

GFI PCI-DSS Compliance and GFI Software products



DISCLAIMER

The Payment Card Industry Data Security Standard (PCI DSS) compliance is a set of specific security standards that were developed by the payment brands * to help the adoption of consistent data security measures to protect sensitive payment-card information. The standard applies to all organizations which hold, process, or exchange cardholder information from any card branded with the logo of the payment brand companies.

* Payment brand companies include American Express, Discover Financial Services, JCB International, and MasterCard Worldwide and Visa Inc. Inc. International.

There are 12 PCI DSS requirements that are organized into six (6) logically related groups. Please see **Chart A, PCI DSS SUMMARY**, below.

Chart A – PCI DSS SUMMARY

	PCI REQUIREMENT
1. BUILD AND MAINTAIN A SECURE NETWORK	
Install and maintain a firewall configuration to protect cardholder data	1
Do not use vendor-supplied defaults for system passwords and other security parameters.	2
2. PROTECT CARDHOLDER DATA	
Protect stored cardholder data	3
Encrypt transmission of cardholder data across open, public networks	4
3. MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM	
Use and regularly update anti-virus software or programs	5
Develop and maintain secure systems and applications	6
4. IMPLEMENT STRONG ACCESS CONTROL MEASURES	
Restrict access to cardholder data by business need-to-know	7
Assign a unique ID to each person with computer access	8
Restrict physical access to cardholder data.	9
5. REGULARLY MONITOR AND TEST NETWORKS	
Track and monitor all access to network resources and cardholder data	10
Regularly test security systems and processes.	11
6. MAINTAIN AN INFORMATION SECURITY POLICY	
Maintain a policy that addresses information security for employees and contractors	12

Simply stated, the foundation of PCI DSS compliance is that merchants must meet these principles and requirements to be PCI DSS compliant. A merchant must demonstrate through representative systems and processes that they meet these requirements. It is the merchant's responsibility to achieve, demonstrate and maintain their compliance across all systems and processes in their organization

The required annual validation of compliance (internal or external) is dependent on the volume of card transactions; with larger volumes requiring more intensive external validation and those merchants with a smaller number of card transactions only requiring internal validation. Merchants with larger volumes of transactions must also have their compliance assessed by an independent assessor, a Qualified Security Assessor (QSA), while those companies handling smaller number of transactions have the option of self-certification through a Self-Assessment Questionnaire (SAQ).

HOW GFI CAN ASSIST IN PCI DSS COMPLIANCE

The remainder of this document outlines what GFI can do to assist in your achieving PCI DSS compliance. GFI Software is not in the services space and we do not have a PCI service practice, and this document will not make you PCI compliant. The intent of this document is to provide you with GFI's understanding of the requirements, and how the GFI Software product line (including three of our flagship products: GFI LANguard, GFI EventsManager and GFI EndPointSecurity) can assist you to meet PCI compliance as outlined in the PCI DSS Requirements created by the PCI Security Standards Council.

We have included several reference documents as part of this guide. For more detailed information regarding PCI DSS regulations please see

1. [CHART D – SUMMARY OF ALL PCI DSS REQUIREMENTS AND](#)
2. [CHART E – PCI DSS REQUIREMENT SUPPORT IN GFI PRODUCTS](#)

GFI Software has three (3) cost-effective solutions that can assist in achieving PCI DSS compliance. These tools, GFI EventsManager, GFI LANguard and GFI EndPointSecurity can assist you in PCI DSS Requirements 1,2,3,5,6,7,10,11, and 12. [CHART B – GFI PRODUCT – USE IN PCI DSS REQUIREMENTS](#) outlines, by PCI sub-requirement where the GFI product will assist in meeting the requirement.

GFI product(s) can assist with PCI compliance with specific features in the product, with reports that are available in the product or with both features and reports. [CHART C - PCI DSS REQUIREMENTS – GFI PRODUCT REPORTS](#) provides links to the actual product report. Just click on the link to see the sample report!

If you have any further questions after completing this document, please do not hesitate to contact your sales representative at (888)243-4329 or 919 379 3397 (outside the USA).

CHART B – GFI PRODUCT – USE IN PCI DSS REQUIREMENTS

GFI PRODUCT	EXPLANATION	VALUE OF GFI PRODUCT TO PCI COMPLIANCE	LEVEL OF COMPLIANCE*
EventsManager	1.2 And 1.4 Request examination and monitoring of the firewall/router configuration files in order to make sure that they are build in accordance to the PCI DSS specification.	EventsManager can monitor changes in the configuration files of the network devices and report on those changes	F,R
LANguard	1.3.9 Requests that personal firewall software is deployed on the employee computers that are connected to the internet	LANguard can automatically deploy personal firewall software in the entire network and report which computers in the network do not have personal firewall installed.	F,R
LANguard	2.1 implies analysis to make sure that systems do not use vendor supplied defaults.	LANguard offers functionality to detect vulnerabilities caused by the use of vendor supplied defaults and can report on the computers that have such vulnerabilities.	F,R
LANguard	2.2.2 Requires detection of unnecessary and insecure services and protocols.	LANguard can detect such services and protocols, including open ports (and ports known as Trojan ports) using its application detection, process inspection and services enumeration functionality. The product can report on these findings as well as report on computers that have unnecessary services or protocols installed.	F,R
LANguard	2.2.3: for a sample of system components, critical servers, etc., requires that tests be performed to verify that the system security parameters are set correctly (according to the configuration standard defined in Requirement 2.2).	LANguard has operating system audit functionality which enables it to read security policies and verify if certain settings are in place or not. LANguard reports on local machine users and the users who never logged on, and can disable users. It can also enumerate Password policy and enable auditing policies.	F,R
LANguard	3.4 implies the use of encryption software at endpoints and on other critical systems	LANguard can detect the presence of encryption software across the network computers and report on the computers lacking this software	F,R
LANguard	5.1 Requires network-wide deployment of anti-virus software.	LANguard can automatically perform this operation via the "customer software deployment" functionality.	F
LANguard	5.2 implies that anti-virus engines are kept up to date in the network.	LANguard can detect anti-virus software that is not up to date, update it and can report on the computers lacking anti-virus software or having outdated version of the software.	F,R
EventsManager	5.2 implies that logs of anti-virus software are enabled and retained.	EventsManager can scan the logs of the anti-virus software and report on the data it gathers	F,R
LANguard	6.1 And 6.2 require that all system components and software have the latest patches installed.	Using its vulnerability scanning and patch detection capabilities, LANguard can periodically scan the entire network to detect new vulnerabilities including SANS Top 20, CVE lists and OVAL. LANguard is CVE and OVAL certified; LANguard can automatically deploy new patches network-wide and can report on the vulnerabilities discovered across the network, the network patching status and on all vulnerable hosts.	F,R
EventsManager	7.1 implies that monitoring should be in place to make sure that the configured user accounts and their corresponding access rights are corresponding to the PCI DSS standard.	EventsManager can monitor changes to user accounts and groups as well as changes to security rights assignment and data access lists; EventsManager also can report on the data it gathers in this report.	F,R

*F = FEATURE

*R = REPORT

CHART B – GFI PRODUCT – USE IN PCI DSS REQUIREMENTS

GFI PRODUCT	EXPLANATION	VALUE OF GFI PRODUCT TO PCI COMPLIANCE	LEVEL OF COMPLIANCE*
EventsManager	8.5.1 requests control over a series of process related to user account management	EventsManager can monitor the account management events and can report on the changes. The report can be used to detect any unauthorized changes to user accounts and user account groups	F,R
LANguard	8.5.3; and 8.5.9 and 8.5.10 implies monitoring the password policy of computers across the network in order to verify that the computer is compliant with the password-related sub requirements	LANguard can perform network-wide monitoring of password policies and report on the findings.	F,R
EventsManager/ LANguard	8.5.4 and 8.5.5 requires immediate revocation of the user accounts of terminated or inactive users	EventsManager can monitor the "user account disabled" and "user account removed" events and report on this data. The report can be used to verify if the accounts of discontinued employees or employees on leave are disabled or removed. Specific to requirement 8.5.5, the corresponding testing procedures require that you verify there are no inactive accounts enabled; EventsManager can monitor the activity of the users and hence help determine the last logon times of user accounts. LANguard offers a user enumeration tool that shows all the user accounts in a domain, and highlights the disabled accounts. This list can also be used to cross-reference user account status with discontinued employees. LANguard can also disable selected user accounts.	F,R
EventsManager/LANguard	8.5.6 requires that the activity of the accounts used by vendors is monitored continuously	EventsManager can monitor user account activity by monitoring the security logs of the corresponding computers. LANguard can enumerate user accounts from the network and enable/disable them as necessary and report on this data.	F,R
EventsManager	8.5.13 implies verification of the account lockout policies.	EventsManager is able to monitor failed logons and alert on situations where the number of failed logons passes a pre-configured threshold and report on this.	F,R
EventsManager	8.5.16 implies monitoring of access to databases holding cardholder data.	EventsManager can perform this task and report on the findings for databases implemented on Microsoft SQL Server technology, using the SQL Audit functionality. This product is able to monitor all aspects of database access and usage under the above circumstances in compliance with C2 security level.	F,R
EventsManager	Requirement 10 requests that audit trails are recorded and retained.	EventsManager is able to record the audit trails throughout the network and retain them in a secured database. The product is able to record all information defined under 10.3 about all the necessary events/actions defined by the sub points of requirement 10. EventsManager can also report on the data.	F,R

*F = FEATURE

*R = REPORT

CHART B – GFI PRODUCT – USE IN PCI DSS REQUIREMENTS

GFI PRODUCT	EXPLANATION	VALUE OF GFI PRODUCT TO PCI COMPLIANCE	LEVEL OF COMPLIANCE*
EventsManager	10.2.2 The requirement implies auditing the administrative users	EventsManager can alert and report on events relating to the administrator	F,R
EventsManager	10.4 requires time synchronization of all critical system clocks	EventsManager is able to monitor the events generated by the time synchronization mechanisms and the "out of sync" errors thrown by the operating system whenever system clocks are not synchronized.	F,R
EventsManager	10.5 implies securing the audit trail data	EventsManager uses a database engine which is able to provide the granularity in terms of access rights which is required. Additionally, it has built-in capabilities to define roles for using the audit trails. One can configure certain users for read-only access, prevent access of other users or offer full access for authorized personnel. It can also monitor object access events in order to determine which files are accessed and by whom.	F,R
EventsManager	Report on Requirement 10.6	EventsManager can automatically generate daily reports and save them or email them to the administrators for review in compliance with requirement 10.6	R
EventsManager	11.1 require periodic assessment of security controls to assure the ability to adequately identify and stop unauthorized access attempts.	EventsManager offers security monitoring features enabling it to alert and report on security configuration changes and unauthorized access.	F,R
EndPointSecurity	11.1. b requires that a tool is used to determine all wireless/removable devices which have been used to connect to the computer systems.	EndPointSecurity is able to both detect the devices currently connected, and the ones connected in the past, and control access to them on a "per user"/"per device type"/"per connectivity protocol" basis.	F
LANguard	11.2 implies periodic use of a vulnerability scanner.	LANguard is a full-fledged OVAL and CVE vulnerability scanning and patch management solution that can be used to comply with this requirement.	F
EventsManager	11.4 implies the use of IPS/IDS systems.	EventsManager is a log monitoring and management solution tool able to monitor the logs. It can detect security breaches at host level after they have occurred (based on logs) and hence can act as a host-based intrusion detection system	F
EventsManager	11.5 implies file integrity monitoring	EventsManager can achieve this task by monitoring object access events on files and folders	F,R
LANguard	12.1.2 implies an annual risk assessment process	LANguard is a fully fledged OVAL and CVE vulnerability scanning and patch management solution, also offering other risk assessment features such as Trojan port detection, and hence can be used to comply with this requirement.	F,R
EndPointSecurity	12.3 implies the use of technology to develop policies and control endpoint (employee-facing technologies) in order to prevent data leakage	EndPointSecurity offers functionality to detect and control access to all types of removable devices, including wireless devices, which the employees might use to extract cardholder information from the company systems. EndPointSecurity also offers extensive reporting on the usage history of such devices including technical details, user information and data transferred.	F,R

*F = FEATURE

*R = REPORT

CHART C – PCI DSS REQUIREMENTS – GFI PRODUCT REPORTS

SUB-REQUIREMENT	GFI PRODUCT REPORT LINK	WHAT REPORT PROVIDES
REQUIREMENT 1: Install and maintain a firewall configuration to protect cardholder data		
1.2: Examine firewall and router configurations to verify that inbound and outbound traffic is limited to only protocols that are necessary for the cardholder data environment	Open Ports Report	Open Ports Report. The report will list all the open ports on the target machines or devices. The product uses multiple advanced techniques for identifying the open ports and the protocols using them. It is also able to identify over 700 Trojan ports, and give information about the malware using them
1.3.9: Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet	Installed Applications by Host Report	Installed Applications by Host Report. This report can be customized to show all hosts having the personal firewall application installed.
1.3.9: Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet	Application Inventory Report	Application Inventory Report. This report can be customized to show all hosts having the personal firewall software installed
REQUIREMENT 2: Do not use vendor-supplied defaults for system passwords and other security parameters		
2.1 Always change vendor-supplied defaults before installing a system on the network	Statistical vulnerability distribution by host Report	ANY Vulnerability related Report customized to show only Low Security Vulnerabilities
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)	System Information Report	System Information Report. This report lists detailed technical information for each host machine, including services, installed applications, policies and devices.
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)	Services Report	Services Report. This report lists service information for each host machine, including description, status, startup type and account name.
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)	Open Ports Report	Open Ports Report. This report lists open ports for each host machine, including port number and name.
2.2.3 Configure system security parameters to prevent misuse Note: the report only covers Audit policy and password policy	Audit Policy Report	Audit Policy Report. This report also lists the audit policy AND PASSWORD POLICY for all the computers in the network. This information is used to determine if there are any computers where password policies are not set to change passwords every 90 days.
REQUIREMENT 3: Malicious individuals (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information		
3.4 Render PAN, at minimum, unreadable anywhere it is stored	Application Inventory Report	Application Inventory Report This report can be customized to show the hosts that have encryption software installed. It can also be customized to show the hosts not having the encryption software installed. One needs to know the name of the encryption software to apply the custom filters.
REQUIREMENT 5: Use and regularly update anti-virus software or programs		
Malicious software, commonly referred to as "malware" – including viruses, worms, and Trojans-enters the network during many business approved activities including employees' e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.		
5.2 Ensure that all anti-virus mechanisms are current, actively running and capable of generating logs. (5.1 covered also)	Anti Virus Applications Report	Anti Virus Applications Report. This report shows all the antivirus applications installed throughout the network, including their up-to-date-state, grouped by host.

5.2 Ensure that all anti-virus mechanisms are current, actively running and capable of generating logs. (5.1 covered also)	Application Inventory Report	Application Inventory Report. This report can be customized to show the hosts that have antivirus installed. It can also be customized to show the hosts not having the antivirus software installed. One needs to know the antivirus software name to apply the custom filters.
REQUIREMENT 6: Develop and maintain secure systems and applications		
<p>Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software. (NOTE: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques).</p>		
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	Missing Patches Grouped by Host Report	Missing Patches Grouped by Host Report. This report lists missing patches grouped by host machine, including URL links providing further information on each missing patch.
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	Missing Patches Grouped by Severity Report	Missing Patches Grouped by Severity Report. This report lists missing patches grouped by severity, including the host machine names for each missing patch.
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	Installed Patches Grouped by Host Report	Installed Patches Grouped by Host Report. This report lists installed patches grouped by host machine, including URL links providing further information on each installed patch.
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	Installed Patches Grouped by Severity Report	Installed Patches Grouped by Severity Report. This report lists installed patches grouped by severity, including the host machine names for each installed patch.
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	Remediation History by Date Report	Remediation History by Date Report. This report displays remediation information grouped by date and time.
6.2 Establish a process to identify newly discovered security vulnerabilities	Remediation History by Date Report	Remediation History by Date Report. This report displays remediation information grouped by date and time.
6.2 Establish a process to identify newly discovered security vulnerabilities	Network Vulnerability Summary Report	Network Vulnerability Summary Report. This report is an executive summary showing vulnerability counts for different categories. The report also identifies the top most vulnerable host machines and products, as well as the most common vulnerabilities detected on the network.
6.2 Establish a process to identify newly discovered security vulnerabilities	Network Vulnerability Trend Report	Network Vulnerability Trend Report. This report graphically illustrates how the number of vulnerabilities on the network has changed over a given time span.
6.2 Establish a process to identify newly discovered security vulnerabilities	Vulnerability Distribution by Host Report	Vulnerability Distribution by Host Report. This report is a statistical summary showing vulnerability counts for each host machine. Statistics are categorized by severity level and vulnerability category.
6.2 Establish a process to identify newly discovered security vulnerabilities	Vulnerability Listing by Category Report	Vulnerability Listing by Category Report. This report lists detected vulnerabilities grouped by category, and the host machines affected by each vulnerability.
6.2 Establish a process to identify newly discovered security vulnerabilities	Vulnerability Listing by Host Report	Vulnerability Listing by Host Report. This report lists the vulnerabilities detected for each host machine on the network.
6.2 Establish a process to identify newly discovered security vulnerabilities	Vulnerability Listing by Severity Report	Vulnerability Listing by Severity Report. This report lists detected vulnerabilities grouped by severity, and the host machines affected by each vulnerability.
6.2 Establish a process to identify newly discovered security vulnerabilities	Open Trojan Ports by Host Report	Open Trojan Ports by Host Report. This report lists open ports, grouped by host machine, which could potentially serve as a backdoor for Trojans.
6.2 Establish a process to identify newly discovered security vulnerabilities	Vulnerable Hosts Based on Vulnerability Level Report	Vulnerable Hosts Based on Vulnerability Level Report. This report lists the most vulnerable host machines for each network security scan, based on vulnerability level.
6.2 Establish a process to identify newly discovered security vulnerabilities	Vulnerable Hosts Based on Open Ports Report	Vulnerable Hosts Based on Open Ports Report. This report lists the most vulnerable host machines, based on the number of open Trojan ports found.
6.2 Establish a process to identify newly discovered security vulnerabilities	Network Patching Status Report	Network Patching Status Report. This report illustrates the status of patches and service packs for host machines on the network.

6.2 Establish a process to identify newly discovered security vulnerabilities	Missing Patches Grouped by Host Report	Missing Patches Grouped by Host Report. This report lists missing patches grouped by host machine, including URL links providing further information on each missing patch.
---	--	--

REQUIREMENT 7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. ("Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access	User Account Management Report	User account management Report. The report will help you achieve the following goals: Find irregular or unusual network account activities, identify administrators who abuse privileges to create or modify accounts and detect patterns of account activities that breach organizational security policies.
7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access	Security group management Report	Security group management Report. Placement of users into security groups, particularly users who have high privileges such as Domain, Schema, or Enterprise Admins, should occur within policy guidelines only, and should make use of established and approved accounts or processes.
7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access	User right assignment policy changes Report	User right assignment policy changes Report. The report will list any change in the user rights assignment policy, with information on who assigned the right, what right was it and to whom was the right assigned.
7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access	System access granted/removed Report	System access granted/removed Report. The report will list for each computer, the users that have been granted system access.
7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access	Failed attempts to access files and registry Report	Failed Attempts to access files and registry Report. The report will list all the failed attempts to access files and registry based on the object access events.
7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access	Successful Attempts to access files and registry Report	Successful Attempts to access files and registry Report. The report will list all the successful attempts to access files and registry based on the object access events.

REQUIREMENT 8: Assign a unique ID to each person with computer access

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

8.5.1 Control addition, deletion, or modification of user IDs, credentials, & other identifier objects	User Account Management Report	User account management Report. The report will help you achieve the following goals: Find irregular or unusual network account activities, identify administrators who abuse privileges to create or modify accounts and detect patterns of account activities that breach organizational security policies.
8.5.1 Control addition, deletion, or modification of user IDs, credentials, & other identifier objects	Security group management Report	Security group management Report. Placement of users into security groups, particularly users who have high privileges such as Domain, Schema, or Enterprise Admins, should occur within policy guidelines only, and should make use of established and approved accounts or processes.
8.5.1 Control addition, deletion, or modification of user IDs, credentials, & other identifier objects	User right assignment policy changes Report	User right assignment policy changes Report. The report will list any change in the user rights assignment policy, with information on who assigned the right, what right was it and to whom was the right assigned.
8.5.1 Control addition, deletion, or modification of user IDs, credentials, & other identifier objects	System access granted/removed Report	System access granted/removed Report. The report will list for each computer, the users that have been granted system access.
8.5.1 Control addition, deletion, or modification of user IDs, credentials, & other identifier objects	Password changes Report	Password changes Report. Password resets should occur within an approved framework only. Properly configured security audit levels should record password resets in the security event logs and identify those resets that do not follow the correct procedures. The report may contain the following sections: "Change password attempts", "User account password set or reset" and "Changes to directory service restore mode passwords".
8.5.5 Remove inactive user accounts at least every 90 days	Groups and Users Report	Groups and Users Report. Shows a list of all the user accounts on all the network computers. For each user, it displays the last logon date which is used to determine if the user was inactive for more than 90 days.

8.5.9 Change user passwords at least every 90 days	Groups and Users Report	Groups and Users Report. Shows a list of all the user accounts on all the network computers. For each user account, the report shows the age of the corresponding password which is used to determine if there are any accounts with passwords older than a certain period.
8.5.9 Change user passwords at least every 90 days	Audit Policy Report	Audit Policy Report. This report also lists the PASSWORD POLICY also for all the computers in the network. This information is used to determine if there are any computers where password policies are not set to change passwords every 90 days.
<p>REQUIREMENT 10: Track and monitor all access to network resources and cardholder data.</p> <p>Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.</p>		
10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.1 All individual accesses to cardholder data - requires path to the data repository to be audited on the computer holding data	All individual access to cardholder data Report	10.2.1 All individual access to cardholder data - when data is stored in files Report The report displays the data relevant to the corresponding requirement.
10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.2 All actions taken by any individual with root or administrative privileges	All actions taken by any individual with root or administrative privileges Report	10.2.2 All actions taken by any individual with root or administrative privileges Report The report displays the data relevant to the corresponding requirement.
10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.3 Access to all audit trails	Access to all Audit Trails Report	10.2.3 Access to all audit trails Report The report displays the data relevant to the corresponding requirement.
10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.4 Invalid logical access attempts	Invalid logical access attempts Report	10.2.4 Invalid logical access attempts Report The report displays the data relevant to the corresponding requirement.
10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.5 Use of identification and authentication mechanisms	Use of identification and authentication mechanisms Report	10.2.5 Use of identification and authentication mechanisms Report. The report displays the data relevant to the corresponding requirement.
10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.6 Initialization of the audit logs	Initialization of the audit logs Report	10.2.6 Initialization of the audit logs Report. The report displays the data relevant to the corresponding requirement.
10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.7 Creation and deletion of system-level objects	Creation and deletion of system-level objects Report	10.2.7 Creation and deletion of system-level objects Report The report displays the data relevant to the corresponding requirement.
10.4 Synchronize all critical system clocks and times	Time synchronization monitoring Report	10.4 Time synchronization monitoring Report. The report will display events generated by the Windows Time service, responsible with time synchronization in Windows environments. Use this report to: a) monitor system time changes and b) monitor the time synchronization process.
10.5.1 Limit viewing of audit trails to those with a job-related need	Esmaudit.csv	Esmaudit.csv The report is generated in the Debug folder of the application if EventsManager auditing is configured properly. This log contains all the activity that users have performed using the EventsManager application.
10.5.2 Protect audit trail files from unauthorized modifications	Esmaudit.csv	Esmaudit.csv The report is generated in the Debug folder of the application if EventsManager auditing is configured properly. This log contains all the activity that users have performed using the EventsManager application.
10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed (except for new data) without generating alerts	Failed Attempts to access files and registry Report	Failed Attempts to access files and registry Report The report will list all the failed attempts to access files and registry based on the object access events.

10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed (except for new data) without generating alerts	Successful Attempts to access files and registry Report	Successful Attempts to access files and registry Report. The report will list all the successful attempts to access files and registry based on the object access events.
10.6 Review logs for all system components at least daily	Generic event trend per hours	Generic event trend per hours. The report is used to display statistical information about the trend of the collected events. First it shows a section with the top 10 computers with the most events, then the top 10 users generating the most events. The events trend chart is being divided per hours and the trend of events for each computer is also shown individually. The report can be used to determine time intervals where an unusually high number of events were generated.
10.6 Review logs for all system components at least daily	Generic event trend per days	Generic event trend per days. The report is used to display statistical information about the trend of the collected events. First it shows a section with the top 10 computers with the most events, then the top 10 users generating the most events. The events trend chart is being divided per days and the trend of events for each computer is also shown individually. The report can be used to determine time intervals where an unusually high number of events were generated.

REQUIREMENT 11: Regularly test security systems and processes.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and customer software should be tested frequently to ensure security controls continue to reflect a changing environment.

11.1.b Verify that a wireless analyzer is used at least quarterly to identify all wireless devices	All devices used - grouped by device Report	All devices used - grouped by device Report. This report shows a list of devices detected by GFI EndPointSecurity agents across the network together with a list of users that have in some way made use of each device.
11.1.b Verify that a wireless analyzer is used at least quarterly to identify all wireless devices	All devices used - grouped by user Report	All devices used - grouped by user Report This report shows a list of users monitored by GFI EndPointSecurity agents across the network together with a list of devices that each user has used.
11.1.b Verify that a wireless analyzer is used at least quarterly to identify all wireless devices	Device access statistics Report	Device access statistics Report. This report shows the number of allowed and denied access requests made by each user for each device, grouped by file system and non file system devices. Each row shows Read-Only and Read-Write (full) access requests that were allowed or denied.
11.1.b Verify that a wireless analyzer is used at least quarterly to identify all wireless devices	Device usage statistics per user Report	Device usage statistics per user Report. This report shows a list of external devices connected by each user together with the number of allowed and denied access requests for each device.
11.2 Run internal vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)	Remediation History by Date Report	Remediation History by Date Report. This report displays remediation information grouped by date and time.
11.2 Run internal vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)	Network Vulnerability Summary Report	Network Vulnerability Summary Report. This report is an executive summary showing vulnerability counts for different categories. The report also identifies the top most vulnerable host machines and products, as well as the most common vulnerabilities detected on the network.
11.2 Run internal vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)	Network Vulnerability Trend Report	Network Vulnerability Trend Report. This report graphically illustrates how the number of vulnerabilities on the network has changed over a given time span.
11.2 Run internal vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)	Security Scans History Report	Network Vulnerability Trend Report. This report graphically illustrates how the number of vulnerabilities on the network has changed over a given time span.
11.2 Run internal vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)	Vulnerability Distribution by Host Report	Vulnerability Distribution by Host Report. This report is a statistical summary showing vulnerability counts for each host machine. Statistics are categorized by severity level and vulnerability category.

11.2 Run internal vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)	Vulnerability Listing by Category Report	Vulnerability Listing by Category Report. This report lists detected vulnerabilities grouped by category, and the host machines affected by each vulnerability.
11.2 Run internal and external network vulnerability scans at least quarterly	Vulnerability Listing by Host Report	Vulnerability Listing by Host Report. This report lists the vulnerabilities detected for each host machine on the network.
11.2 Run internal vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)	Vulnerability Listing by Severity Report	Vulnerability Listing by Severity Report. This report lists detected vulnerabilities grouped by severity, and the host machines affected by each vulnerability.
11.2 Run internal vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)	Open Trojan Ports by Host Report	Open Trojan Ports by Host Report. This report lists open ports, grouped by host machine, which could potentially serve as a backdoor for trojans.
11.2 Run internal vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)	Vulnerable Hosts Based on Vulnerability Level Report	Vulnerable Hosts Based on Vulnerability Level Report. This report lists the most vulnerable host machines for each network security scan, based on vulnerability level.
11.2 Run internal vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)	Vulnerable Hosts Based on Open Ports Report	Vulnerable Hosts Based on Open Ports Report. This report lists the most vulnerable host machines, based on the number of open Trojan ports found.
11.2 Run internal vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)	Network Patching Status Report	Network Patching Status Report. This report illustrates the status of patches and service packs for host machines on the network.
11.2 Run internal vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)	Missing Patches Grouped by Host Report	Missing Patches Grouped by Host Report. This report lists missing patches grouped by host machine, including URL links providing further information on each missing patch.
11.2 Run internal vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)	Remediation History by Host	Remediation History by Host This report displays remediation information grouped by host machine, including remediation details such as date and status.
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises	Account Lockouts Report	Account Lockouts Report . This report lists all locked out accounts, including those which can indicate a brute force attack
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises	Account Logons Report	Account Logons Report. This report shows all successful logons grouped by users, allowing you to quickly see which computers a user has logged on to.
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises	Failed Logon Count on Each Computer	Failed Logon Count on Each Computer. This report lists the failed logins on each computer, as well as the type of failure.
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises	Failed Logons	Failed Logons. This report lists logon failures per computer, and shows the reason for the failures
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises	Logoff Report	Logoff Report. This report lists all logoff events including the logon type

11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises	Successful Logon Count on Each Computer	Successful Logon Count on Each Computer. This report shows logons by computer and allows you to quickly view the most accessed computers
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises	Successful Logons Grouped by Computers	Successful Logons Grouped By Computers Report. This report lists all successful logons and shows logon type
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises	Successful Logons Grouped by Users	Successful logons Grouped by Users report This report displays all successful logons to see all machines a user has logged on to.
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises	Failed Attempts to access files and registry Report	Failed Attempts to access files and registry Report. The report will list all the failed attempts to access files and registry based on the object access events.
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises	Successful Attempts to access files and registry Report	Successful Attempts to access files and registry Report. The report will list all the successful attempts to access files and registry based on the object access events.
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises	Object Deleted with details Report	Object Deleted with details Report. The report will show all deleted files, registry keys, etc.
11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files	Failed Attempts to access files and registry Report	Failed Attempts to access files and registry Report. The report will list all the failed attempts to access files and registry based on the object access events.
11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files	Successful Attempts to access files and registry Report	Successful Attempts to access files and registry Report. The report will list all the successful attempts to access files and registry based on the object access events.

REQUIREMENT 12: Maintain a policy that addresses information security for employees and contractors.

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of this requirement, "employees" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the company's site.

12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	Network Vulnerability Summary Report	Network Vulnerability Summary Report. This report is an executive summary showing vulnerability counts for different categories. The report also identifies the top most vulnerable host machines and products, as well as the most common vulnerabilities detected on the network.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	Network Vulnerability Trend Report	Network Vulnerability Trend Report. This report graphically illustrates how the number of vulnerabilities on the network has changed over a given time span.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	Vulnerability Distribution by Host Report	Vulnerability Distribution by Host Report. This report is a statistical summary showing vulnerability counts for each host machine. Statistics are categorized by severity level and vulnerability category.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	Vulnerability Listing by Category Report	Vulnerability Listing by Category Report. This report lists detected vulnerabilities grouped by category, and the host machines affected by each vulnerability.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	Vulnerability Listing by Host Report	Vulnerability Listing by Host Report. This report lists the vulnerabilities detected for each host machine on the network.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	Vulnerability Listing by Severity Report	Vulnerability Listing by Severity Report. This report lists detected vulnerabilities grouped by severity, and the host machines affected by each vulnerability.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	Open Trojan Ports by Host Report	Open Trojan Ports by Host Report. This report lists open ports, grouped by host machine, which could potentially serve as a backdoor for trojans.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	Vulnerable Hosts Based on Vulnerability Level Report	Vulnerable Hosts Based on Vulnerability Level Report. This report lists the most vulnerable host machines for each network security scan, based on vulnerability level.

12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	Vulnerable Hosts Based on Open Ports Report	Vulnerable Hosts Based on Open Ports Report. This report lists the most vulnerable host machines, based on the number of open trojan ports found.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	Network Patching Status Report	Network Patching Status Report. This report illustrates the status of patches and service packs for host machines on the network.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	Missing Patches Grouped by Host Report	Missing Patches Grouped by Host Report. This report lists missing patches grouped by host machine, including URL links providing further information on each missing patch.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	Remediation History by Host	Remediation History by Host. This report displays remediation information grouped by host machine, including remediation details such as date and status.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	Baseline Changes Comparison Report	Baseline Changes Comparison Report. This report compares results between a chosen computer, used as benchmark, and host machines scanned with the same profile.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	Network Security Log by Date Report	Network Security Log by Date Report. This report compares results of consecutive scans that have a common profile and target, grouped by scan date.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	Network Security Log by Host Report	Network Security Log by Host Report. This report compares results of consecutive scans that have a common profile and target, grouped by host machine.
12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors	Device usage summary Report	Device usage summary Report. The charts in this report display percentages of allowed versus denied access for different devices across all monitored computers on the network. It also lists the top 10 users with Allowed or Denied access.
12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors	Device access trends Report	Device access trends Report. This is a trend report showing the change in device access attempts over time. The graphs plot both the allowed and denied access counts per day.
12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors	Top active users /computers Reports	Top active users /computers Reports. These reports show lists of monitored users /machines who /that have the highest amount of device activity
12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors	Users who accessed devices on more than one machine Report	Users who accessed devices on more than one machine Report. This report displays the users who were accessing devices on more than one machine.
12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors	Machines which had more than one user accessing devices Report	Machines which had more than one user accessing devices Report. This report displays the machines which had more than one user accessing the devices.
12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors	Connected devices outside working hours Report	Connected devices outside working hours Report. This report show the devices which were connected outside the working hours.
12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors	All devices used - grouped by device Report	All devices used - grouped by device Report. This report shows a list of devices detected by GFI EndPointSecurity agents across the network together with a list of users that have in some way made use of each device.
12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors	All devices used - grouped by user Report	All devices used - grouped by user Report. This report shows a list of users monitored by GFI EndPointSecurity agents across the network together with a list of devices that each user has used.
12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors	Device access statistics Report	Device access statistics Report. This report shows the number of allowed and denied access requests made by each user for each device, grouped by file system and non file system devices. Each row shows Read-Only and Read-Write (full) access requests that were allowed or denied.
12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors	Device usage statistics per user Report	Device usage statistics per user Report. This report shows a list of external devices connected by each user together with the number of allowed and denied access requests for each device.

CHART D – SUMMARY OF ALL PCI DSS REQUIREMENTS

	EventsManager Support Level**	LANguard Support Level**	EndPoint Security Support Level**	Milestone*	Comments
Requirement 1: Install and maintain a firewall configuration to protect cardholder data					
1.1 Establish firewall and router configuration standards that include the following:				6	
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.				6	Process/Policy driven requirement - outside scope of software solution
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks.				1	Outside scope of GFI products
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.				2	Outside scope of GFI products
1.1.4 Description of groups, roles, and responsibilities for logical management of network components.				6	Process/Policy driven requirement - outside scope of software solution
1.1.5 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.				2	Process/Policy driven requirement - outside scope of software solution
1.1.6 Requirement to review firewall and router rule sets at least every six months.				6	Outside Scope of GFI products
1.2 Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.	B,D	B,D		2	
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.				2	Outside scope of GFI products
1.2.2 Secure and synchronize router configuration files.				2	Outside scope of GFI products
1.2.3 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.				2	Outside scope of GFI products
1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include:	B,D	B,D		2	
1.3.1 Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.				2	Outside scope of GFI products
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.				2	Outside scope of GFI products
1.3.3 Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.				2	Outside scope of GFI products

See Footnotes

CHART D – SUMMARY OF ALL PCI DSS REQUIREMENTS

	EventsManager Support Level**	LANguard Support Level**	EndPoint Security Support Level**	Milestone*	Comments
1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.				2	Outside scope of GFI products
1.3.5 Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.				2	Outside scope of GFI products
1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)				2	Outside scope of GFI products
1.3.7 Place the database in an internal network zone, segregated from the DMZ.				2	Outside scope of GFI products
1.3.8 Impalement IP masquerading to prevent the internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies - for example, port address translation (PAT).				2	Outside scope of GFI products
1.3.9 Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet		A,B,C,D		2	
1.4 Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).				2	
Requirement 2: Do not use vendor-supplied default passwords					
2.1 Always change vendor-supplied defaults before installing a system on the network		B,C,D		2	
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.				2	Outside scope of GFI products
2.2 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.				3	Process/Policy driven requirement - outside scope of software solution
2.2.1 Implement only one primary function per server.				3	Outside scope of GFI products
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)		B, D		3	
2.2.3 Configure system security parameters to prevent misuse		B, D		3	

See Footnotes

CHART D – SUMMARY OF ALL PCI DSS REQUIREMENTS

	EventsManager Support Level**	LANguard Support Level**	EndPoint Security Support Level**	Milestone*	Comments
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.				3	Outside scope of GFI products
2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SLL/TLS for web-based management and other non-console administrative access.				2	Outside scope of GFI products
2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in <i>Appendix A: Additional PCI DDS Requirements for Shared Hosting Providers</i> .				3	Process/Policy driven requirement - outside scope of software solution
Requirement 3: Protect stored cardholder data					
3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal and/or regulatory purposes, as documented in the data retention policy.				1	Process/Policy driven requirement - outside scope of software solution
3.2 Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:				1	Outside scope of GFI products
3.2.1 Do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively calls full track, track, track 1, track 2, and magnetic-stripe data.				1	
3.2.2 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.				1	Process/Policy driven requirement - outside scope of software solution
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.				1	Process/Policy driven requirement - outside scope of software solution
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed)				5	Process/Policy driven requirement - outside scope of software solution
3.4 Render PAN, at minimum, unreadable anywhere it is stored		B,C,D		5	

See Footnotes

CHART D – SUMMARY OF ALL PCI DSS REQUIREMENTS

	EventsManager Support Level**	LANguard Support Level**	EndPoint Security Support Level**	Milestone*	Comments
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.				5	Outside scope of GFI products
3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse:				5	Process/Policy driven requirement - outside scope of software solution
3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.				5	Process/Policy driven requirement - outside scope of software solution
3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.				5	Process/Policy driven requirement - outside scope of software solution
3.6 Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:				5	Process/Policy driven requirement - outside scope of software solution
3.6.1 Generation of strong cryptographic keys.				5	Process/Policy driven requirement - outside scope of software solution
3.6.2 Secure cryptographic key distribution.				5	Process/Policy driven requirement - outside scope of software solution
3.6.3 Secure cryptographic key storage.				5	Process/Policy driven requirement - outside scope of software solution
3.6.4 Periodic cryptographic key changes - As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically - At least annually				5	Process/Policy driven requirement - outside scope of software solution
3.6.5 Retirement or replacement of old or suspected compromise cryptographic keys				5	Process/Policy driven requirement - outside scope of software solution
3.6.6 Split knowledge and establishment of dual control of cryptographic keys				5	Process/Policy driven requirement - outside scope of software solution
3.6.7 Prevention of unauthorized substitution of cryptographic keys				5	Process/Policy driven requirement - outside scope of software solution

See Footnotes

CHART D – SUMMARY OF ALL PCI DSS REQUIREMENTS

	EventsManager Support Level**	LANguard Support Level**	EndPoint Security Support Level**	Milestone*	Comments
3.6.8 Requirement for cryptographic key custodians to sign a form stating that they understand and accept their key-custodian responsibilities				5	Process/Policy driven requirement - outside scope of software solution
Requirement 4: Encrypt transmission of cardholder data across open, public networks					
4.1 Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks				2	Outside scope of GFI products
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission. - For new wireless implementations, it is prohibited to implement WEP after March 31, 2009. - For current wireless implementations, it is prohibited to use WEP after June 20, 2010.				2	Outside scope of GFI products
4.2 Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, and chat).				2	Outside scope of GFI products
Requirement 5: Use and regularly update anti-virus software or programs					
5.1 Deploy anti-virus software on all systems commonly affected by viruses		A		2	
5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software				2	Outside scope of GFI products
5.2 Ensure that all anti-virus mechanisms are current, actively running and capable of generating logs	B, D	A, C, D		2	
Requirement 6: Develop and maintain secure systems and applications					
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release		A, C, D		3	
6.2 Establish a process to identify newly discovered security vulnerabilities		A, C, D		3	
6.3 Develop software applications in accordance with PCI DDS (for example, secure authentication and logging) and based on industry best practices and incorporate information security throughout the software development life cycle. These processes must include the following:				3	Process/Policy driven requirement - outside scope of software solution
6.3.1 Testing of all security patches, and system and software configuration changes before deployment, including but not limited to the following:				3	Process/Policy driven requirement - outside scope of software solution
6.3.1.1 Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)				3	Process/Policy driven requirement - outside scope of software solution

See Footnotes

CHART D – SUMMARY OF ALL PCI DSS REQUIREMENTS

	EventsManager Support Level**	LANguard Support Level**	EndPoint Security Support Level**	Milestone*	Comments
6.3.1.2 Validation of proper error handling				3	Process/Policy driven requirement - outside scope of software solution
6.3.1.3 Validation of secure cryptographic storage				3	Process/Policy driven requirement - outside scope of software solution
6.3.1.4 Validation of secure communications				3	Process/Policy driven requirement - outside scope of software solution
6.3.1.5 Validation of proper role-based access control (RBAC)				3	Process/Policy driven requirement - outside scope of software solution
6.3.2 Separate development/test, and production environments				3	Process/Policy driven requirement - outside scope of software solution
6.3.3 Separation of duties between development/test, and production environments.				3	Process/Policy driven requirement - outside scope of software solution
6.3.4 Production data (live PANs) are not used for testing or development.				3	Process/Policy driven requirement - outside scope of software solution
6.3.5 Removal of test data and accounts before production systems become active.				3	Process/Policy driven requirement - outside scope of software solution
6.3.6 Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers.				3	Process/Policy driven requirement - outside scope of software solution
6.3.7 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.				3	Process/Policy driven requirement - outside scope of software solution
6.4 Follow change control procedures for all changes to system components. The procedures must include the following:				6	Process/Policy driven requirement - outside scope of software solution
6.4.1 Documentation of impact				6	Process/Policy driven requirement - outside scope of software solution
6.4.2 Management sign-off by appropriate parties				6	Process/Policy driven requirement - outside scope of software solution
6.4.3 Testing of operational functionality				6	Process/Policy driven requirement - outside scope of software solution

See Footnotes

CHART D – SUMMARY OF ALL PCI DSS REQUIREMENTS

	EventsManager Support Level**	LANguard Support Level**	EndPoint Security Support Level**	Milestone*	Comments
6.4.4 Back-out procedures				6	Process/Policy driven requirement - outside scope of software solution
6.5 Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in software development processes, to include the following:				3	Process/Policy driven requirement - outside scope of software solution
6.5.1 Cross-site scripting (XSS)				3	Process/Policy driven requirement - outside scope of software solution
6.5.2 Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.				3	Process/Policy driven requirement - outside scope of software solution
6.5.3 Malicious file execution				3	Process/Policy driven requirement - outside scope of software solution
6.5.4 Insecure direct object references				3	Process/Policy driven requirement - outside scope of software solution
6.5.5 Cross-site request forgery (CSRF)				3	Process/Policy driven requirement - outside scope of software solution
6.5.6 Information leakage and improper error handling				3	Process/Policy driven requirement - outside scope of software solution
6.5.7 Broken authentication and session management.				3	Process/Policy driven requirement - outside scope of software solution
6.5.8 Insecure cryptographic storage				3	Process/Policy driven requirement - outside scope of software solution
6.5.9 Insecure communications				3	Process/Policy driven requirement - outside scope of software solution
6.5.10 Failure to restrict URL access				3	Process/Policy driven requirement - outside scope of software solution

See Footnotes

CHART D – SUMMARY OF ALL PCI DSS REQUIREMENTS

	EventsManager Support Level**	LANguard Support Level**	EndPoint Security Support Level**	Milestone*	Comments
<p>6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by <i>either</i> of the following methods:</p> <ul style="list-style-type: none"> - Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes. - Installing a web-application firewall in front of public-facing web applications. 				3	Process/Policy driven requirement - outside scope of software solution
Requirement 7: Restrict access to cardholder data by business need-to-know					
<p>7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access</p>	B, D			4	
<p>7.1.1 Restrictions of access rights to privileged user IDs to least privileges necessary to perform job responsibilities.</p>				4	Process/Policy driven requirement - outside scope of software solution
<p>7.1.2 Assignment of privileges is based on individual personnel's job classification and function.</p>				4	Process/Policy driven requirement - outside scope of software solution
<p>7.1.3 Requirement for an authorization form signed by management that specifies required privileges.</p>				4	Process/Policy driven requirement - outside scope of software solution
<p>7.1.4 Implementation of an automated access control system.</p>				4	Outside scope of GFI products
<p>7.2 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 following:</p>				4	Outside scope of GFI products
<p>7.2.1 Coverage of all system components</p>				4	Process/Policy driven requirement - outside scope of software solution
<p>7.2.2 Assignment of privileges to individuals based on job classification and function.</p>				4	Process/Policy driven requirement - outside scope of software solution
<p>7.2.3 Default "deny-all" setting.</p>				4	Process/Policy driven requirement - outside scope of software solution
Requirement 8: Assign a unique ID to each person with computer access					
<p>8.1 Assign all users a unique username before allowing them to access system components or cardholder data.</p>				4	Process/Policy driven requirement - outside scope of software solution

See Footnotes

CHART D – SUMMARY OF ALL PCI DSS REQUIREMENTS

	EventsManager Support Level**	LANguard Support Level**	EndPoint Security Support Level**	Milestone*	Comments
8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: - Password or passphrase - Two-factor authentication (e.g., token devices, smart cards, biometrics, or public keys)				4	Outside scope of GFI products
8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certifications.				4	Outside scope of GFI products
8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography based on approved standards (defined in <i>PCI DSS Glossary, Abbreviations, and Acronyms</i>)				4	Outside scope of GFI products
8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:				4	
8.5.1 Control addition, deletion, or modification of user IDs, credentials, & other identifier objects	D			4	Outside scope of GFI products
8.5.2 Verify users identify before performing password resets.				4	Process/Policy driven requirement - outside scope of software solution
8.5.3 Set first-time passwords to a unique value for each user & change immediately after first use		B,D		4	Outside scope of GFI products
8.5.4 Immediately revoke access for any terminated users	D	B,D		4	Process/Policy driven requirement - outside scope of software solution
8.5.5 Remove inactive user accounts at least every 90 days	B,D	B,D		4	
8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed	B,D	B,D		4	
8.5.7 Communicate password procedures and policies to all users who have access to cardholder data.				4	Process/Policy driven requirement - outside scope of software solution
8.5.8 Do not use group, shared, or generic accounts and passwords.				4	Process/Policy driven requirement - outside scope of software solution

See Footnotes

CHART D – SUMMARY OF ALL PCI DSS REQUIREMENTS

	EventsManager Support Level**	LANguard Support Level**	EndPoint Security Support Level**	Milestone*	Comments
8.5.9 Change user passwords at least every 90 days	D	B, D		4	
8.5.10 Require a minimum password length of at least seven characters		B, D		4	
8.5.11 Use passwords containing both numeric and alphabetic characters.				4	Outside scope of GFI products
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.				4	Outside scope of GFI products
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts				4	
8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.				4	Outside scope of GFI products
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.				4	Outside scope of GFI products
8.5.16 Authenticate all access to any database containing cardholder data	B, D			4	
Requirement 9: Restrict physical access to cardholder data.					
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.				5	Outside scope of GFI products
9.1.1 Use video cameras or other access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.				5	Process/Policy driven requirement - outside scope of software solution
9.1.2 Restrict physical access to publicly accessible network jacks.				5	Process/Policy driven requirement - outside scope of software solution
9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices.				5	Process/Policy driven requirement - outside scope of software solution
9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible.				5	Process/Policy driven requirement - outside scope of software solution
9.3 Make sure all visitors are handled as follows:				5	Process/Policy driven requirement - outside scope of software solution
9.3.1 Authorized before entering areas where cardholder data is processed or maintained. Authorized before entering areas where cardholder data is processed or maintained.				5	Process/Policy driven requirement - outside scope of software solution
9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees.				5	Process/Policy driven requirement - outside scope of software solution

See Footnotes

CHART D – SUMMARY OF ALL PCI DSS REQUIREMENTS

	EventsManager Support Level**	LANguard Support Level**	EndPoint Security Support Level**	Milestone*	Comments
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.				5	Process/Policy driven requirement - outside scope of software solution
9.4 Use a visitor log to maintain a physical audit trail or visitor activity. Document the visitor's name, the firm represented, and the employee authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.				5	Process/Policy driven requirement - outside scope of software solution
9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.				5	Process/Policy driven requirement - outside scope of software solution
9.6 Physically secure all paper and electronic media that contain cardholder data.				5	Process/Policy driven requirement - outside scope of software solution
9.7 Maintain strict control over the internal and external distribution or any kind of media that contains cardholder data, including the following:				5	Process/Policy driven requirement - outside scope of software solution
9.7.1 Classify the media so it can be identified as confidential.				5	Process/Policy driven requirement - outside scope of software solution
9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked.				5	Process/Policy driven requirement - outside scope of software solution
9.8 Ensure management approves any and all media containing cardholder data that is moved from a secured area (especially when the media is distributed to individuals).				5	Process/Policy driven requirement - outside scope of software solution
9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data.				5	Process/Policy driven requirement - outside scope of software solution
9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.				5	Process/Policy driven requirement - outside scope of software solution
9.10 Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:				1	Process/Policy driven requirement - outside scope of software solution
9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.				1	Process/Policy driven requirement - outside scope of software solution
9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data				1	Process/Policy driven requirement - outside scope of software solution
Requirement 10: Track and monitor all access to network resources and cardholder data					

See Footnotes

CHART D – SUMMARY OF ALL PCI DSS REQUIREMENTS

	EventsManager Support Level**	LANguard Support Level**	EndPoint Security Support Level**	Milestone*	Comments
10.1 Log all individual user access to system components, especially administrative users	A,B,C,D			4	
10.2 Implement automated audit trails for all system components to reconstruct the following events:	A,B,C,D			4	
10.2.1 All individual accesses to cardholder data	A,B,C,D			4	
10.2.2 All actions taken by any individual with root or administrative privileges	A,B,C,D			4	
10.2.3 Access to all audit trails	A,B,C,D			4	
10.2.4 Invalid logical access attempts	A,B,C,D			4	
10.2.5 Use of identification and authentication mechanisms	A,B,C,D			4	
10.2.6 Initialization of the audit logs	A,B,C,D			4	
10.2.7 Creation and deletion of system-level objects	A,B,C,D			4	
10.3 Record at least the following audit trail entries for all system components for each event	A,B,C,D			4	
10.4 Synchronize all critical system clocks and times	B,D			4	
10.5 Synchronize all critical system clocks and times.				6	Outside scope of GFI products
10.5.1 Limit viewing of audit trails to those with a job-related need	A,B,C,D			6	
10.5.2 Protect audit trail files from unauthorized modifications	A,B,C,D			6	
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.				6	Outside scope of GFI products
10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.				6	Process/Policy driven requirement - outside scope of software solution
10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed (except for new data) without generating alerts	A,B,C,D			6	
10.6 Review logs for all system components at least daily	A,B,C,D			4	
10.7 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).				4	Process/Policy driven requirement - outside scope of software solution
Requirement 11: Regularly test security systems and processes					
11.1 Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts	B, D		A,B,C,D	6	

See Footnotes

CHART D – SUMMARY OF ALL PCI DSS REQUIREMENTS

	EventsManager Support Level**	LANguard Support Level**	EndPoint Security Support Level**	Milestone*	Comments
11.2 Run internal and external network vulnerability scans at least quarterly		A,B,C,D		2	
11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:				6	Outside scope of GFI products
11.3.1 Network-layer penetration tests.				6	Outside scope of GFI products
11.3.2 Application-layer penetration tests.				6	Outside scope of GFI products
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises	A,B,C,D			2	
11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files	A,B,C,D			4	
Requirement 12: Maintain a policy that addresses information security for employees and contractors					
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:				6	
12.1.1 Addresses all PCI DSS requirements.				1	Process/Policy driven requirement - outside scope of software solution
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment		A,B,C,D		6	
12.1.3 Includes a review at least once a year and updates when the environment changes.				6	Process/Policy driven requirement - outside scope of software solution
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).				6	Process/Policy driven requirement - outside scope of software solution
12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:			A,B,C,D	6	
12.3.1 Explicit management approval			A,B,C,D	6	
12.3.2 Authentication for use of the technology			A,B,C,D	6	
12.3.3 A list of all such devices and personnel with access			A,B,C,D	6	

See Footnotes

CHART D – SUMMARY OF ALL PCI DSS REQUIREMENTS

	EventsManager Support Level**	LANguard Support Level**	EndPoint Security Support Level**	Milestone*	Comments
12.3.5 Acceptable uses of the technology			A,B,C,D	6	
12.3.6 Acceptable network locations for the technologies			A,B,C,D	6	
12.3.7 List of company-approved products.				6	Process/Policy driven requirement - outside scope of software solution
12.3.8 Automatic disconnect of sessions for remote access technologies after a specify period of inactivity.				6	Process/Policy driven requirement - outside scope of software solution
12.3.9 Activation of remote access technologies for vendors only when needed by vendors, with immediate deactivation after use.				6	Process/Policy driven requirement - outside scope of software solution
12.3.10 When accessing cardholder data remotely via modem, prohibition of storage of cardholder data onto local hard drives, floppy disks, or other external media. Prohibition of cut-and-paste and print functions during remote access			A,B,C,D	6	
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.				6	Process/Policy driven requirement - outside scope of software solution
12.5 Assign to an individual or team the following information security management responsibilities:				6	Process/Policy driven requirement - outside scope of software solution
12.5.1 Establish, document, and distribute security policies and procedures.				6	Process/Policy driven requirement - outside scope of software solution
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.				6	Process/Policy driven requirement - outside scope of software solution
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.				6	Process/Policy driven requirement - outside scope of software solution
12.5.4 Administer user accounts, including additions, deletions, and modifications.				6	Process/Policy driven requirement - outside scope of software solution
12.5.5 Monitor and control all access to data.				6	Process/Policy driven requirement - outside scope of software solution
12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.				6	Process/Policy driven requirement - outside scope of software solution

See Footnotes

CHART D – SUMMARY OF ALL PCI DSS REQUIREMENTS

	EventsManager Support Level**	LANguard Support Level**	EndPoint Security Support Level**	Milestone*	Comments
12.6.1 Educate employees upon hire at least annually.				6	Process/Policy driven requirement - outside scope of software solution
12.6.2 Require employees to acknowledge at least annually that they have read and understood the company's security policy and procedures.				6	Process/Policy driven requirement - outside scope of software solution
12.7 Screen potential employees prior to hire to minimize the risk of attacks from internal sources.				6	Process/Policy driven requirement - outside scope of software solution
12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:				2	Process/Policy driven requirement - outside scope of software solution
12.8.1 Maintain a list of service providers.				2	Process/Policy driven requirement - outside scope of software solution
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.				2	Process/Policy driven requirement - outside scope of software solution
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.				2	Process/Policy driven requirement - outside scope of software solution
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status.				2	Process/Policy driven requirement - outside scope of software solution
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.				6	Process/Policy driven requirement - outside scope of software solution
12.9.1 Create the incident response plan to be implemented in the event of a system breach. Ensure the plan addresses the following, at a minimum: - Roles, responsibilities and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum - Specific incident response procedures - Business recovery and continuity procedures - Data back-up processes - Analysis of legal requirements for reporting compromises - Coverage and responses of all critical system components - Reference or inclusion of incident response procedures from the payment brands				6	Process/Policy driven requirement - outside scope of software solution
12.9.2 Test the plan at least annually.				6	Process/Policy driven requirement - outside scope of software solution

See Footnotes

CHART D – SUMMARY OF ALL PCI DSS REQUIREMENTS

	EventsManager Support Level**	LANguard Support Level**	EndPoint Security Support Level**	Milestone*	Comments
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.				6	Process/Policy driven requirement - outside scope of software solution
12.9.4 Provide appropriate training to staff with security breach response responsibilities.				6	Process/Policy driven requirement - outside scope of software solution
12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.				6	Process/Policy driven requirement - outside scope of software solution
12.9.6 Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.				6	Process/Policy driven requirement - outside scope of software solution
Requirement A.1: Shared hosting providers must protect the cardholder data environment					
A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4:				3	Process/Policy driven requirement - outside scope of software solution
A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.				3	Process/Policy driven requirement - outside scope of software solution
A.1.2 Restrict each entity's access and privileges to own cardholder data environment only.		A, C		3	
A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DDS Requirement 10.				3	Process/Policy driven requirement - outside scope of software solution
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.				3	Process/Policy driven requirement - outside scope of software solution

FOOT NOTES:

* Milestone - suggested order of implementation efforts to meet PCI-DSS requirements. The order is NOT mandatory but a guide based on the PCI Security Standards Council published "Prioritized Approach for PCI DSS 1.2": https://www.pcisecuritystandards.org/education/docs/Prioritized_Approach_PCI_DSS_1_2.pdf

A: the product offers functionality directly requested by particular PCI DSS requirements in order to achieve compliance

B: the product offers functionality that can aid enforcement or enforce particular PCI DSS requirements once they are in place, via monitoring, alerting and/or reporting. Particularly useful for periodic reviews and assessments

C: the product offers functionality to report on compliance status of hosts in regards with a particular PCI DSS requirement

D: the product is able to report on the data gathered as part of support levels A and B processes for a particular PCI DSS requirement

CHART E – PCI DSS REQUIREMENTS SUPPORT IN GFI PRODUCTS

Requirement 1: Install and maintain a firewall configuration to protect cardholder data			
	EventsManager Support Level**	LANguard Support Level**	EndPointSecurity Support Level**
1.2 Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.	B,D	B,D	-
1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include:	B,D	B,D	-
1.3.9 Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet	-	A,B,C,D	-
Requirement 2: Do not use vendor-supplied default passwords			
	EventsManager Support Level**	LANguard Support Level**	EndPointSecurity Support Level**
2.1 Always change vendor-supplied defaults before installing a system on the network	-	B,C,D	-
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)	-	B,D	-
2.2.3 Configure system security parameters to prevent misuse	-	B,D	-
Requirement 3: Protect stored cardholder data			
	EventsManager Support Level**	LANguard Support Level**	EndPointSecurity Support Level**
3.4 Render PAN, at minimum, unreadable anywhere it is stored	-	B,C,D	-
Requirement 5: Use and regularly update anti-virus software or programs			
	EventsManager Support Level**	LANguard Support Level**	EndPointSecurity Support Level**
5.1 Deploy anti-virus software on all systems commonly affected by viruses	-	A	-
5.2 Ensure that all anti-virus mechanisms are current, actively running and capable of generating logs	B,D	A,C,D	-

See Footnotes

CHART E – PCI DSS REQUIREMENTS SUPPORT IN GFI PRODUCTS

Requirement 6: Develop and maintain secure systems and applications			
	EventsManager Support Level**	LANguard Support Level**	EndPointSecurity Support Level**
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release	-	A,CD	-
6.2 Establish a process to identify newly discovered security vulnerabilities	-	A, C,D	-
Requirement 7: Restrict access to cardholder data by business need-to-know			
	EventsManager Support Level**	LANguard Support Level**	EndPointSecurity Support Level**
7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access	B,D	-	-
Requirement 8: Assign a unique ID to each person with computer access			
	EventsManager Support Level**	LANguard Support Level**	EndPointSecurity Support Level**
8.5.1 Control addition, deletion, or modification of user IDs, credentials, & other identifier objects	D	-	-
8.5.3 Set first-time passwords to a unique value for each user & change immediately after first use	-	B,D	-
8.5.4 Immediately revoke access for any terminated users	D	B,D	-
8.5.5 Remove inactive user accounts at least every 90 days	B,D	B,D	-
8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed	B,D	B,D	-
8.5.9 Change user passwords at least every 90 days	-	B,D	-
8.5.10 Require a minimum password length of at least seven characters	-	B,D	-
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts	-	-	-
8.5.16 Authenticate all access to any database containing cardholder data	B,D	-	-

See Footnotes

CHART E – PCI DSS REQUIREMENTS SUPPORT IN GFI PRODUCTS

Requirement 10: Track and monitor all access to network resources and cardholder data			
	EventsManager Support Level**	LANguard Support Level**	EndPointSecurity Support Level**
10.1 Log all individual user access to system components, especially administrative users	A,B,C,D	-	-
10.2 Implement automated audit trails for all system components to reconstruct the following events:	A,B,C,D	-	-
10.2.1 All individual accesses to cardholder data	A,B,C,D	-	-
10.2.2 All actions taken by any individual with root or administrative privileges	A,B,C,D	-	-
10.2.3 Access to all audit trails	A,B,C,D	-	-
10.2.4 Invalid logical access attempts	A,B,C,D	-	-
10.2.5 Use of identification and authentication mechanisms	A,B,C,D	-	-
10.2.6 Initialization of the audit logs	A,B,C,D	-	-
10.2.7 Creation and deletion of system- level objects	A,B,C,D	-	-
10.3 Record at least the following audit trail entries for all system components for each event	A,B,C,D	-	-
10.4 Synchronize all critical system clocks and times	B,D	-	-
10.5.1 Limit viewing of audit trails to those with a job-related need	A,B,C,D	-	-
10.5.2 Protect audit trail files from unauthorized modifications	A,B,C,D	-	-
10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed (except for new data) without generating alerts	A,B,C,D	-	-
10.6 Review logs for all system components at least daily	A,B,C,D	-	-
Requirement 11: Regularly test security systems and processes			
	EventsManager Support Level**	LANguard Support Level**	EndPointSecurity Support Level**
11.1 Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts	B,D	-	A,B,C,D
11.2 Run internal and external network vulnerability scans at least quarterly	-	A,B,C,D	-
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises	A,B,C,D	-	-

See Footnotes

CHART E – PCI DSS REQUIREMENTS SUPPORT IN GFI PRODUCTS

11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files	A,B,C,D	-	-
Requirement 12: Maintain a policy that addresses information security for employees and contractors			
	EventsManager Support Level**	LANguard Support Level**	EndPointSecurity Support Level**
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	-	A,B,C,D	-
12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:	-	-	A,B,C,D
12.3.1 Explicit management approval	-	-	A,B,C,D
12.3.2 Authentication for use of the technology	-	-	A,B,C,D
12.3.3 A list of all such devices and personnel with access	-	-	A,B,C,D
12.3.5 Acceptable uses of the technology	-	-	A,B,C,D
12.3.6 Acceptable network locations for the technologies	-	-	A,B,C,D
12.3.10 When accessing cardholder data remotely via modem, prohibition of storage of cardholder data onto local hard drives, floppy disks, or other external media. Prohibition of cut-and-paste and print functions during remote access	-	-	A,B,C,D

**FOOTNOTES:

- A: the product offers functionality directly requested by particular PCI DSS requirements in order to achieve compliance
- B: the product offers functionality that can aid enforcement or enforce particular PCI DSS requirements once they are in place, via monitoring, alerting and/or reporting. Particularly useful for periodic reviews and assessments
- C: the product offers functionality to report on compliance status of hosts in regards to a particular PCI DSS requirement
- D: the product is able to report on the data gathered as part of support levels A and B processes for a particular PCI DSS requirement

GFI Disclaimer

The information provided in this document regarding PCI DSS Requirements represents GFI's understanding of the PCI DSS V1.2 established by the PCI Security Standards Council. GFI does not write or maintain the requirements; this document was created based on our review and understanding of the requirements within PCI DSS V1.2 and the information contained in this document represents the current view of GFI on the issues discussed as of the date of publication.

The information regarding the GFI product line and its use in PCI is based on our review and understanding of the requirements. GFI has not intentionally misrepresented its products or use in PCI DSS compliance. In the event that you believe there is an inaccuracy, please contact GFI. This Document is for informational purposes only. GFI does not assume liability for the PCI DSS Requirements, your interpretation of them or your company's implementation

It is always suggested that you contact a person who is certified in the implementation of the PCI DSS Requirements.

GFI MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. GFI, GFI EndPointSecurity, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor and their product logos are either registered trademarks or trademarks of GFI Software Ltd. in the United States and/or other countries. All product or company names mentioned herein may be the trademarks of their respective owners.