carmasec
security. done. right.

ISO 27001 vs. PCI DSS

Was unterscheidet ISO 27001 und PCI DSS in der Praxis?

Zu meiner Person

carmasec
security. done. right.

- Janina Walgenbach
- 29 Jahre
- Quereinsteigerin (Geowissenschaften)
- Ehemalige Auditorin für **PCI DSS**
- Jetzt Beraterin für **ISO 27001**, **Cyber Resilience Act** (CRA) und weitere Informationssicherheits- Frameworks

Opener: Kreditkarte

Vorwissen für PCI DSS

carmasec
security. done. right.

Bank

EMV - Chip

Ablaufdatum

Name des Karteninhabers

Kreditkarteninstitut

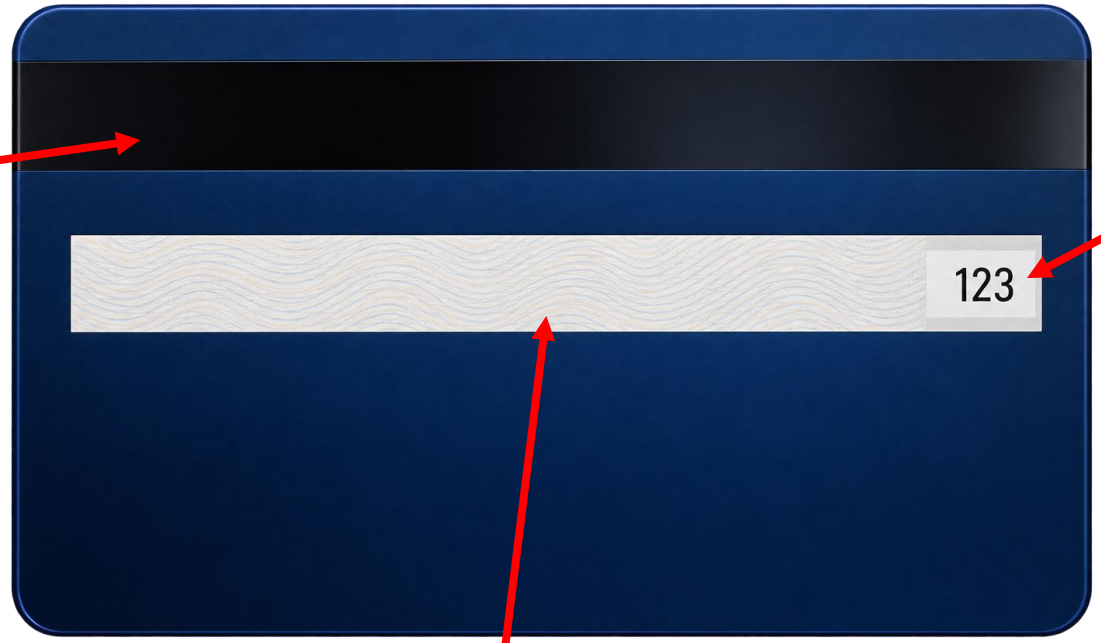
PAN (Primary Account Number)

Wer hier besitzt eine Kreditkarte?

Opener: Kreditkarte

Vorwissen für PCI DSS

carmasec
security. done. right.



Was ist PCI DSS ?

Vorwissen für PCI DSS

carmasec
security. done. right.

- Standard für **Kreditkartensicherheit**
- **P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard
- **2006** Gründung PCI Security Standards Council (PCI SSC)
- Vereinheitlichung der Sicherheitsprogramme
- **Ziel:** Schutz von Karteninhaberdaten
- **Scope**: Organisationen, die Kartenzahlungen speichern, verarbeiten oder übertragen
- Folgt einem Level-System (1-4) abhängig von Anzahl Transaktionen

Die 5 Gründungsmitglieder:

VISA

mastercard

AMERICAN EXPRESS

DISCOVER

JCB

Anforderungen des PCI DSS

Vorwissen für PCI DSS

carmasec
security. done. right.

Req. 1
Netzwerksicherheit

Req. 4
Verschlüsselung

Req. 7
Zugriffsmanagement

Req. 10
Logging Monitoring

Req. 2
Härtung

Req. 5
Malware-Schutz

Req. 8
IAM

Req. 11
Testing

Req. 3
Datenbank-Sicherheit

Req. 6
Wartung, Entwicklung von Systemen

Req. 9
Physische Sicherheit

Req. 12
Organisatorische Sicherheit

Anforderungen des ISO 27001?

Vorwissen für ISO 27001

carmasec
security. done. right.

Organisatorische Unterschiede und Gemeinsamkeiten

carmasec
security. done. right.

ISO 27001	PCI DSS
Internationale Norm	Industriestandard
Veröffentlich durch die **ISO / IEC**	Veröffentlich durch das **PCI SSC**
Schutz aller **Informationen**	Schutz von **Karteninhaberdaten**
Zertifizierung **freiwillig**	Meist **verpflichtend** durch Acquirer
Zertifikat **3 Jahre** gültig Erstzertifizierung, 2 \überwachungsaudit	Compliance gültig für **1 Jahr** Neuzertifizierung jedes Jahr
Non-Compliance: Nachteil am Markt	Non-Compliance: Vertragsstrafen, Entzug der Kartenzahlungsfähigkeit
Auditdurchführung von **akkreditierten Zertifizierungsstellen** (z.B. TÜV)	Auditdurchführung nur durch **QSA (Qualified Security Assessor) Companies** - QSA's müssen ihre Zertifizierung jährlich erneuern
Scope ist i.d.R. die **gesamte Organisation**	Scope wird hier als **CDE** (Cardholder Data Environment) bezeichnet. - Bereiche können **out-of-scope** betrachtet werden (Approval Auditor)
Risiken können / müssen akzeptiert werden	**Wenig Spielraum** (Customized Approach, Compensating Control)

Detailgrad der Anforderungen

carmasec
security. done. right.

ISO 27001

Logging & Monitoring (8.15)

Zugriffe müssen protokolliert werden.

PCI DSS

Logging & Monitoring (10.5.1)

Audit Logs müssen mindestens 12 Monate aufbewahrt werden, die letzten 3 Monate müssen sofort zur Analyse verfügbar sein

---

ISO 27001

Uhren Synchronisation (8.17)

Uhren von informationsverarbeitenden Systemen der Organisation sollen mit offiziellen Zeitquellen synchronisiert sein

PCI DSS

Uhren Synchronisation (10.6.1 – 10.6.3)

- … müssen mit Zeitsynchronisierungstechnologien synchronisiert werden
- Ein – oder mehrere designierte Zeitserver …
- Basiert auf internationaler Atomzeit (UTC)
- Zeitaktualisierungen dürfen nur von Branchenakzeptierten Quellen (…)

Zugriff auf Zeitdaten ist auf Personal entspr. Business-need zu gewähren

Alle Änderungen an Zeiteinstellungen auf kritischen Systemen werden protokolliert (…)

Synergien

Wir haben bereits ISO 27001, was würde uns das für PCI DSS bringen?

carmasec
security. done. right.

- **ISO 27001** bildet den Rahmen, **PCI DSS** technische Umsetzungen
- ISO 27001 beantwortet das **WAS** ; PCI DSS beantwortet das **WAS** und **WIE**
- Kernprozesse sind Grundlage für die Umsetzung von Anforderungen
- Erfahrung in Audits und Zertifizierungsverfahren

Danke für Eure Aufmerksamkeit!

Bei Fragen stehe ich gerne zur Verfügung

carmasec
security. done. right.

Hinweis zu Abbildungen:

Einzelne Grafiken und Illustrationen dieser Präsentation wurden mithilfe generativer KI erstellt und anschließend redaktionell geprüft.

Lust auf Kontakt?

carmasec
security. done. right.

Janina Walgenbach

janina.walgenbach@carmasec.com

carmasec GmbH & Co. KG