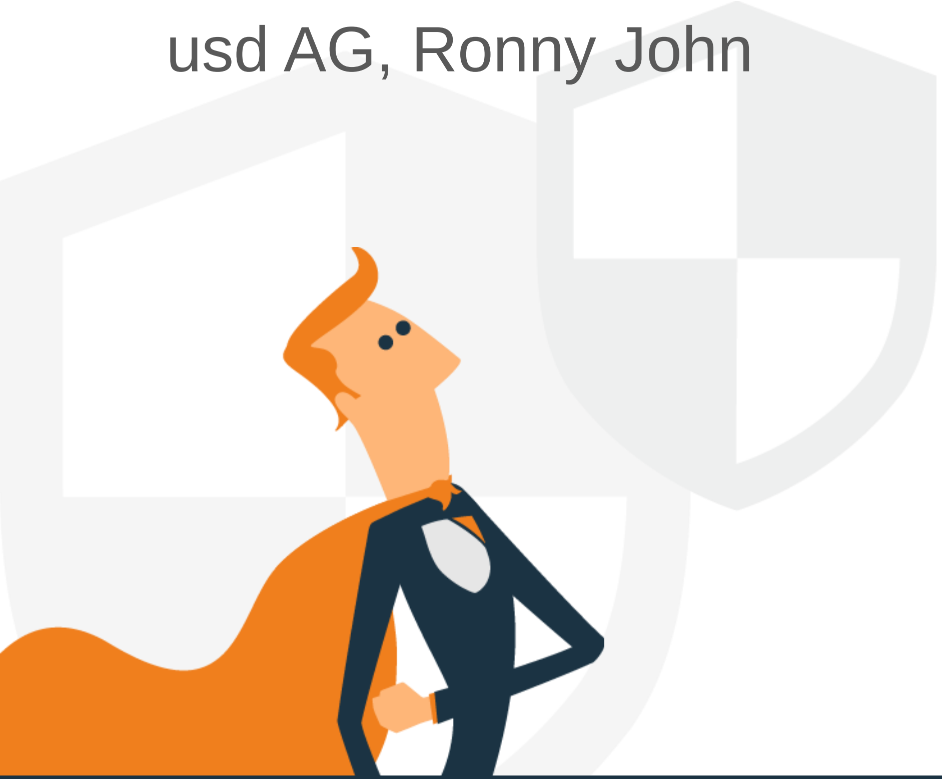
more security. usd

Security Management - Payment Security

Guest Lecture, 23.06.2015

usd AG, Ronny John



Agenda

- Introduction
- Context of IT Management and IT Security Management Systems
- PCI DSS Compliance
  - Overview
  - Scope and deep dive to selected requirements
  - Compliance Program for Merchants and Service Providers
  - Certification Process (Onsite Assessment)
- Summary

more security. usd

Introduction

usd AG & Ronny John

Mission & Facts

We protect companies and their customers against hackers and criminals.

- Owner managed, independent company
- Three locations in Neu-Isenburg, Darmstadt, Overath (close to Cologne)
- 11,6 million euro turnover in 2014
- 80 Employees…

…and always looking for new Heroes

Focus & Services

Security Management

Security Analysis & Pentests

PCI & Payment Security

Security Awareness

Security Recruiting

usd Academy

Ronny John

- Studies of *Electrical Engineering and Information Technology* at Darmstadt University of Technology
- IT Security Auditor and Consultant since 2007
- CISA & CISM (ISACA)
- QSA & PA-QSA (PCI SSC)
- Head of and responsible for the **Security Management Consulting** department at usd AG

Context of IT Management and IT Security Management Systems

IT & IT Security Management Systems

In organizations IT and IT Security Management systems are used:

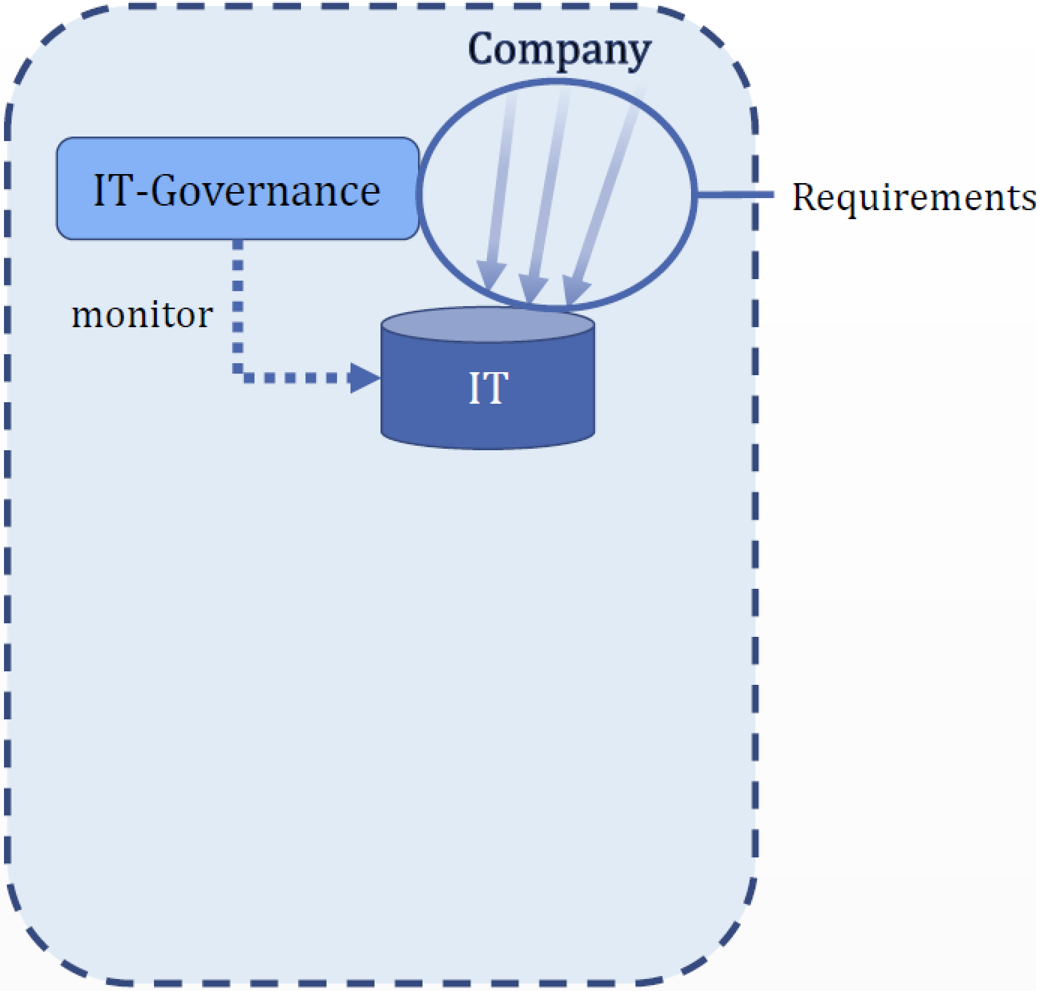
- to **establish**,
- to **implement**,
- to **operate**,
- to **monitor**, and
- to continuously **assess** and **improve**

their IT and risks associated with IT.

IT and IT Security Management is influenced by the requirements of an organization itself and of external stakeholders…

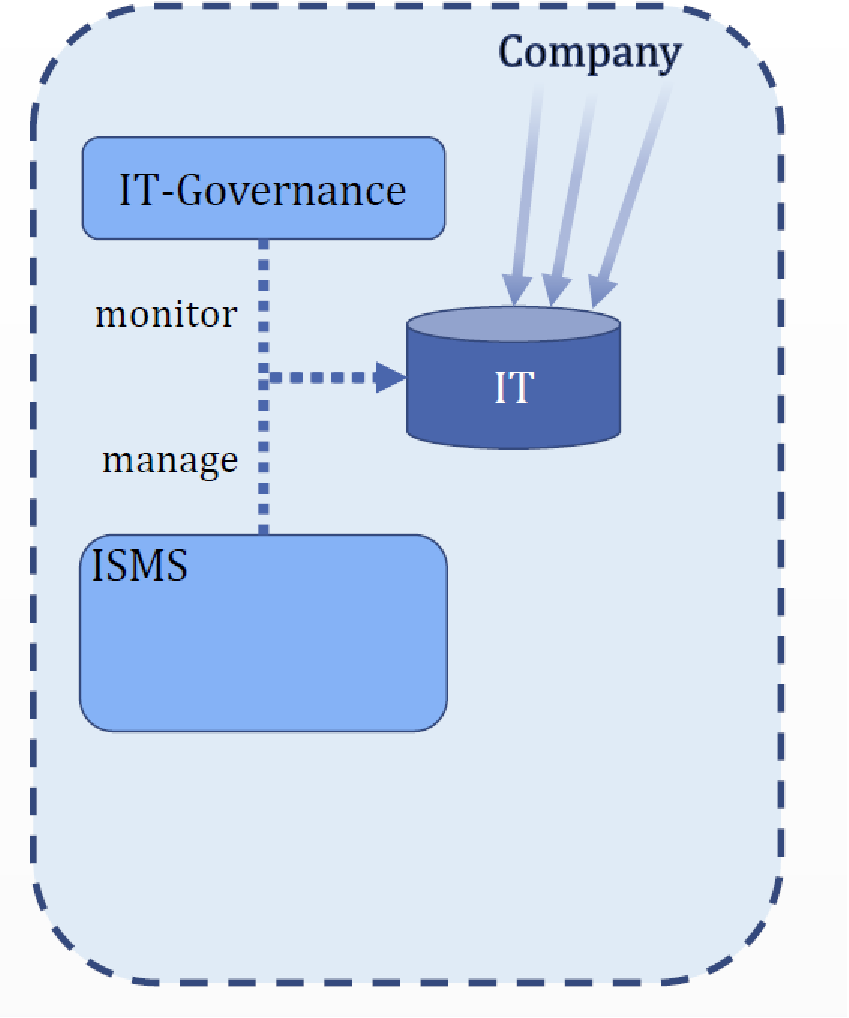
IT Governance

- Ensure that the company’s IT sustains and extends the company’s strategies and objectives



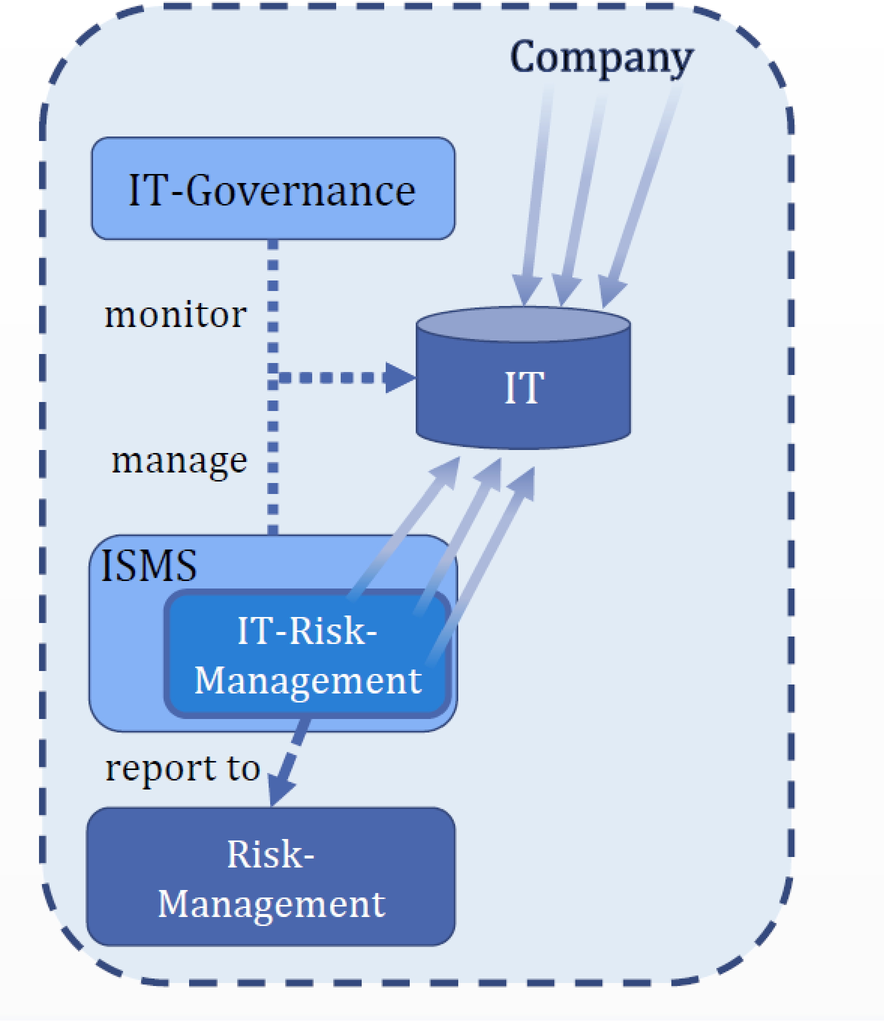
ISMS

- An Information Security Management System (ISMS) manages the IT regarding information security and IT related risks
- Based on a PDCA approach
- Typical protection targets of an ISMS are:
  - Confidentiality
  - Integrity
  - Availability
  - Authenticity (financial industry)



Risk-Management

- IT-Risk-Management is a part of the ISMS
- It contributes to the company wide risk management
- Often based on ISO 27005
- IT-Risk-Management influences IT (e.g. by applying additional security measures based on a risk determination)

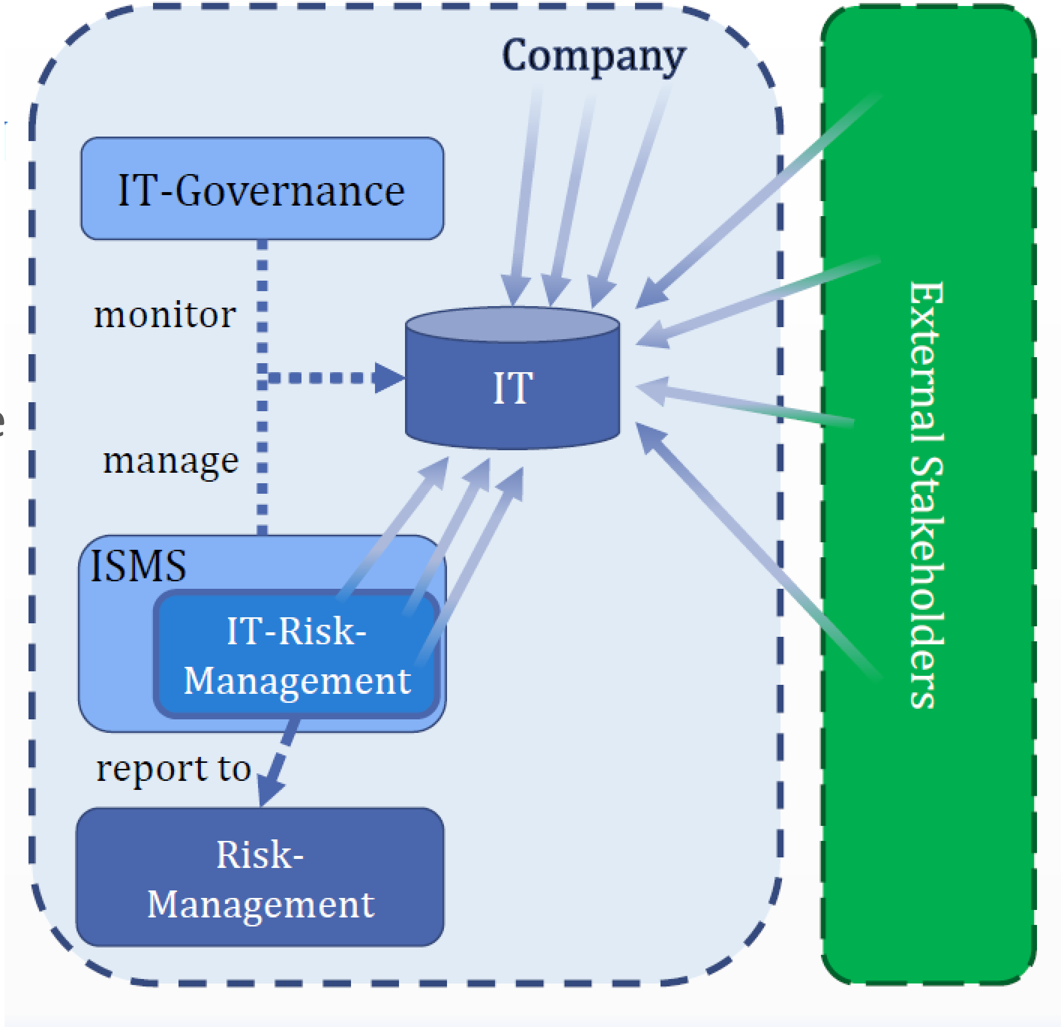


Internal & External Requirements

- IT must cope not only with internal but also with external requirements…

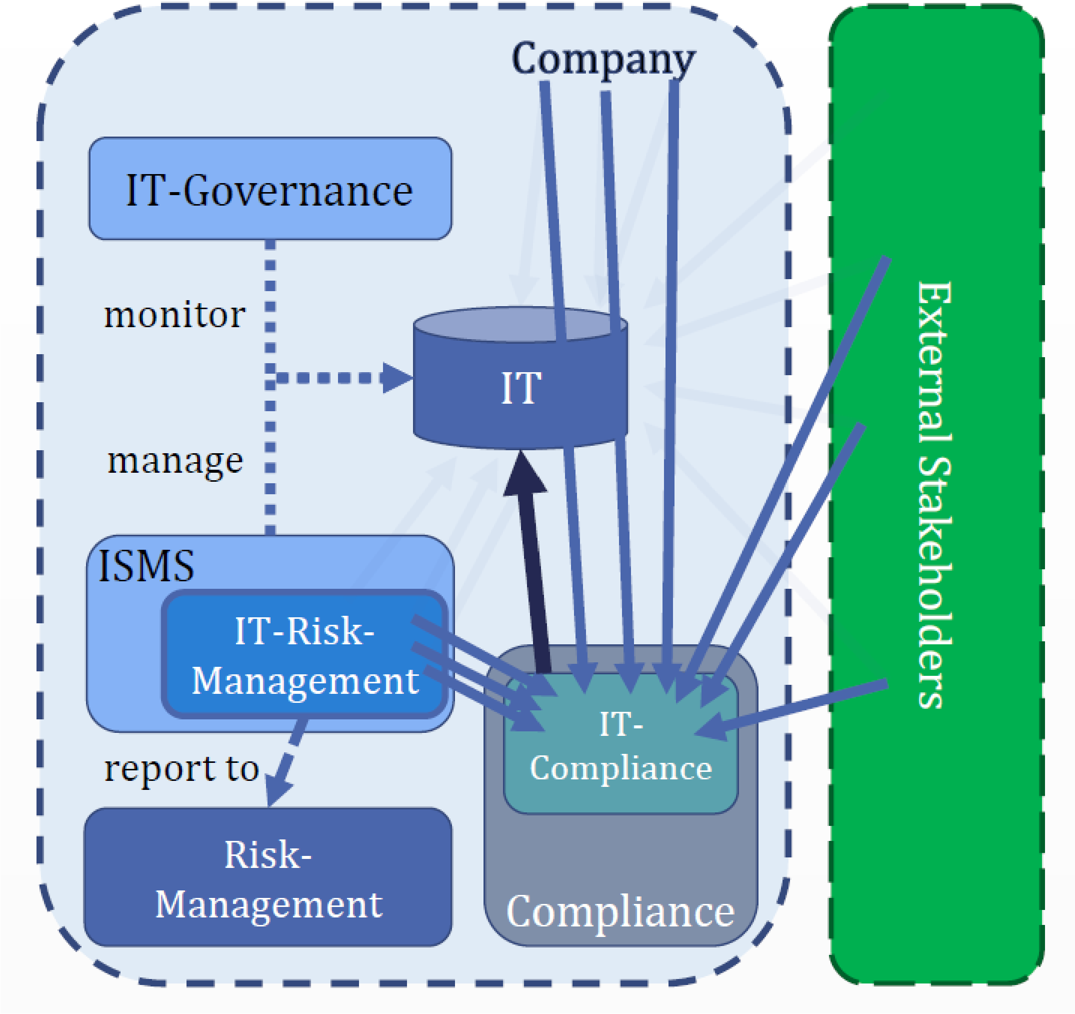
- External stakeholders have
  - **legal**,
  - **regulatory**, and/or
  - **business/contractual**

  constraints and requirements



IT Compliance

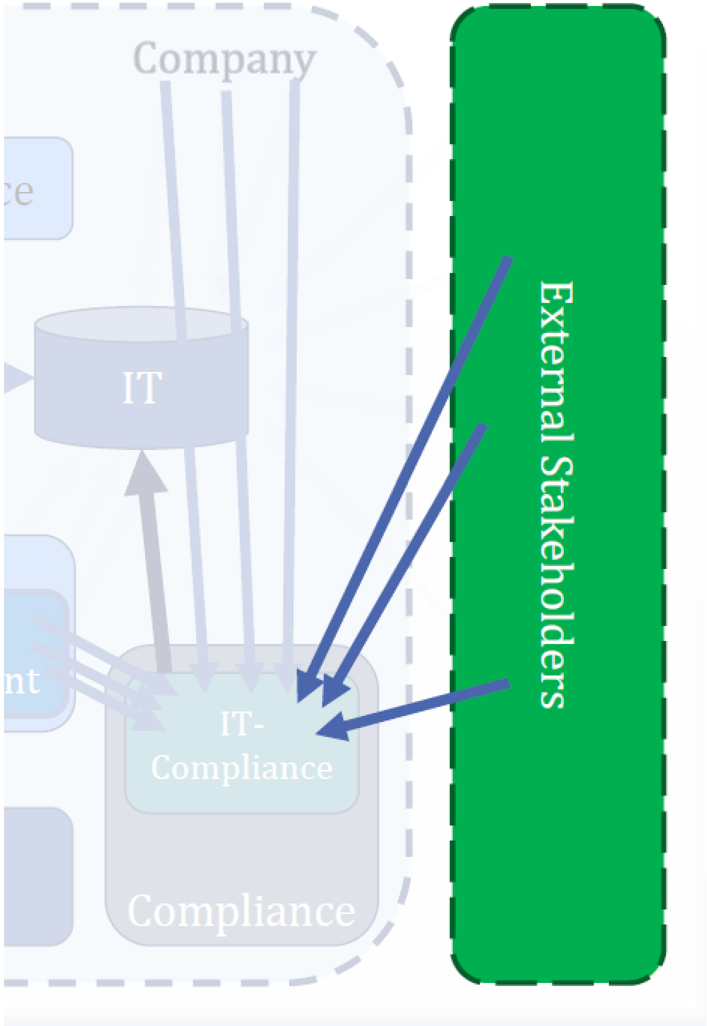
- IT Compliance ensures that internal and external requirements are known, and efficiently and effectively met and supported by IT
- Often, high risks are associated with compliance requirements



Focus on external requirements (1)

- Examples:
  - BDSG, GoBS, GDPdU, KonTraG, Basel II, SOX, Euro-SOX (Legal), IT Sicherheitsgesetz
  - MaRisk (Regulatory)
  - SLAs, RFI/RFP Requirements, PCI DSS, ISO 27001 (Business or contractual)

- In the following we will focus on the business requirement **PCI DSS**
  - also titled “PCI” or “Payment Security”

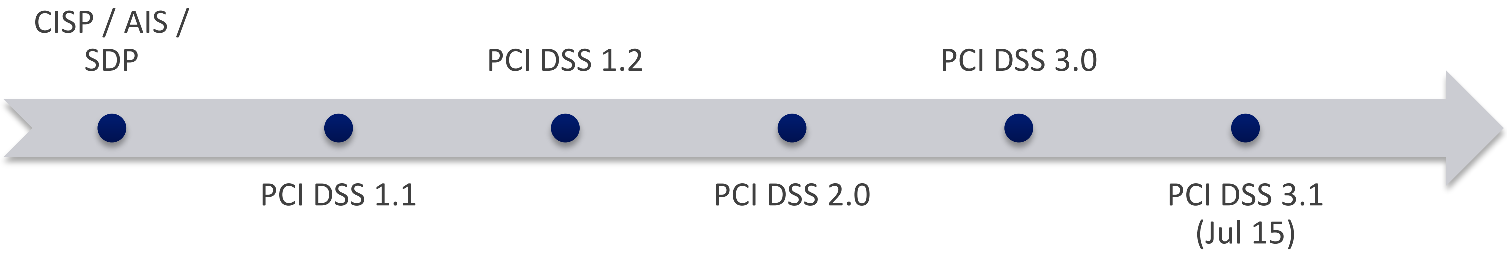


PCI DSS

Overview

History of Payment Security

- The credit card organizations have been concerned about the security of their credit cards for many years
- Previously each organization developed their own security programs
  - Visa: Account Information Security (AIS)
  - MasterCard: Site Data Protection Program (SDP)
  - American Express: Data Security Operating Policy
- Since 2006 a common international standard for the security of credit card data exists



PCI Data Security Standard

- The **P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard (PCI DSS) is a security standard managing the protection of credit card data
- Current Version: 3.1 (July 2015)
- Goals
  - Improved protection of credit card payment against theft or misuse
  - Significant increase of the general security standards and the acceptance in the credit card industry
  - Reducing liability risks

PCI – Payment Card Industry

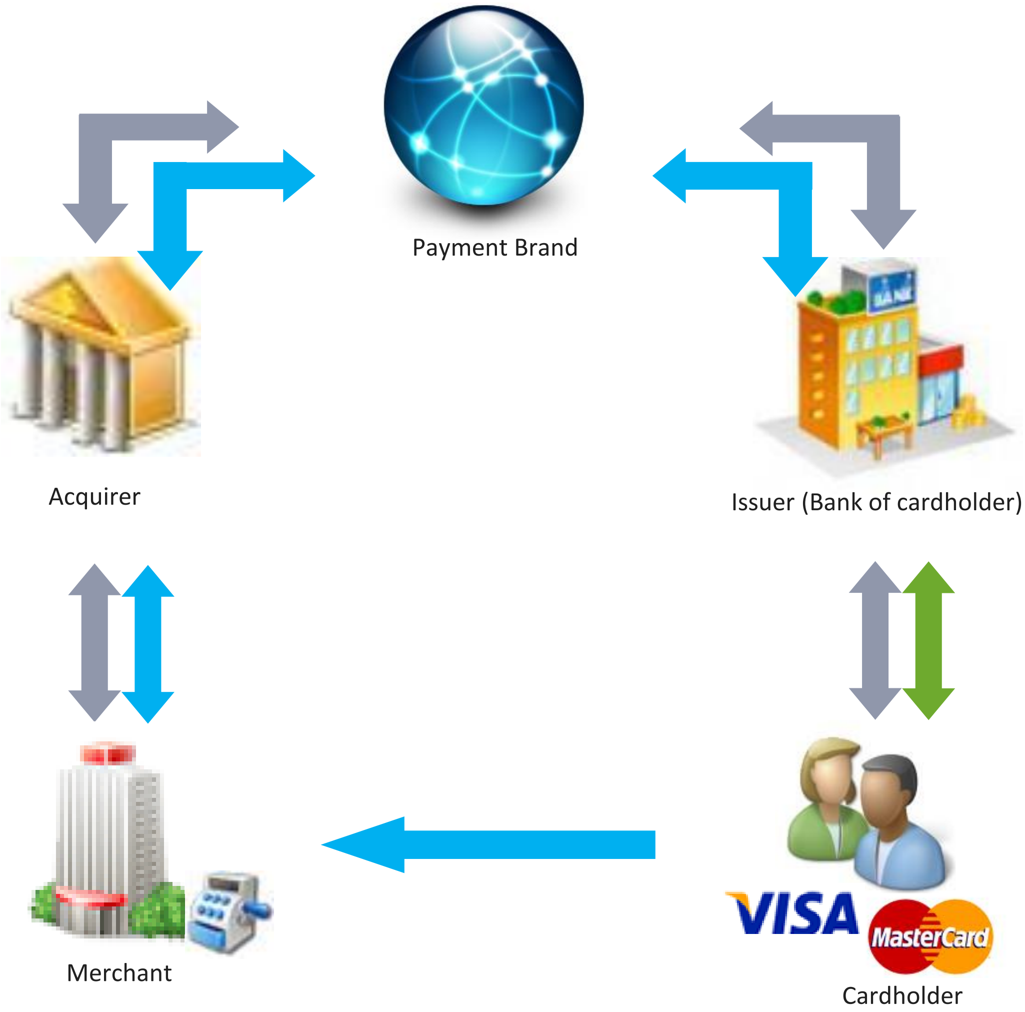
- PCI Security Standards Council (PCI SSC)
  - https://www.pcisecuritystandards.org
- Founding members
  - American Express
  - Discover Financial Services
  - JCB International
  - MasterCard Worldwide
  - Visa Inc.
- Duties and responsibilities
  - Continuous development, improvement, dissemination and implementation of the PCI standards
  - Training and accreditation of the auditors and auditing companies (QSA, PA-QSA, ASV, PTS)

PCI DSS Compliance

- Each credit card organization (payment brand) develops and enforces its own payment security compliance programs
  - Requirements for the classification and rating of merchants and service providers
  - Requirements for the kind of validation and reporting
  - Maintains a list of all certified service providers
  - Compliance programs for acquirers (merchant compliance)
  - Determination of deadlines („compliance mandates“)
  - Own security awareness programs

- Example Visa: Account Information Security (AIS)
- Example MasterCard: Site Data Protection (SDP)

Process of credit card transactions



Payment Brand

Acquirer

Issuer (Bank of cardholder)

Merchant

Cardholder

Protection of credit card data (1)

- Cardholder data that is relevant regarding transactions and therefore deserves protection consists of
  - PAN (Primary Account Number)
  - Cardholder name
  - Expire date
- This cardholder data is allowed to be stored
- PAN has to be protected

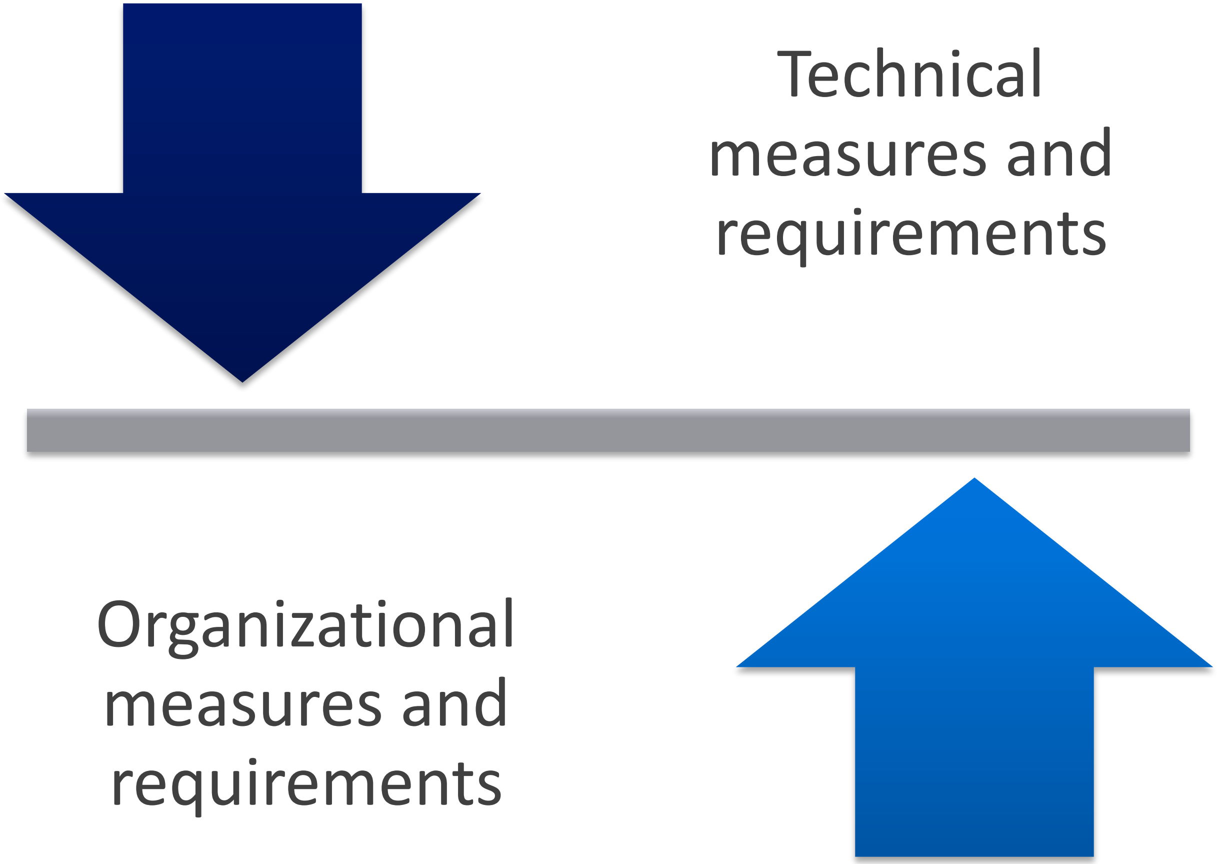
Protection of credit card data (2)

- Very critical (sensitive) credit card data
  - Card validation code (CVV2, CVC2)
  - PIN number
  - Complete image of the chip/magnetic stripe
- May only be cached temporarily until the transaction is authorized
- Must be deleted after authorization

PCI DSS – Goals and Requirements (1)

Control Objectives	No.	Requirements
Build and maintain a secure network	1	Install and maintain a firewall configuration
	2	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3	Protect stored cardholder data
	4	Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5	Use and regularly update anti-virus software
	6	Develop and maintain secure systems and applications
Implement strong access control measures	7	Restrict access to cardholder data by business need-to-know
	8	Assign an unique ID to each person with computer access
	9	Restrict physical access to cardholder data
Regularly monitor and test networks	10	Track and monitor all access to network resources and cardholder data
	11	Regularly test security systems and processes
Maintain an information security policy	12	Maintain a policy that addressees information security

PCI DSS – Goals and Requirements (2)



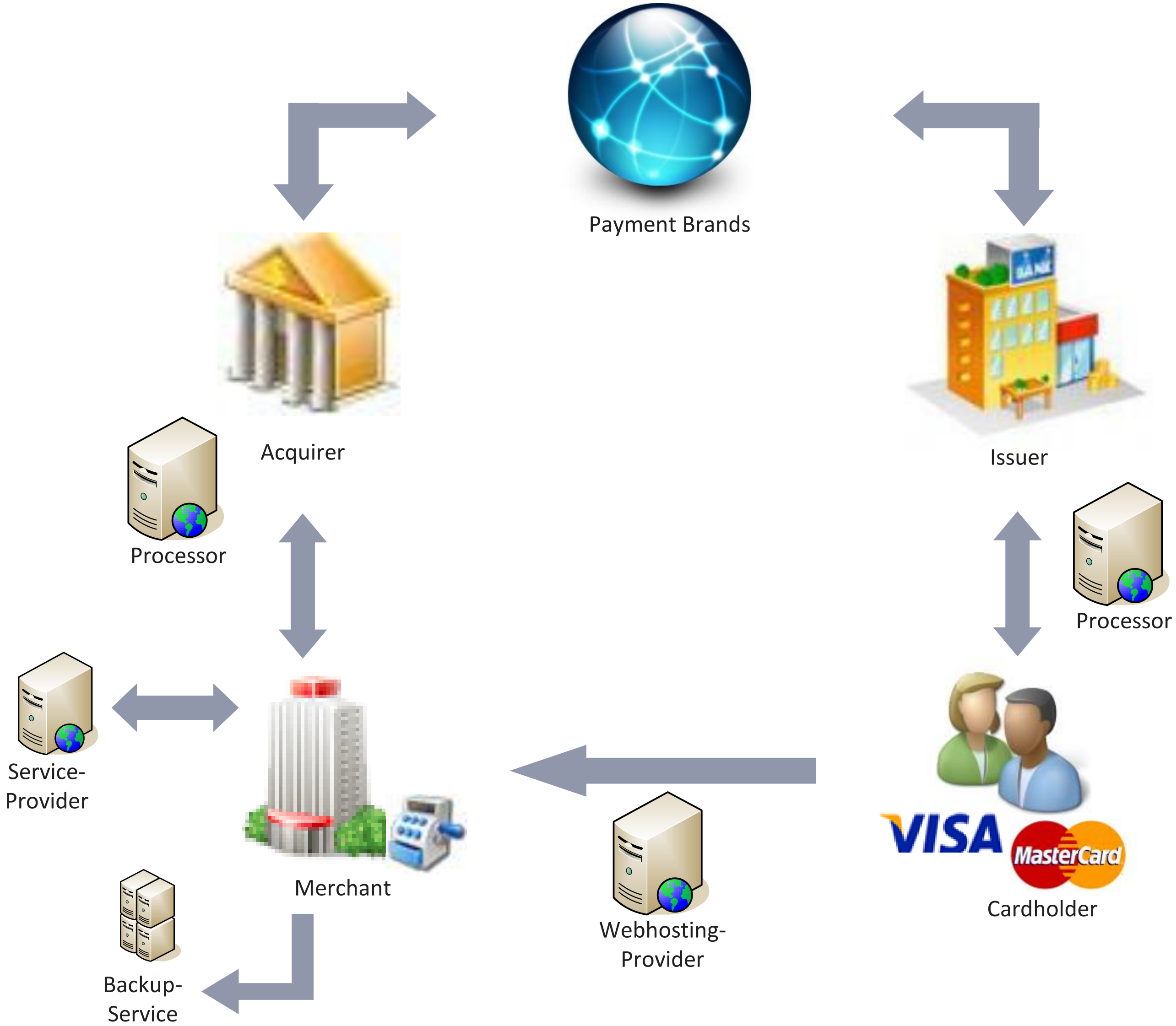
Technical measures and requirements

Organizational measures and requirements

Scope of the PCI Standard (1)

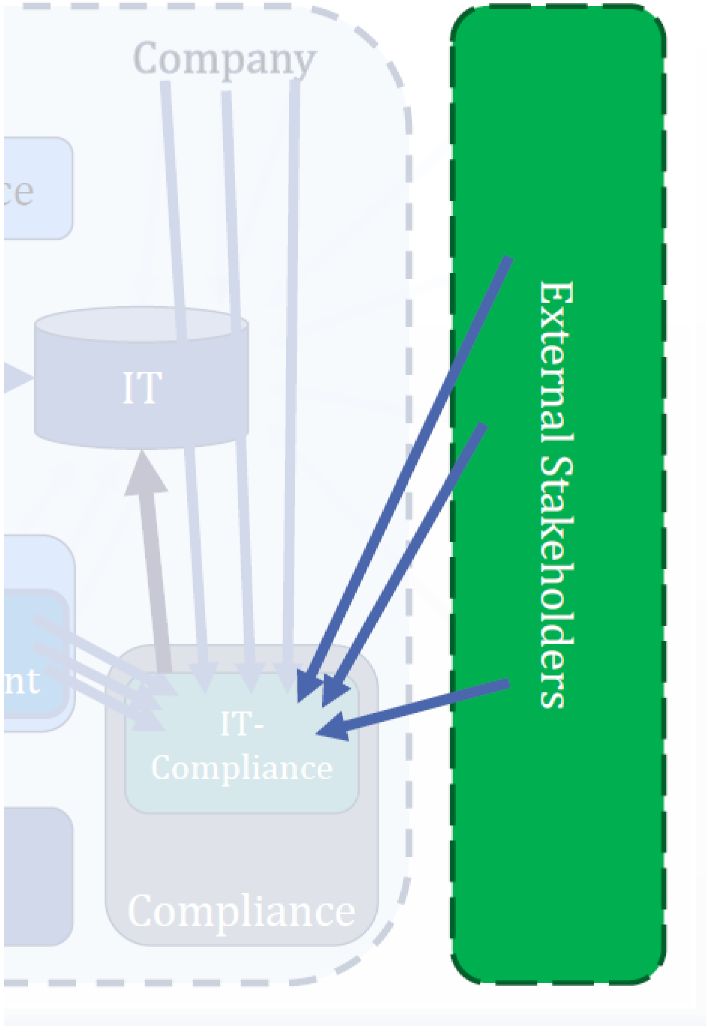
- The standard applies to all companies involved in the processing, storing or transmitting of credit card data
  - Acquirers, Issuers
  - Merchants
  - Service Providers
    - for money transfer
    - IT services
    - other services including access or a security impact to credit card data

Scope of the PCI Standard (2)



Review…

- In context of Payment Security, external stakeholders can be:
  - The Payment Brands (Visa, MC & Co.) for Banks, Merchants, Service Providers
  - Acquiring and Issuing Banks for Merchants
  - Merchants for Payment Service Provider



PCI DSS

Scope and deep dive to selected requirements

Scope

- The PCI DSS security requirements apply to all system components in the **C**ardholder **D**ata **E**nvironment (CDE)
- The CDE is defined as the part of the company's network that is comprised of **all system components** that **store**, **process** or **transmit** credit card data
- Reducing the scope by either changing processes or by using **segmentation** is the first and valuable step in a PCI DSS certification project

- Segmentation is often implemented on network level and can be achieved by the use of firewalls, routers, subnets, VLANs etc.

Selected requirements in detail

Control Objectives	No.	Requirements
Build and maintain a secure network	1	Install and maintain a firewall configuration
	2	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3	Protect stored cardholder data
	4	Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5	Use and regularly update anti-virus software
	6	Develop and maintain secure systems and applications
Implement strong access control measures	7	Restrict access to cardholder data by business need-to-know
	8	**Assign an unique ID to each person with computer access**
	9	Restrict physical access to cardholder data
Regularly monitor and test networks	10	Track and monitor all access to network resources and cardholder data
	11	Regularly test security systems and processes
Maintain an information security policy	**12**	**Maintain a policy that addressees information security**

Requirement 8: User accounts

- Assign all users a unique user account
- Group accounts and shared passwords/tokens are not permitted
- Inactive accounts have to be disabled after 90 days
- Remove accounts of employees that have left the company immediately
- Users have to authenticate with a password (or a sec. token)
- Passwords have to be rendered unreadable during transmission and storage
- Verify user identity before performing password resets
- Disable all accounts used by vendors (or enable only when needed and monitor vendor activities)

Requirement 8: Password Policy

- Set passwords for first-time use to unique values and change immediately after first login
- Minimum password length of at least seven characters containing both numeric and alphabetic characters
- Change user passwords after 90 days
- The last four passwords may not be re-used
- Lockout user accounts after six access attempts for at least 30 minutes
- User have to re-authenticate after a session has been idle for more than 15 minutes

Requirement 12: Information Security Policy

- Create an information security policy and distribute it to all relevant personnel and to vendors and business partners
  - The policy must be reviewed and updated once a year
  - The employees must acknowledge annually that they have read and understood the information security policy
- Implement a risk-assessment process that identifies critical assets, threats, and vulnerabilities, and results in a formal risk assessment (e.g. based on ISO 27005, etc.)
  - The process must be performed at least annually

Requirement 12: Employee-facing Technology

- Develop usage policies for critical technologies (Internet, e-mail, PDAs, smartphones, laptops, wireless technologies, remote access technologies) which are directly accessible by the employees
  - Explicit approval of the management is necessary to use the technologies
  - Users must authenticate in order to use the technologies
  - An inventory for all systems and products must be maintained
  - Systems and products must be labelled (owner, contact information, purpose)
- Usage policies
  - Which systems and products may be used
  - How and where these systems and products may be used
  - Copying credit card data onto these systems is prohibited

Requirement 12: IT Security Responsibilites

- An IT Security Officer (ISO) must be nominated
- The following responsibilities must be assigned to the security officer or a team:
  - Maintenance of the information security policy
  - Definition and implementation of necessary security processes
  - Monitoring of log files (access and system)
  - Administration of the user accounts
  - Administration and control of access to credit card data

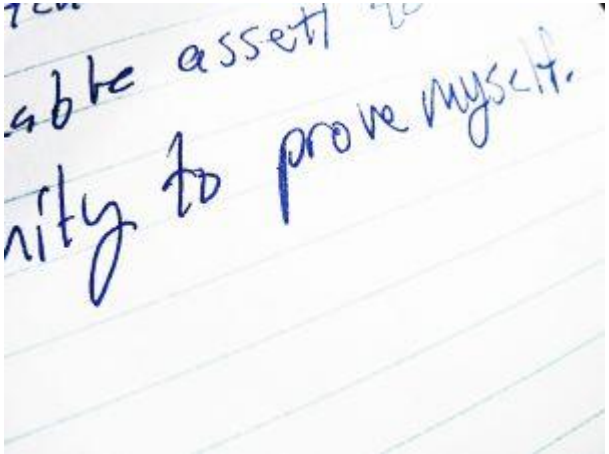
Requirement 12: Security Awareness

- Employees must be educated upon hire and annually regarding the handling of credit card data
  - Do not copy credit card data
  - Do not pass credit card data to third parties
  - Store paper receipts securely
  - Shred paper-based information if not needed any more
  - Proper handling of system components
  - Instruction to follow security processes
  - General IT security training (spam, malware, viruses)

- Training should be based on e.g. posters, letters, memos, meetings, web-based training
- Every employee has to acknowledge annually that he has read and understood the information security policy

Requirement 12: Responsibilities of HR

- Perform background checks on potential personnel for jobs with access to critical system components (Administrator, Security Officer, Manager)
  - Identity
  - Correspondence
  - Detailed CV
  - Qualification and professionalism
  - All other noticeable problems



Requirement 12: Contracts with Providers

- If cardholder data is shared with a service provider or the service provider has access to such data, the contract must include a clause, in which the provider acknowledges that he is responsible for the security of the cardholder data in his possession
- Maintain a list of all service providers
- Maintain a document about which PCI DSS requirements are managed by the service provider and which by the entity

- Verify the compliance status of the service provider annually
- Implement a process for engaging service providers

Requirement 12: Incident Response Plan

- Incident response plan (IRP) in the case of credit card data compromise
  - Preservation of evidence
  - Inform acquirer and appropriate public authorities
  - Provide a “Compromised Entity Details Report” to the payment brands or the acquirer (in case entity is a merchant)
  - Report of all compromised accounts within 7 days
- Specific personnel must be available at any time (24/7)
- IRP has to be tested annually and updated if needed
- Provide training to employees with corresponding responsibilities

more security. usd

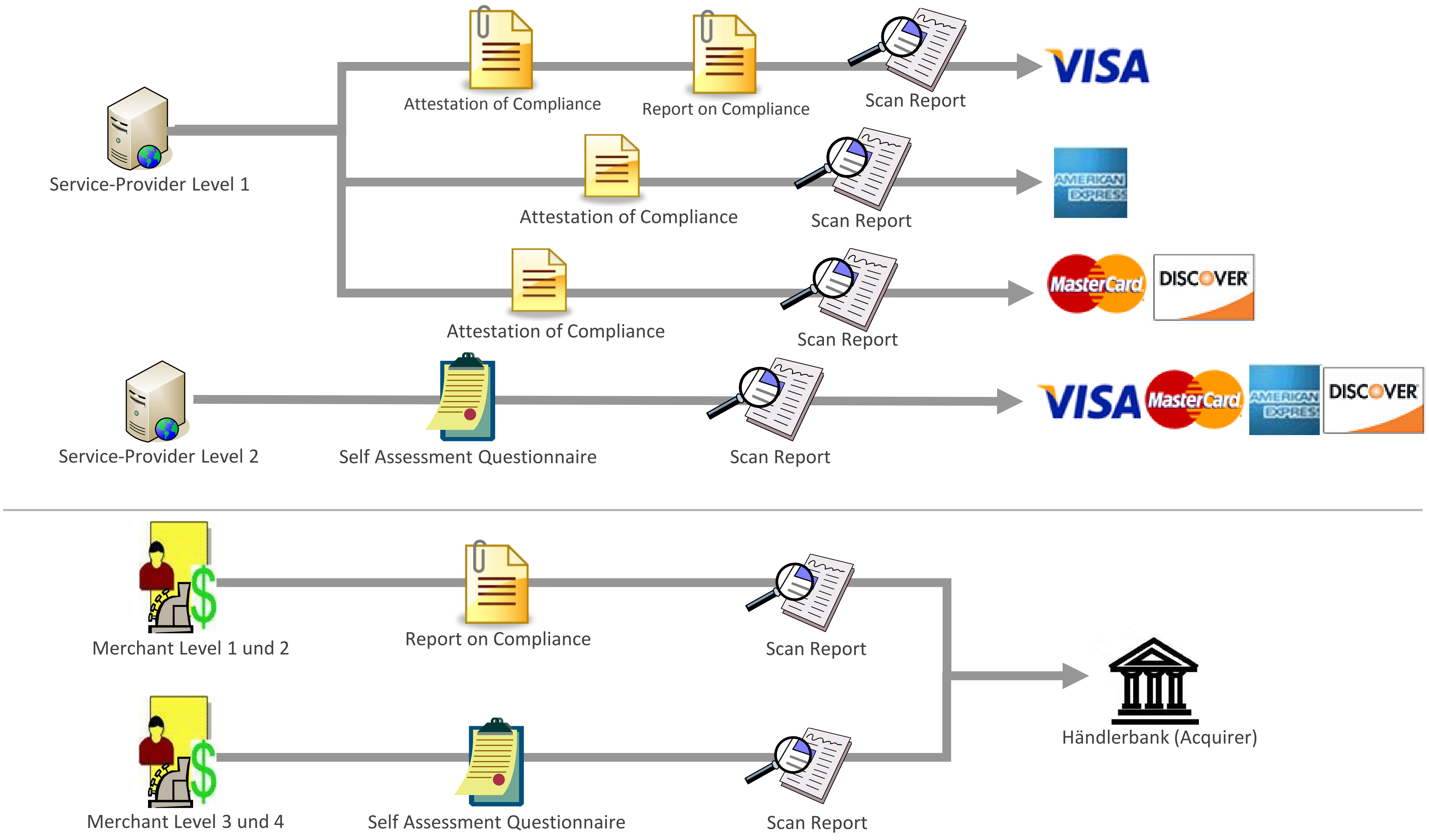
PCI DSS

Compliance Program
for Merchants and Service Providers

PCI DSS Compliance

- **Merchants and service providers are classified into different levels each with differing requirements regarding the compliance process**
- This classification depends on the number of processed transactions and the accepted card brands
- Generally, an acquirer is entitled to increase the level for every merchant and may demand an audit
- In case of a compromise merchants and service providers are immediately classified level 1

PCI DSS Reporting



Service-Provider Level 1

Attestation of Compliance

Report on Compliance

Scan Report

Attestation of Compliance

Scan Report

Attestation of Compliance

Scan Report

Service-Provider Level 2

Self Assessment Questionnaire

Scan Report

Merchant Level 1 und 2

Report on Compliance

Scan Report

Merchant Level 3 und 4

Self Assessment Questionnaire

Scan Report

Händlerbank (Acquirer)

Service Providers

- Organizations that process, store or transmit credit card data on behalf of another entity (e.g. merchants)
- Organizations that provide services that control or could impact the security of cardholder data
- Explicitly excluded are network operators that have no access to credit card data (public networks)
  - e.g. Telekom: provides network infrastructure for data transfer, but has no access to encrypted data

PCI DSS Classification - Service Provider

Level	American Express	MasterCard	Visa Europe
1	All service providers	Service providers that stores, processes and/or transmits over 300,000 transactions per year	Service providers that stores, processes and/or transmits over 300,000 transactions per year
2	-	Service providers that stores, processes and/or transmits less than 300,000 transactions per year	Service providers that stores, processes and/or transmits less than 300,000 transactions per year

PCI DSS Methods of validation - Service Providers

Strength of validation method

Risk

Classification	Self-Assessment-Questionnaire	Security Scan	Onsite Audit
Level-1 Service Providers	-	Quarterly	Annually
Level-2 Service Providers	Annually	Quarterly	-

more security. usd

PCI DSS Classification - Merchants

Level	American Express	MasterCard	Visa Europe
1	> 2,5 million transactions per year	> 6 million transactions per year	> 6 million transactions per year
2	50,000 to 2,5 million transactions per year	1 million to 6 million transaction per year	1 million to 6 million transactions per year
3	< 50,000 transactions per year	20,000 to 1 million transactions per year	20,000 to 1 million e-commerce transactions per year
4	-	All other merchants	20,000 to 1 million non e-commerce transactions per year
	-	-	< 20,000 e-commerce transactions per year

PCI DSS Methods of validation - Merchants

Strength of validation method

Risk

Level	Self-Assessment-Questionnaire	Security Scan	Onsite Audit
Level-1 merchant	-	Quarterly	Annually
Level-2 merchant (MC*)	-	Quarterly	Annually
Level-2 merchant (VISA, MC*)	Annually	Quarterly	-
Level-3 merchant	Annually	Quarterly	-
Level-4 merchant **	Annually	Quarterly	-

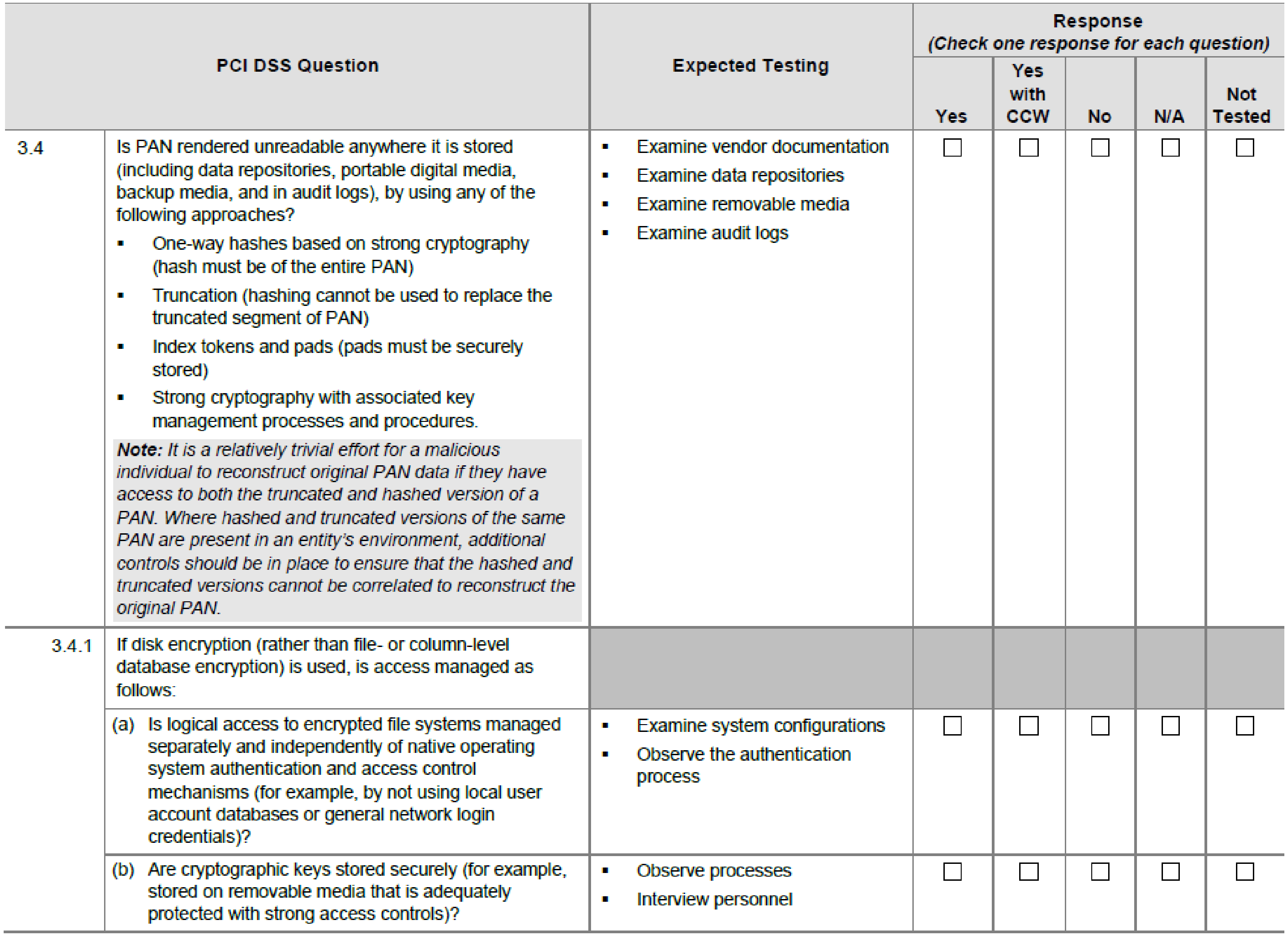
MC: Level-2 merchants can can have their PCI compliance certified either via an onsite-audit, conducted by a QSA, or via an SAQ with the help of an ISA

VISA: Level-3 merchants and level-4 e-commerce merchants can have their own PCI compliance certified to the acquirer (via SAQ) or use a certified service provider

Assessment Types

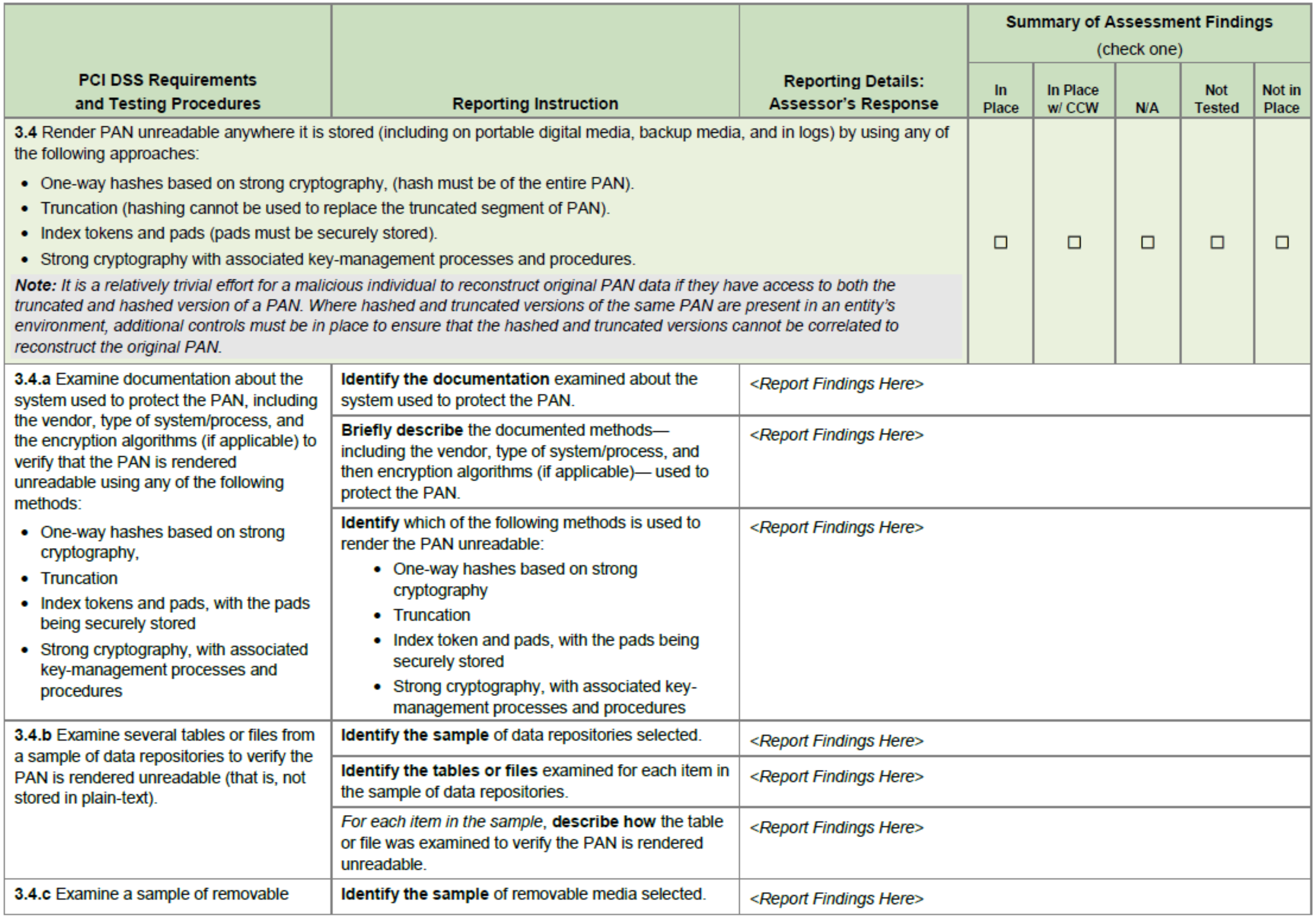
- Self-Assessment-Questionnaire (SAQ)
  - Depending on the merchant’s business processes special kind of questionnaire are available which differ in size and complexity
- Onsite-Assessment
  - Performed by an QSA or an internal qualified assessor according to defined testing procedures and reporting instructions

Example: Self-Assessment-Questionnaire



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
3.4	Is PAN rendered unreadable anywhere it is stored (including data repositories, portable digital media, backup media, and in audit logs), by using any of the following approaches? ▪ One-way hashes based on strong cryptography (hash must be of the entire PAN) ▪ Truncation (hashing cannot be used to replace the truncated segment of PAN) ▪ Index tokens and pads (pads must be securely stored) ▪ Strong cryptography with associated key management processes and procedures. ***Note:*** *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*	▪ Examine vendor documentation ▪ Examine data repositories ▪ Examine removable media ▪ Examine audit logs	□	□	□	□	□
3.4.1	If disk encryption (rather than file- or column-level database encryption) is used, is access managed as follows:						
	(a) Is logical access to encrypted file systems managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials)?	▪ Examine system configurations ▪ Observe the authentication process	□	□	□	□	□
	(b) Are cryptographic keys stored securely (for example, stored on removable media that is adequately protected with strong access controls)?	▪ Observe processes ▪ Interview personnel	□	□	□	□	□

Example: Onsite Assessment Report

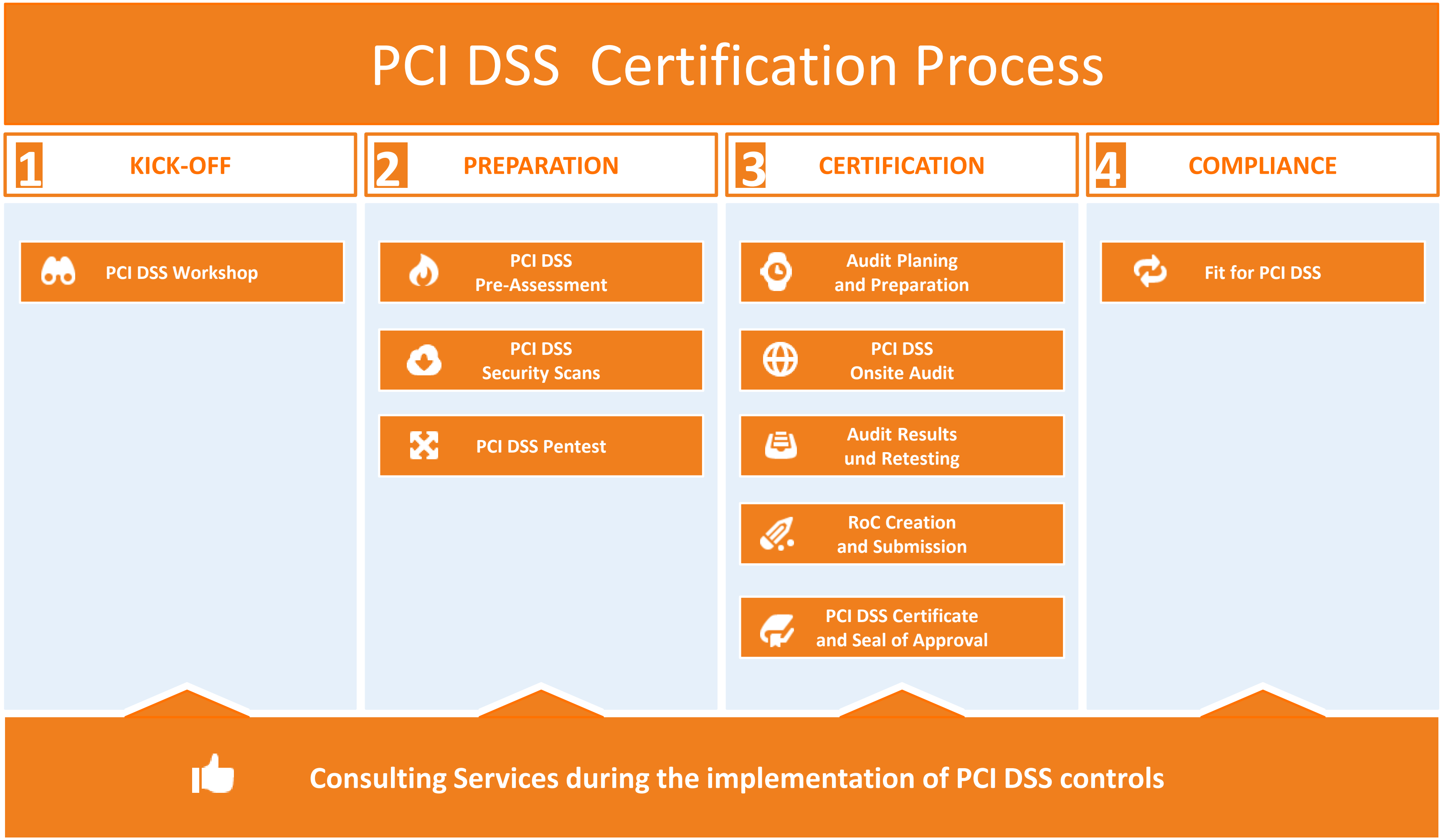


PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN). • Truncation (hashing cannot be used to replace the truncated segment of PAN). • Index tokens and pads (pads must be securely stored). • Strong cryptography with associated key-management processes and procedures. ***Note:** It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*			□	□	□	□	□
3.4.a Examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the following methods: • One-way hashes based on strong cryptography, • Truncation • Index tokens and pads, with the pads being securely stored • Strong cryptography, with associated key-management processes and procedures	**Identify the documentation** examined about the system used to protect the PAN.	*<Report Findings Here>*					
	Briefly describe the documented methods—including the vendor, type of system/process, and then encryption algorithms (if applicable)— used to protect the PAN.	*<Report Findings Here>*					
	Identify which of the following methods is used to render the PAN unreadable: • One-way hashes based on strong cryptography • Truncation • Index token and pads, with the pads being securely stored • Strong cryptography, with associated key-management processes and procedures	*<Report Findings Here>*					
3.4.b Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).	**Identify the sample** of data repositories selected.	*<Report Findings Here>*					
	Identify the tables or files examined for each item in the sample of data repositories.	*<Report Findings Here>*					
	For each item in the sample, **describe how** the table or file was examined to verify the PAN is rendered unreadable.	*<Report Findings Here>*					
3.4.c Examine a sample of removable	**Identify the sample** of removable media selected.	*<Report Findings Here>*					

PCI DSS

Certification Process (Onsite Assessment)

Certification process overview for Level 1 entities



PCI DSS Certification Process

1 KICK-OFF

- PCI DSS Workshop

2 PREPARATION

- PCI DSS Pre-Assessment
- PCI DSS Security Scans
- PCI DSS Pentest

3 CERTIFICATION

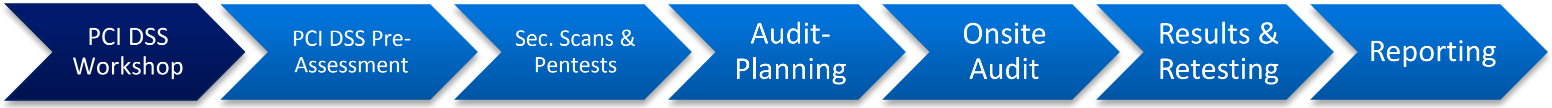
- Audit Planing and Preparation
- PCI DSS Onsite Audit
- Audit Results und Retesting
- RoC Creation and Submission
- PCI DSS Certificate and Seal of Approval

4 COMPLIANCE

- Fit for PCI DSS

Consulting Services during the implementation of PCI DSS controls

Phase 1 – Scope Workshop



PCI DSS Workshop

PCI DSS Pre-Assessment

Sec. Scans & Pentests

Audit-Planning

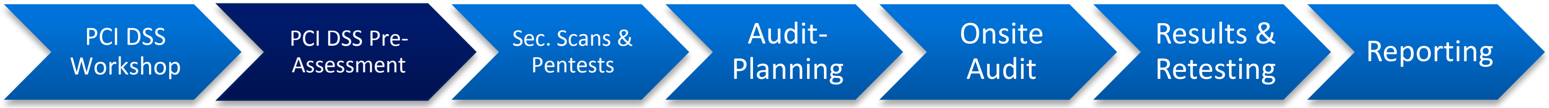
Onsite Audit

Results & Retesting

Reporting

- Overview and introduction to the standard
- Preliminary definition of the audit scope
- Data flow analysis of credit card data
  - Identification of all business areas and processes that deal with credit card data
  - Identification of all systems and applications that stores, processes or transmits credit card data
- Planning of the following work phases

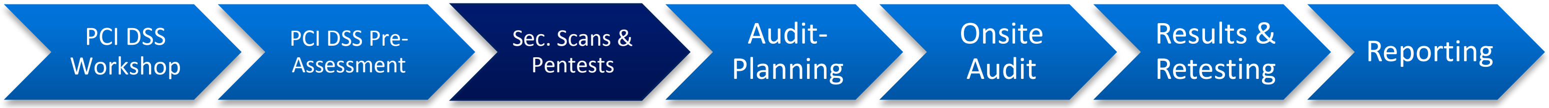
Phase 2 – Pre-Assessment



PCI DSS Workshop → PCI DSS Pre-Assessment → Sec. Scans & Pentests → Audit-Planning → Onsite Audit → Results & Retesting → Reporting

- Examination
  - of relevant systems, applications and locations
  - of documentation and processes
- Result
  - Description of the deviations from the standard („Gaps“)
  - Action Plan including recommendations and schedule

Phase 3 – Security Scans & Penetration tests



PCI DSS Workshop

PCI DSS Pre-Assessment

Sec. Scans & Pentests

Audit-Planning

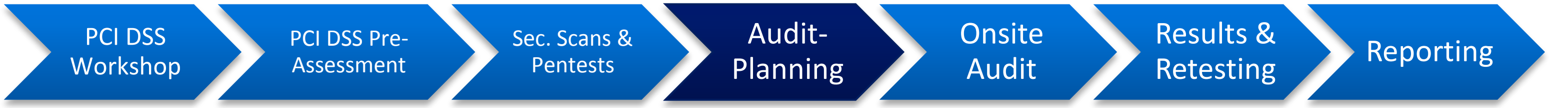
Onsite Audit

Results & Retesting

Reporting

- Quarterly Vulnerability scans (ASV scans)
  - Identification of security risks in all systems and services that are reachable from the Internet
  - Vulnerability scans have to be performed by an ASV (Approved Scanning Vendor)
- Yearly Penetration test
  - Network-layer, system-layer and application-layer tests
  - Testing from outside and inside the network
  - Tests to verify the effectiveness of segmentation controls

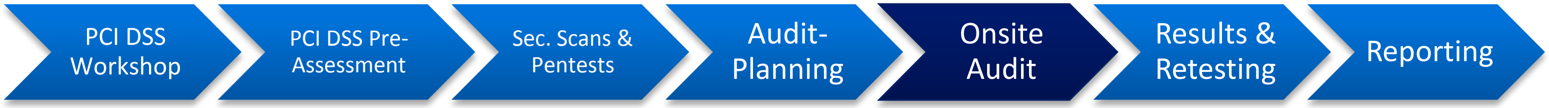
Phase 4 – Planning



PCI DSS Workshop → PCI DSS Pre-Assessment → Sec. Scans & Pentests → Audit-Planning → Onsite Audit → Results & Retesting → Reporting

- Define audit scope in in cooperation with the customer
- Develop an audit agenda
- Scheduling of audit sessions and topics

Phase 5 – Onsite Audit



PCI DSS Workshop

PCI DSS Pre-Assessment

Sec. Scans & Pentests

Audit-Planning

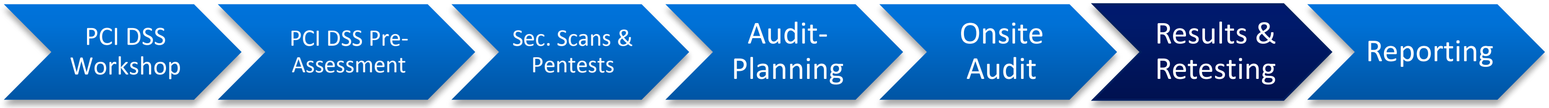
Onsite Audit

Results & Retesting

Reporting

- The audit is always an onsite formal process
- Sampling of technical systems
- Review of documentation (policies & procedures)
- Review of evidence (checklists, tickets, signed forms)
- Interviews with employees to verify the availability and knowledge of policies and procedures

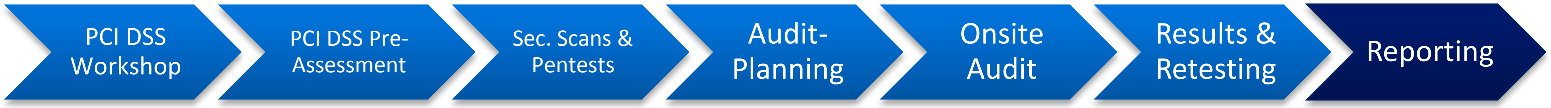
Phase 6 – Results



PCI DSS Workshop → PCI DSS Pre-Assessment → Sec. Scans & Pentests → Audit-Planning → Onsite Audit → Results & Retesting → Reporting

- Documentation of found deviations with corresponding correction measures
- Customer has the ability to correct all deviations during the onsite audit and later (timeframe in understanding with the auditor)
- Re-testing is possible or needed

Phase 7 – Reporting



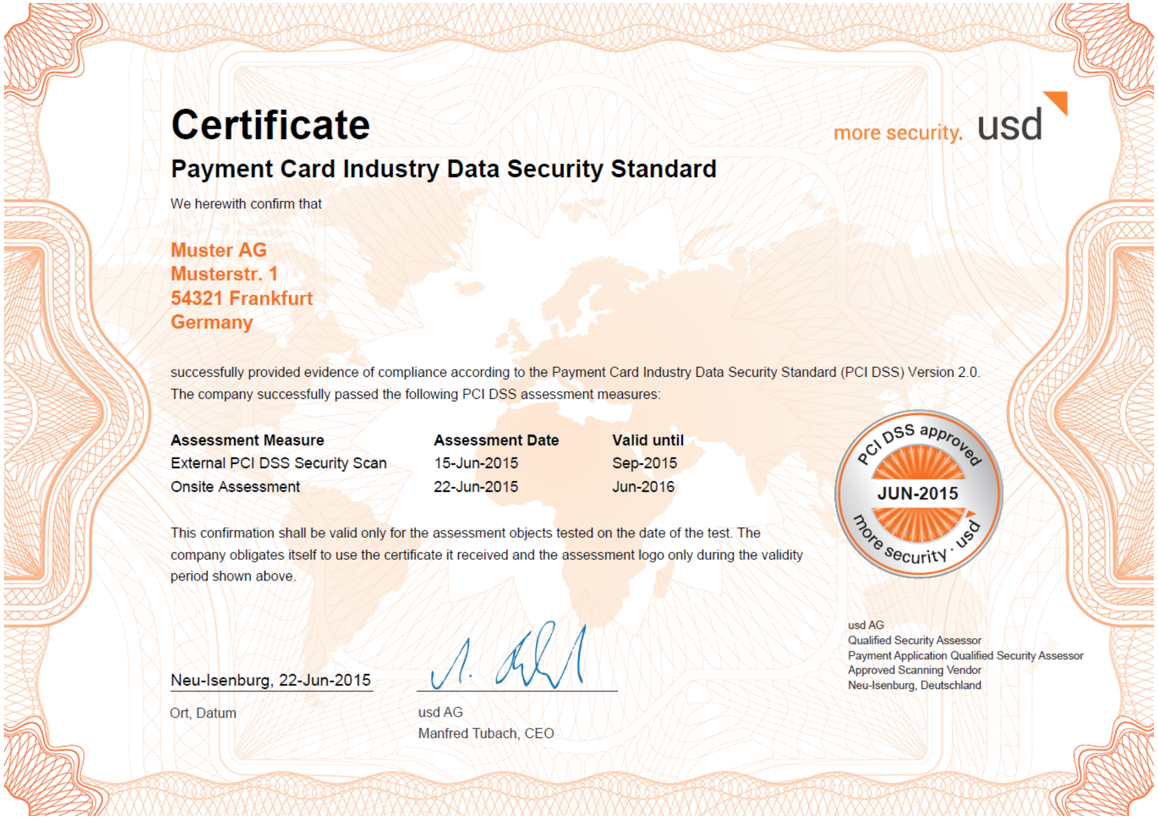
- Writing of the “Report on Compliance” (RoC) by the QSA
  - After completion of the onsite audit
  - Review through the customer
- Signing of the “Attestation of Compliance” (AoC)
  - by QSA and Entity
- Submitting the AoC towards the relevant entities
  - Listing on Visa and MasterCard website

Certificate issued by Assessor

- **The Certificate** - the most important result… ;-)

Certificate issued by Assessor

- But seriously, demonstration of an high security standard is important for current business partners and new clients



Certificate

more security. usd

Payment Card Industry Data Security Standard

We herewith confirm that

Muster AG
Musterstr. 1
54321 Frankfurt
Germany

successfully provided evidence of compliance according to the Payment Card Industry Data Security Standard (PCI DSS) Version 2.0. The company successfully passed the following PCI DSS assessment measures:

Assessment Measure	Assessment Date	Valid until
External PCI DSS Security Scan	15-Jun-2015	Sep-2015
Onsite Assessment	22-Jun-2015	Jun-2016

PCI DSS approved
JUN-2015
more security · usd

This confirmation shall be valid only for the assessment objects tested on the date of the test. The company obligates itself to use the certificate it received and the assessment logo only during the validity period shown above.

Neu-Isenburg, 22-Jun-2015
Ort, Datum

usd AG
Manfred Tubach, CEO

usd AG
Qualified Security Assessor
Payment Application Qualified Security Assessor
Approved Scanning Vendor
Neu-Isenburg, Deutschland

Summary

Summary

- Today IT & IT Security Management is challenged by a lot of internal and external requirements
- Addressing security standards, such as PCI DSS, are complex and expensive
- Compliance Management must be used to address and fulfill efficiently all internal and external requirements
- IT Security Management must be flexible enough to support different compliance topics and to help optimizing regularly audit and certification tasks

Any Questions?

usd AG

Ronny John

Frankfurter Str. 233, Haus C1
63263 Neu-Isenburg
Germany

Phone: +49 6102 8631-350
Mail: ronny.john@usd.de