comforte

Quick Reference Guide to
3 Ways to Reduce PCI DSS v3.2 Audit Scope

Secure Connections

WHAT? Requirement 2.3 – Encrypt non-console admin access
Requirement 4.1 – Encrypt Cardholder data sent over the internet
WHY? Especially important to e-commerce websites, but also for companies who accept payments through their website, sending card data over the internet are subject to man-in-the-middle (MiTM) attacks to steal card data.
HOW? Use encryption technology called TLS (versions 1.2 and above) for securing card data that is transmitted between websites, systems processing the card data, payments service providers, and other companies involved in the payments process.

Protect Cardholder Data

WHAT? Requirement 3.4 – Render PAN unreadable anywhere it is stored
WHY? Organizations are required to protect stored cardholder data anywhere it is stored. What better way is there to protect cardholder data, if the cardholder data is removed altogether?
HOW? Encryption satisfies Req 3.4 however leaves your system IN-scope, because with encryption the data is still there - it is just scrambled with strong cryptography. Tokenization is emerging as a best practice because tokenization REPLACES the original CDE with a surrogate (token) value. Therefore, Scope is reduced with tokenization.

Manage Encryption Keys

WHAT? Requirement 3.5 – Implement procedures to protect encryption keys used to secure stored cardholder data
WHY? Improve Key Management responsibilities to ensure decryption of cardholder data is more difficult
HOW? Tokenization doesn't use keys to protect cardholder data, therefore this requirement is reduced (Note: Encryption is used to Secure Connections as defined in Req 2.3 and 4.1, therefore key management will still be required in this capacity)

Learn more about how enterprise data protection can benefit your organization here or contact us to discuss your data protection requirements: www.comforte.com.

Follow us on social media:

comforte

PCI DSS$^{v3.2}$ Requirements Summary Table

Quick reference guide summarizing PCI requirements and common technologies deployed to meet the requirements

PCI Req.	PCI Requirement	Description	Technologies commonly used
2.3 4.1 8.2.1	• Use strong cryptography to protect sensitive data sent over the internet	• Encrypt all non-console administrative access; • Safeguard sensitive cardholder data during transmission over open, public networks; • Render all authentication credentials (such as passwords/phrases) unreadable during transmission	• TLS • SSH
3.4 6.4.3 8.2.1	• Use strong cryptography to protect sensitive data when stored	• Render PANs unreadable when stored including on portable digital media, backup media, and in logs • Render all authentication credentials (such as passwords/phrases) unreadable when stored • Ensure Production data (live PANs) are not used for testing or development	• Data Discovery • Backup Tape Encryption • Encryption • Tokenization • Format Preserving Encryption (FPE)
3.3	• Mask PAN when displayed	• First 6 and last 4 digits of PAN are the max numbers to be displayed. Only users with a legitimate business need can see full PAN	• Tokenization • Format Preserving Encryption (FPE) • Data Masking
10	• Track and monitor all access to network resources and cardholder data	• Implement audit trails to link all access to system components to each individual user, including access to cardholder data	• Audit log generation • Application Logging • Keystroke Logging
7 8 10.5	• Restrict access • User authentication and password management	• Restrict access to cardholder data by business need to know • Assign a unique ID to each person with computer access (no ID sharing) • Secure audit trails so they cannot be altered	• Identity Access Management (IAM) • Password control and management
10.6 11.4 11.5	• Review logs and security events daily • Intrusion detection • File integrity monitoring	• Identify anomalies or suspicious activity • Detect and prevent intrusions into the network • Deploy a change-detection mechanism to alert personnel to unauthorized modification	• SIEM integration • Intrusion detection & prevention • File Integrity Monitoring