CorreLog Alignment to PCI Security Standards Compliance

Achieving PCI DSS compliance is a process. There are many systems and countless moving parts that all need to come together to keep user payment card data secure. The PCI Security Standards Council has published a standard designed to maintain transaction security. This document looks at specific PCI DSS requirements by number and provides a brief overview of what needs to be done by the processor and/or merchant to remain compliant. Additionally, this document outlines the CorreLog functionality that addresses each requirement line item listed.

CorreLog®
www.correlog.com

CorreLog

Proactive Security Correlation & Log Management

Table of Contents

PCI DSS Requirement 1.1.6:

What is this requirement?
Requirement to review firewall and router rule sets at least every six months.

How to be Compliant?
All firewall and router activity should be continuously monitored for accuracy relative to configuration and security policy. Events that do not fall within policy should be flagged and appropriate personnel alerted so that appropriate corrective action can be taken.

CorreLog Support for PCI DSS Requirement:
To achieve compliance with this regulation, CorreLog supports a variety of intrusion detection, protection systems, firewalls and routers including Cisco, SourceFire, McAfee and many others. CorreLog provides real time alerts for configuration changes to firewall and routers. CorreLog analyzes and correlates events across these systems in order to provide a more deep inspection of the firewall and router events than what can be accomplished through any one system. Analysis of the data can confirm the accuracy of the firewall and router configurations. Long term trending over days, week and month s can further identify configuration or policy issues.

To accomplish this, **CorreLog** provides six reports:

- All Perimeter Activity Report
- Firewall Device Activity Report
- Firewall Blacklist Report
- Firewall Whitelist Report
- Top IP Addresses
- Firewall and Router Configuration Change report

Prerequisites:

Define a list representing the IP addresses of Firewall and Routers.

Reporting Data Points in CorreLog:

External IP Address, Country Code, Local Address, Source Address, Protocols, Severity

PCI DSS Requirement 1.2.1:

What is this requirement?
Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.

How to be Compliant?
Monitor all traffic inbound and outbound from the cardholder data environment. Any traffic outbound or inbound that does not adhere to security policy should be flagged with notification sent to responsible personnel.

CorreLog Support for PCI DSS Requirement:
To achieve compliance with this regulation, CorreLog analyzes inbound and outbound traffic relative to the cardholder data environment. Lists are defined which identify the IP addresses of the cardholder data environment. Any traffic activity that does not adhere to cardholder security policy is flagged and alerts are generated to the proper personnel. Reports reflecting all activity can be scheduled and routed to appropriate personnel automatically.

To accomplish this, **CorreLog** provides two reports:

- Cardholder Data Access Report
- Cardholder Data Violation Report

Prerequisites:

Define a list representing the IP addresses of Cardholder data System(s) Environment.
Define a list representing the IP addresses of Systems that are approved to access the Cardholder data System(s)

Reporting Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 1.3.1:

What is this requirement?
Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

How to be Compliant?
Implement a DMZ and verify that it limits inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

CorreLog Support for PCI DSS Requirement:
To achieve compliance with this regulation, CorreLog analyzes in real-time inbound and outbound traffic relative to the cardholder data environment. Any traffic activity that is inbound from outside the DMZ from system components that are not authorized as part of the cardholder security policy is flagged with alerts generated to the proper personnel.

To accomplish this, **CorreLog** provides three reports:

- Cardholder Data Access Report
- Cardholder Data Access Top IP Addresses Report
- Cardholder Data Violation Report

Prerequisites:

Define a list representing the IP addresses of system components within the DMZ Environment. Define a list representing the IP addresses of components that are authorized to access the Cardholder data environment.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 1.3.2:

What is this requirement?
Limit inbound Internet traffic to IP addresses within the DMZ.

How to be Compliant?
Monitor all inbound traffic relative to the DMZ environment. Any IP traffic that originates outside the DMZ should be flagged as not compliant relative to security policy. Alerts, tickets and reports should be generated and distributed to the proper personnel.

CorreLog Support for PCI DSS Requirement:
To achieve compliance with this regulation, CorreLog analyzes in real-time inbound and outbound traffic relative to the cardholder data environment. Any traffic activity that is inbound from outside the DMZ and thus does not adhere to cardholder security policy is flagged with alerts generated to the proper personnel.

To accomplish this, **CorreLog** provides three reports:

- Cardholder Data Access Report
- Cardholder Data Access Top IP Addresses Report
- Cardholder Data Violation Report

Prerequisites:

Define a list representing the IP addresses within the DMZ Environment.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 1.3.3:

What is this requirement?
Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.

How to be Compliant?
Monitor all IP traffic inbound and outbound from the cardholder environment. Any direct inbound or outbound traffic from cardholder data environment and the internet should be flagged with alerts sent to responsible personnel.

CorreLog Support for PCI DSS Requirement:
To achieve compliance with this regulation, CorreLog analyzes in real-time all inbound and outbound traffic relative to the cardholder data environment. Any IP traffic inbound or outbound whose origination or destination is the internet and thus does not conform to cardholder data security policy is flagged with alerts generated to the proper personnel.

To accomplish this, **CorreLog** provides three reports:

- Cardholder Data Access Report
- Cardholder Data Access Top IP Addresses Report
- Cardholder Data Internet Access Violation Report

Prerequisites:

Define a list representing the IP addresses of Cardholder data System(s) Environment.
Define a list representing the IP addresses of Internet Access Devices.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 1.3.4:

What is this requirement?
Do not allow internal addresses to pass from the internet into the DMZ.

How to be Compliant?
Monitor all inbound IP traffic from the internet to the DMZ. Any direct inbound traffic from internet should be flagged with alerts sent to responsible personnel.

CorreLog Support for PCI DSS Requirement:
To achieve compliance with this regulation, CorreLog analyzes in real-time all inbound and outbound traffic relative to the cardholder data environment. Any IP traffic inbound from the internet whose destination is the DMZ and does not conform to cardholder data security policy is flagged with alerts generated to the proper personnel.

To accomplish this, **CorreLog** provides three reports:

- Cardholder Data Access Report

- Cardholder Data Access Top IP Addresses Report
- Cardholder Data Internet Access Violation Report

Prerequisites:

Define a list representing the IP addresses of Cardholder data System(s) Environment.
Define a list representing the IP addresses of Internet Access Devices.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 1.3.5:

What is this requirement?
Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.

How to be Compliant?
Monitor all IP traffic outbound from the cardholder environment. Any unauthorized outbound IP traffic to the internet should be flagged with alerts sent to responsible personnel.

CorreLog Support for PCI DSS Requirement:
To achieve compliance with this regulation, CorreLog analyzes in real-time all inbound and outbound traffic relative to the cardholder data environment. Any unauthorized outbound IP traffic whose destination is the internet is flagged with alerts generated to the proper personnel.

To accomplish this, **CorreLog** provides two reports:

- Cardholder Data Access Report
- Cardholder Data Internet Access Violation Report

Prerequisites:

Define a list representing the IP addresses of Cardholder data System(s) Environment.
Define a list representing the IP addresses of authorized system components.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 3.2.2:

What is this requirement?
Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not present transactions.

How to be Compliant?
Examine data sources listed below and verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance:

- Incoming transaction data
- All logs (for example, transaction, history, debugging, error)
- History files
- Trace files
- Several database schemas
- Database contents

CorreLog Support for PCI DSS Requirement:
To help achieve compliance to this requirement, CorreLog captures and analyzes all event data from all systems and applications handling cardholder data. The event data is analyzed for card verification data and if it is detected, alerts and tickets are generated to the appropriate personnel. In addition, CorreLog has the unique capability to also monitor database tables and trace files with the same alert and ticketing capabilities. Note that all card verification can be masked out on all reports, alerts and tickets.

With this data and CorreLog's capabilities, compliance with PCI DSS Requirement 3.2.2 can be easily established.

To accomplish this, **CorreLog** provides one report:

- Card Verification Data Violation Report

Prerequisites:

Define a macro representing a mask for the card verification data.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 3.2.3:

What is this requirement:
Do not store the personal identification number (PIN) or the encrypted PIN block.

What Needs To Be Done:
For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance:

- Incoming transaction data
- All logs (for example, transaction, history, debugging, error)
- History files
- Trace files
- Several database schemas
- Database contents

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog captures and analyzes all event data from all systems and applications handling cardholder data. The event data is analyzed for card PIN data and if it is detected, alerts and tickets are generated to the appropriate personnel. In addition, CorreLog has the unique capability to also monitor database tables and trace files with the same alert and ticketing capabilities. Note that all card PIN data can be masked out on all reports, alerts and tickets.

With this data and CorreLog's capabilities, compliance with PCI DSS Requirement 3.2.3 can be easily established.

To accomplish this, **CorreLog** provides one report:

- Card PIN Data Violation Report

Prerequisites:

Define a macro representing a mask for the card PIN data.
Define a list representing the IP addresses of Cardholder data System(s) Environment.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 4.1:

What is this requirement:
Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.

Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:

- The Internet
- Wireless technologies,
- Global System for Mobile communications (GSM)
- General Packet Radio Service (GPRS).

What Needs To Be Done:
Monitor all cardholder data IP traffic that is being transmitted over open, public networks to ensure that strong cryptographic security protocols are being employed. Any unauthorized protocols should be flagged with alerts sent to responsible personnel.

CorreLog Support for PCI DSS Requirement:
To achieve compliance with this regulation, CorreLog analyzes in real-time inbound and outbound IP traffic relative to the cardholder data environment, which includes the communication protocols that are employed. Any traffic activity that occurs over open or public networks that does not employ cryptographic security that adheres to cardholder data security policy is flagged with alerts generated to the proper personnel.

With this data and CorreLog's capabilities, compliance with PCI DSS Requirement 4.1 can be easily established.

To accomplish this, **CorreLog** provides one report:

- Cardholder Data Protocol Violation Report.

Prerequisites:

Define a list representing the IP addresses of Cardholder data System(s) Environment.
Define a list representing authorized protocols for the cardholder data environment.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 5.2:

What is this requirement:
Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.

What Needs To Be Done:
Verify that all anti-virus software is current, actively running, and generating logs.

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog captures all log files from anti-virus programs and can determine when the programs are not functioning. CorreLog can capture the log files and analyze them to determine whether the anti-virus programs have been updated and are current. With this data and CorreLog's capabilities, compliance with PCI DSS Requirement 5.2 can be easily established.

To accomplish this, **CorreLog** provides one report:

- Anti-Virus Violation Report.

Prerequisites:

Define a list representing the IP addresses of Cardholder data System(s) Environment.
Define a list representing all of the authorized UserIDs for the cardholder data environment.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 7.1.x:

What is this requirement:
Limit access to system components and cardholder data to only those individuals whose job requires such access.

What Needs To Be Done:
All user access to system components and cardholder data should be logged along with the accessing UserID of the individual. Any UserID that is not identified as an authorized user should be flagged with alerts sent to responsible personnel. In addition, any changes to access rights should be logged and reported on.

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog captures all cardholder data access activity which includes the UserID of the requestor. The UserID's owner or user's name is associated to all UserIDs in the CorreLog system. A whitelist of UserIDs that are authorized to access cardholder data is maintained. Resource accesses that are not authorized are flagged with alerts and tickets generated, then sent to responsible personnel. In addition, CorreLog logs and reports on all access rights changes to the cardholder data environment.

With this data and CorreLog's capabilities, compliance with PCI DSS Requirement 7.1.x can be easily established.

To accomplish this, **CorreLog** provides two reports:

- Cardholder Data Access Violation Report.
- Access Rights Changes to the Cardholder Data Environment.

Prerequisites:

Define a list representing the IP addresses of Cardholder data System(s) Environment.
Define a list representing all of the authorized UserIDs for the cardholder data environment.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 8.1:

What is this requirement:
Assign all users a unique ID before allowing them to access system components or cardholder data.

What Needs To Be Done:
Ensuring that each user has a unique UserID assigned to them is critical to protecting cardholder data. Each data access or system manipulation involving cardholder data needs to be securely logged with the association of the UserID to the individual who owns and is solely responsible for the UserID. Ultimately every data access to cardholder data should be linked to a UserID and its owner. Generic UserIDs and those being shared among multiple users should be immediately identified with corrective action taken.

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog identifies and logs all accesses to cardholder data systems along with the UserID and its owner's name. UserIDs that do not have an associated owner or those belonging to generic accounts are easily identified. Where UserIDs are being shared, CorreLog has unique capabilities that allow it to track login sessions, identifying those situations where UserIDs are being shared or are being used contiguously by multiple users. In all cases, reports and alerts can be sent to responsible personnel for corrective action.

With this data and CorreLog's capabilities, compliance with PCI DSS Requirement 8.1 can be easily established.

To accomplish this, **CorreLog** provides two reports:

- Cardholder Data Access Report
- Shared and Generic UserID Usage Report

Prerequisites:

Define a list representing the IP addresses of Cardholder data System(s) Environment.
Define a list representing all of the authorized UserIDs for the cardholder data environment.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 8.5.4:

What is this requirement:
Immediately revoke access for any terminated users.

What Needs To Be Done:
Ensuring that that the cardholder data system access for terminated users has been revoked is critical to ensuring the security of cardholder data. When a user is terminated or should no longer have access, their access should be removed from relevant systems.

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog logs all access to cardholder data systems along with a list of terminated employees. Any access or attempted access by these terminated users can be immediately identified with alerts generated to responsible personnel for corrective action.

With this data and CorreLog's capabilities, compliance with PCI DSS Requirement 8.5.4 can be easily established.

To accomplish this, **CorreLog** provides one report:

- Cardholder Data Access Terminated User Report

Prerequisites:

Define a list representing the IP addresses of Cardholder data System(s) Environment.
Define a list representing terminated Users.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 10.1:

What is this requirement:
Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.

What Needs To Be Done:
Identifying all logical accesses to cardholder data is a critical component of PCI DSS compliance. All accesses to system components should be logged with the association of the responsible UserID and its owner. While the audit data should encompass all systems, it should be easily broken down and grouped by system and UserID where it can be easily analyzed. Specific emphasis should be placed on the grouping and analysis of access to those systems that house cardholder data. This requirement places particular emphasis on those users with privileged access such as administrative users, given their ability to make system changes which can have dramatic impacts on systems and applications.

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog logs all accesses to system and application components with the association of the UserID and its owner. CorreLog automatically breaks the event data by system and user, allowing all accesses to system and application components to be isolated and viewed in the data and timestamp order in which they occurred for any period of time. Privileged user access is isolated enterprise wide across differing systems and specific to those systems that house cardholder data. Reports and alerts can be generated to the responsible personnel.

With this data and CorreLog's capabilities, the relevant information can be isolated, and compliance to PCI DSS Requirement 10.1 can be easily established.

To accomplish this, **CorreLog** provides two reports:

- Cardholder Data System User Access Report
- Privileged User Access Report

Prerequisites:

Define a list representing the UserIDs of privileged users.
Define a list representing the IP addresses of Cardholder data System(s) Environment.
Define a list representing all of the authorized UserIDs for the cardholder data environment.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 10.2.1:

What is this requirement:
Implement automated audit trails for all system components to reconstruct all individual accesses to cardholder data.

What Needs To Be Done:
It is critical that user access to the cardholder data environment be logged and constantly monitored. All user actions should be logged in real-time with date and time stamp.

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog logs in real-time all user access events to the cardholder data environment in date and time stamp order in which they occurred. The event data can subsequently be searched, correlated and analyzed for anomalous behavior. Alerts can be generated to responsible personnel.

To accomplish this, **CorreLog** provides one report:

- User Cardholder Data Activity Report

Prerequisites:

Define a list representing the IP addresses of Cardholder data System(s) Environment.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 10.2.2:

What is this requirement:
Implement automated audit trails for all system components to reconstruct all actions taken by any individual with root or administrative privileges.

What Needs To Be Done:
It is critical that users with privileged access be constantly monitored with respect to their accesses and actions in the cardholder data environment. All privileged user actions should be logged in real-time with data and time stamp. The event data should be isolated where they can be easily be searched, correlated and analyzed for anomalous behavior.

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog logs in real-time all privileged user activity in the cardholder data environment in date and time stamp order in which they occurred. Those with privileged access are isolated, correlated and analyzed with any anomalous behavior triggering alerts to responsible personnel.

To accomplish this, CorreLog provides one report:

- Privileged User Cardholder Data Activity Report

Prerequisites:

Define a list representing the UserIDs of privileged users.
Define a list representing the IP addresses of Cardholder data System(s) Environment.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 10.2.3:

What is this requirement:
Implement automated audit trails for all access to all audit trails.

What Needs To Be Done:
It is critical that access to all audit trails be logged in a secure manner. Any access or modifications including the clearing of the logs should be logged in real-time to a centralized repository.

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog logs in real-time all user access events to the audit trails themselves, which includes the clearing of logs. The UserID of all accesses are associated with the events. CorreLog securely logs accesses to itself into the audit log repository along with all other captured events. In the event that log event sources cease to forward events to CorreLog, CorreLog can identify the condition and generate alerts.

To accomplish this, **CorreLog** provides two reports:

- Log Cleared Action Report.
- CorreLog Access Activity Report

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 10.2.4:

What is this requirement?
Implement automated audit trails for all invalid logical access attempts to the cardholder data environment.

How to be Compliant?

All access attempts to the cardholder data environment and specifically invalid logical access attempts should be logged.

CorreLog Support for PCI DSS Requirement:

To achieve compliance to this requirement, CorreLog logs all access attempts to the cardholder data environment in real-time with data and time stamp. Invalid login attempts are specifically isolated with alerts generated upon detection of any anomalous behaviors.

To accomplish this, CorreLog provides one report:

- Cardholder Data Invalid Login Report

Prerequisites:

Define a list representing the IP addresses of Cardholder data System(s) Environment.
Define a correlation thread capturing all invalid access attempts to the cardholder data environment.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 10.2.5:

What is this requirement?

Implement automated audit trails to verify the use of identification and authentication methods.

How to be Compliant?

All successful and failed access attempts to the cardholder data environment should be logged in real-time with date and time stamps. The relevant communication protocols and authentication subsystems should also be logged with each access attempt.

CorreLog Support for PCI DSS Requirement:

To achieve compliance to this requirement, CorreLog logs all successful and failed access attempts to the cardholder data environment in real-time with the date and time stamps. The relevant communication protocols and authentication subsystems are identified and logged.

With this data and CorreLog’s capabilities, compliance with PCI DSS Requirement 10.2.5 can be easily established.

To accomplish this, **CorreLog** provides one report:

- Cardholder Data User Access Report

Prerequisites:

Define a list representing the IP addresses of Cardholder data System(s) Environment.
Define a list representing all of the authorized UserIDs for the cardholder data environment.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 10.2.6:

What is this requirement?
Implement automated audit trails to verify the proper initialization and functionality of the audit logs.

How to be Compliant?
The initialization and functionality of the audit logs such as failure to audit, event log full, log file corrupt, log cleared and any condition that inhibits the full functioning of the audit log should be logged.

CorreLog Support for PCI DSS Requirement:
CorreLog logs all events from the audit log sources including event related to the condition of the audit log processes themselves. CorreLog can also provide alerts when audit log sources cease communication. With this data and CorreLog's capabilities, compliance with PCI DSS Requirement 10.2.6 can be easily established.

To accomplish this, **CorreLog** provides one report:

- Audit Log Initialization and Functionality Report.

PCI DSS Requirement 10.2.7:

What is this requirement?
Implement automated audit trails to verify the creation and deletion of system level objects are logged.

How to be Compliant?
The manipulation of system level objects such as the access, creation and deletion of Active Directory objects should be logged.

CorreLog Support for PCI DSS Requirement:
CorreLog logs all manipulation to system level objects involving Active Directory with alerts and reports generated to responsible personnel. With this data and CorreLog's capabilities, compliance with PCI DSS Requirement 10.2.7 can be easily established.

To accomplish this, **CorreLog** provides one report:

- System Level Object Manipulation Report.

Prerequisites:

Define a correlation thread capturing system-level object manipulations.

Data Points in CorreLog:

Date, time, IP Address, System Name, UserID

PCI DSS Requirement 10.3.x:

What is this requirement?
Record the following information for each audit trail entry: user identification, type of event, date and time, success or failure, origination of the event, name of the affected data, system component, or resource.

How to be Compliant?
Ensuring that each access to cardholder data is properly logged and time stamped is critical to protecting cardholder data. Each data access should include the UserID the type of event, the date and time stamp, success or failure, the origination of the event, the name of the affected system, system component, or resource.

CorreLog Support for PCI DSS Requirement:
CorreLog logs all user identification and system component information relative to successful or failed access attempts. With this data and CorreLog's capabilities, compliance with PCI DSS Requirement 10.3.x can be easily established.

PCI DSS Requirement 10.5.1:

What is this requirement?
Limit viewing of audit trails to those with a job related need.

How to be Compliant?
Access to event log data should be strictly controlled and limited to those with a job-related need. Since it is nearly impossible to protect access to event data residing in their individual native repositories across the entire enterprise, event data should be captured and housed in a central repository with strict access control. Those with access to the original event data repositories should not have access to the central repository.

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog captures event data from servers, mainframes and applications in real-time to a central repository. The CorreLog solution has granular access control features that allow specific access to be granted based on a need-to-know basis. All access to CorreLog solution is logged within CorreLog itself.

With this data and CorreLog’s capabilities, compliance with PCI DSS Requirement 10.5.1 can be easily established.

PCI DSS Requirement 10.5.2:

What is this requirement?
Protect audit trail files from unauthorized modifications.

How to be Compliant?
The integrity of event data needs to be maintained and access strictly controlled and limited to those with a job related need, which includes those with privileged access. The greatest threat to event data is inadvertent or malicious destruction. Event data can be intentionally cleared from a log or it can be damaged or lost through a hardware or software failure.

Since it is nearly impossible to protect access to event data residing in their individual native repositories across the entire enterprise, event data should be captured in real-time as they occur and housed in a central repository with strict access control. Those with access to the original event data repositories should not have access to the central repository. In addition, the repository itself should be protected against destruction or deletion of data.

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog captures event data from network devices, servers, mainframes and applications in real-time to a central repository. By design, the CorreLog solution does not possess the capability to delete or alter event data that it has captured. In addition, the CorreLog repository is protected with encryption to identify any external modifications.

With this data and CorreLog’s capabilities, compliance with PCI DSS Requirement 10.5.2 can be easily established.

PCI DSS Requirement 10.5.3:

What is this requirement?
Promptly back-up audit trail files to a centralized log server or media that is difficult to alter.

How to be Compliant?
Since it is nearly impossible to protect event data residing in their individual native repositories across the entire enterprise, event data should be captured in real-time as it occurs and housed in

a central repository with strict access control. All event log repositories need to be captured in real-time and stored in a secure central repository with its own access management.

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog captures event data from network devices, servers, mainframes and applications in real-time and stores them in a central repository. By design, the CorreLog solution does not possess the capability to delete or alter event data that it has captured and the repository is protected with encryption to identify any external modifications or tampering.

The CorreLog solution utilizes a simple flat file structure for its repository for scalability and manageability. The structure is easily backed up with any commercial back and recovery solution. The log and archive files that are part of the repository are managed automatically through internal processes.

With this data and CorreLog's capabilities, compliance with PCI DSS Requirement 10.5.3 can be easily established.

PCI DSS Requirement 10.5.4:

What is this requirement?
Write logs for external-facing technologies onto a log server on the internal LAN.

What Needs To Be Done:
All event log repositories for external-facing technologies need to be captured in real-time and stored in a secure central repository on the internal LAN.

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog captures event data in real-time from anywhere in the network, which includes external-facing devices and applications. The CorreLog data repository is stored on an internal LAN network accessible only to the CorreLog solution.

With this data and CorreLog's capabilities, compliance with PCI DSS Requirement 10.5.4 can be easily established.

PCI DSS Requirement 10.5.5:

What is this requirement?
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).

How to be Compliant?
Processes should be put into place to identify any external modifications or deletions to the event

log repositories. Any deletions or modifications should be identified immediately in real-time and alerts should be generated to responsible personnel.

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog employs several methods together. First, CorreLog captures and centralizes the event log data in real-time which makes protecting the integrity of the event far more effective. Second, CorreLog monitors all external log sources for tampering such as log clear commands. Third, CorreLog employs encryption and hashing functionality around its own repository in order to detect an alteration to the stored log files.

With this data and CorreLog's capabilities, compliance with PCI DSS Requirement 10.5.5 can be easily established.

PCI DSS Requirement 10.6:

What is this requirement?
Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).

Note: Log harvesting, parsing, and alerting tools may also be used to meet compliance with requirement 10.6.

How to be Compliant?
Event and log data should be captured from all intrusion detection systems (IDS), identity and access management systems (IdAM) and accounting protocol (AAA) servers. The data should be continually correlated and analyzed relative to security policy with reports and alerts generated to responsible personnel.

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog captures event data from IDS, IdAM and AAA applications and devices in real-time. The event data is stored in a central repository where the data is correlated and analyzed with all other event data that is being captured. Alerts and reports are generated based on anomalous behavior.

With this data and CorreLog's capabilities, compliance with PCI DSS Requirement 10.6 can be easily established.

PCI DSS Requirement 10.7:

What is this requirement?
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 back-up).

How to be Compliant?
All event data must be securely retained and accessible for forensic analysis for a period of at least three months online and one year in the archive.

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog can retain online data for up to 500 days and archive data for up to 5000 days. The CorreLog solution has a unique architecture that allows the archive data to be immediately accessible for search and other forensic activities.

With this data and CorreLog's capabilities, compliance with PCI DSS Requirement 10.7 can be easily established.

PCI DSS Requirement 11.4:

What is this requirement?
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.

How to be Compliant?
It is critical that IDS and IPS systems be deployed and their event data be captured in real-time and combined with other network event data. The combined data needs to be correlated and analyzed holistically to provide a complete forensic accounting of events.

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog can retain online data for up to 500 days and archive data for up to 5,000 days. The CorreLog solution has a unique architecture that allows the archived data to be immediately accessible for search and other forensic activities.

With this data and CorreLog's capabilities, compliance with PCI DSS Requirement 11.4 can be easily established.

PCI DSS Requirement 11.5:

What is this requirement?
Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

How to be Compliant?
File Integrity Monitoring software (FIM) should be deployed across the entire PCI DSS infrastructure to monitor all critical operating system and applications system files as least weekly.

CorreLog Support for PCI DSS Requirement:
To achieve compliance to this requirement, CorreLog has a File Integrity Monitor adapter that is scalable and can scan tens of thousands of files in multiple directories in a few minutes and permit as frequent as hourly checks. First a configuration baseline is established. Then, the Monitor constantly checks the file creation time, modify time and file size to determine if a file has been changed from the baseline. When file changes are detected, alerts and tickets are automatically generated in the CorreLog solution to alert responsible personnel.

With this data and CorreLog's capabilities, compliance with PCI DSS Requirement 11.5 can be easily established.

About the PCI Security Standards Council

The PCI Security Standards Council (SSC) offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step. The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents. More information on the PCI SSC can be found at www.pcisecuritystandards.org.

About CorreLog, Inc.

CorreLog, Inc. is the leading independent software vendor (ISV) for IT security log management and event correlation. CorreLog's flagship product, the CorreLog Enterprise Server, combines log management, Syslog, Syslog-NG, SNMP, auto-learning functions, neural network modeling, proprietary semantic correlation, automated help-desk ticketing and reporting functions into a unique multi-platform security solution. CorreLog Enterprise Server operates across Windows, UNIX, Linux and mainframe platforms, shipping with an out-of-box PCI DSS compliant CorreLog agent for IBM z/OS, the world's most popular mainframe operating system.

CorreLog delivers an essential viewpoint via dashboard console, providing verifiable and actionable information on the activity of users, devices, and applications to proactively meet organizational SLAs and regulatory requirements. Additionally, CorreLog automatically identifies and responds to any suspicious behavior, network attacks, or policy violations by indexing and correlating user activity and event logs, then archives the data in an enterprise server system location. This allows customer organizations to quickly identify then proactively respond to compliance violations, policy breaches, cyber-attacks and insider threats. For auditing and forensics, CorreLog facilitates regulatory requirements set forth by PCI DSS, HIPAA, SOX, FISMA, NERC, NCUA, and many other standards. CorreLog markets its solutions through both direct and indirect partner channels. More info can be found at www.correlog.com.