CORE
CONCEPT
SECURITY

PCI Compliance Service

The Payment Card Industry Data Security Standard (PCI DSS) has been out for 15 years, and every merchant and service provider falls somewhere within the following 6 categories:

1. Never heard of the PCI DSS;
2. Heard of the PCI DSS, never been asked to comply;
3. Been asked to comply, have done nothing;
4. Been asked to comply, done something, still not compliant;
5. Compliant once; and
6. Compliant over multiple years

Regardless of the size of your organisation, your payment methods, or where you are in the above categories, if you accept branded payment cards you have work to do. That work can either be a once a year effort with zero benefit to the business, or it can result in a measurable increase in your cybersecurity capability that covers your *whole* business.

The CCS PCI Compliance Service has been developed by highly experienced practitioners and refined over hundreds of assessments performed globally. Whether you're a small merchant who needs help filling out a Self-Assessment Questionnaire (SAQ) or an FTSE/Fortune 100 multi-national looking for a fresh pair of eyes, CCS's proven and pragmatic approach will get you where you *need* to be. Even if you don't know where that is!

In the end, PCI compliance should spit out the back-end of a security program done well, the SSC PCI Compliance Service will provide you options for both.

Methodology

CCS utilises an assessment process perfected over a multitude and enormous variety of engagements. The validation of compliance to the 12 Domains of the PCI DSS requires a significant effort on behalf of the organisation in question. CCS will provide all necessary guidance to give you two options:

1. Do X much for PCI compliance;
2. Do Y much for real security, PCI compliance is included.

Like all CCS services, the PCI Compliance Service is designed to teach you how to do things yourself. In addition to guiding you towards full compliance with the requirements as written, we will also provide you with the following guidance towards a real security program.

- What you do with guidance is up to you, you will already be PCVI compliant either way.

PCI DSS Domain Requirement	Example of Value-Add Guidance
1: Install and maintain a firewall configuration to protect cardholder data	· Use firewall logs to determine server/desktop misconfiguration(s) · Expand segmentation into business-wide secure architecture
2: Do not use vendor-supplied defaults for system passwords and other security parameters	· Baseline your configurations for real-time 'white-list' comparisons · Implement process for software/application pre-approval
3: Protect stored cardholder data	· Options for descoping cardholder data · Options for outsourcing cardholder data processing
4: Encrypt transmission of cardholder data across open, public networks	
5: Protect all systems against malware and regularly update anti-virus software or programs	· Alternatives to CotS anti-malware
6: Develop and maintain secure systems and applications	· Sustainable risk and vulnerability management processes · Sustainable change management program
7: Restrict access to cardholder data by business need to know	· Implement true role-based access control (RBAC) · Implement appropriate user access management
8: Identify and authenticate access to system components	· Alternatives to username/password · User access audit and accountability
9: Restrict physical access to cardholder data	· Implementing visitor's management · Appropriate management of physical access
10: Track and monitor all access to network resources and cardholder data	· Automating log file review and alerting · Use logs for real incident response
11: Regularly test security systems and processes	· Testing for real-world scenarios · Alternative technologies to IDS and file integrity monitoring
12: Maintain a policy that addresses information security for all personnel	· Policy set that enables the business · Security awareness that makes a difference

Assessment Plan

A more detailed Project Definition Plan (PDP) will be made available well in advance of project kick-off, but in essence:

Phase 0: PCI Scoping Exercise (performed on[1] or off-site) - [no charge]

- Determine initial scope of assessment including locations, payment channel(s), and estimated number and variety of assets;
- Provide Statement of Work (SoW) for remaining assessment activity

Phase 1: Obtain Assessment Pre-Requisites - if available (performed off-site)

- Network and/or Data Flow Diagram(s);
- Asset Register(s);
- Policy Set (Policies, Procedures, and Standards);
- Stakeholder Matrix/Org Chart (key stakeholders per business function); and
- Latest Risk Assessment Report and/or Risk Register

Phase 2: Kick-Off / Relevant PCI Training Modules (performed on-site)

- Meet briefly with senior leadership to gauge commitment and garner their support;
- Meet with key stakeholders to agree project activities;
- Meet individually with key stakeholders to discuss relevant business processes, primary assets, and available resources;
- Perform deeper dive into current security controls;
- Perform walk-through of facilities (if applicable)

Phase 3: Reporting (performed off-site)

- Produce comprehensive Assessment Analysis Report with definitive list of action items for each stakeholder (sample here);

Phase 4: Provide Ongoing Guidance to Stakeholders (performed on & off-site)

- Produce comprehensive Assessment Analysis Report with definitive list of action items for each stakeholder (sample here);

Phase 5: Presentation of Findings to Senior Leadership (performed on-site) - Optional

- Meet briefly with senior leadership to present findings and discuss strategic options

Timeframe

The entire assessment can be performed in as little as a few days for very small environment requiring an SAQ, or many months for a larger / distributed / complex environment requiring a full Report on Compliance (RoC). A full scoping exercise will be performed prior to any work taking place and contracts are signed.

Deliverables

Assessment gap analysis, SAQ, or full Report on Compliance, depending on the SoW

[1] Onsite scoping exercise is only available in the London area.