Automation Suite for GPG 13 Compliance

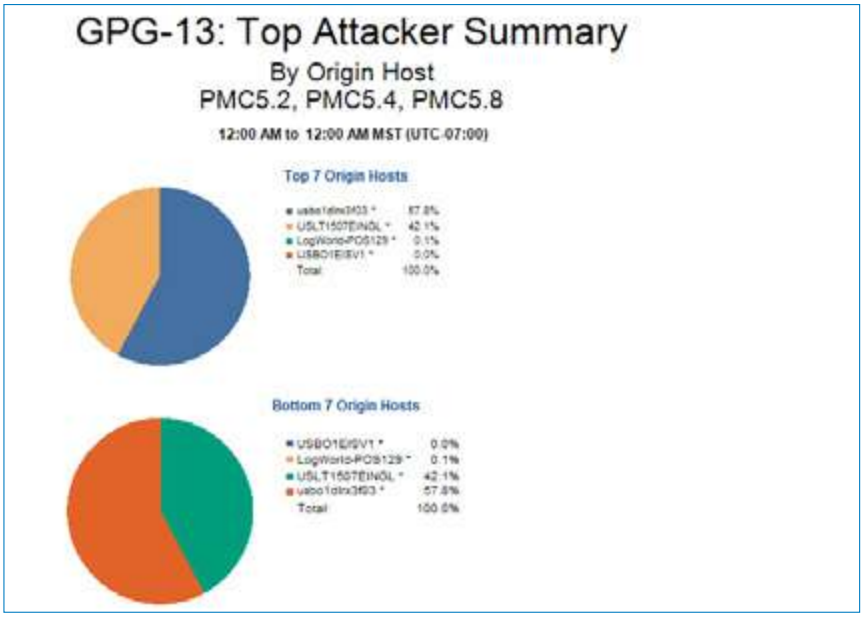
GPG 13 Compliance Assurance with LogRhythm

Protective Monitoring for HMG ICT Systems is based on CESG's Good Practice Guide no.13 (GPG 13.). It provides a framework for treating risks to systems, and includes guidance for configuring and collecting ICT log information in order to provide an audit trail of security relevant events of interest. These guidelines were put in place to provide security administrators and other IT professionals with an audit trail of relevant security- and operations-related events on their network. The 12 Protective Monitoring Controls (PMC) within GPG-13 describe specific requirements that an organization must meet in everyday practice as well as in audit situations. These requirements can help an organization in IT forensics, incident response and management, and maintaining the integrity of their individual enterprise.

All HMG organisations, whether central or local government, police, fire, health, and education authorities are mandated to comply with policy, standard, legislative and regulatory requirements. Protective Monitoring with its levels of log management and reporting can help in forensic readiness, incident management and most importantly, delivering against these regulatory requirements by providing evidence of compliance to the auditors.

Log collection, analysis, and storage are integral to meeting the GPG-13 control requirements. Log analysis, in and of itself, can be an enormous effort. Considering that networks can produce millions of individual log messages a day (sometimes every hour), monitoring an organization's log data can be a time-consuming and costly endeavour. By using LogRhythm to automate log management, event messages from across an organization's network can be consolidated in a single location where continuous, automated correlation and analysis enforce GPG-13 requirements and real-time alerts immediately expose areas of non-compliance for quick remediation.

In order to adhere to GPG-13's PMC requirements, organizations can harness LogRhythm's powerful, out-of-the-box compliance suites for continuous monitoring of their environment. LogRhythm offers three GPG-13 modules with increasing degrees of granularity in the Protective Monitoring Controls; GPG 13 (standard), GPG-13 Compliance Automation Suite and GPG-13 Advanced Compliance Suite. In this document, we will focus on the GPG-13 Advanced Compliance Suite. The GPG-13 Advanced Compliance Suite was designed specifically with each PMC in mind, with coverage across each Recording Profile (A, B, C, and D). LogRhythm's GPG-13 alerts, reports, and investigations can help identify critical issues on a network and can help notify the proper parties. With reports and alarms covering an array of issues, from top attackers to malware outbreaks, the LogRhythm solution can help any organization meet their reporting requirements.



GPG-13: Audit Success Executive Summary Screenshot

The tables on the subsequent pages outline how LogRhythm supports requirements of the GPG-13 Protective Monitoring Controls. The "How LogRhythm Supports Compliance" column describes the capabilities LogRhythm provides that directly meet or augment support for GPG-13 compliance objectives.

Control Title	Control Description	Accounting Recommendations	How LogRhythm Supports Compliance
PMC1 - Accurate time in logs	Provide a means of providing accurate time in logs and synchronisation between system components with a view to facilitating collation of events between those components. This can be achieved by any or all of the following means: • Providing a master clock system component which is synchronised to an atomic clock; • Updating device clocks from the master clock using the Network Time Protocol (NTP); • Record time in logs in a consistent format (Universal Co-ordinated Time (UTC) is recommended); • As a fall-back, checking and updating device clocks on a regular basis (e.g. weekly). Projects should define the error margin for time accuracy according to business requirements. The following issues also need to be considered: • Some devices may not support clock synchronisation and need to be manually maintained; • Although recording time in UTC, the human interface should also support local time; • Clocks drift on mobile devices (e.g. Portable Electronic Devices (PEDs)) may require correction upon attachment.	1. Each and every event record should include a simple time-stamp. 2. Alert messages may reference related events and should also be time-stamped. 3. Log file extracts should include an accurate time-stamp that is digitally signed. 4. Transactions with a high integrity requirement should have a hash of the transaction time stamped, digitally signed and a copy of the transaction record retained.	LogRhythm provides direct support of GPG-13 control objective PMC1 in several ways. Each and every event record and alert message includes a simple time stamp. LogRhythm independently synchronizes the timestamps of all collected log entries, ensuring that all log data is time-stamped to a standard time regardless of the time zone and clock settings of the logging hosts. The product is also capable of reporting time inaccuracies along the collection path. Further augmented support of GPG-13 control objectives within PMC1 is provided through support of UTS-validated, time-stamped digital signatures of collected log files. Where the customer defines transactions having a high integrity requirement, LogRhythm can provide augmented support to control objective PMC1.4.
PMC2 - Recording relating to business traffic crossing a boundary	The objective of this control is to provide reports, monitoring, recording and analysis of business traffic crossing a boundary with a view to ensuring traffic exchanges are authorised, conform to security policy, transport of malicious content is prevented and alerted, and that other forms of attack by manipulation of business traffic are detected or prevented. The main requirement is to provide an accountable record of imports and exports executed by internal users and to track cross-boundary information exchange operations and the utilisation of any externally visible interfaces. This includes all checking of cross-boundary movement of information, content checking and quarantining services. Application based checks can be applied to business traffic to accept legitimate transactions and reject and alert malformed exchanges.	1. Malware detection at the boundary. 2. Every change in status of the boundary antimalware signatures. 3. Blocked web browsing activities. 4. Blocked file import attempts across the boundary. 5. Blocked file export attempts across the boundary. 6. Enhancement to Events 4. and 5. records to include file content. 7. Enhancement to Events 4. and 5. records, where processed by a guard processor. 8. Allowed web browsing activities across the boundary. 9. File import across the boundary that are allowed. 10. Allowed file export across the boundary. 11. Enhancement to Events 9. and 10. records to include file content. 12. Enhancement to Events 9. and 10. records, where processed by a guard processor. 13. Files entered into a transfer cache. 14. Access of files entered into a transfer cache.	LogRhythm directly supports GPG-13 control objectives within PMC2 by collecting boundary device logs and by producing reports and alerts for malware detection, signature updates, denied/allowed file import/export activity and denied/allowed web browsing attempts. LogRhythm also provides supplemental support for GPG-13 control objectives within PMC2 by providing details of changes to network files. LogRhythm's File Integrity Monitor (FIM) can be configured to monitor system file or directory activity, deletions, modification, and permission changes. The file integrity capability is completely automated and the agent can be configured to either scan for files/directory changes on a schedule or the kernel level driver can automatically detect file integrity activity in real-time. Where transfer caches based on bespoke technologies are in use, LogRhythm can provide augmented support to control objective PMC2.13

Control Title	Control Description	Accounting Recommendations	How LogRhythm Supports Compliance
PMC3 - Recording relating to suspicious behaviour at a boundary	The objective of this control is to provide reports, monitoring, recording and analysis of network activity at the boundary with a view to detecting suspect activity that would be indicative of the actions of an attacker attempting to breach the system boundary or other deviation from normal business behaviour. The main requirement is to receive information from firewalls and other network devices for traffic and traffic trend analysis. This will enable detection of common attacks such as port scanning, malformed packets and illicit protocol behaviours. An intrusion detection service is a recommended defence at the boundary with any untrusted network (e.g. the Internet). It may also be a mandated requirement in codes of connection for membership of community of interest networks (such as GSI). Whenever it is implemented then it is recommended it includes a Recordable Report profile of at least B.	1. Packets being dropped by boundary firewalls. 2. All boundary monitoring system console messages at Critical status and above. 3. User authentication failures on boundary devices and systems. 4. The detection of all suspected attacks at the boundary. 5. All boundary monitoring system console messages at Error status. 6. User sessions on boundary devices and consoles of boundary management systems. 7. All changes to boundary firewall and other relevant device rule-bases. 8. All actions invoked by users in response to an external attack notification. 9. Every change in status of the external attack recognition software (Security Information and Event Management systems (SIEM), Network Behaviour Analysis (NBA), IDS or IPS) signature base. 10. All boundary monitoring system console messages at Warning status and below. 11. All commands issued to boundary devices and consoles of boundary monitoring systems. 12. Packets being passed by boundary firewalls. 13. Enhancement to Event 1. records to include full packet capture. 14. All automated responses at the boundary (by an IPS). 15. Enhancement to Event 10. records to include full packet capture.	LogRhythm provides direct support for GPG-13 control objectives within PMC3 by collecting boundary device logs from routers, firewalls, VPN servers, etc. LogRhythm correlation rules provide alerting on unauthorized or suspicious activity. LogRhythm investigations and reports provide evidence of internal/ external boundary activity and threats including network denials.
PMC4 - Recording of workstation, server or device status	The objective of this control is to detect changes to device status and configuration. Changes may occur through accidental or deliberate acts by a user or by subversion of a device by malware (e.g. installation of trojan software or so called "rootkits"). It will also record indications that are typical of the behaviour of such events (including unexpected and repeated system restarts or addition of unidentified system processes). It also attempts to detect other unauthorised actions in tightly controlled environments (e.g. attachment of USB storage devices). This includes extension to extensive monitoring of any business critical file areas.	1. All critical host messages at Critical status and above (servers and selected workstations). 2. Malware detection incident on any host (workstation or server). 3. All critical host messages at Error status and above (servers and selected workstations). 4. Every change in status of any hosts antimalware software signature base. 5. Every failing file system access attempt should be logged and reportable. 6. Changes to file or path access rights within system folders. 7. Change in status of all networked hosts. 8. Change in status of attachment of devices attached to controlled hosts. 9. Change in status of storage volumes of monitored hosts. 10. Change in software configuration status. 11. Changes detected to files within system folders. 12. All critical host messages at Warning status or below (servers and selected workstations). 13. Any changes to system configuration (or registry) settings any host. 14. Change in status of system processes on monitored hosts. 16. Enhancement to Event 10. records to include package software inventory. 17. Enhancement to Event 11. records to include the contents of changes to files. 18. Enhancement to Event 13. records to include the content of changes to configuration settings.	LogRhythm provides direct support for GPG-13 control objectives within PMC4 by being able to collect reports and alerts on hosts with a critical status, including changes detected to files systems within system folders and malware detection on any host (workstation or server). LogRhythm also reports on error/warning statuses of critical hosts (workstation or sever), status changes of anti-malware software signature base, failing file system access attempts through advanced Unix auditing, and changes in software configuration status. LogRhythm also augments control objectives within PMC4 by reporting on all changes to system configuration (or registry) settings on hosts, changes in status to system processes on monitored hosts, changes to file or path access rights within system folders, statuses of all network hosts, statuses of attachment devices to controlled hosts and changes in status of storage volumes of monitored hosts. LogRhythm can provide augmented support to control objectives PMC4.16, 4.17 and 4.18.

Control Title	Control Description	Accounting Recommendations	How LogRhythm Supports Compliance
PMC5 - Recording relating to suspicious internal network activity	The objective of this control is to monitor critical internal boundaries and resources within internal networks to detect suspicious activity that may indicate attacks either by internal users or by external attackers who have penetrated to the internal network. Likely targets for heightened internal monitoring include: • core electronic messaging infrastructure (e.g. email servers and directory servers); • sensitive databases (e.g. HR databases, finance, procurement/ contracts, etc.); • information exchanges with third parties; • project servers and file stores with strict "need to know" requirements.	1. Packets being dropped by internal firewalls. 2. All internal monitoring system console messages at Critical status and above. 3. User authentication failures on internal network devices and monitoring consoles. 4. All internal monitoring system console messages at Error status. 5. User sessions on internal network devices and monitoring consoles. 6. All changes to internal firewall and other relevant device rule-bases. 7. The detection of all suspected internal attacks. 8. All internal monitoring system console messages at Warning status or below. 9. All commands issued to internal network devices and central consoles of internal monitoring systems should be logged and reportable. 10. Packets being passed by internal firewalls should be logged and reportable. 11. Enhancement to Events 1. records to include full packet capture. 12. All actions invoked by users in response to an internal attack notification. 13. Every change in status of the internal attack recognition software (SIEM, NBA, IDS or IPS) signature base. 14. All automated responses at internal network control points (by an IPS). 15. Enhancement to Events 10. records to include full packet capture.	LogRhythm directly supports GPG-13 control objectives within PMC5 by reporting and alerting on all internal monitoring systems as critical status, user authentication failures on network devices and monitoring consoles, and the detection of all suspected internal attacks. Further, LogRhythm reports on packets being dropped or passed by internal firewalls, every status change on internal attack recognition software signature base, all internal monitoring systems at error/warning status, and changes to internal firewall and other relevant device rule bases. LogRhythm also augments GPG-13 control objectives within PMC5 by reporting and alerting on all automated response from internal network control points by an IPS. Further, LogRhythm will report on all actions invoked by users in response to an internal attack notification, user's sessions on internal network and monitoring devices. LogRhythm can provide augmented support to control objectives PMC5.11, and 5.15.
PMC6 - Recording relating to network connections	The objective of this control is to monitor temporary connections to the network either made by remote access, virtual private networking, wireless or any other transient means of network connection. This includes: • Environments which are permissive and that support Wireless LANs (WLANs), mobile users and remote working and it includes • More restrictive environments in which the attachment of modems and wireless access points are prohibited.	1. User authentication failures for remote access. 2. All unsuccessful Virtual Private Network (VPN) node registrations. 3. Changes of status of dynamic IP address assignments. 4. User sessions via remote access. 5. Changes in status of VPN node registration. 6. All rejected attempts to connect equipment to protected network attachment points. 7. All network connection console messages at Critical status and above. 8. User authentication failures on network connection consoles. 9. All network connection console messages at Error status. 10. All cases of attachment attempts of wireless devices to legitimate wireless access points. 11. User sessions on network connection consoles. 12. The detection of all suspected wireless attacks. 13. All network connection console messages at Warning status or below. 14. All commands issued to network connection consoles 15. All actions invoked by users in response to an internal attack notification. 16. Every change in status of the internal attack recognition software (WIDS) signature base. 17. Detection of all rogue wireless interfaces and wireless access points should be logged, reportable and alerted.	LogRhythm directly supports GPG-13 control objectives within PMC6 by reporting and alerting on user authentication failures for remote access, authentication failures on network connection consoles, detection of all suspected wireless attacks, detection of rogue wireless interfaces and access points, unsuccessful VPN node registrations, all network connection consoles at critical status, and rejected attempts to connect equipment to protected network attachment points. LogRhythm also reports on all network connection consoles at warning/error status, changes of WIDS signature bases, changes in VPN node registration statuses and changes to dynamic IP address assignments through custom audit configs (Linux) and tuning the auditing in Windows. LogRhythm augments GPG-13 control objectives within PMC6 by reporting on user sessions on network connection consoles and remote access points, including user actions in response to internal attack notifications and all cases of attachment attempts of wireless devices to legitimate wireless access points based on the customer defining a list of approved wireless access points. LogRhythm can provide augmented support to control objective PMC6.14

Control Title	Control Description	Accounting Recommendations	How LogRhythm Supports Compliance
PMC7 - Recording of session activity by user and workstation	To monitor user activity and access to ensure they can be made accountable for their actions and to detect unauthorised activity and access that is either suspicious or is in violation of security policy requirements. This is intended to support accountability requirements such that users can be held to account for actions they perform on ICT systems.	1. User network sessions. 2. User network account status change. 3. Changes to network user privileges and user group status and membership. 4. Use of any application or database administrative facility. 5. User network account status changes to locked-out state should be alerted. 6. Change in privilege level status of a user on a server or critical workstation. 7. Invocation of any accountable user transaction (including interactions with applications and database servers). 8. Local user sessions on critical workstations. 9. Local user account status change on critical workstations should be logged and reportable. 10. Changes to critical workstation user accounts and group membership or status. 11. Running of all network commands and executables. 12. Enhancement to Event 7. records to include transaction contents. 13. Running of all critical workstation commands and executables.	LogRhythm directly supports GPG-13 control objectives within PMC7 by alerting on network user accounts changed to a status of locked-out. Reporting will also directly support control objectives based on changes to network user accounts, privileges and user group assignments. LogRhythm augments GPG-13 control objectives within PMC7 by reporting on privilege access escalation on servers or critical workstations, running of all network commands and executables and local user account status changes on critical workstation. Where the customer defines "accountable user transactions", LogRhythm can provide augmented support to control objectives PMC7.7 and 7.12
PMC8 - Recording of data backup status	To provide a means by which previous know working states of information assets can be identified and recovered from in the event that either their integrity or availability is compromised. Providing and audit trail of backup and recovery operations is essential part of the backup process and will enable identification of the most reliable source of the prior know good states of the information assets to be recovered in the event of data corruption, deletion or loss. The need for more sophisticated backup and recovery facilities are generally driven by higher levels of risk to Integrity and Availability properties. There is a complimentary requirement for online storage failure events to be alerted, this is met by PMC4 Recordable Event 1 (the detection of any server storage failure should be classed as an alertable Critical event).	1. Backup, test and recovery operations. 2. Backup, test and recovery operation failures should be alerted. 3. Enhancement of Event 1. records to include operation file catalogue details. 4. Enhancement of Event 3. records to include site reference and version information.	LogRhythm directly supports GPG-13 control objectives in PMC8 by alerting on backup operation failures. LogRhythm provides augmented support of GPG-13 control objectives in PMC8 by reporting backup operations including enhancements within PMC8.3/8.4.

Control Title	Control Description	Accounting Recommendations	How LogRhythm Supports Compliance
PMC9 - Alerting critical events	To allow critical classes of events to be notified in as close to real-time as is achievable. The aware level requirement is for console based alerts that can be watched for by duty Security Managers. It would be expected that extensive projects (with continuous monitoring requirement) would require a Security Operations Centre with summary wall displays (with the most complex scenario implementing redundant monitoring centres). It should be noted that alerts themselves are recordable events. Smaller projects can have a solution to fit their size and would typically only require a profile A solution with simple monitoring facilities (a Security Manager workstation). Smaller projects may also consider combination of functions (e.g. security and network management) provided this does not conflict with segregation requirements. Secondary alerting channels may also be supported for projects that cannot provide continuous console manning (e.g. SNMP, email, SMS, etc.) via either in hours or out of hours services.	1. Alert messages routed to Security Manager console(s). 2. Simple alert notifications sent via secondary channels (email, SMS, pager, etc.). 3. Configuration changes of alerts and secondary alerts. 4. Graphical display of alert streams on consoles or wall displays. 5. Enhancement of Event 1. reports to include multicasting of alerts to several sites.	LogRhythm provides support for GPG-13 control requirement PMC9 by allowing real-time dashboard display with drilldown to underlying event records and custom alerts. LogRhythm can also enable alert thresholds and set remediation processes to be initiated.
PMC10 - Reporting on the status of the audit system	To support means by which the integrity status of the collected accounting data can be verified. The Aware segment requirements comprise the need to inspect log status on end devices and alerting of log error or other security relevant conditions. Upper segment requirements expand to include the requirement for log collection and query systems (ultimately served as a resilient solution). Smaller (especially single location) projects can have a solution to fit their size and would typically only require a profile level A solution without log collection facilities (perhaps assisted by COTS log analysis tools).	1. Log resets, error conditions, failures and threshold exceptions. 2. Query of status of active log storage on all devices on which logs are kept either locally or centrally. 3. Optionally provide a time record of Event 2. information, displaying trends. 4. Enhancement to Event 2. records to include log rotation information. 5. Movement of segments and messages along the log collection chain. Message time-stamps should not be superceded. 6. Query at central collector(s) to provide a report of log sources. 7. Optionally provide a time record of Event 5. in graphical form, displaying trends over time. 8. Integrity checks failures at any point in the log handing chain. 9. Log access query requests including requests for production of log extracts. 10. The central collector(s) should be able to query the online and selectively retrieved archive accounting data.	LogRhythm provides direct support for GPG-13 control objectives within PMC10 by collecting, analysing, and allowing for the query of all audit processing log messages. LogRhythm correlation rules provide alerting on processing activity, including audit log clearing, audit log rotation, audit logging stoppage, and failed audit log writes. Archive integrity is protected by cryptographic hashes, and the SecondLook tool allows investigation of historic log information directly from archive. Individual devices can be monitored by running reports on the status and detection of loss of "heartbeats". LogRhythm also directly supports control objectives within PMC10 by reporting on above mentioned audit processing log messages many of which are fundamental tenets of the way the LogRhythm works.

Control Title	Control Description	Accounting Recommendations	How LogRhythm Supports Compliance
PMC11 - Production of sanitised and statistical management reports	To provide management feedback on the performance of the protective monitoring system in regard of audit, detection and investigation of information security incidents.	Exact report content requirements needs to be agreed with management and it needs to be ensured that the contents are readily digestible by the target community. The objectives of such reporting are to: • Promulgate awareness of the current information security situation to management and staff; • Demonstrate the ongoing contribution and return on investment of Protective Monitoring services deployed on a project; • Support business cases for improvement; • Provide evidence for IA capability maturity assessment. All reports need to be designed with this in mind. Examples of appropriate content for management reports includes: • Trends of attacks over current period plus history • Performance of detection and defence mechanisms (including percentage ratio of: real alerts / (real + false alerts) • Rolling "top 10" attacks experienced • Geographic representation of where the attacks are coming from • Statistics on internal violations • Sanitised summaries of significant ongoing events or investigations • Summary of current audit and compliance check results These will be combined with information from other sources (e.g. SIEM system) to provide a complete information security status report. Due to the broad range of outputs possible no Accounting Recommendations table is provided for this risk treatment. Requirements for management reports will largely dictated by the technology adopted for any given project. The more advanced log management and SIEMs can be expected to provide report tem-plating as well as a series of proforma reports. It is possible that some tools will support multiple purposes and can provide support for: • information security incident management • computer forensic investigations In these cases they should be able to provide complete information security status reports.	LogRhythm's GPG-13 compliance suite comes with pre-packaged reports specifically designed to be consumed by the organization's management. A wide variety of reports are provided out of the box including information such as "top 10" lists (of attackers, targeted hosts, etc.) and Geographic IP (GeoIP) information to pinpoint the origin location of detected attacks. These reports provide feedback to management on the overall success and improvement areas of the organization's GPG-13 compliance program.

Control Title	Control Description	Accounting Recommendations	How LogRhythm Supports Compliance
PMC12 - Providing a legal framework for Protective Monitoring activities	To ensure that all monitoring and interception of communications is conducted lawfully and that accounting data collected by the system is treated as a sensitive information asset in its own right. The most significant aspect of ensuring Protective Monitoring is lawful is ensuring that it is justified. A major part of the evidence for that justification is that the risk management process ensures there is neither too much nor too little. There are certain aspects of user consent that need to be recorded as part of the system implementation. As for the other treatments the degree of rigour and trust in these increased along the scale of increasing segment. It is important to seek legal advice on compliance with the law and wording of all related screen messages and documents. Online electronic sign up may also be supplemented, or alternatively replaced, by manual records of user agreements and monitoring policies.	1. User sign up operations. 2. It should be possible to configure alerts for user sign up refusals. 3. Enhancement to Event 1. reports to include a user digital signature. Log records should also be recorded for each re-affirmation. 4. Enhancement to Event 3. reports to include a hardware token or smartcard reference. Log records should also be recorded for authorisation transaction involving that user.	LogRhythm provides support for GPG-13 control requirement PMC12 through a combination of secure log collection, storage, and archiving; cryptographic hash technology, reporting and investigation tools, and access controls.