

PCI DSS COMPLIANCE CHECKLIST

Title: PCI DSS compliance Checklist	Legend	Fully Compliant	Partially Compliant	Not Compliant	Not Applicable
		FC <input type="checkbox"/>	PC <input type="checkbox"/>	NC <input type="checkbox"/>	NA <input type="checkbox"/>
Requirement		FC	PC	NC	NA
Firewalls					
Have you Installed a firewall to ensure network security and prevent unauthorized access?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you documented the configuration of the firewall?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you identified all the unsafe protocols, services, allowed ports in your BE (Business Environment)?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you perform regular reviews of your firewall to make sure your firewall rule sets are compatible with your procedures?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you mapped a network topology diagram that defines all connections between the cardholder data medium and other networks.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you Installed a personal firewall or any software with equivalent functionality on user devices?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you changed the default passwords on your Reuters, software, and hardware?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS COMPLIANCE CHECKLIST

Title: PCI DSS compliance Checklist	Legend	Fully Compliant	Partially Compliant	Not Compliant	Not Applicable
		FC <input type="checkbox"/>	PC <input type="checkbox"/>	NC <input type="checkbox"/>	NA <input type="checkbox"/>
Requirement		FC	PC	NC	NA
Password Management					
Have you established configuration standards for all systems in your BE?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Did you ensure that servers perform only one primary function to avoid coexisting different core functions on the same server and requiring different security levels?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you implemented measures to enable only necessary services, protocols, background procedures as required for business needs?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you keep an inventory of system components that are covered by PCI DSS?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you checked policies and operating procedures for managing manufacturer defaults and other security parameters are documented, in use, and known to all affected parties?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS COMPLIANCE CHECKLIST

Title: PCI DSS compliance Checklist	Legend	Fully Compliant	Partially Compliant	Not Compliant	Not Applicable
		FC <input type="checkbox"/>	PC <input type="checkbox"/>	NC <input type="checkbox"/>	NA <input type="checkbox"/>
Requirement		FC	PC	NC	NA
Protecting Cardholder Data					
Have you developed a data retention policy that specifies what data should be stored and where that data is located? Thus, when no longer needed, these data can be safely deleted or destroyed.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you ensure that sensitive authentication data after authorization is not stored? If sensitive authentication data is received, make all data unrecoverable after the authorization process is complete.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you implemented controls to mask the PAN when it is displayed? Only employees with a legitimate business need can see more than the first six / last four PAN digits.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you use hashing, truncation, strong cryptography, or index tokens to make PAN unreadable wherever it is stored.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you use hashing, truncation, strong cryptography, or index tokens to make PAN unreadable wherever it is stored.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS COMPLIANCE CHECKLIST

Title: PCI DSS compliance Checklist	Legend	Fully Compliant	Partially Compliant	Not Compliant	Not Applicable
		FC <input type="checkbox"/>	PC <input type="checkbox"/>	NC <input type="checkbox"/>	NA <input type="checkbox"/>
Requirement		FC	PC	NC	NA
Encryption					
Have you used strong cryptography and security protocols to protect sensitive cardholder data over public networks during transmission?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Never send unprotected PANs through end-user messaging technologies.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you document security policies and operational procedures for encrypting cardholder data transfers?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Malware					
Did you install antivirus software on all systems commonly infected with malware?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are those Antivirus programs running their latest versions?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you deployed controls to check that antivirus programs in your organization's endpoints are working continuously?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ensure security policies and operating procedures are documented, used, and understood by all affected parties to protect networks against malware. Did you?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS COMPLIANCE CHECKLIST

Title: PCI DSS compliance Checklist	Legend	Fully Compliant	Partially Compliant	Not Compliant	Not Applicable
		FC <input type="checkbox"/>	PC <input type="checkbox"/>	NC <input type="checkbox"/>	NA <input type="checkbox"/>
Requirement		FC	PC	NC	NA
Updating Hardware and Software					
Have you deployed a vulnerability detection mechanism? if yes, have you started assign a risk score to newly discovered vulnerabilities?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you installed the manufacture-released latest updates on all your software to protect them from vulnerabilities?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you develop PCI DSS compliant software?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you set up processes to monitor change management control for all system component changes?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you built software that focuses on creating a secure coding environment?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do your software developers participate in updating their coding techniques atleast once a year?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you test your external facing web apps and mobile apps atleast once annually?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you document all your security protocols and operating practices to develop and maintain secure systems and applications?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS COMPLIANCE CHECKLIST

Title: PCI DSS compliance Checklist	Legend	Fully Compliant	Partially Compliant	Not Compliant	Not Applicable
		FC <input type="checkbox"/>	PC <input type="checkbox"/>	NC <input type="checkbox"/>	NA <input type="checkbox"/>
Requirement		FC	PC	NC	NA
Access Restrictions					
Does your organization limit access to system components and cardholder data based on business needs?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you restrict access based on the need-to-know principle?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you documented your policies and measures on how you restrict access to secure card data		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ID Management					
Have you ensured that policies and procedures to properly handle user IDs across all system components for service accounts and administrators is in place?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Did you provide your admins with user authentication management using multi-factor authentication for all individual non-console administrative access and all remote access to the CDE.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Did you document authentication policies and procedures? Is this document shared with all the users?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Did you train your team on the disadvantages of using group IDs, shared IDs and passwords?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are all your cardholder data storing cloud containers accessible only by programmatic methods?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS COMPLIANCE CHECKLIST

Title: PCI DSS compliance Checklist	Legend	Fully Compliant	Partially Compliant	Not Compliant	Not Applicable
		FC <input type="checkbox"/>	PC <input type="checkbox"/>	NC <input type="checkbox"/>	NA <input type="checkbox"/>
Requirement		FC	PC	NC	NA
Physical Restrictions					
Have you implemented appropriate facility entry controls to restrict and monitor physical access to systems in the cardholder data environment?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you have measures in place to quickly distinguish staff and guests on-site?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Here are a few things you must do to protect physical assets:</p> <ul style="list-style-type: none"> -Provide control of physical access to sensitive areas for on-site personnel -Physically protect all media. -Maintain tight control over any media distributed internally or externally. -Maintain tight control over media storage and accessibility. -Destroy media, when a business or legal purposes no longer require it. -Take and secure tampering and tampering measures for devices that capture payment card data. 		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>