# Compliance Report PCI DSS 2.0

Generated by Check Point Compliance Blade, on April 16, 2018 15:41 PM

Check Point
SOFTWARE TECHNOLOGIES LTD.

1

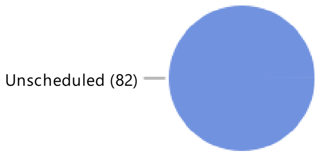
**90%**
Compliance

## About PCI DSS 2.0

PCI-DSS is a legal obligation mandated not by government but by the credit card companies. Any company that is involved in the transmission, processing or storage of credit card data, must be compliant with PCI-DSS. PCI is divided into 12 main requirements, and further broken down into approximately 200 control areas. There are different levels of PCI compliance depending on the number of transactions that are being processed by the company.

## 82 Action Items

| | | |
|---|---|---|
| 🟥 | Overdue | 0 items |
| 🟧 | Upcoming | 0 items |
| 🟨 | Future | 0 items |
| 🟦 | Unscheduled | 82 items |



## 191 Security Best Practices

related to this regulation

| | | |
|---|---|---|
| 🟩 | 57% | Secure |
| 🟨 | 6% | Good |
| 🟧 | 6% | Medium |
| 🟥 | 31% | Poor |

## 52 Regulatory Requirements

| | |
|---|---|
| 🟩 | 22 Compliant |
| 🟨 | 22 Good |
| 🟧 | 5 Medium |
| 🟥 | 3 Poor |

## Blades

Security Status by Blade

| | |
|---|---|
| Firewall | 82% |
| URL Filtering | 46% |
| IPSec VPN | 85% |
| IPS | 53% |

# Regulatory Requirement Summary ( 1 out of 4 )

2

| Id | Description | Status |
|---|---|---|
| 030005 | Establish firewall and router configuration standards that include documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure [Original PCI DSS 2.0 Reference: Requirement 1: Install and maintain a firewall configuration to protect cardholder data: 1.1.5] | Good |
| 030007 | Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment [Original PCI DSS 2.0 Reference: Requirement 1: Install and maintain a firewall configuration to protect cardholder data: 1.2.1] | Compliant |
| 030009 | Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment [Original PCI DSS 2.0 Reference: Requirement 1: Install and maintain a firewall configuration to protect cardholder data: 1.2.3] | Compliant |
| 030011 | Limit inbound Internet traffic to IP addresses within the DMZ [Original PCI DSS 2.0 Reference: Requirement 1: Install and maintain a firewall configuration to protect cardholder data: 1.3.2] | Medium |
| 030012 | Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment [Original PCI DSS 2.0 Reference: Requirement 1: Install and maintain a firewall configuration to protect cardholder data: 1.3.3] | Compliant |
| 030013 | Do not allow internal addresses to pass from the Internet into the DMZ [Original PCI DSS 2.0 Reference: Requirement 1: Install and maintain a firewall configuration to protect cardholder data: 1.3.4] | Poor |
| 030014 | Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet [Original PCI DSS 2.0 Reference: Requirement 1: Install and maintain a firewall configuration to protect cardholder data: 1.3.5] | Compliant |
| 030015 | Implement stateful inspection, also known as dynamic packet filtering [Original PCI DSS 2.0 Reference: Requirement 1: Install and maintain a firewall configuration to protect cardholder data: 1.3.6] | Compliant |
| 030017 | Do not disclose private IP addresses and routing information to unauthorized parties [Original PCI DSS 2.0 Reference: Requirement 1: Install and maintain a firewall configuration to protect cardholder data: 1.3.8] | Poor |
| 030021 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards [Original PCI DSS 2.0 Reference: Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters: 2.2] | Medium |
| 030024 | Configure system security parameters to prevent misuse [Original PCI DSS 2.0 Reference: Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters: 2.2.3] | Medium |
| 030025 | Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers [Original PCI DSS 2.0 Reference: Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters: 2.2.4] | Good |
| 030026 | Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access [Original PCI DSS 2.0 Reference: Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters: 2.3] | Compliant |
| 030046 | Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks [Original PCI DSS 2.0 Reference: Requirement 4: Encrypt transmission of cardholder data across open, public networks: 4.1] | Compliant |
| 030049 | Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers) [Original PCI DSS 2.0 Reference: Requirement 5: Use and regularly update anti-virus software or programs: 5.1] | Compliant |

# Regulatory Requirement Summary ( 2 out of 4 )

3

| Id | Description | Status |
|---|---|---|
| 030050 | Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software [Original PCI DSS 2.0 Reference: Requirement 5: Use and regularly update anti-virus software or programs: 5.1.1] | 🟨 Good |
| 030051 | Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs [Original PCI DSS 2.0 Reference: Requirement 5: Use and regularly update anti-virus software or programs: 5.2] | 🟨 Good |
| 030052 | Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release [Original PCI DSS 2.0 Reference: Requirement 6: Develop and maintain secure systems and applications: 6.1] | 🟨 Good |
| 030053 | Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities [Original PCI DSS 2.0 Reference: Requirement 6: Develop and maintain secure systems and applications: 6.2] | 🟩 Compliant |
| 030076 | For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: 1) Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes, 2) Installing a web-application firewall in front of public-facing web applications [Original PCI DSS 2.0 Reference: Requirement 6: Develop and maintain secure systems and applications: 6.6] | 🟥 Poor |
| 030077 | Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities [Original PCI DSS 2.0 Reference: Requirement 7: Restrict access to cardholder data by business need to know: 7.1.1] | 🟩 Compliant |
| 030078 | Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the assignment of privileges is based on individual personnel"s job classification and function [Original PCI DSS 2.0 Reference: Requirement 7: Restrict access to cardholder data by business need to know: 7.1.2] | 🟩 Compliant |
| 030079 | Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the requirement for a documented approval by authorized parties specifying required privileges [Original PCI DSS 2.0 Reference: Requirement 7: Restrict access to cardholder data by business need to know: 7.1.3] | 🟩 Compliant |
| 030080 | Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the implementation of an automated access control system [Original PCI DSS 2.0 Reference: Requirement 7: Restrict access to cardholder data by business need to know: 7.1.4] | 🟩 Compliant |
| 030081 | Establish an access control system for systems components with multiple users that restricts access based on a user"s need to know, and is set to "deny all" unless specifically allowed. This access control system must include coverage of all system components [Original PCI DSS 2.0 Reference: Requirement 7: Restrict access to cardholder data by business need to know: 7.2.1] | 🟩 Compliant |
| 030082 | Establish an access control system for systems components with multiple users that restricts access based on a user"s need to know, and is set to "deny all" unless specifically allowed. This access control system must include the assignment privileges to individuals based on job classification and function [Original PCI DSS 2.0 Reference: Requirement 7: Restrict access to cardholder data by business need to know: 7.2.2] | 🟩 Compliant |

# Regulatory Requirement Summary ( 3 out of 4 )

4

| Id | Description | Status |
|---|---|---|
| 030083 | Establish an access control system for systems components with multiple users that restricts access based on a user"s need to know, and is set to "deny all" unless specifically allowed. This access control system must include a default "deny-all" setting [Original PCI DSS 2.0 Reference: Requirement 7: Restrict access to cardholder data by business need to know: 7.2.3] | 🟩 Compliant |
| 030085 | In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: a) Something you know, such as a password or passphrase, b) Something you have, such as a token device or smart card, c) Something you are, such as a biometric [Original PCI DSS 2.0 Reference: Requirement 8: Assign a unique ID to each person with computer access: 8.2] | 🟩 Compliant |
| 030086 | Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties [Original PCI DSS 2.0 Reference: Requirement 8: Assign a unique ID to each person with computer access: 8.3] | 🟩 Compliant |
| 030087 | Render all passwords unreadable during transmission and storage on all system components using strong cryptography [Original PCI DSS 2.0 Reference: Requirement 8: Assign a unique ID to each person with computer access: 8.4] | 🟩 Compliant |
| 030101 | Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID [Original PCI DSS 2.0 Reference: Requirement 8: Assign a unique ID to each person with computer access: 8.5.14] | 🟩 Compliant |
| 030102 | If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session [Original PCI DSS 2.0 Reference: Requirement 8: Assign a unique ID to each person with computer access: 8.5.15] | 🟩 Compliant |
| 030125 | Implement automated audit trails for all system components to reconstruct all individual accesses to cardholder data [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources and cardholder data: 10.2.1] | 🟨 Good |
| 030126 | Implement automated audit trails for all system components to reconstruct all actions taken by any individual with root or administrative privileges [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources and cardholder data: 10.2.2] | 🟨 Good |
| 030127 | Implement automated audit trails for all system components to reconstruct access to all audit trails [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources and cardholder data: 10.2.3] | 🟨 Good |
| 030128 | Implement automated audit trails for all system components to reconstruct invalid logical access attempts [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources and cardholder data: 10.2.4] | 🟨 Good |
| 030129 | Implement automated audit trails for all system components to reconstruct use of identification and authentication mechanisms [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources and cardholder data: 10.2 5] | 🟨 Good |
| 030130 | Implement automated audit trails for all system components to reconstruct initialization of the audit logs [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources and cardholder data: 10.2.6] | 🟨 Good |
| 030131 | Implement automated audit trails for all system components to reconstruct creation and deletion of system-level objects [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources and cardholder data: 10.2.7] | 🟨 Good |
| 030132 | Record user identification in the audit trail entries for all system components for all events listed in 10.2.1 - 10.2.7 [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources and cardholder data: 10.3.1] | 🟨 Good |
| 030133 | Record event type in the audit trail entries for all system components for all events listed in 10.2.1 - 10.2.7 [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources and cardholder data: 10.3.2] | 🟨 Good |

# Regulatory Requirement Summary ( 4 out of 4 )

| Id | Description | Status |
|---|---|---|
| 030134 | Record date and time in the audit trail entries for all system components for all events listed in 10.2.1 - 10.2.7 [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources and cardholder data: 10.3.3] | Good |
| 030135 | Record a success or failure indication in the audit trail entries for all system components for all events listed in 10.2.1 - 10.2.7 [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources and cardholder data: 10.3.4] | Good |
| 030136 | Record the origination of the event in the audit trail entries for all system components for all events listed in 10.2.1 - 10.2.7 [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources and cardholder data: 10.3.5] | Good |
| 030137 | Record the identity or name of the affected data, system component or resource in the audit trail entries for all system components for all events listed in 10.2.1 - 10.2.7 [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources and cardholder data: 10.3.6] | Good |
| 030144 | Promptly backing up audit trail files to a centralized log server or media that is difficult to alter [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources and cardholder data: 10.5.3] | Medium |
| 030145 | Write logs for external-facing technologies onto a log server on the internal LAN [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources and cardholder data: 10.5.4] | Medium |
| 030146 | Use file integrity monitoring or change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert) [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources and cardholder data: 10.5.5] | Compliant |
| 030148 | Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup) [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources and cardholder data: 10.7] | Good |
| 030156 | Use intrusion detection systems, and/or intrusion prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines, baselines, and signatures up-to-date [Original PCI DSS 2.0 Reference: Requirement 11: Regularly test security systems and processes: 11.4] | Good |
| 030170 | Ensure usage policies for critical technologies require automatic disconnect of sessions for remote access technologies after a specific period of inactivity [Original PCI DSS 2.0 Reference: Requirement 12: Maintain a policy that addresses information security for all personnel: 12.3.8] | Good |
| 030192 | Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems [Original PCI DSS 2.0 Reference: Requirement 12: Maintain a policy that addresses information security for all personnel: 12.9.5] | Good |