FLEXENTIAL

SOLUTION OVERVIEW: PCI DSS & HIPAA

Compliance with Confidence for PCI DSS and HIPAA

Architecture & Transformation

Optimized Clouds

DevOps

Cybersecurity

Compliance

Disaster Recovery

PROFESSIONAL SERVICES

PCI DSS and HIPAA Compliance Overview

Complying with PCI DSS requirements and HIPAA rules can be extremely complex and time-consuming. Yet compliance knowledge, staffing, budgets and management support are often insufficient. Certified Flexential consultants, including PCI Qualified Security Assessors (QSAs) and HealthCare Information Security and Privacy Practitioners (HCISPP), combine deep expertise with effective compliance services to support your organization's compliance strategy, helping to avoid heavy fines, business loss and reputation compromise.

Financial and health data are two of the most sensitive types of information that organizations manage. These kinds of data also happen to be the most attractive to cybercriminals. While PCI DSS focuses on protecting cardholder data and HIPAA on protecting patient data, both fall under detailed compliance guidelines that keep private information safe from theft or public exposure—either accidentally or intentionally.

Yet, despite the real risks and severe consequences of compliance gaps, only the highest PCI DSS level requires third-party verification. Self-assessments are allowed for other PCI DSS levels and HIPAA, but these are riskier and often difficult to answer accurately. Self-assessments also lack recommendations for designing environments that meet compliance controls. Yet, many organizations find it challenging to independently determine which systems, applications and parts of the network may be in scope for an assessment. Equally daunting is understanding and choosing appropriate compensating controls to meet compliance requirements.

Achieving and maintaining a mature data security compliance program is very seldom solely the result of a standard formula. It is a continuously evolving process in which capabilities and processes are developed over time, where various adjustments (some micro, some macro) are made based on observations at points in time.[1]

2020 Payment Security Report, Verizon, October 2020

Flexential Professional Services for Compliance

Flexential's certified cybersecurity and compliance experts offer professional compliance audits, assessments—including assistance with PCI self-assessments—validation, recommendations, guidance, remediation and program management. Services include independent, third-party compliance verification where required or requested. Flexential will tailor services to customer-specific considerations to meet and maintain effective PCI DSS and HIPAA compliance.

PCI DSS and HIPAA Compliance Challenges

Factors that prevent organizations from meeting compliance needs:

- Poor understanding of compliance requirements
- Unknown and unaddressed compliance gaps
- Lack of experienced staff
- Shortage of certified experts
- Absence of a cohesive compliance strategy
- Insufficient funding
- Insufficient upper management support
- Inadequate planning for future requirements
- Lack of risk awareness & management

Flexential's Approach

- Risk-based
- Consultative
- Tailored engagements
- Detailed, actionable and prioritized guidance
- Highly certified security and compliance experts

Effective Assessments and Testing—Expert Guidance and Verification

Flexential provides Reports on Compliance (ROCs), Attestations of Compliance (AOCs) and assistance completing Self-Assessment Questionnaires (SAQs). Customers receive prioritized, detailed, actionable guidance on what is working and what is missing.	Gain practical information and active assistance to achieve compliance and decrease risks.
Multiple experts certified as PCI Qualified Security Assessors (QSA) and HealthCare Information Security and Privacy Practitioner (HCISSP).	Understand how to interpret and comply with rules and requirements.
Flexential tailors services to each customer engagement.	Maximize value and ROI with services adapted to specific needs.
A full suite of PCI DSS and HIPAA compliance services, including assessments, audits, testing, third-party verification, self-assessment assistance, guidance, remediation, and ongoing program management.	Simplify with multiple services from a single compliance service provider.
Ongoing compliance management program with expert monitoring for new or revised regulations.	Proactively manage compliance.

PCI DSS and HIPAA Overview

	PCI DSS	HIPAA
Assessment Guidelines	Exacting, highly detailed requirements for SAQ and ROC	Risk assessment required; no certification requirement
Application(s)	Covers cardholder data security	Encompasses security, safety, and privacy of data, plus fraud, abuse and waste prevention
Who Must Comply	Only covered entities must comply	Covered entities *and* all business associates must comply
Meaningful Use Component	Does not address meaningful use	Addresses meaningful use, including theft, loss and unauthorized access

Engage a trusted partner to achieve and maintain compliance

Most organizations recognize that inadequate compliance is a risk that leaves them vulnerable to significant financial and reputational damage. Yet, other priorities and overtaxed resources make it challenging to achieve compliance, and once achieved, complex and continuously evolving rules and regulations create challenges for maintaining compliance.

For organizations without a fully staffed compliance department— including certified, in-house experts — engaging trusted external resources eases compliance challenges. Flexential's knowledgeable consultants can execute required compliance activities, provide detailed guidance, and support the organization in sustaining a proactive and prepared compliance posture.

Achieve and maintain your organization's mandated compliance by leveraging a trusted partner's extensive compliance expertise, experience and certifications.

Flexential's PCI DSS & HIPAA Professional Services Portfolio

PCI DSS	HIPAA
PCI Scope Discovery	HIPAA Compliance Gap Analysis
PCI Gap Analysis	HIPAA Compliance Assessment
PCI Self-Assessment Questionnaire (SAQ) Assistance	HIPAA Risk Assessment
PCI Report on Compliance (ROC)	Cloud Compliance Reporting & Enablement for HIPAA
PCI Risk Assessment	
PCI Penetration Test	
Cloud Compliance Reporting & Enablement for PCI DSS	

Flexential Professional Services PCI DSS and HIPAA Certifications

- CISSP® — Certified Information Systems Security Professional
- CISA — Certified Information Systems Auditor
- PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™ — Payment Card Industry Data Security Standard
- OSCP — Offensive Security Certified Professional
- OSCE — Offensive Security Certified Expert
- HCISPP® — HealthCare Information Security and Privacy Practitioner
- CISM — Certified Information Security Manager
- CDPSE — Certified Data Privacy Solutions Engineer
- CRISC — Certified in Risk and Information Systems Control

1 Van Oosten, C. 2020 Payment Security Report. Verizon. https://enterprise.verizon.com/resources/reports/2020-payment-security-report.pdf