STRONDEX

PCI DSS Compliance — Top 10 Controls

The highest-impact controls, pulled from our 78-point PCI DSS Compliance checklist.

Start here. These are the controls that block the most risk (and the ones auditors and cyber-insurance carriers ask about first). Work top-down — severity is highest at the top.

1	CRITICAL	**Define and document the Cardholder Data Environment (CDE).** **Verify:** Produce a current data-flow diagram and inventory identifying every system that stores, processes, or transmits cardholder data, plus connected system…
2	CRITICAL	**Isolate the CDE from out-of-scope systems with network segmentation.** **Verify:** Use firewalls, VLANs, or access controls so only required traffic reaches the CDE; without segmentation, the entire network is in scope.
3	CRITICAL	**Install firewalls at every internet connection and between the DMZ and internal network.** **Verify:** Deploy network security controls at each trust boundary so internet-facing traffic terminates in a DMZ, never directly on internal systems.
4	CRITICAL	**Allow no direct public access between the internet and any CDE component.** **Verify:** Ensure no CDE system has a public IP or inbound internet route; all access passes through controlled, proxied paths.
5	CRITICAL	**Change all vendor-supplied default passwords before production deployment.** **Verify:** Set unique, strong credentials on every new system, application, and appliance before it goes live.
6	CRITICAL	**Change all vendor-supplied default security parameters.** **Verify:** Harden defaults beyond passwords — SNMP community strings, sample apps, default keys, and insecure services.
7	CRITICAL	**Do not store Primary Account Numbers (PANs) after authorization without a defined business need.** **Verify:** Eliminate PAN storage wherever possible; where it's required, document the business justification and retention.
8	CRITICAL	**Never store sensitive authentication data after authorization.** **Verify:** Ensure full magnetic-stripe data, CVV/CVC, and PIN/PIN blocks are never written to logs, databases, or files after a transaction is authorized.
9	CRITICAL	**Encrypt all cardholder data transmitted over open public networks.** **Verify:** Use TLS 1.2 or higher with strong ciphers for any card data crossing the internet or other untrusted networks.
10	CRITICAL	**Do not use SSL or early TLS (1.0 / 1.1) for cardholder data.** **Verify:** Disable SSLv3, TLS 1.0, and TLS 1.1 on all endpoints handling card data.