

Hands-on Workshop on Applying PCI Guidelines To Retail IT Infrastructure

Innoviti Embedded Solutions Pvt Ltd



PCI Guidelines Checklist

Please select the appropriate “Compliance Status” for each requirement.

PCI Requirement	Description	Compliance Status (Select One)
1	Install and maintain a firewall configuration to protect cardholder data.	<input type="checkbox"/> Yes <input type="checkbox"/> No
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	<input type="checkbox"/> Yes <input type="checkbox"/> No
3	Protect stored cardholder data.	<input type="checkbox"/> Yes <input type="checkbox"/> No
4	Encrypt transmission of cardholder data across open, public networks.	<input type="checkbox"/> Yes <input type="checkbox"/> No
5	Use and regularly update anti-virus software.	<input type="checkbox"/> Yes <input type="checkbox"/> No

PCI Guidelines Checklist Contd...

6	Develop and maintain secure systems and applications.	<input type="checkbox"/> Yes	<input type="checkbox"/> No
7	Restrict access to cardholder data by business need to know.	<input type="checkbox"/> Yes	<input type="checkbox"/> No
8	Assign a unique ID to each person with computer access.	<input type="checkbox"/> Yes	<input type="checkbox"/> No
9	Restrict physical access to cardholder data.	<input type="checkbox"/> Yes	<input type="checkbox"/> No
10	Track and monitor all access to network resources and cardholder data.	<input type="checkbox"/> Yes	<input type="checkbox"/> No
11	Regularly test security systems and processes.	<input type="checkbox"/> Yes	<input type="checkbox"/> No
12	Maintain a policy that addresses information security.	<input type="checkbox"/> Yes	<input type="checkbox"/> No

Brief Introduction to PCI DSS Requirements

Build & Maintain a Secure Network

- ✓ Install & Maintain a Firewall Configuration to protect data.
- ✓ Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data




- ✗ Protect Stored Data
- ✗ Encrypt Transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program



- ✓ Use and regularly update anti-virus software.
- ✗ Develop and Maintain Secure Systems and Applications.

PCI DSS Requirements (Contd.)

Implement Strong Access Control Measures

-  Restrict Access to Data by business need-to-know.
-  Assign a unique id to each person with computer access.
-  Restrict physical access to cardholder environment.

Regularly Monitor and Test Networks

-  Track and Monitor all access to network resources and cardholder data.
-  Regularly test security systems and processes.

Maintain a Information Security Policy

-  Maintain a policy that addresses information security.

Thank You