

# DIGITSEC FOR COMMERCE CLOUD



## PCI-DSS COMPLIANCE [v3.21. & v4.0]



### PCI REQUIREMENT

### DIGITSEC CONTROL

PCI requirements are set to optimize security of Credit, Debit and Cash transactions & protect cardholders against PII misuse

DigitSec can assist in self-assessment and work as a tool to help with executing compliance requirements



#### DATA PRIVACY

Req 3.2: Ensure non-storage of sensitive authentication data



Assesses to highlight incorrect encapsulation of sensitive data



#### SECURITY DEVELOPMENT

Req 6.1: Establish a process to identify security vulnerabilities and assign a CVSS risk ranking



Comprehensive process with an elaborate (CVSS) score-based risk ranking



#### INJECTION FLAW DIAGNOSIS

Req 6.5.1: Check SQL injection, OS Command Injection, LDAP and XPath injection, and other flaws



Identifies all injection flaws and prescribes specific remediation



#### VULNERABILITY TRACE

Req 6.5.6: All high-risk vulnerabilities are to be identified



Promptly captures and flags all high-risk vulnerabilities

# PCI REQUIREMENT

# DIGITSEC CONTROL



## CROSS-SITE SCRIPTING CHECK

Req 6.5.7: Check for XSS web security vulnerability



## ACCESS CONTROL

Req 6.5.8: Prevent insecure direct access and restrict URL, directory & user access



## DIAGNOSE EXPLOITS

Req 6.5.9: Cross-site Request Forgery (CSRF) prevention.



## SECURITY MAINTENANCE

Req 6.6: Review web applications via application vulnerability security assessment tools after any changes.



## AUTHENTICATED SCANNING

Req 11.3.1.2: New requirement to perform internal vulnerability scans via authenticated scanning.



## ROUTINE SCANS

Req 11.3.1.3 & 11.3.2.1: New Separated requirement to perform internal and external vulnerability scans and rescans



Scans to prevent plausible Cross-Site Scripting injections



Audits access control to cardholder data



Checks for Cross-site Request Forgery (CSRF)



Reviews all code for vulnerabilities and provides instructions for patches



Evaluates open vulnerabilities and internal security configurations via authenticated testing



Run unlimited scans and get direct remediation guidelines