Netsurion®

Powering Secure and Agile Networks

GCSx CoCo Compliance Guide

How Netsurion® Can Help You Achieve and Maintain Compliance

GCSx CoCo Compliance Overview

Government Connect (GC) is a recognized, accredited and trusted secure government network for all Local Authorities (LAs) in England and Wales. The network is called GCSx and it enables secure data sharing up to RESTRICTED level across government.

The Code of Connection (CoCo) defines the standards and processes that an authority must comply with before connecting to GCSx.

For up-to-date information regarding the actual policy Public Sector organizations should always contact the National Cyber Security Centre (NCSC) or refer to their FAQ's for the Code of Compliance.

Protective Monitoring

The policy is not reproduced here and public sector bodies should obtain it from the NCSC. However, in summary the logging requirements regarding user access to your network and systems include recording the following events:

- Unauthorized application access (where applicable)
- File access attempts to protectively marked information (e.g. RESTRICTED data).
- Unsuccessful login / logout
- Successful login / logout
- Privileged system changes (e.g. account management, policy changes, device configuration)

Logs should be kept for at least 6 months. This may include the use of backup tapes but logs should be easily available for use as part of your incident response policy, as well as help with an investigation. In practice this may need a system which maintains logs readily recoverable from any archive.

Netsurion Provides a Full View of the Entire IT Infrastructure

EventTracker improves security, helps organizations demonstrate compliance, and increases operational efficiencies. Netsurion enables your organization to be more aware of potential security risks and internal/external threats. It provides you with the ability to respond to a security incident with comprehensive data and forensic tools for analysis. The time required to investigate and mitigate security incidents can be greatly reduced, minimizing potential exposure and costs.

Netsurion's Managed Threat Protection is our managed services offering to enhance the value of EventTracker implementations. Our expert staff can assume responsibility for some or all EventTracker SIEM-related tasks, including system management, incident reviews, daily/weekly log reviews, configuration assessments, and audit support. We augment your IT Security team, allowing you to focus on your priorities by leveraging our expertise, discipline and efficiency.

Scalable, Log Collection and Processing with Notifications based on Criticality

EventTracker provides automatic consolidation of thousands or even millions of audit events to meet the needs of any size organization. The inbound log data is identified by EventTracker's built-in manufacturers Knowledge Base, which contains log definitions for thousands of types of log events, and automatically identifies which events are critical to security standard.

EventTracker provides real-time and batch aggregation of all system, event and audit logs from your firewalls, IDS/IPS, network devices, Windows, Linux/Unix, VMware ESX, Citrix, databases, MS Exchange web servers, EHRs and more.

Ease of Deployment and Scalability

EventTracker is available on premises or as a highly scalable cloud-based SIEM and Log Management solution. It offers several deployment options to meet the needs of organizations with a few dozen systems or those with thousands of systems spread across multiple locations. EventTracker Cloud is available as an AMI on Amazon EC2, Microsoft Azure or your cloud infrastructure provider of choice. It supports multi-tenant implementations for MSSP organizations serving the needs of smaller customers.

GCSx CoCo Compliance Requirements

CESG Memo 22

Requirements	Netsurion Capability
CESG memo 22 states that logs should record the following for users on your network. a. Successful login / logout b. Unsuccessful login / logout c. Unauthorized application access (where applicable) d. File access attempts to protectively marked information (e.g. RESTRICTED /PROTECTED data). e. Privileged system changes (e.g. account management, policy changes, device configuration) Logs should be kept for a minimum of 6 months. They should form part of your incident response policy, as well as help with a wider CESG investigation.	EventTracker's alerting capability can detect and notify individuals of activity that may constitute an incident. EventTracker's notification capabilities can route alerts to the appropriate individual based on group membership or relationship to the impacted system. EventTracker reports provide summary and detailed level reporting of incident based alerts. EventTracker completely automates the process and requirement of collecting and retaining audit logs. EventTracker retains logs in compressed archive files for cost effective, easy-to-manage, long term storage. Log archives can be restored quickly and easily, months or years later in support of after-the-fact investigations. Using EventTracker can identify authentication failures and successes across the infrastructure.
Reveal a unique identification (ID), e.g. the ID of the individual or process performing a function (this may be an anonymous or default account, or an automated ID, e.g. database process).	EventTracker captures log-in details for individuals or processes accessing information or executing commands within a company's asset base. This information can be searched, reported and alerted on.
Reveal the date and time of an event or function or series of related functions.	EventTracker preserves original date and timestamps for received logs, and by using the system it is possible to correlate and aggregate activity across a wide range of servers/devices and databases within the estate.
Identify the physical or logical address (or both) where the function took place (this could be a terminal address, boundary device port address or similar).	EventTracker receives log information across multiple platforms and it preserves the physical and logical information about activity on the network or servers, desktops, etc.
Reveal the type of service being executed, e.g. logon or logoff, boundary proxy service, address resolution, but particularly unsupported services or protocols, or services not approved within the terms of a security policy.	Reports can be established to mirror a client's security policy and to alert when behavior is identified outside the norm. New services started for instance, is a predefined report present on.
Identify the execution of privileged commands, e.g. to extend access rights, assume additional privileges, password changes, adjust boundary device configuration, backup and restore or archive operations.	EventTracker provides detailed reporting, analysis and real-time monitoring on privileged command execution across network device, servers, databases and applications including, but not limited to, extended access rights, access granted, and password changes, backup and restore operations, etc.

Subscription Process

Requirements	Netsurion Capability
4.5 Supply User Details Each LA must provide details of GCSx Users in accordance with the GC Directory User Template for initial population of the GC Directory. The template will be accompanied by appropriate guidance notes.	EventTracker can be a valuable tool in discovering and documenting the user base and provide this information in an easily exportable format. Simply providing the Active Directory list may not satisfy the GCSx requirement as it would not detail active users nor users who need the specific GCSx access.
5.3 Configure Server Equipment The LA is responsible for the configuration of their internal equipment (including router(s), firewall(s) and mail server(s)). The GCSx Pre-Connection Take On Guide provides an overview of the required configuration information. The technical information specific to each LA will be provided directly to each LA under separate cover. This information will be classified RESTRICTED and must be handled accordingly.	EventTracker can help to discover and document the asset base and identify all systems passing traffic through the network, and assist with transition to GCSx. EventTracker can also track configuration changes on internal equipment and hence detect when changes may have occurred that may compromise the GCSx connection requirements.
6.2 Re-submit (annually) CoCo Statement of Compliance GC will be responsible for auditing a percentage of LAs regarding CoCo compliance. CESG will be responsible for auditing the GC Process in this regard. CESG & OGC buying solutions will have access to any and all Documentation in this regard at any time.	Providing responses to external audit is extremely challenging, particularly when the system to gather the information is home-grown and does not have a preconfigured reporting engine. Intelligent reporting system that can rapidly (if not automatically) report on audit requirements as specified by GCSx, it can classify your events and incidents to align to Section 2.3 of the CoCo so that the reports generates are ready for submission to the auditors.

General Technical Requirements

Requirements	Netsurion Capability
Use of group logins should be restricted The key requirement here is for individual accountability, which of course can be weakened by the use of group logins. If a secondary login is required as part of established business process, you would be advised to investigate whether sufficient accountability is still offered. If this is in doubt, you should look at alternative means of enabling access to the required service that offers sufficient accountability.	EventTracker provides detailed analysis, reporting and monitoring of log-in activity. If the individual is not identifiable through the use of a group ID on a server, Event Tracker may be able to identify the individual through information captured via the application log.

General Technical Requirements *continued*

Requirements	Netsurion Capability
Information classified as "PROTECT and RESTRICTED" must have access to it logged. (Source- GC- Operational Support Guide).	EventTracker can align to a client's Information Classification policy and can monitor access to those documents in real-time. Specific alerts can be created to inform administrators or auditors of access to these files and the access must be logged and reported upon.
Identify the physical or logical address (or both) where the function took place (this could be a terminal address, boundary device port address or similar)	EventTracker receives log information across multiple platforms and it is possible to capture physical and logical information about activity on the network or servers, desktops, etc. In addition to the information contained in the original log message, EventTracker adds meta-data such as site, priority, direction, overall message description, etc
NISCC recommends a default deny policy Any network service that is not a business requirement should be blocked. This applies to all of the IP and TCP header fields that are subject to filtering, but to IP addresses and port numbers in particular. Logging all denied traffic is also recommended.	EventTracker can take logging messages from all forms of network and security devices and can report on all denied traffic. EventTracker can also be configured to monitor for traffic that should be denied, thereby ensuring effective firewall policies are in place.
Auditing and logging (including CDRs) must be enabled on the server. These logs should be reviewed regularly for security and access violations. Should the need arise to investigate an intrusion or abuse; logs should be stored for a period of time in accordance with an Organization security policy. Logs should be saved on a hardened logging server and backed up regularly, because the integrity of the logs stored on the source server cannot be guaranteed if there is an intrusion. The log server should only accept log entries from authorized machines. Enable system logging and logging of call detail records (CDRs). Regularly review logs for discrepancies. (Source- 15. NIST Security Guidance for VoIP Systems).	EventTracker can act as the centralized logging solution for VoIP logs. EventTracker can automate the review process and proactively monitor for access violations. EventTracker also provides an automated investigation (forensics) feature to detect and analyses intrusion or abuse; logs can be stored for a period of time in accordance with an organization's security policy. Logs are saved in a tamper-proof hardened logging which can be backed up regularly.

CoCo Section 2.3

Requirements	Netsurion Capability
Both the term 'event' and 'incident' are used in section 2.3 of the CoCo, but the term 'incident' is what is important in this section. An event is an observable change to the normal expected behavior of a system, whereas an incident is an event attributable to a human course and signifies malicious intent. To better understand the area of security incident management, refer to BS ISO /IEC 27002 (formerly 17799).	EventTracker can classify your events and incidents to align to Section 2.3 of the CoCo so that real-time alerts may be generated based on the risk to identify incident response occurrences. Reports automatically generated by EventTracker are ready for submission to the auditors.

IT Health Check Requirement

Requirements	Netsurion Capability
Scope of a typical ITHC includes: a. Network summary that will identify all IP addressable devices. b. Network Analysis, exploitable switches, gateways. c. Vulnerability analysis, patch levels, poor passwords, services used d. Exploitation (Optional), next step after a, b & c but LA should be aware of the danger of potentially crashing / making the system Unstable e. Summary Report with recommendations.	EventTracker can capture log information from all devices within a network, identify the devices within that network, and provide this in an easily exportable format.

GCSx Operational Support Guide

Requirements	Netsurion Capability
Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms: ▪ User challenge and authentication ▪ (username/password or digital ID/Certificate) ▪ Logging use at level of individual ▪ Firewalls and intrusion-detection systems and procedures; server authentication ▪ OS-specific/application-specific security measures.	EventTracker can split up tasks and keep log information organized through restricted analysts and alarm viewers. EventTracker can track an alarm status, delegate it to someone, change its current state (working, escalated), and add comments.

How Netsurion Can Help

Not sure where to begin? Netsurion helps you reduce cyber risk, augment your IT team's skills, and spend less time on documentation and compliance readiness. Contact us and our experts can advise you on the path to achieve GCSx CoCo preparedness.

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's managed platform approach of combining purpose-built technology and a team of cybersecurity experts gives customers and partners the ultimate flexibility to adapt and grow while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multilocation businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn.