TOPCERTIFIER
www.topcertifier.com

サービス方法論
PCI DSS
ペイメントカード業界のデータセキュリティ標準

TOPCERTIFIER
www.topcertifier.com

はじめに PCI DSS

TOPCertifier は、PCI DSS ギャップ分析の簡易チェックリストを提供して、特定に役立てます。組織が PCI DSS (支払い) に準拠するために改善が必要な分野 カード業界データ セキュリティ標準) の要件。このチェックリストは、基本的な事項を提供します。PCI DSS との整合性を評価するためのフレームワークであり、PCI DSS への最初のステップとして機能します。
コンプライアンスの評価.

セクション 1: データセキュリティ

- 支払いカードのデータは送信中および保存中に適切に暗号化されていますか
- CVV 番号などの機密認証データは承認後に保存されませんか
- カード会員データと機密認証データを保護するためのポリシーはありますか

セクション 2: ネットワークとファイアウォールのセキュリティ

- ネットワーク構成とファイアウォール ルールは定期的に確認され、更新されていますか
- カード会員データの流れを示すネットワーク図はありますか
- ネットワークインフラストラクチャを保護するためのセキュリティポリシーと手順は整備されていますか

セクション 3: アクセス制御

- ユーザーのアクセス権限はビジネス上の必知事項に基づいて制限されていますか
- ネットワークへのリモート アクセスのために実装された多要素認証です
- ユーザーアカウントは、終了または役割の変更の際に直ちに非アクティブ化されますか

セクション 4: 脆弱性管理

- 脆弱性に対処するためにセキュリティ パッチがすぐに適用されていますか
- 脆弱性スキャンと侵入テストのプロセスはありますか
- 重要なセキュリティパッチはレビューされ、リスクに基づいて優先順位が付けられていますか

セクション 5: セキュリティ ポリシーと手順

- 包括的なセキュリティ ポリシーと手順が文書化され、配布されていますか
- 従業員向けのセキュリティ意識向上トレーニング プログラムはありますか
- セキュリティ ポリシーは必要に応じてレビューされ、更新されていますか

セクション 6: 監視とロギング

- セキュリティ イベントとログは定期的に確認および監視されていますか
- 不審なアクティビティに対してリアルタイムで警告を行うプロセスはありますか
- インシデント対応と報告手順は確立されていますか

セクション 7: インシデントへの対応

- セキュリティインシデントに対処するための手順を概説したインシデント対応計画はありますか
- 従業員はセキュリティインシデントを認識して報告する方法について訓練を受けていますか
- インシデント後の分析と改善のための文書化されたプロセスはありますか

セクション 8: 身体的セキュリティ

- カード所有者のデータへの不正アクセスを防ぐための物理的アクセス制御が導入されていますか
- 安全なエリアへのアクセスは制限され監視されています
- ビデオ監視と訪問者の記録は機密エリアに対して維持されていますか

セクション 9: サードパーティのサービスプロバイダー

- サードパーティ ベンダーは PCI DSS 準拠について評価されていますか
- カード所有者のデータ保護を確実にするために、サービスプロバイダーと書面による契約が締結されていますか
- サードパーティのセキュリティ慣行を監視および評価するプロセスはありますか

このチェックリストは高レベルの概要を提供するものであり、次のチェックリストを実行することが不可欠であることに注意してください。組織のプロセスとコンテキストに特化した徹底的な分析。さらに、それは PCI DSS の専門家またはコンサルタントと協力して、包括的な調査を実施することをお勧めします。組織のギャップ分析。