PCI DSS Checklist

Prepared by: RSI Security

RSI Security has devised this checklist to help you gauge where your organization stands with being Payment Card Industry Data Security Standard (PCI DSS) compliant.

How to use the checklist:

Each question is answered with either a "Yes" or a "No", circle or mark that box accordingly. You will notice there are numbers in the yes and no columns. At the end of the checklist you will tally up how many number ones you marked or circled. The number one represents risk, thus you will understand your organization's level of current risk by evaluating how many number ones were marked.

Scoring your checklist:

If you marked all number zeros in the checklist, your company has a very low threat level and is right on track to being PCI DSS compliant. Otherwise if you have any ones marked you understand that those are areas of concern and vulnerabilities that must be addressed. Being compliant means abiding by ALL of the PCI standards.

It should be noted that this is not a comprehensive list of all of the PCI DSS requirements, this is an overview of them. Upon completing this checklist, review it with a Qualified Security Assessor (QSA) to assure your organization has the proper policies and procedures in place to best mitigate risk and protect data.

Questions? We can help!

If at any point during this checklist you struggle to answer any of the questions or notice you need help, we are here to assist! RSI Security is a Qualified Security Assessor (QSA) and an Approved Scanning Vendor (ASV) with over 10 years of experience as top-of-the-line service providers helping organizations mitigate risk and achieve PCI DSS compliance success. Speak with one of our representatives today.

Contact Us: 858.999.3030 | info@rsisecurity.com | www.rsisecurity.com

	Questions	Yes	No	Description
1	Do you store cardholder's primary account number, expiration dates, or verification codes?	1	0	
2	Do you have point of sale devices (POS)?	1	0	
3	Do you use payment applications that store, process or transmit cardholder data and/or sensitive authentication data as part of the authorization or settlement?	1	0	
4	Do you have a cardholder data environment (CDE)?	1	0	The cardholder data environment (CDE) is comprised of people, processes, and technologies that store, process, or transmit cardholder data or. sensitive authentication data.
5	Have you performed deep scoping exercise to identify and document all systems applicable for PCI DSS compliance?	0	1	The first step of PCI DSS is to accurately determine the scope of the environment.
6	Have you used segmentation to reduce your PCI DSS scope?	0	1	Reduction of scope can lower the cost of the PCI DSS assessment, lower the cost and difficulty of implementing and maintaining PCI DSS controls, and reduce risk for the entity
7	Is there a current network diagram that documents all connections between the cardholder data environment (CDE) and other networks, including any wireless networks?	0	1	
8	Do you buy and use only approved PIN entry devices at your points-of-sale validated payment software at your POS or website shopping cart?	0	1	
9	Do you use a firewall to protect your CDE network and PCs?	0	1	
10	Do you ensure your wireless router is password-protected and uses encryption?	0	1	
11	Do you use strong passwords as well as change default passwords on hardware and software?	0	1	
12	Do you regularly check PIN entry devices and PCs to make sure no one has installed rogue software or “skimming” devices?	0	1	
13	Do you encrypt transmission of cardholder data across open, public networks?	0	1	
14	Do you protect all systems against malware and regularly update antivirus software or programs?	0	1	

15	Do you develop and maintain secure systems and applications?	0	1	
16	Do you restrict access to cardholder data by business need-to-know basis?	0	1	
17	Do you identify and authenticate access to system components?	0	1	
18	Do you use SSL/early TLS as a security control without the compensating controls?	1	0	
19	Have you implemented policies and operational procedures to restrict physical access to cardholder data?	0	1	
20	Do you track and monitor all access to network resources and cardholder data?	0	1	
21	Do you regularly test security systems and processes including performing network penetration tests and vulnerability scans by an approved scanning vendor (ASV)?	0	1	
22	Have you implemented an incident response plan?	0	1	
23	Have you performed background checks and personnel risk assessment to minimize the threat from internal sources?	0	1	
24	Have you clearly defined and established information security roles and responsibilities for all personnel?	0	1	
25	Do you perform a formal risk assessment that identifies critical assets, threats, and vulnerabilities?	0	1	
26	Have you implemented a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures?	0	1	
27	Are security policies and operational procedures documented, in use, and known to all affected parties?	0	1	
28	Do you follow the PCI Data Security Standard?	0	1	
29	Is your PCI DSS compliance validated with attestation?	0	1	
	Sub Total (tally up the 1's in each column)			
	PCI Compliance Risk Number (add total number of 1's together)			

Risk Score Summary:

Less than 3 = You appear to have minimal risk and are on track to being fully PCI compliant

3 - 10 = You have medium risk and are almost there with full PCI compliance

Greater than 10 = You have substantial risk and have a long way to go before becoming PCI compliant

If you have any ones marked you understand that those are areas of concern and vulnerabilities that must be addressed. Being compliant means abiding by ALL of the PCI standards.