SecurityMetrics Guide to

PCI DSS Compliance

A Resource for Merchants and Service Providers to Become Compliant

[SEVENTH EDITION]

securityMETRICS®

ABOUT SECURITYMETRICS

We secure peace of mind for organizations that handle sensitive data. We have tested over 1 million systems for data security and compliance. Industry standards don't keep up with the threat landscape, which is why we hold our tools, training, and support to a higher, more thorough standard of performance and service. Never have a false sense of security.™

FOREWORD

No matter the advances in cyber security technology and despite government initiatives and regulations, attackers will continue to work to steal unprotected payment card data.

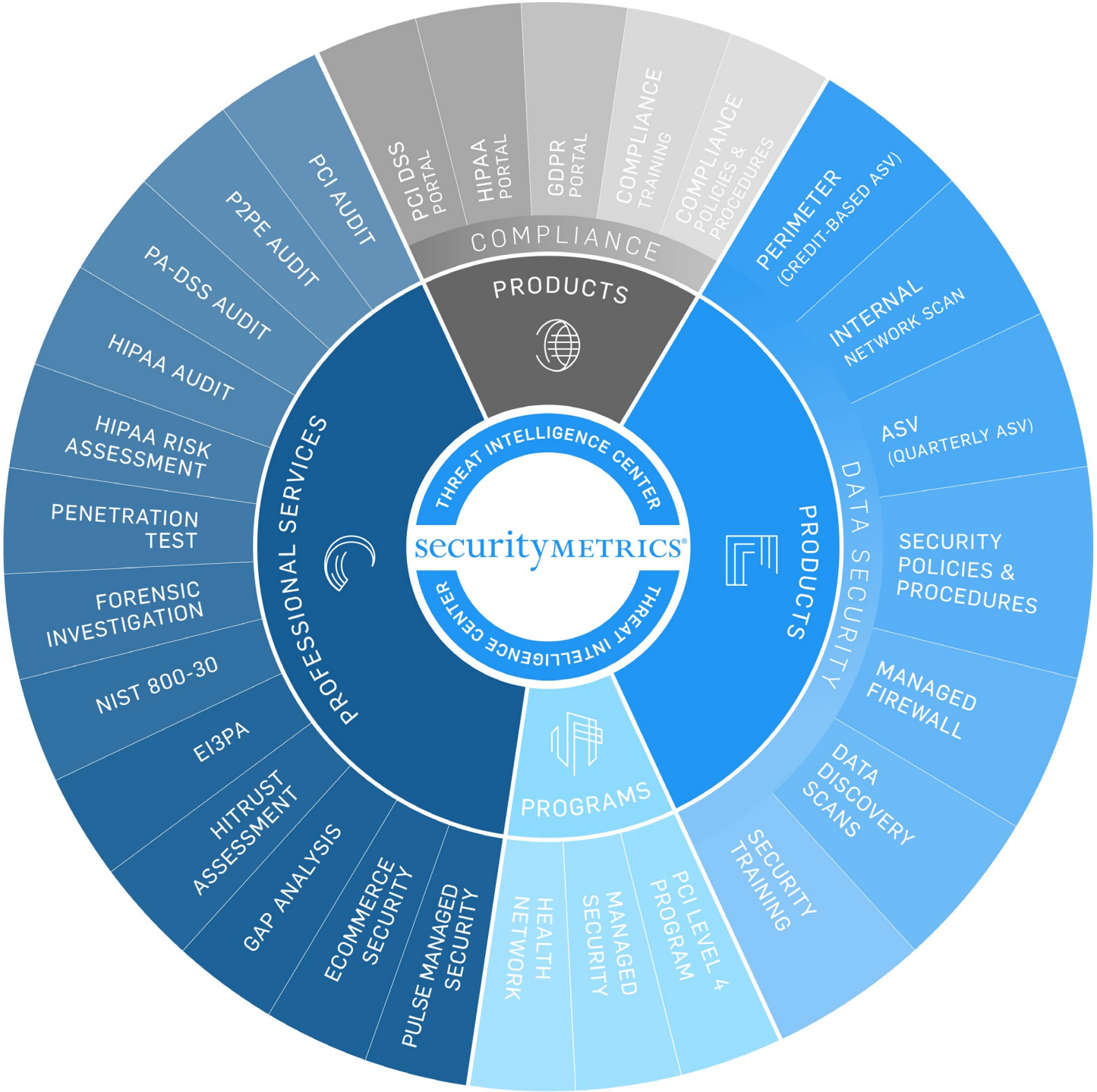
Some organizations have simple, easy-to-correct vulnerabilities that could lead to data breaches. In other instances, organizations with intricate IT defenses and processes are overridden by an employee opening a phishing email.

Our guide was specifically created to help merchants and service providers address the most problematic issues within the 12 PCI DSS requirements, including auditors' best practices and IT checklists.

Our guide is not intended to be a legal brief on all requirements and aspects of PCI compliance. Rather, it approaches PCI from the perspective of a security analyst, focusing on how to protect your cardholder data. Thus, we recommend using it as a resource to help with your PCI compliance efforts.

Ultimately, our goal is to help you better protect your data from inevitable future attacks.

MATT HALBLEIB
SecurityMetrics Audit Director
CISSP | CISA | QSA (P2PE) | PA-QSA (P2PE)


securityMETRICS
THREAT INTELLIGENCE CENTER
THREAT INTELLIGENCE CENTER
COMPLIANCE
PCI DSS PORTAL
HIPAA PORTAL
GDPR PORTAL
COMPLIANCE TRAINING
COMPLIANCE POLICIES & PROCEDURES
PRODUCTS
PERIMETER (CREDIT-BASED ASV)
INTERNAL NETWORK SCAN
ASV (QUARTERLY ASV)
DATA SECURITY
SECURITY POLICIES & PROCEDURES
MANAGED FIREWALL
DATA DISCOVERY SCANS
SECURITY TRAINING
PROGRAMS
PCI LEVEL 4 PROGRAM
MANAGED SECURITY
HEALTH NETWORK
PROFESSIONAL SERVICES
PCI AUDIT
P2PE AUDIT
PA-DSS AUDIT
HIPAA AUDIT
HIPAA RISK ASSESSMENT
PENETRATION TEST
FORENSIC INVESTIGATION
NIST 800-30
EI3PA
HITRUST ASSESSMENT
GAP ANALYSIS
ECOMMERCE SECURITY
PULSE MANAGED SECURITY

All inquiries should be addressed to:
SecurityMetrics
1275 West 1600 North
Orem, UT 84057

Or contact:
marketing@securitymetrics.com

Portions of this guide were adapted from material previously published on securitymetrics.com/blog and securitymetrics.com/learn.

International Standard Book Number: 978-1-7346465-5-9

CONTENTS

HOW TO READ THIS GUIDE

Whether you're a new employee with limited PCI knowledge or an experienced system administrator, our guide aims to help you secure your environment and for your organization to become compliant with PCI DSS requirements. We designed this document as a reference guide to address the most challenging aspects of PCI DSS compliance.

Depending on your background, job role, and your organization's needs, some sections in this guide may be more useful than others. Rather than reading our guide cover to cover, we recommend using it as a resource for your PCI compliance efforts.

The following chart displays an overview of the PCI Security Standards Council's Prioritized Approach. The Prioritized Approach offers organizations a risk-based roadmap to address issues on a priority basis, while also supporting organizational financial and operational planning.

The Prioritized Approach is broken down into the following six milestones (based on high-level compliance and security goals):

MILESTONES	GOALS
1	Remove sensitive authentication data and limit data retention
2	Protect systems and networks, and be prepared to respond to a system breach
3	Secure payment card applications
4	Monitor and control access to your systems
5	Protect stored cardholder data
6	Finalize compliance efforts, and ensure all controls are in place

NOTE

The information described in this guide is presented as a reference and is not intended to replace security assessments, tests, and services performed by qualified security professionals. Users are encouraged to consult with their companies' IT professionals to determine their needs to procure security services tailored to those needs.

PCI DSS REQUIREMENTS	MILESTONES					
	1	2	3	4	5	6
Requirement 1 **Protect Your System with Firewalls**	●	●				●
Hardware firewalls		●				
Software firewalls		●				
Properly configure firewalls		●				●
Network segmentation		●				
Test and monitor configuration						●
Requirement 2 **Use Adequate Configuration Standards**		●	●			
Default password weaknesses		●				
System hardening			●			
System configuration management		●	●			
Requirement 3 **Secure Cardholder Data**	●				●	
Cardholder data trends	●				●	
Know where all cardholder data resides	●				●	
Requirement 4 **Secure Data Over Open and Public Networks**		●				
Stop using SSL/early TLS		●				
Requirement 5 **Protect Systems with Anti-Virus**		●				
Regularly update your anti-virus		●				
Requirement 6 **Update Your Systems**			●			●
Regularly update and patch system(s)			●			●
Establish software development processes			●			●
Web application firewalls			●			
Requirement 7 **Restrict Access**					●	
Restrict access to cardholder data and systems					●	
Requirement 8 **Use Unique ID Credentials**		●			●	
Weak passwords and usernames		●			●	
Implement multi-factor authentication		●				
Requirement 9 **Ensure Physical Security**	●	●				●
Control physical access to your workplace		●				●
Keep track of POS terminals		●				
Train employees early and often		●				●
Physical security best practices	●	●				●
Requirement 10 **Implement Logging and Log Management**					●	
System logs and alerting					●	
Establishing log management					●	
Log management system rules					●	
Requirement 11 **Conduct Vulnerability Scans and Penetration Testing**		●			●	
Understand your environment		●			●	
Vulnerability scanning basics		●				
Penetration testing basics		●				
Vulnerability scanning vs. penetration testing		●				
Requirement 12 **Start Documentation and Risk Assessments**	●	●				●
Regularly document business practices		●				●
Establish a risk assessment process	●					
PCI DSS training best practices		●				●

INTRODUCTION

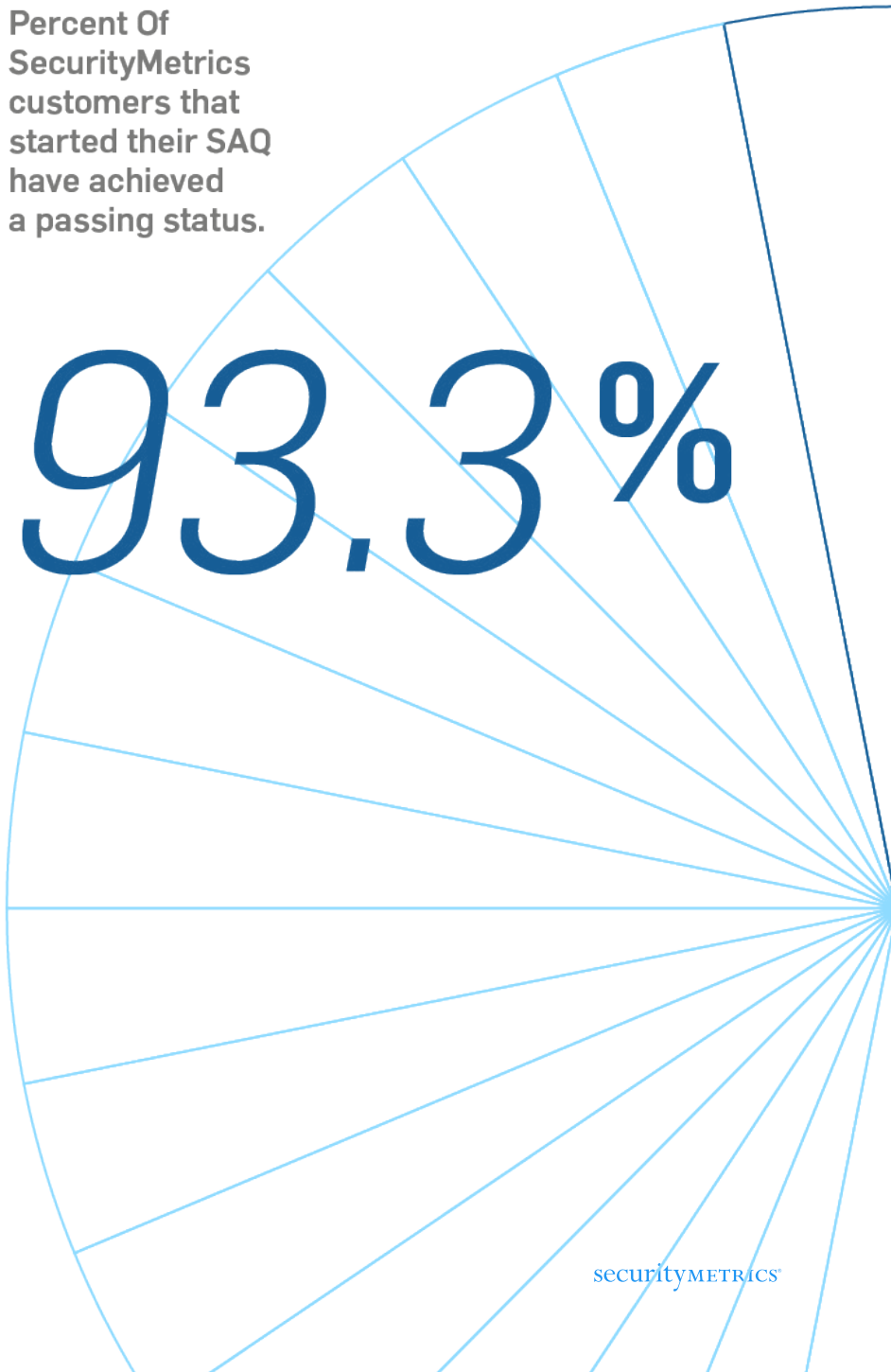
PCI DSS COMPLIANCE OVERVIEW

PAYMENT SECURITY

The Payment Card Industry Data Security Standard (PCI DSS) was established in 2006 by the major card brands (e.g., Visa, MasterCard, American Express, Discover Financial Services, JCB International).

All businesses that process, store, or transmit payment card data are required to implement the security standard to prevent cardholder data theft. The investigation of numerous credit card data compromises has confirmed that the security controls and processes required in the PCI DSS are essential to protecting cardholder data.

Merchants often have a difficult time attaining (or maintaining) compliance for a variety of reasons. Many smaller merchants believe it's too technical or costly, while others simply don't believe it's effective and refuse to comply.



REQUIREMENT 1

PROTECT YOUR SYSTEM WITH FIREWALLS

- *Install a hardware and software firewall*
- *Configure firewalls for your environment*
- *Have strict firewall rules*

REQUIREMENT 2

USE ADEQUATE CONFIGURATION STANDARDS

- *Change default passwords*
- *Harden your systems*
- *Implement system configuration management*

REQUIREMENT 3

PROTECT STORED DATA

- *Find where card data is held*
- *Craft your card flow diagram*
- *Encrypt stored card data*

REQUIREMENT 4

SECURE DATA OVER OPEN AND PUBLIC NETWORKS

- *Know where data is transmitted and received*
- *Encrypt all transmitted cardholder data*
- *Stop using SSL and early TLS*

REQUIREMENT 5

PROTECT SYSTEMS WITH ANTI-VIRUS

- *Create a vulnerability management plan*
- *Regularly update anti-virus*
- *Maintain an up-to-date malware program*

REQUIREMENT 6

UPDATE YOUR SYSTEMS

- *Consistently update your systems*
- *Apply all critical/high patches to systems and software*
- *Establish secure software development processes*

REQUIREMENT 7

RESTRICT ACCESS

- *Restrict access to cardholder data*
- *Document who has access to the card data environment*
- *Establish a role-based access control system*

REQUIREMENT 8

USE UNIQUE ID CREDENTIALS

- *Use unique ID credentials for every employee*
- *Disable/delete inactive accounts*
- *Configure multi-factor authentication*

REQUIREMENT 9

ENSURE PHYSICAL SECURITY

- *Control physical access at your workplace*
- *Keep track of POS terminals*
- *Train your employees often*

REQUIREMENT 10

IMPLEMENT LOGGING AND LOG MONITORING

- *Implement logging and alerting*
- *Establish log management*
- *Create log management system rules*

REQUIREMENT 11

CONDUCT VULNERABILITY SCANS AND PENETRATION TESTING

- *Know your environment*
- *Run vulnerability scans quarterly*
- *Conduct a penetration test*

REQUIREMENT 12

START DOCUMENTATION AND RISK ASSESSMENTS

- *Document policies and procedures for everything*
- *Implement a risk assessment process*
- *Create an incident response plan (IRP)*

TOP 10

FAILING SAQ SECTIONS

We scanned our merchant database in search of the top 10 areas where SecurityMetrics merchant customers struggle to become compliant. Starting with the least adopted requirement, these are the results:

1

Requirement 12.1

Establish, publish, maintain, and disseminate a security policy.

2

Requirement 12.1.1

Review the security policy at least annually and update the policy when the environment changes.

3

Requirement 12.4

Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.

4

Requirement 12.5.3

Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.

5

Requirement 12.6.a

Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.

6

Requirement 12.10.1

Create an incident response plan to be implemented in the event of system breach.

In 2021, it took the average SecurityMetrics customer 20.33 days to reach PCI DSS compliance, with an average number of 0.98 support calls.

7

Requirement 12.8.5

Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

8

Requirement 12.8.4

Maintain a program to monitor service providers' PCI DSS compliance status at least annually.

9

Requirement 12.3.1

Verify that the usage policies include processes for explicit approval from authorized parties to use the technologies.

10

Requirement 12.8.3

Verify that the usage policies define all critical devices and personnel authorized to use the devices.