



## GCSX Code of Connection Compliance Support with GFI Products



## Code of Connection Controls

		Products offering support				
4	Configuration	GFI EventsManager™	GFI LANguard™	GFI EndPointSecurity™	GFI MailDefense Suite™	What does support consist of?
4.1	Configuration: All local and remote attached devices and network infrastructure supporting devices are security-hardened in accordance with the Guidance Notes.	-	✓ F, R	-	-	GFI LANguard is an award-winning network security scanner providing certified vulnerability detection, network security audit and patch management functions, including automatic remediation functionality.
4.3	Organizations have in place a configuration control process which prevents unauthorized changes to the standard build of network devices and hosts.	✓ R	✓ F, R	-	-	GFI LANguard provides network security auditing functions which can be used in conjunction with the result comparison feature to determine any changes. GFI EventsManager performs log-based change detection and change monitoring, providing appropriate reports.
<b>5</b>	<b>Compliance Checking</b>					
5.3	All devices are scanned for the presence of security vulnerabilities at least quarterly.	-	✓ F, R	-	-	GFI LANguard offers functionality to scan for security vulnerabilities both manually and based on a schedule.
5.4	Organizations verify hardware and software configurations against unauthorized changes at least once during any period of 12 months.	✓ R	✓ F, R	-	-	GFI LANguard provides network security auditing functions which can be used in conjunction with the result comparison feature to determine any changes. GFI EventsManager performs log-based change detection and change monitoring, providing appropriate reports.
<b>10</b>	<b>Mobile/Home Working</b>					
10.3	Any use of portable electronic devices will be authorized, managed, configured and operated in accordance with CESG guidance.	-	-	✓ F, R	-	GFI EndPointSecurity offers a solution for managing portable devices within an organization. It provides policy-based granular access control for any kind of removable device attached to systems throughout the network on a “per user/group” basis.
10.5	Personal firewalls are installed, enabled and subject to configuration management for all remote working devices.	-	✓ R	-	-	GFI LANguard can detect the presence of personal firewall software and report on the data it gathers, enabling you to identify endpoints that do not have the personal firewall installed.

**Products offering support**

		<b>GFI EventsManager</b>	<b>GFI LANGuard</b>	<b>GFI EndPointSecurity</b>	<b>GFI MailDefense Suite</b>	
<b>13</b>	<b>Protective Monitoring</b>					<b>What does support consist of?</b>
13.2	Audit logs recording user activities; exceptions and information security events are available to be produced to assist in investigations and access control monitoring.	✓ F, R	-	-	-	GFI EventsManager offers functionality to collect, analyze, interpret and archive event logs from various sources, including security logs. It provides relevant reports for the data it gathers.
13.3	All logs are maintained for a minimum of six months.	✓ F, R	-	-	-	GFI EventsManager can store logs both in an SQL Server database and in a file-based storage format. The amount of logs that can be stored is only limited by the hardware capabilities of the server running GFI EventsManager.
<b>14</b>	<b>Patch Management</b>					
14.1	A patch management policy is in place and documented for all software (including firmware) used on the network.	-	✓ F, R	-	-	GFI LANGuard can help create a very flexible patch management policy. With GFI LANGuard, the important stages of such a policy (identification of missing patches, downloading of new patches and deployment of the new patches) can be performed either manually, or automatically. Thus you can chose to automatically discover and download missing patches, but manually deploy them after they have been tested.
14.2	Patches are applied in a timely fashion and audited to ensure compliance. Please state your organization's patch delay time (e.g. from a patch being issued, identified as critical/patch requires to be applied, tested, installed, verified etc) when applying usability, fault and security patches.	-	✓ F, R	-	-	GFI LANGuard is backed up by a team of security experts that monitor the appearance of new patches for Microsoft software in real time. The response time of GFI LANGuard for Microsoft software is a few hours since the release of the patch. This means that within a few hours after the release, GFI LANGuard is able to identify the missing patch, download and deploy it network wide.
<b>15</b>	<b>Removable Media</b>					
15.1	Access to removable media is disabled.	-	-	✓ F, R	-	As soon as the GFI EndPointSecurity agent is deployed on to a client computer, access to removable devices is blocked. The administrator needs to specifically grant access within the relevant policy, so until that happens, all removable devices are disabled.

**Products offering support**

		<b>GFI EventsManager</b>	<b>GFI LANGuard</b>	<b>GFI EndPointSecurity</b>	<b>GFI MailDefense Suite</b>	
<b>15</b>	<b>Removable Media</b>					<b>What does support consist of?</b>
15.2	Removable media is handled in accordance with National Policy and CESSG guidance.	-	-	✓ F, R	-	GFI EndPointSecurity allows full flexibility in management of removable media.
<b>19</b>	<b>Content Analysis</b>					
19.1	The organization identifies and isolates malicious software (at least viruses, macros, dangerous file types, mobile code and spyware).	-	-	-	✓ F (email)	GFI MailDefense Suite offers antivirus scanning using multiple antivirus engines for all email communications including attachments.
19.2	Content analysis of all incoming and outgoing data including virus checking emails and attachments is performed at the gateway and the host.	-	-	-	✓ F (email)	GFI MailDefense Suite offers antivirus scanning using multiple antivirus engines for all email communications, at gateway level. It can be used in conjunction with a host-based antivirus program.
19.3	The gateway and hosts use content analysis software from different vendors.	-	-	-	✓ F (email)	GFI MailDefense Suite offers antivirus scanning using multiple antivirus engines for all email communications. The product operates at gateway level and can be used in conjunction with a host-based antivirus program.
19.4	Organizations filter against a white list of allowed attachment file types.	-	-	-	✓ F	GFI MailDefense Suite offers the ability to filter attachments based on true file type checking.
<b>21</b>	<b>Email</b>					
21.2	The automatic execution of email content is disabled.	-	-	-	✓ F	GFI MailDefense Suite can be used to disable, and thus prevent execution of, email content code.
21.3	Dangerous file types, such as executables and scripts or password protected files are not allowed via email.	-	-	-	✓ F	GFI MailDefense Suite can be used to manage the types of files that are allowed to be sent or received as attachments to email communication.
21.4	Encrypted files are not sent via email.	-	-	-	✓ F (PGP only)	GFI MailDefense Suite can be used to block emails and attachments that are encrypted with PGP and password protected archives.

**Products offering support**

21	Email	GFI EventsManager	GFI LANGuard	GFI EndPointSecurity	GFI MailDefense Suite	What does support consist of?
21.5	File attachments and extensions are validated to prevent attachment spoofing.	-	-	-	✓ F	GFI MailDefense Suite can be configured to analyze attachments based on true file type checking. At the same time the product is able to scan the attachments with multiple antivirus engines.
21.6	Email is not automatically forwarded outside the GCSX.	-	-	-	✓ F	GFI MailDefense Suite can be configured to block delivery of email to certain addresses.
23 Mail Labeling						
23.1	The mail client or user adds security labels to each email that carries a protective marking of PROTECT or higher.	-	-	-	✓ F	GFI MailDefense Suite can be configured to add custom disclaimers to all outgoing email communication.

## CSEG MEMORANDUM No. 22 General and Security Requirements

		Products offering support				
		GFI EventsManager	GFI LANGuard	GFI EndPointSecurity	GFI MailDefense Suite	What does support consist of?
GR21	General Requirement #21 – Log File Integrity	✓ F, R	-	-	-	GFI EventsManager provides the ability to collect all log files into a database. It provides role based authentication to the GFI EventsManager console and logging of all the log related operations. GFI EventsManager provides encryption for the log data transported across distributed instances.
GR22	General Requirement #22 – Log Retention	✓ F, R	-	-	-	GFI EventsManager provides the ability of storing logs both in an SQL server database and in its own file-based format. Data compression is available for the export operations. The product can handle six months of data generated in an SME environment.
GR23	General Requirement #23 – Audit Frequency	✓ F	-	-	-	GFI EventsManager support real-time collection and analysis of logs. It stores the entire information providing the ability of performing forensic investigations at a later stage too.
GR24	General Requirement #24 – Vulnerability Assessment	-	✓ F, R	-	-	GFI LANGuard offers functionality to scan for security vulnerabilities both manually and based on a schedule. The product has industry certification for vulnerability scanning and management.
GR25	General Requirement #25 – Protective measures against threats	✓ F, R	✓ F, R	-	-	GFI EventsManager can act as a host-based IDS solution for computers running Windows Vista and newer, including the server family from Microsoft. It uses the events logged by the Windows Filtering Platform in order to determine suspicious behavior of the users and processes running on computers network wide. GFI LANGuard offers security vulnerability scanning and port scanning in order to determine potential threat-prone system. The product is able to push patches in order to fix security vulnerabilities.

**Products offering support**

		<b>GFI EventsManager</b>	<b>GFI LANGuard</b>	<b>GFI EndPointSecurity</b>	<b>GFI MailDefense Suite</b>	<b>What does support consist of?</b>
--	--	--------------------------	---------------------	-----------------------------	------------------------------	--------------------------------------

SR1	Security Requirement #1 (SR1) – Clock synchronization	✓ R	-	-	-	GFI EventsManager provides the ability to monitor the time synchronization process by collecting and analyzing the information logged by NTP servers and clients.
SR2	Security Requirement #2 (SR2) – Unique Identification	✓ F	-	-	-	GFI EventsManager preserves the original state of the log entries, including the computer where the event was logged. Network related events also contain information about external computers that act as sources of the actions which lead to the logging of the events. This information is also preserved by GFI EventsManager. The product identifies and preserves the user responsible for the actions that lead to the creation of the log entries. It is able to analyze, filter and report on all the information above.
SR3	Security Requirement #3 (SR3) – Managing date/time of an event	✓ F	-	-	-	GFI EventsManager preserves the original state of the log entries, including the date and time. The product enables filtering and sorting by date and time, as well as defining time periods for the reports.
SR4	Security Requirement #4 (SR4) – Identify the physical and logical address	✓ F	-	-	-	When data is available, GFI EventsManager can automatically perform WHOIS queries on the source addresses that generated log entries across the entire network. The functionality is based on the log entries generated by the Windows Filtering Platform when a computer communicates with an external IP address. Just holding the mouse over the external address on the GFI EventsManager dashboard will automatically display the WHOIS information for that address.
SR5	Security Requirement #5 (SR5) – Identify source and destination	✓ F, R	-	-	-	The network communication logs, such as the ones generated by the Windows Filtering Platform, or network device logs in Syslog format, contain the source and destination IPs as well as the direction of the communication. When data is available, GFI EventsManager records all this information and is able to filter/sort and report on it.

**Products offering support**

		<b>GFI EventsManager</b>	<b>GFI LANGuard</b>	<b>GFI EndPointSecurity</b>	<b>GFI MailDefense Suite</b>	<b>What does support consist of?</b>
--	--	--------------------------	---------------------	-----------------------------	------------------------------	--------------------------------------

SR6	Security Requirement #6 (SR6) – Reveal the type of service	✓ F, R	-	-	-	The network communication logs, such as the ones generated by the Windows Filtering Platform, or firewall logs in Syslog format, contain the port used for communication. The port used identifies the protocol used. When data is available, GFI EventsManager records the information about the port and is able to filter/sort and report on it. Additionally, GFI EventsManager enables process level analysis in order to determine what processes and services run on Windows machines.
SR7	Security Requirement #7 (SR7) – Identify privileged commands	✓ F, R	-	-	-	GFI EventsManager is able to record privilege system changes as required; additionally, it has the unique capability of identifying if the user performing an action that generates an event, is an administrator or not. The product is able to report on the information it gathers and analyzes.
SR8	Security Requirement #8 (SR8) – Identify unauthorized applications	✓ F, R	-	-	-	GFI EventsManager is able to record events like applications being installed or removed, applications crashing or hanging and the creation of new processes.
SR10	Security Requirement #10 (SR10) – Analyze content of objects	✓ F	-	-	-	GFI EventsManager features complete log entry collection and advanced processing and filtering capabilities enabling advanced analysis and forensics.
SR13	Security Requirement #13 (SR13) – Reveal non-typical gaps in accounting logs	✓ F, R	-	-	-	GFI EventsManager is able to provide a statistical view of the log collection process, highlighting the current and past trends. The reports presented in this respect enable identifying the gaps.
SR16	Security Requirement #16 (SR16) – Bandwidth and performance	✓ F	-	-	-	GFI EventsManager can monitor log entries from the Performance Logs and Alerts service on Windows operating systems.

## ISO/IEC 27002 Controls

		Products offering support				
		GFI EventsManager	GFI LANguard	GFI EndPointSecurity	GFI MailDefense Suite	What does support consist of?
4.1	Assessing security risks	-	✓ F, R	-	-	GFI LANguard is an award-winning network security scanner providing certified vulnerability detection, network security audit and patch management functions, including automatic remediation functionality. The product can play a major part in the security risk assessment strategy.
4.2	Treating security risks	-	✓ F, R	-	-	GFI LANguard features active remediation enabling automatic deployment of patches that address security risks.
7.1.1	Inventory of assets	-	✓ F, R	-	-	
10.4.1	Protection against malicious code	✓ F, R	-	-	-	GFI EventsManager provides the ability to see in real time suspicious network activity, using the events generated by the Windows Filtering Platform. When data is available, GFI EventsManager can help you identify potentially compromised computers and stop them from spreading the malicious code or performing the malicious activity. Additionally, GFI EventsManager can collect and report on logs of network equipments capable of identifying attacks or malicious code, such as firewalls, antivirus software and IDS systems.
10.6.2	Security of network services (mail)	-	-	-	✓ F	GFI MailDefense Suite is a powerful package that consists of two leading GFI Software products, GFI MailSecurity and GFI MailEssentials, which together filter and clean all inbound and outbound email and protect your environment from email-borne threats.
10.10.1	Audit logging	✓ F, R	-	-	-	GFI EventsManager is a central log management solution that collects and analyzes information in real time. The information is saved to a database for reporting and compliance purposes.

**Products offering support**

		<b>GFI EventsManager</b>	<b>GFI LANGuard</b>	<b>GFI EndPointSecurity</b>	<b>GFI MailDefense Suite</b>	<b>What does support consist of?</b>
--	--	--------------------------	---------------------	-----------------------------	------------------------------	--------------------------------------

10.7.1	Management of removable media	-	-	✓ F, R	-	GFI EndPointSecurity enables organizations to fully control and manage the removable media. It enables user-based access control to removable devices as well as file type based filtering of the data which is transferred.
10.10.2	Monitoring system use	✓ F, R	-	-	-	GFI EventsManager can collect log entries from a variety of computers and devices. It supports Windows .evt and .evtx formats to collect information from Windows hosts, Syslog and SNMP Traps to collect information from Linux/Unix machines and network devices (routers, firewalls, etc), W3C format to collect information from the web and email servers and database auditing. The information above can be used to monitor the use of all the systems throughout the network.
10.10.3	Protection of log information	✓ F	-	-	-	GFI EventsManager centralizes log information from across the network into a Microsoft SQL Server database. The database engine has all the necessary capabilities to allow secure configurations and well as disaster recovery operations. Additionally, GFI EventsManager can export log data into files that are encrypted using an algorithm in compliance with NIST SP 800-67.
10.10.4	Administrator and operator logs	✓ F, R	-	-	-	GFI EventsManager is able to record privilege system operations; additionally it has the unique capability of identifying if the user performing an action that generates an event, is an administrator or not. The product is able to report on the information it gathers and analyzes.
10.10.5	Fault logging	✓ F	-	-	-	GFI EventsManager is capable of collecting, analyzing and alerting on log entries created on system or service failure. The product is also able to report on the data it alerts on.

**Products offering support**

		<b>GFI EventsManager</b>	<b>GFI LANGuard</b>	<b>GFI EndPointSecurity</b>	<b>GFI MailDefense Suite</b>	<b>What does support consist of?</b>
--	--	--------------------------	---------------------	-----------------------------	------------------------------	--------------------------------------

10.10.6	Clock synchronization	✓ R	-	-	-	GFI EventsManager provides the ability to monitor the time of synchronization process by collecting and analyzing the information logged by NTP servers and clients.
11.2.1	User registration	✓ R	-	-	-	GFI EventsManager is able to collect and report on information regarding user registration, authentication, account management and activity.
11.2.2	Privilege management	✓ R	-	-	-	GFI EventsManager is able to record privilege system changes as required; additionally, it has the unique capability of identifying if the user performing an action that generates an event, is an administrator or not. The product is able to report on the information it gathers and analyzes.
11.2.3	User password management	✓ R	-	-	-	GFI EventsManager is able to collect and report on information regarding password management events logged to the security logs.
11.2.4	Review of user access rights	✓ R	-	-	-	GFI EventsManager is able to collect and report on information concerning user rights assignment.
11.5.1	Secure logon procedures	✓ R	-	-	-	GFI EventsManager is able to collect and report on information regarding the use of the authentication and authorization mechanisms, as well as their system functionality.
11.5.2	User identification and authentication	✓ R	-	-	-	GFI EventsManager is able to collect and report on user identification and authentication events.
11.5.3	Password management system	✓ R	-	-	-	GFI EventsManager is able to collect and report on information regarding password management events logged to the security logs.

		Products offering support				What does support consist of?
		GFI EventsManager	GFI LANguard	GFI EndPointSecurity	GFI MailDefense Suite	
12.6.1	Control of technical vulnerabilities	-	✓ F, R	-	-	GFI LANguard provides the ability to manage and control the technical vulnerabilities network wide.
13.1.1	Reporting IS events	✓ R	-	-	-	GFI EventsManager collects and analyzes log data from various systems, thus being able to report on information security events.
13.1.2	Reporting IS weaknesses	-	✓ R	-	-	GFI LANguard is an award-winning network security scanner providing certified vulnerability detection, network security audit and patch management functions. It is able to report on the security status of all hosts.
13.2.3	Collection of evidence	✓ F, R	-	-	-	GFI EventsManager archives all logs and provides advanced filtering capabilities for forensic investigation.

Legend: **F** – Feature  
**R** – Reports

#### GFI Disclaimer

© 2010. GFI Software. The information provided in this document regarding the requirements of GCSX Code of Connection represents GFI's understanding of the GCSX Code of Connection Standard v4.1 established by Government Connect. GFI does not write or maintain the requirements; this document was created based on our review and understanding of the requirements within GCSX Code of Connection Standard v4.1 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 GCSX Code of Connection is based on our review and understanding of the requirements. GFI has not intentionally misrepresented its products or use in GCSX Code of Connection 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 GCSX Code of Connection 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 GCSX Code of Connection compliance.

All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document. If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.