PCI DSS checklist

A practical guide to assessing your PCI DSS compliance posture

Requirements		Notes
☐	Install and maintain network security controls to protect cardholder data environments.	
☐	Apply secure configurations to all system components, including removing default passwords and unnecessary services.	
☐	Protect stored cardholder data using encryption or other approved methods.	
☐	Encrypt transmission of cardholder data across open, public networks.	
☐	Protect systems from malware and regularly update antimalware tools.	
☐	Develop and maintain secure systems and applications, including timely patching and vulnerability remediation.	
☐	Restrict access to cardholder data based on business need-to-know.	
☐	Identify and authenticate access to system components, including use of multifactor authentication where required.	
☐	Restrict and monitor physical access to cardholder data and systems.	
☐	Log and monitor all access to system components and cardholder data.	
☐	Test security systems and processes regularly, including vulnerability scans and penetration testing.	
☐	Maintain a security policy that addresses PCI DSS requirements and is reviewed regularly.	

Need help with PCI DSS compliance?

Wipfli helps organizations assess and strengthen their PCI DSS compliance programs, from readiness assessments to ongoing monitoring and advisory support. Contact us to evaluate your PCI compliance posture.

Learn more about Wipfli's regulatory and risk compliance services.