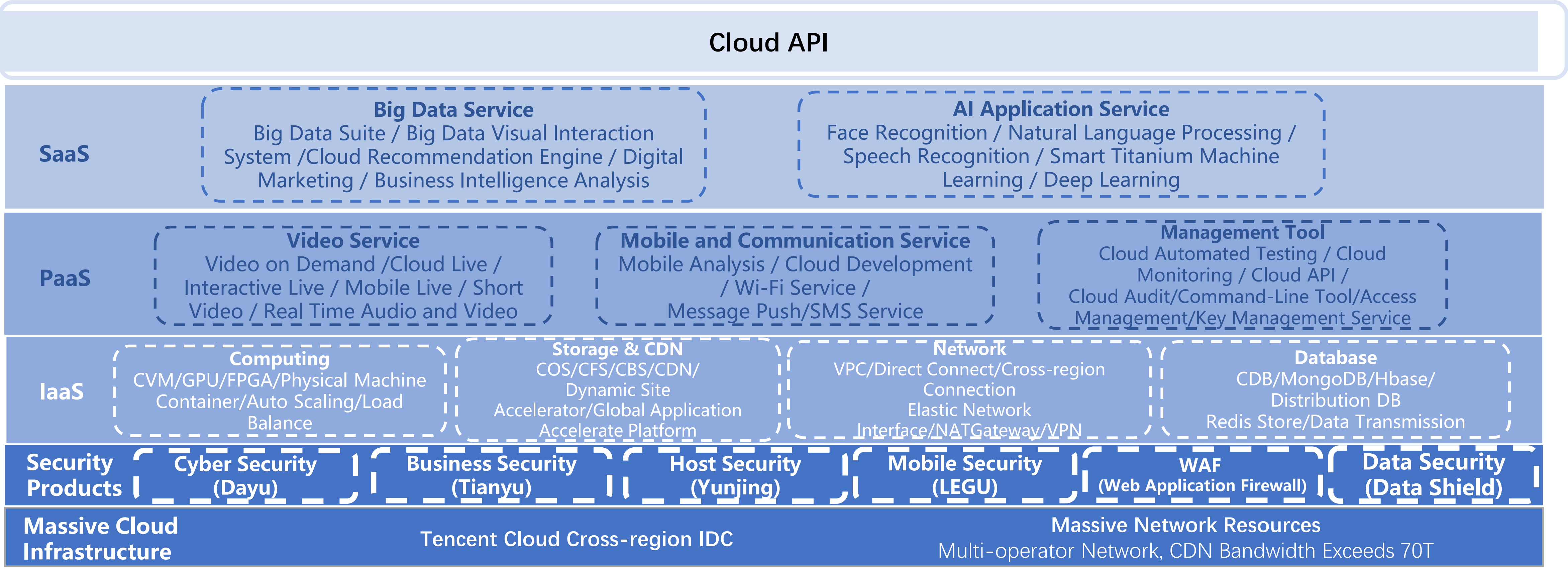
Implement Tencent's cloud security compliance system into the security management and control of Tencent's cloud product planning, development and design, operation and maintenance support and service support throughout the product life cycle.

the information security provider

腾讯标准
Tencent Standard

PCI Security Standards Council ®

Case Study - Tencent Cloud
- Tencent Cloud Product and Service Structure



Cloud API

SaaS

Big Data Service
Big Data Suite / Big Data Visual Interaction System /Cloud Recommendation Engine / Digital Marketing / Business Intelligence Analysis

AI Application Service
Face Recognition / Natural Language Processing / Speech Recognition / Smart Titanium Machine Learning / Deep Learning

PaaS

Video Service
Video on Demand /Cloud Live / Interactive Live / Mobile Live / Short Video / Real Time Audio and Video

Mobile and Communication Service
Mobile Analysis / Cloud Development / Wi-Fi Service / Message Push/SMS Service

Management Tool
Cloud Automated Testing / Cloud Monitoring / Cloud API / Cloud Audit/Command-Line Tool/Access Management/Key Management Service

IaaS

Computing
CVM/GPU/FPGA/Physical Machine Container/Auto Scaling/Load Balance

Storage & CDN
COS/CFS/CBS/CDN/ Dynamic Site Accelerator/Global Application Accelerate Platform

Network
VPC/Direct Connect/Cross-region Connection
Elastic Network Interface/NATGateway/VPN

Database
CDB/MongoDB/Hbase/ Distribution DB
Redis Store/Data Transmission

Security Products

Cyber Security (Dayu)

Business Security (Tianyu)

Host Security (Yunjing)

Mobile Security (LEGU)

WAF (Web Application Firewall)

Data Security (Data Shield)

Massive Cloud Infrastructure

Tencent Cloud Cross-region IDC

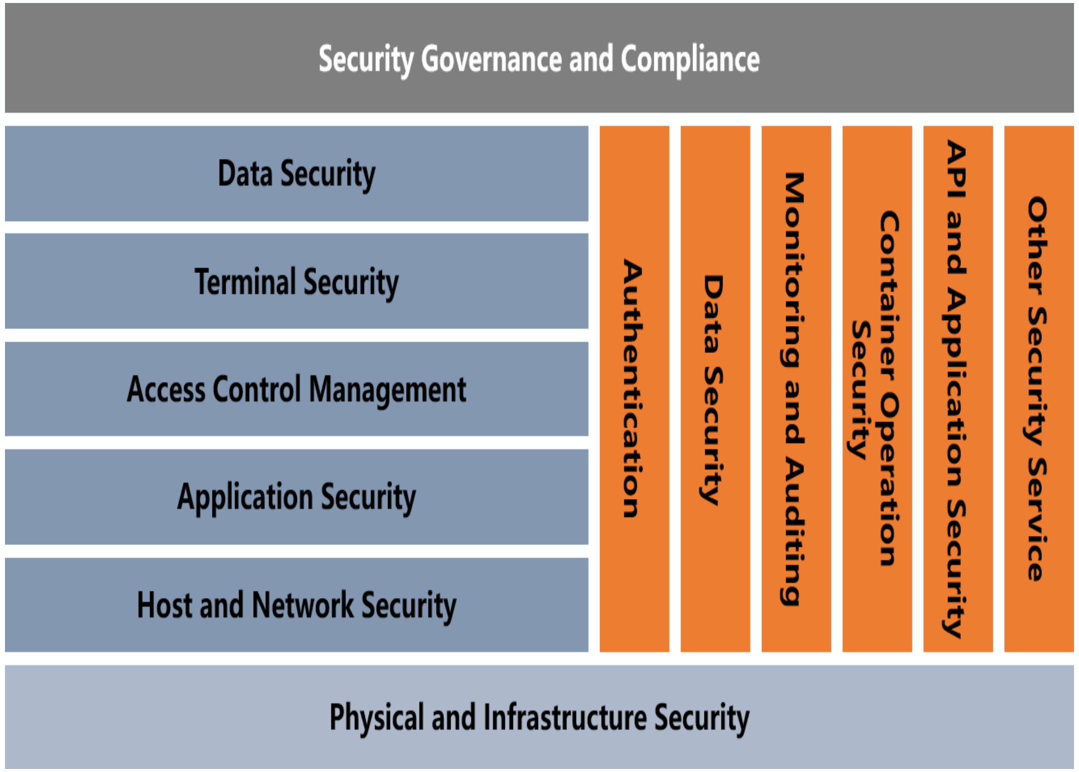
Massive Network Resources
Multi-operator Network, CDN Bandwidth Exceeds 70T

@sec the information security provider

腾讯标准 Tencent Standard

PCI Security Standards Council ®

Case Study - Tencent Cloud
- Tencent Cloud Security Model


Security Governance and Compliance

Data Security

Terminal Security

Access Control Management

Application Security

Host and Network Security

Authentication

Data Security

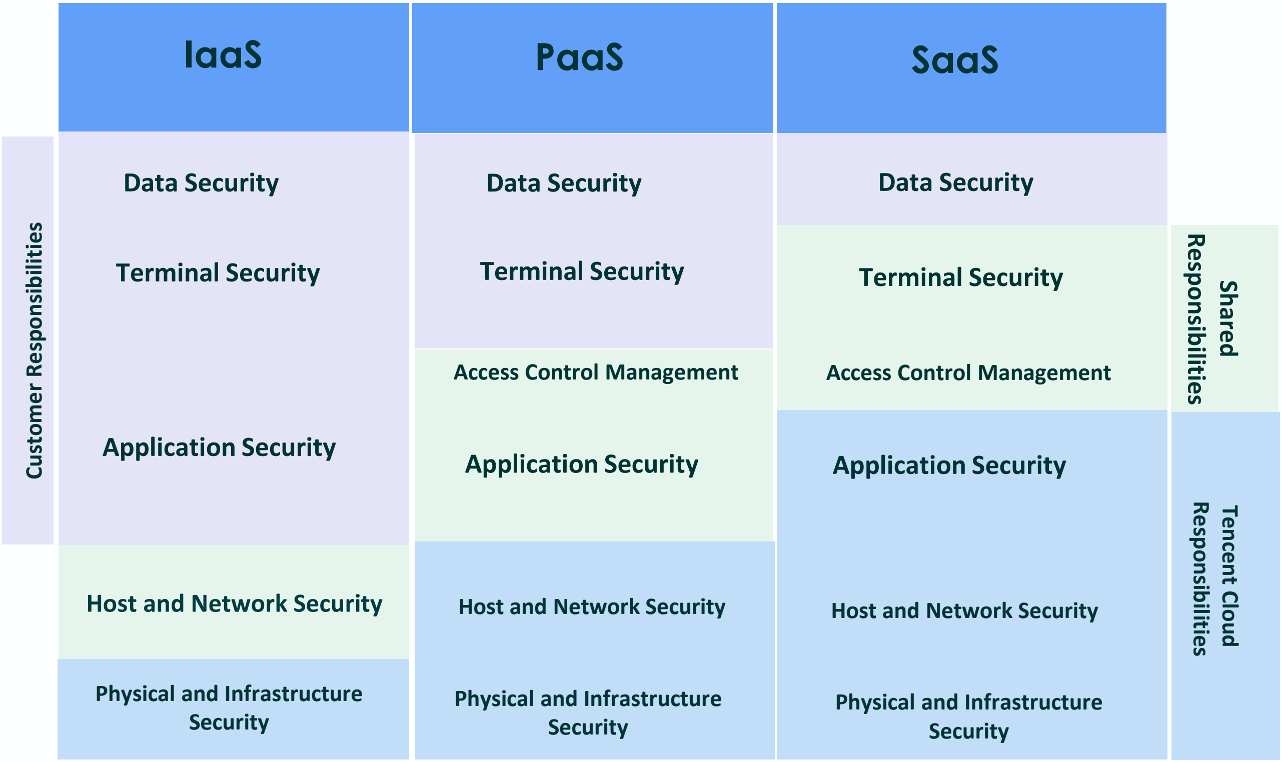
Monitoring and Auditing

Container Operation Security

API and Application Security

Other Security Service

Physical and Infrastructure Security


IaaS	PaaS	SaaS
Data Security	Data Security	Data Security
Terminal Security	Terminal Security	Terminal Security
	Access Control Management	Access Control Management
Application Security	Application Security	Application Security
Host and Network Security	Host and Network Security	Host and Network Security
Physical and Infrastructure Security	Physical and Infrastructure Security	Physical and Infrastructure Security

Customer Responsibilities

Shared Responsibilities

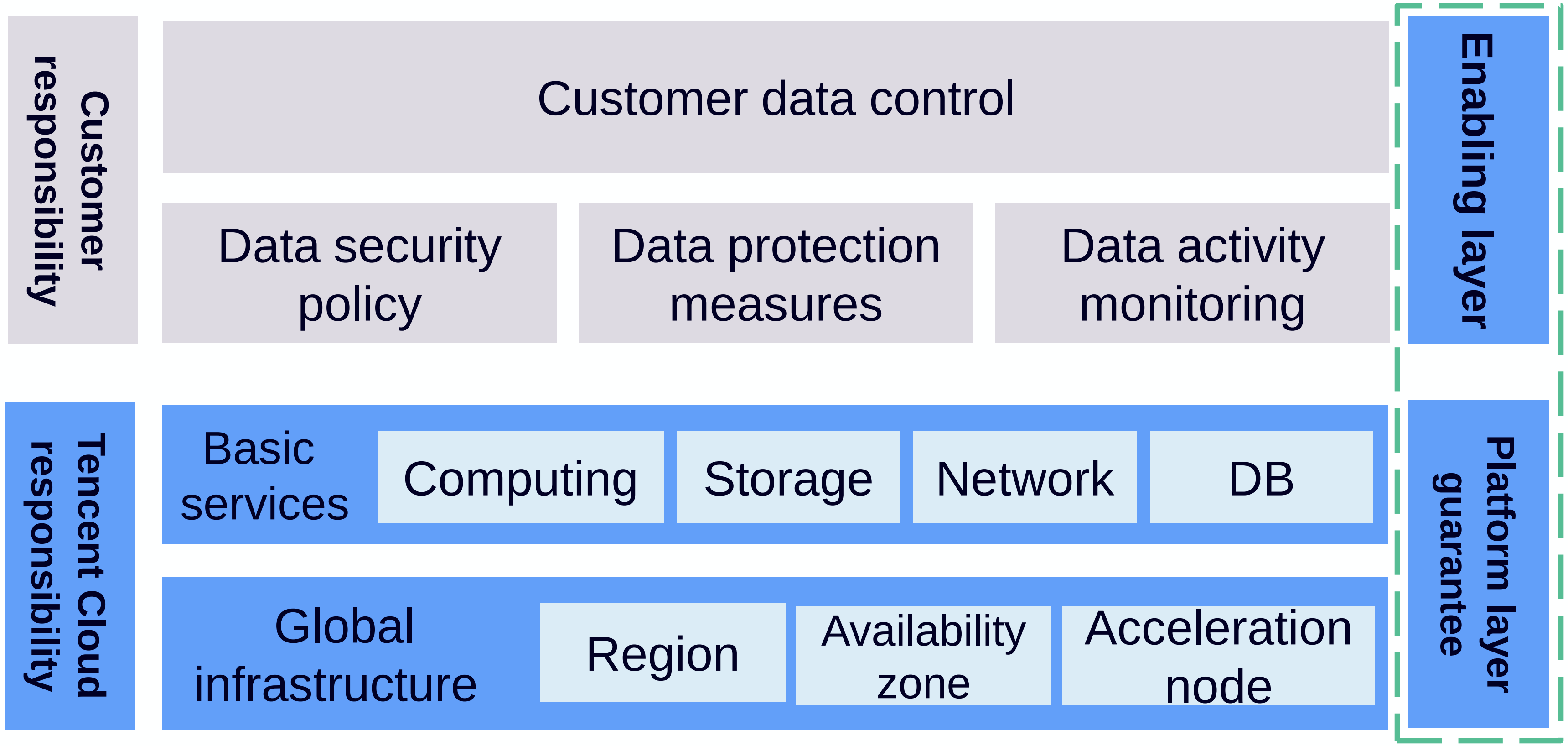
Tencent Cloud Responsibilities

the information security provider

腾讯标准 Tencent Standard

Security Standards Council

Case Study - Tencent Cloud
- Tencent Cloud Security Model



Customer responsibility

Customer data control

Data security policy

Data protection measures

Data activity monitoring

Enabling layer

Tencent Cloud responsibility

Basic services

Computing

Storage

Network

DB

Global infrastructure

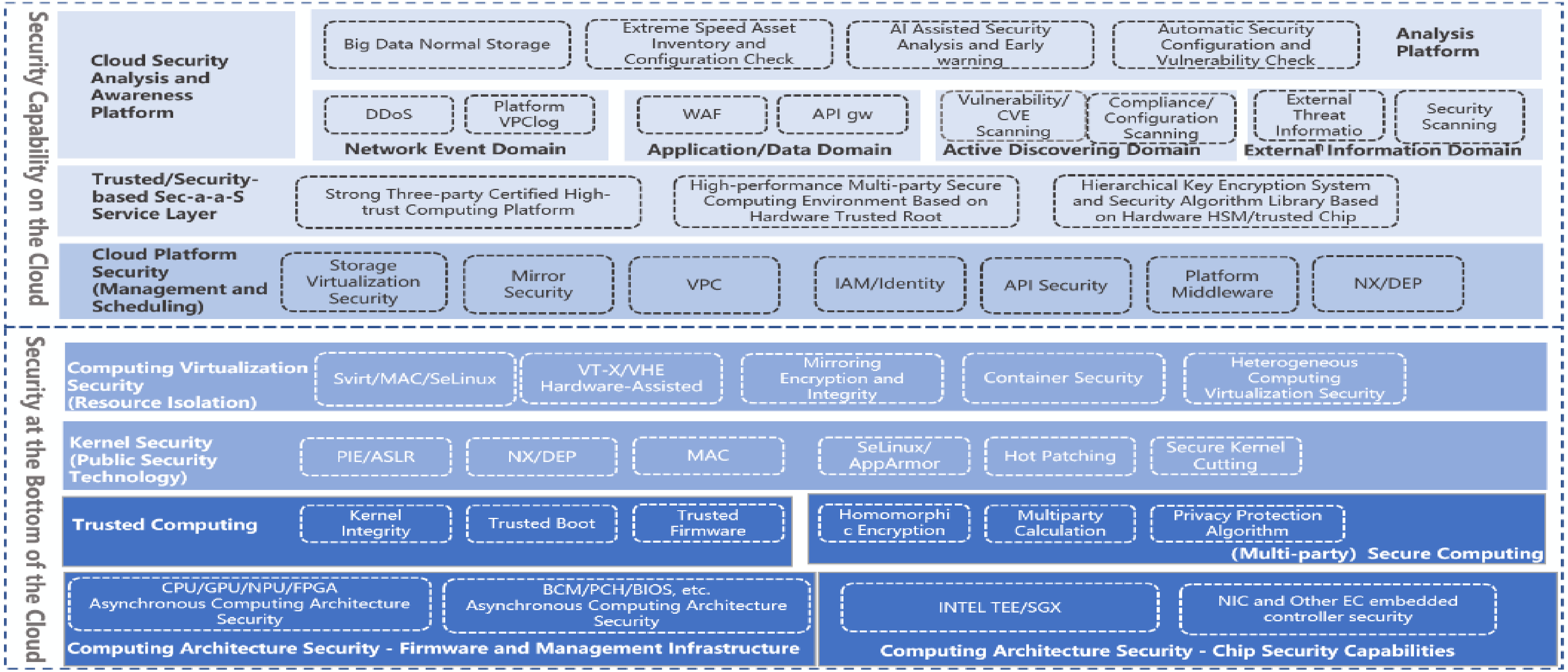
Region

Availability zone

Acceleration node

Platform layer guarantee

Case Study - Tencent Cloud
- Tencent Cloud Security Model



Security Capability on the Cloud

Cloud Security Analysis and Awareness Platform

Big Data Normal Storage | Extreme Speed Asset Inventory and Configuration Check | AI Assisted Security Analysis and Early warning | Automatic Security Configuration and Vulnerability Check | Analysis Platform

DDoS | Platform VPClog — Network Event Domain

WAF | API gw — Application/Data Domain

Vulnerability/ CVE Scanning | Compliance/ Configuration Scanning — Active Discovering Domain

External Threat Informatio | Security Scanning — External Information Domain

Trusted/Security-based Sec-a-a-S Service Layer

Strong Three-party Certified High-trust Computing Platform | High-performance Multi-party Secure Computing Environment Based on Hardware Trusted Root | Hierarchical Key Encryption System and Security Algorithm Library Based on Hardware HSM/trusted Chip

Cloud Platform Security (Management and Scheduling)

Storage Virtualization Security | Mirror Security | VPC | IAM/Identity | API Security | Platform Middleware | NX/DEP

Security at the Bottom of the Cloud

Computing Virtualization Security (Resource Isolation)

Svirt/MAC/SeLinux | VT-X/VHE Hardware-Assisted | Mirroring Encryption and Integrity | Container Security | Heterogeneous Computing Virtualization Security

Kernel Security (Public Security Technology)

PIE/ASLR | NX/DEP | MAC | SeLinux/ AppArmor | Hot Patching | Secure Kernel Cutting

Trusted Computing

Kernel Integrity | Trusted Boot | Trusted Firmware

Homomorphic Encryption | Multiparty Calculation | Privacy Protection Algorithm — (Multi-party) Secure Computing

CPU/GPU/NPU/FPGA Asynchronous Computing Architecture Security | BCM/PCH/BIOS, etc. Asynchronous Computing Architecture Security — Computing Architecture Security - Firmware and Management Infrastructure

INTEL TEE/SGX | NIC and Other EC embedded controller security — Computing Architecture Security - Chip Security Capabilities

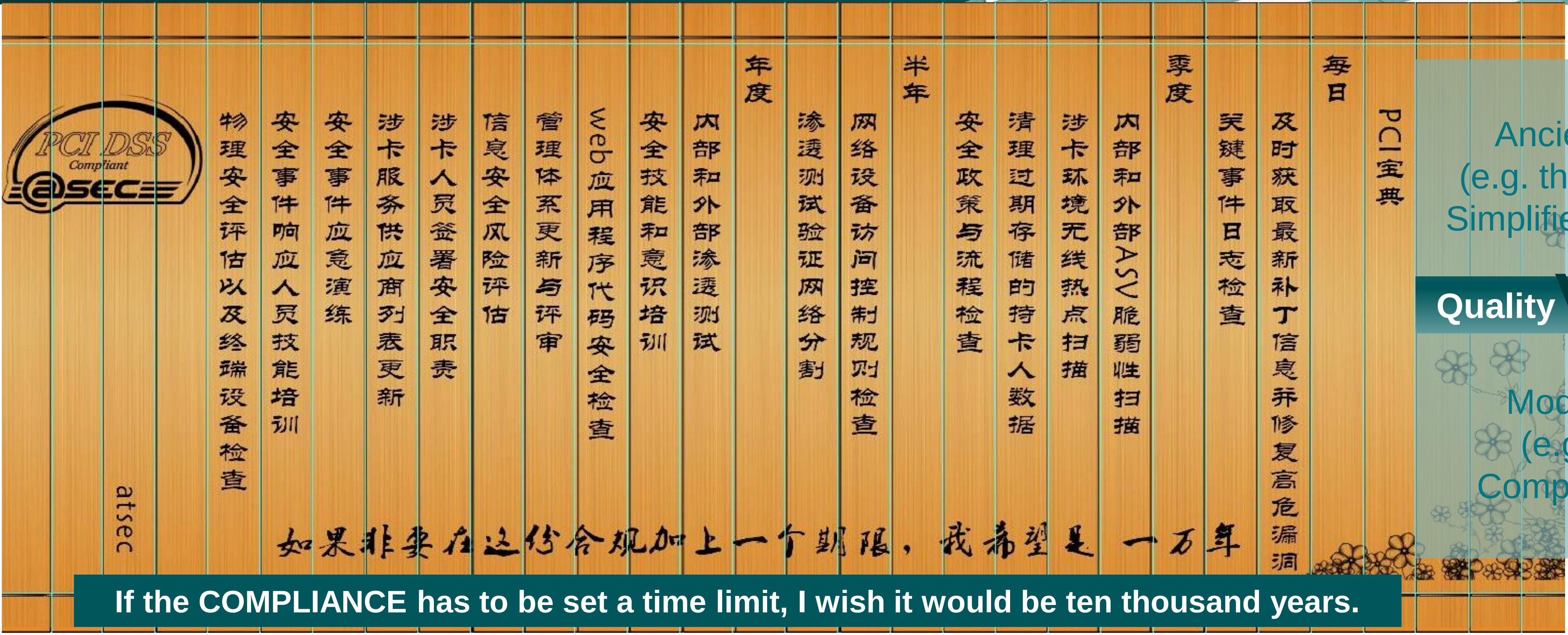
@sec the information security provider

腾讯标准 Tencent Standard

PCI Security Standards Council ®

Compliance Maintenance

Integrity the requirements into daily job activities!



PCI宝典

每日

及时获取最新补丁信息并修复高危漏洞

关键事件日志检查

季度

内部和外部ASV脆弱性扫描

涉卡环境无线热点扫描

清理过期存储的持卡人数据

安全政策与流程检查

半年

网络设备访问控制规则检查

渗透测试验证网络分割

年度

内部和外部渗透测试

安全技能和意识培训

web应用程序代码安全检查

管理体系更新与评审

信息安全风险评估

涉卡人员签署安全职责

涉卡服务供应商列表更新

安全事件应急演练

安全事件响应人员技能培训

物理安全评估以及终端设备检查

如果非要在这份合规加上一个期限，我希望是一万年

If the COMPLIANCE has to be set a time limit, I wish it would be ten thousand years.

Ancient Civilization
(e.g. the Art of Warfare):
Simplified & Summarized

Quality & Knowledge

VS

Modern Standard
(e.g. PCI DSS):
Complete & Accurate

Summary

Compliance process is a “romantic drama”

Just like “A Walk in the Clouds”, the characters are looking for true love;

“A PCI Walk in the Clouds”, the industry should work together to get ready for change because of new development, seek the true compliance, and improve the overall information security.

Thanks