

Government Connect:

Ensuring GCSx compliance in local government



Overview

As governments cast a wider net on their ability to share sensitive information among agencies, security requirements dictate that a sophisticated internal networking environment be developed. Government Connect (GC) is a recognised, 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.

GC is critical as it allows local authorities and central government to exchange information securely over a private network rather than the internet. This is of upmost importance for government at a time when episodes of data loss continue to appear in the press. In this regard, local authorities need to sign up to the Code of Connection (CoCo) that defines the minimum standards and processes that an authority must comply with before being able to connect to GCSx. Achieving compliance to the CoCo requires the local authority to provide a compliance statement and supporting comment against a number of security control measures.

Organisations need to be connected to the system by 31 March 2009. At that time, DWP will cease the provision of RESTRICTED data to local authorities and the receipt of "sensitive personal data" from local authorities through means other than a government approved secure IT communications channel. This essential measure means that all local authorities (LAs) need to make information security a top priority and to commit to completing the Government Connect implementation process without delay.

"Many businesses have found that data protection regulations cannot be taken lightly. One of the biggest challenges is proving compliance and LogLogic's MX2010 provides the perfect monitoring and reporting solution."

Paul Fisher
Editor, SC Magazine
July 2008

Automating Compliance. Mitigating Risk.

AWARDS AND REVIEWS



Log and Audit Requirements

The CESG Infosec Memorandum No. 22 lays out guidance on the development of a protective monitoring policy for information systems within government, its agencies, and related commercial organizations where they must conform with the terms of the Manual of Protective Security (MPS).

As per the memo, logs should record the following for users on your network:

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

Logs should be kept for a minimum of 6 months, including the use of backup tapes if necessary. They should be easily available for use as part of your incident response policy, as well as help with a wider CESG investigation. To fully comply with the controls (2.13.1 & 2.13.3), local authorities will need a central audit server that can pull the logs from all the devices and applications on the network into one location.

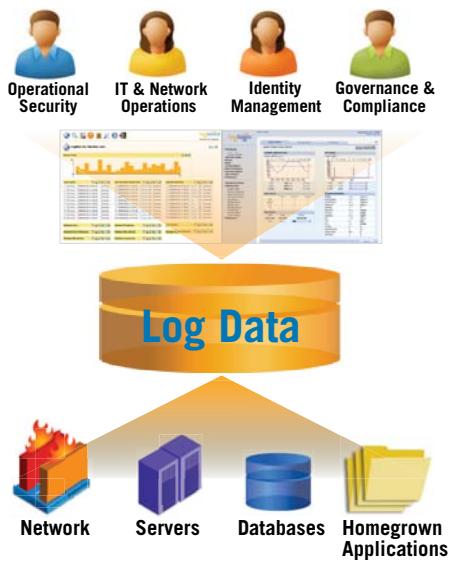
Meeting the requirements

LogLogic provides the undisputed leading Log Management solution, with its array of options from an open log services platform to a fully integrated log data warehouse, and multidimensional analytics. LogLogic caters for both large and small local authorities by providing a mixture of solutions to address different requirements. Organisations wishing to meet the GCSx requirements will find that the LogLogic solution will meet the requirements as well as offer substantial other security and operational benefits throughout the IT environment.

Key Benefits

- Speed of implementation
- Ability to collect all logs, including custom logs
- Forensic capability
- Reports to help evidence other controls within the GCSx framework.

The LogLogic Government Connect Solution: Open Log Management and Intelligence



LogLogic for Compliance

LogLogic 4 helps companies meet GC compliance by automating compliance activities and dramatically improve audit accuracy. Additionally, LogLogic 4 improves operations with automated, real-time reporting and alerting and the ability to map those reports and alerts to that meet the GC requirements of Memo 22. It accelerates time to risk mitigation, with the ability to search through terabytes of data in seconds. An integral part of its comprehensive LMI platform, LogLogic Compliance & Control Suites™ automate and simplify the process of using log data to evidence and enforce business and IT policies—and can be installed in minutes, delivering results in seconds.

LogLogic for Operations

Aside from security and compliance, logs help organizations address operational issues such as problem isolation, troubleshooting, service level and performance management, configuration and change management, capacity planning and business analysis. Advanced features in LogLogic 4 and embedded ITIL IT Services Management best practices reports make log data available for operational applications.

LogLogic for Security and Forensics

LogLogic reduces reporting and forensics requirements, like those found in the GC requirements, from weeks to months, boosting IT productivity and streamlining the audit process. LogLogic also enables data to be stored in a tamper-proof environment for use in litigation and investigations.

Multidimensional Log Analysis

LogLogic 4 is the first solution to deliver both search and normalization in a single platform. Together, search and indexed reporting provide universal log processing coverage of all log sources out of the box, including homegrown and custom applications. Normalization provides in-depth analytics and business intelligence for the most frequently used data center applications.

More Information:

Visit www.loglogic.com or contact a LogLogic representative by email: governmentconnect@loglogic.com or by phone: Tel: +44 (0) 870 351 7594

LOGLOGIC 4 FEATURES

- COLLECT
100% of log data, 100% of the time, from any device, including databases, servers and applications using a drop-in appliance and auto log source identification.
- ANALYZE
Industry-first combination of indexing and search technology with deep parsing and normalization—with reports and machine learning alerts available for known and unknown log data, real-time data and historical information.
- APPLY
Out-of-the-box search, reports and alerts, as well as deep compliance content in the form of Compliance & Control Suites. Customer and partner applications and mash-ups are available through the open web services API.
- RETAIN
Store raw and normalized log data in separate data structures, and protect the chain of custody over the archives for immutability. Replay and re-analyze any segment, any time for forensics and root-cause analysis.

JOIN OUR WEEKLY
DEMO AND FREQUENT
WEBCASTS. >>

Visit LogLogic.com
for more information.



LogLogic, Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Product Specifications are subject to change without notice.

©2008 LogLogic, Inc. All rights reserved. LogLogic is a trademark of LogLogic, Inc. All other products or services mentioned are the trademarks, service marks, registered trademarks or registered service marks of their respective owners.