PCI DSS 4.0 Automated Mapping Summary

Accurately automate the assessment of PCI DSS testing procedures relating to network devices

PCI DSS 4.0 Mapping Document

Titania software is trusted by hundreds of QSAs and ISAs globally to accurately automate the assessment of PCI DSS 4.0 network testing procedures across 6 of the 12 requirements. The findings report automatically prioritizes identified risks by criticality to the network, which can be used to inform remediation workflows and improve PCI DSS compliance posture.

PICI Core Principle	Requirement	Requirement Description	Nipper	Nipper Resilliance	See page
Build and Maintain a Secure Network and Systems	**1**	Install and Maintain Network Security Controls	✓	✓	3
	2	Apply Secure Configurations to All System Components	✓	✓	3
Protect Account Data	**3**	Protect Stored Account Data			
	4	Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks			
Maintain a Vulnerability Management Program	**5**	Protect All Systems and Networks from Malicious Software			
	6	Develop and Maintain Secure Systems and Software	✓	✓	4
Implement Strong Access Control Measures	**7**	Restrict Access to System Components and Cardholder Data by Business Need to Know			
	8	Identify Users and Authenticate Access to System Components	✓	✓	4
	9	Restrict Physical Access to Cardholder Data			
Regularly Monitor and Test Networks	**10**	Log and Monitor All Access to System Components and Cardholder Data	✓	✓	5
	11	Test Security of Systems and Networks Regularly	✓	✓	5
Maintain an Information Security Policy	**12**	Support Information Security with Organizational Policies and Programs			

PCI DSS Core Principle: Build and Maintain a Secure Network of Systems

Requirement Family	Requirement Description	Security Requirement	Testing Procedure Covered in Report	Included in PCI DSS Compliance Report*	Included in Nipper Resilience Dashboard	Requirement Supported by Using Nipper/Nipper Resilience
1	Install and Maintain Network Security Controls	1.2.1	1.2.1.b	✓		
		1.2.5	1.2.5.b	✓		
		1.2.6	1.2.6.b	✓		
		1.2.7				✓**
		1.3.1	1.3.1.b	✓		
		1.3.2	1.3.2.b	✓		
		1.3.3	1.3.3	✓		
		1.4.1	1.4.1.b	✓		
		1.4.2	1.4.2	✓		
		1.4.3	1.4.3	✓	✓	
		1.4.4	1.4.4.b	✓		
		1.4.5	1.4.5.a	✓		
2	Apply Secure Configurations to all System Components	2.2.1	2.2.1.c	✓		
		2.2.2	2.2.2.c	✓	✓	
		2.2.4	2.2.4.b	✓	✓	
		2.2.5	2.2.5.b	✓		
		2.2.6	2.2.6.a	✓		
			2.2.6.c	✓		
		2.2.7	2.2.7.a	✓	✓	
			2.2.7.c	✓	✓	
		2.3.1	2.3.1.b	✓		

* Available in both Nipper and Nipper Resilience
** Using Nipper or Nipper Resilience to review configurations at least once every six months helps to meet this requirement

PCI DSS Core Principle: Maintain a Vulnerability Management Program

Requirement Family	Requirement Description	Security Requirement	Testing Procedure Covered in Report	Included in PCI DSS Compliance Report*	Included in Nipper Resilience Dashboard	Requirement Supported by Using Nipper/Nipper Resilience
6	Develop & Maintain Secure Systems and Software	6.3.1				✓**

* Available in both Nipper and Nipper Resilience
** Defining in policy and procedure documents that Nipper or Nipper Resilience is used to maintain secure systems can support demonstration of compliance with 6.3.1.a

PCI DSS Core Principle: Implement Strong Access Control Measures

Requirement Family	Requirement Description	Security Requirement	Testing Procedure Covered in Report	Included in PCI DSS Compliance Report*	Included in Nipper Resilience Dashboard	Requirement Supported by Using Nipper/Nipper Resilience
8	Identify Users & Authenticate Access to System Components	8.2.1	8.2.1.b	✓		
		8.2.8	8.2.8	✓	✓	
		8.3.2	8.3.2a	✓	✓	
		8.3.2	8.3.4a	✓	✓	
			8.3.4.b	✓	✓	
		8.3.6	8.3.6	✓	✓	
		8.3.7	8.3.7	✓	✓	
		8.3.9	8.3.9	✓	✓	

* Available in both Nipper and Nipper Resilience

PCI DSS Core Principle: Regularly Monitor and Test Networks

Requirement Family	Requirement Description	Security Requirement	Testing Procedure Covered in Report	Included in PCI DSS Compliance Report*	Included in Nipper Resilience Dashboard	Requirement Supported by Using Nipper/Nipper Resilience
10	Identify Users & Authenticate Access to System Components	10.2.1	10.2.1	✓	✓	
			10.2.1.2	✓	✓	
			10.2.1.3	✓	✓	
			10.2.1.4	✓	✓	
			10.2.1.5	✓	✓	
		10.2.2	10.2.2	✓	✓	
		10.3.3	10.3.3	✓	✓	
		10.6.1	10.6.1	✓	✓	
		10.6.2	10.6.2	✓	✓	
		10.6.3	10.6.3a	✓	✓	
11	Test Security of Systems and Networks Regularly	11.3.1				✓**
		11.4.2				✓***

* Available in both Nipper and Nipper Resilience
** Nipper Resilience can be scheduled to automatically meet the requirement for regular vulnerability scans, or it can be written into a policy to use Nipper for checks according to a schedule
*** Nipper Resilience can be scheduled to automatically meet the requirement for regular penetration testing, or it can be written into a policy to use Nipper for tests according to a schedule

TITANIA

Get in touch to arrange a demonstration of how to automate the process of assessing network infrastructure and prioritizing remediation based on PCI DSS risk.

Request a demo

USA
Suite 600,
2451 Crystal Dr, 6th Floor,
Arlington, VA 22202

UK
167-169 Great Portland Street,
London, England,
W1W 5PF