PCI Compliance Checklist for Modern Organizations

Section A - Planning & Prep for PCI Compliance

1. Understand your org's PCI compliance level

- [ ] **Assess your organizations PCI requirements**

  PCI compliance obligations are determined by the number of annual transactions your organization processes or the means by which you process payments. Your compliance requirements will vary depending on which criteria you meet. See here for more information.

2. Define the Cardholder Data Environment (CDE) by identifying all "in-scope" systems

- [ ] **Create data flow diagrams to map lifecycle of cardholder and/or authentication data**

  Modeling how you ingest, transmit, and store cardholder data as well as any account authorization data will help you understand the lifecycle of PCI and determine in the process of normal business operations what systems are intended to be in-scope.

- [ ] **Build an asset inventory**

  Use best practices to build an inventory of IT systems critical to your business processes, as well as the data contained within these systems. Then leverage the inventory you create to identify in scope systems connected to your CDE and to remove PCI from out-of-scope systems.

Section B - Network Architecture and Scope Configuration

3. Isolate out-of-scope systems and ensure they don't contain cardholder data

- [ ] **Segment out-of-scope systems with proper controls**

  Use network segmentation, firewalls, physical and logical access controls, and other relevant techniques and technologies to ensure that out-of-scope systems remain unconnected to in-scope systems. See here for guidance.

- [ ] **Conduct regular audits & monitoring of out-of-scope systems**

  In order to ensure continuous PCI compliance, use tools like Data Loss Prevention to regularly scan and monitor out-of-scope systems for PCI to prevent accidental sharing and storage of cardholder and/or authentication data in out-of-scope systems.

  All efforts must demonstrate compliance with PCI DSS requirement 3 which requires not sending unprotected, plaintext primary account numbers in systems like email and instant messaging, which Nightfall can help with.

4. Reduce PCI scope wherever possible

- [ ] **Implement processes to reduce collection of PCI to minimum required for business need**

  Within in-scope systems continuously develop processes to reduce your intake of PCI to only what is required for business need. This may include effectively leveraging processes like **tokenization, point to point encryption, or offloading certain aspects of your cardholder data management to trusted third-parties.**

PCI Compliance Checklist for Modern Organizations

Section C - Implementation of PCI Controls

5. Ensure you're following the 12 PCI requirements within in-scope systems

- [ ] **Install and maintain a firewall to protect cardholder data.**

  Use proper controls to segment networks and manage/monitor traffic accessing cardholder data. Within the cloud, leverage tools that prevent data from leaving your environments, like Nightfall.

- [ ] **Protect stored cardholder data**

  Cardholder data, including authorization data, must not be stored in plaintext and should be encrypted when at rest/not in use. Use technologies like Nightfall to scan and remove this data in real time.

- [ ] **Use and regularly update antivirus software**

  Keep antivirus software and malware protections on systems up-to-date and to run scans regularly.

- [ ] **Restrict access to cardholder data by business need to know**

  Have strong authentication and access control measures in place that can be used to restrict cardholder data access.

- [ ] **Restrict physical access to cardholder data**

  Physical access to cardholder data (via CDs, thumb drives, hard disks or on premise terminals, must be restricted.

- [ ] **Regularly test security systems and processes**

  Conduct regular vulnerability scanning and pen testing of systems to ensure that systems are kept secure.

- [ ] **Ensure assets are not using vendor-supplied passwords or security defaults**

  Always change security configurations from vendor defaults on devices and accounts. Especially passwords. You can monitor cloud systems for password leakage with Nightfall.

- [ ] **Encrypt cardholder data transmitted over public networks**

  Any cardholder data in-transit over exposed, public networks must be encrypted. Use technologies like TLS to ensure data is protected in transmission. Tools like Nightfall can ensure that plaintext primary account numbers aren't circulating when transmitted over cloud environments.

- [ ] **Develop and maintain secure systems and applications**

  Apply updates for servers and applications in use, including hotfixes. Having a thorough DevSecOps process for any custom code or applications being developed.

- [ ] **Assign a unique ID to each person with access to systems**

  Create identifiers for user accounts, so you can monitor them and determine when anomalous behavior is taking place.

- [ ] **Track and monitor access to systems and cardholder data**

  Regularly review logs within your systems to ensure that anomalous behavior, like unauthorized accounts accessing sensitive information, isn't occurring.

- [ ] **Maintain an information security policy for all employees and contractors**

  Develop practices like security reviews, tabletop exercises, incident response plans, disaster recovery plans, etc. to ensure your security program is up-to-date.

Disclaimer: While we have made every attempt to ensure that the information contained in this guide is accurate to our best efforts, Shoreline Labs, Inc., is not responsible for any errors or omissions, or for any result obtained from the use of this information. This guide is based on a specific point in time, and is no guarantee of completeness, accuracy, timeliness, or of the results obtained from the use of this information. Nothing in this guide should be used as a substitute for the independent investigations and the sound technical and business judgment of your legal and compliance professionals. We do not accept any liability if this guide is used for an alternative purpose from which it is intended, nor to any third party for any purpose. In no event will Shoreline Labs, Inc., its employees or agents, be liable to you or anyone else for any decision made or action taken in reliance on this guide or for any consequential, special or similar damages, even if advised of the possibility of such damages.