

Achieving Compliance with GSi Code of Connection (CoCo) with *Lumension*[®] Solutions

May 2009

WP-EN-05-11-09

Introduction

In November 2005, The Government published 'Transformational Government – Enabled by Technology', which documents the steps necessary to achieve effective delivery of technology for Government. To develop the necessary trust and confidence within the Public Sector communities and between Government and the citizens, a common approach to risk management and the implementation of an Information Assurance framework becomes increasingly important.

The aim of the Code of Connection (CoCo) is to develop the trust required both within and between communities, which then allows more effective use of shared systems and services. The CoCo provides a minimum set of security standards that organisations must adhere to when joining the GSi.

This paper addresses some of the key challenges of achieving and maintaining compliance with the GSi Code of Connection (CoCo) for the GCSX.

Who Has to Comply?

Any organisation that is allowed to join the GSi, must comply with CoCo standards and submit to annual audits. These types of organisations include:

- » Home Civil Service departments and their executive agencies.
- » Non-Departmental Public Bodies - Other agencies and Non-Departmental Public Bodies (NDPBs).
- » Public Sector - The devolved administrations, regional assemblies and local authorities at any levels.

- » Other bodies - Those private organisations that deal with protectively marked information on behalf of government organisations.

What are the Code of Connection Standards?

The GSi central infrastructure is accredited and is continually reviewed by The Pan Government Accreditor. Although Cable & Wireless manages many of the risks facing GSi centrally, many risks facing the GSi are introduced by the connections from the GSi member networks. Participation in the GSi requires organisations to reliably identify and appropriately manage all risks associated with the network it intends to connect to the GSi central infrastructure. This includes:

- » vulnerabilities within or around the system or service;
- » threats that are in a position to exploit those vulnerabilities; and
- » the impact of any resulting compromises.

Organisations must be able to demonstrate that their risk management activities reduce the identified vulnerabilities to an acceptable level.

Challenges of Compliance

Organisations connecting to GCSx must first perform an audit of existing capabilities against CoCo requirements. Based on the audit findings the organisation must then complete the CoCo, including proposed resolution actions and timelines for those mandated controls marked as non-compliant. The completed CoCo must be sent by the organisation's Section 151 Officer to Government Connect.

The requirement for an annual health check for any GSi-connected system means that any drift from compliance can introduce significant remedial costs from a re-authorisation standpoint to ensure continued connectivity. Furthermore, organisations must ensure that:

1. Connections to external networks are approved;
2. Statements required for GSi authorisation are in place;
3. Appropriate security barriers between domains and the GSi central infrastructure exist;
4. Sensitive information is protected via encryption when required.

How Lumension Helps

Lumension solutions can help organisations reduce the cost of complying with the Code of Connection through a proactive approach to IT security and risk management.

[Lumension® Vulnerability Management](#) delivers automated vulnerability assessment and patch management through an integrated solution that enables local authorities to automatically detect risks, deploy patches and defend their business information across a complex, highly-distributed environment with greater efficiency and minimal impact to productivity. All of these activities are seamlessly integrated into a single management console for complete visibility into your network.

With [Lumension® Endpoint Protection](#), you can regain control of endpoints, such as desktops, laptops, servers, kiosks and POS systems, and the software that is executing on them. You can centrally manage, monitor, and control applications with a [whitelist](#) approach that allows only authorized applications to run - ensuring no malware, spyware, keyloggers, Trojans, worms, viruses, zero-day threats and unwanted or unlicensed software will execute on your network. IT and end-user productivity can also be improved by preventing unwanted applications from causing configuration issues and consuming network bandwidth.

[Lumension® Data Protection](#) enables local authorities to balance productivity and security challenges. Specifically, employees and partners need access to data; and more employees are working remotely

nowadays, thus requiring access from outside the network. However, the potential impact of data loss is a very real concern, be it accidental or malicious. And today, removable devices (such as USB flash drives) and media (such as CDs/DVDs) are the most common data leakage routes -- no file copy limits, no encryption, no audit trails and no central management. Lumension Data Protection enforces organisation-wide usage policies for removable devices, removable media, and data (such as read/write, encryption). Using a [whitelist](#) / "default deny" approach, administrators can centrally manage devices and data and enforce encryption of data.

The Local Government Association and the Society of Information Technology Management (SOCITM) published their guidelines for local council information security and data handling in November 2008. This was designed to provide a local government response to the Information Commissioner's "Data Handling Procedures in UK Government" published in June 2008.

In October 2008 the Information Commissioner, Richard Thomas reported to Parliament that a total of 277 data breaches had been reported to him in the twelve months following the HMRC loss of two CDs containing 25 million child benefit records in 2007. These information security incidents were reported from central and local government departments; the NHS; law enforcement; education; charities and the private sector. While Thomas acknowledged that this figure could reflect the fact that organisations have introduced more auditing in response to the Data Handling in UK Government Guidelines, nevertheless the local government document acknowledges that these incidents have

led to a loss of public confidence in the safety of their personal information. More recently, 7,851 un-encrypted children's records which were stored on a laptop stolen from the car of a Surrey County Council contractor, demonstrated that data held on portable storage devices represents a significant risk.

The Local Government Data Handling Guidelines, written by Paul Coen, Chief Executive of the Local Government Association and Steve Thomas, Chief Executive of the Welsh Local Government Association were written for local council staff at all levels in response to high profile losses of public data.

The guidelines call for all local councils to work to recover the public's trust in the government's ability to safeguard their personal information. The guidelines reflect the good practice set out in the ISO/ IEC 2700 Information Security Management Systems and set out the fundamental steps that every council should take to mitigate risks to information.

In particular, the local government guidelines call for the appointment of a Senior Information Risk Officer (SIRO) to be appointed by each local council to ensure accountability for the protection of citizens' information. The guidelines call for councils to foster a culture where all staff recognise that personal information is a precious asset and take all reasonable steps to protect it. While acknowledging that no council can ever claim to be immune from data security breaches, the local government document defines best practices that all councils must strive to consistently meet or exceed, so that the public can be reassured that all reasonable steps have been taken to protect their information.

The following document provides a summary of the key parts of the local government guidelines and demonstrates how the Lumension solution portfolio helps local councils to ensure that best practice is consistently followed when assessing and removing risks to citizens' information.

Requirements Mapped to Lumension Solutions

Please review the table below to learn more about how you can utilise Lumension solutions to address many critical CoCo requirements which are also mapped to BS ISO/IEC 27001:2005.

CoCo Requirements (ISO 27001 cross-reference)	How Lumension Addresses CoCo Requirements
Incident Response	
2.3 : (ISO27001 13.11)	Lumension Endpoint and Data Protection can log any attempts by users to bypass the corporate policy for device and application usage at an endpoint. This information can be viewed either by scheduling regular reports, or logs can be sent to third party products for consolidated security log alerting.
IP Addressing	
2.7.1 : (ISO 27001 11.4.7)	<i>Lumension</i> ® Security Configuration Management, a component of Lumension Vulnerability Management, can be configured to detect for this setting as an incorrect configuration on servers or workstations. This would appear in the reports allowing appropriate actions to be taken to correct the issue.
Intrusion Detection	
2.9 : (ISO 27001 11.4.7)	As 2.7.1
2.9.2 : (ISO 27001 11.4.7)	As 2.7.1
Mobile Working	
2.10.2 : (ISO 27001 11.4.7)	Lumension Data Protection can ensure that any removable media, including USB removable storage and CD/DVD are encrypted with AES 256 Bit encryption. FIPS 140-2 and CAPS approval is in process for the Lumension Encryption Kernel.
2.10.3 : (ISO 27001 11.4.7)	Lumension Data Protection can ensure BlackBerry devices cannot be used as replacements for approved encrypted removable storage by controlling access to all devices that connect through any connection method to an endpoint, including, but not exclusively USB and Bluetooth.

Achieving Compliance with GSi Code of Connection (CoCo) with Lumension Solutions

CoCo Requirements (ISO 27001 cross-reference)	How Lumension Addresses CoCo Requirements
Proxies	
2.11 : (ISO 27001 11.4.7)	As 2.7.1
2.11.2 : (ISO 27001 11.4.7)	As 2.7.1
2.11.3 : (ISO 27001 11.4.3)	As 2.7.1
2.11.4 :	As 2.7.1
Protective Marking	
2.13 : (ISO 27001 10.10.1)	Lumension Endpoint and Data Protection provide the ability to monitor user behaviour with regards to application and device access. Suspicious application and device access can be notified to the user locally and to centralised administrators. Users under particular suspicion can have their device access shadowed, this allows administrators to record file names or cache an exact copy of any data that is imported or exported from the system onto approved external devices.
2.13.1 : (ISO 27001 10.10.6)	<p>The reporting console within both Lumension Endpoint and Data Protection allows administrators to view comprehensive information about users' application and device access. Administrators can configure their own custom log requirements to ensure they see the data they require. For example a user plugging in a BlackBerry via USB is recorded as one event type, however if a user were to attempt to read or write data to the BlackBerry this is a separate event type. This granular logging and reporting allows more focused investigations into genuine attempts to subvert security, or in certain circumstances highlights a new business requirement.</p> <p>Lumension Scan's comprehensive reports are stored as required to identify system vulnerability trends to ensure compliance drift does not affect the secure posture of the system.</p>
2.13.2 : (ISO 27001 10.10.6)	As 2.7.1
2.13.3 : (ISO 27001 10.10.3)	Lumension Endpoint and Data Protection can retain logs for as long as required, with simple routines to delete or archive data beyond a retention policy.

Achieving Compliance with GSi Code of Connection (CoCo) with Lumension Solutions

CoCo Requirements (ISO 27001 cross-reference)	How Lumension Addresses CoCo Requirements
Operating System	
2.14 : (ISO 27001 11.6.1)	As 2.7.1
2.14.1 : (ISO 27001 11.6.1)	As 2.7.1
Configuration	
2.15 : (ISO 27001 12.15.1)	As 2.7.1 If templates for hardened hosts are required these can be downloaded from http://nvd.nist.gov/scap.cfm .
Software Policies	
2.16 : (ISO 27001 12.4.1)	Lumension Endpoint Protection uses an application whitelisting approach which covers all types of executable code. With this approach it is not possible for any applications, dlls, etc. to execute – protecting the hosts from malware, unlicensed and unwanted applications, Zero-day attacks, and enforcing software change control policies. Lumension Scan also provides the ability to detect where configurations have been changed from the required state to comply with the CoCo and highlight these as issues to be resolved.
2.16.1 : (ISO 27001 12.4.1)	as 2.16

CoCo Requirements (ISO 27001 cross-reference)	How Lumension Addresses CoCo Requirements
Patch Management	
2.17 : (ISO 27001 12.6.1)	<p>The Lumension Vulnerability Management solution delivers automated vulnerability assessment and patch management through an integrated solution that enables businesses to automatically detect risks, deploy patches and defend their business information across a complex, highly-distributed environment with greater efficiency and minimal impact to productivity. All of these activities are seamlessly integrated into a single management console for complete visibility into your network.</p> <p>The Lumension Vulnerability Management solution provides audits and remediation with wide support across major OS platforms (Windows, Linux, MacOS, Sun Solaris, HP, etc.), POSIX and infrastructure devices.</p> <p>Vulnerability audits include security configurations, OS and application vulnerabilities, null passwords, patch-level related vulnerabilities, known hacking tools, malware, common worms, and P2P software checks.</p>
2.17.1 : (ISO 27001 12.4.1)	<p>Lumension has a dedicated team which works with software vendors to ensure software patches are identifiable and can be remediated. Lumension Patch and Remediation™, a component of Lumension Vulnerability Management, provides a flexible platform to deploy patches in a sensible manner to ensure business continuity as well as patch compliance.</p>
2.17.2 : (ISO 27001 12.4.1)	<p>Lumension Endpoint Protection by default will deny any applications not on the approved list. If a particular piece of software was currently in use and subsequently deemed un-patchable an administrator could remove this application from the whitelist and endpoints would be updated accordingly.</p>

CoCo Requirements (ISO 27001 cross-reference)	How Lumension Addresses CoCo Requirements
<p>2.17.3 : (ISO 27001 12.5.1)</p>	<p>Lumension Scan is able to identify out of date software with known vulnerabilities. The vulnerability reports will highlight where a known upgrade path is available. This enables the organisation to identify an upgrade path for un-patchable software where a known vulnerability exists.</p> <p>If required the unpatchable software can be automatically removed or denied execution using Lumension products</p> <p>Where there is no upgrade path available Lumension Application Control's approach of only allowing trusted applications can be used to ensure the risk from un-patched software is mitigated.</p>
<p>Vulnerability Scanning</p>	
<p>2.18 : (ISO 27001 15.2.2)</p>	<p>Lumension Scan and Patch and Remediation provide the ability to identify security vulnerabilities on a regular basis. By default the Patch and Remediation client checks once each day to determine compliance with mandatory baselines and scheduled deployments, whereas scans and reports can be run as often as required.</p> <p>Typically this would be a monthly cycle as most software vendors use a monthly cycle with occasional critical patches being made available as and when necessary.</p> <p>Once the new software patches become available Lumension Patch and Remediation will show these as unresolved vulnerabilities in the next reports, ensuring that critical vulnerabilities are more difficult to miss.</p>
<p>2.18.1 : (ISO 27001 15.2.1)</p>	<p>As 2.7.1</p>
<p>2.18.2 : (ISO 27001 15.2.1 & 15.2.2)</p>	<p>Lumension Scan is a network and credential-based scanner and therefore requires very little resources on the target being scanned. It also uses an approach which does not attempt to exploit a vulnerability, but instead uses defined fingerprints to determine the existence of a vulnerability and is run from a dedicated machine. The result of this is an agent-less, secure approach to scans which cannot cause a machine to blue screen during a check.</p>

Achieving Compliance with GSi Code of Connection (CoCo) with Lumension Solutions

CoCo Requirements (ISO 27001 cross-reference)	How Lumension Addresses CoCo Requirements
2.18.3 : (ISO 27001 15.2.1 & 15.2.2)	Lumension works with major software vendors to ensure that signatures are up-to-date and provide accurate vulnerability detection. Lumension Patch and Remediation is supported by these vendors with regards to the detection and remediation of vulnerabilities.
Web Browsers	
2.19 : (ISO 27001 11.2.2)	As 2.7.1 (using Lumension Security Configuration Management) If templates for hardened web browsers are required these can be downloaded from http://nvd.nist.gov/scap.cfm .
2.19.1 : (ISO 27001 11.2.2)	As 2.7.1
2.19.2 : (ISO 27001 10.4.2)	As 2.7.1
2.19.3 : (ISO 27001 10.4.2)	As 2.7.1
2.19.4 : (ISO 27001 10.4.2)	As 2.7.1 This can be detected with Lumension Scan but can also be controlled using Lumension Endpoint Protection as the Java Virtual machine would not be allowed to run unless it was placed into the whitelist of applications.
Content Analysis	
2.20 : (ISO 27001 10.4.1)	Lumension Endpoint Protection will intercept execution of all application code, both good and bad, and check their validity against the whitelist before it can execute on a workstation or server which is protected. This content analysis is carried out on a hash of the executable code to maintain integrity of the system. This ensures that no virus, malware, unwanted application can be executed on the endpoint. This technology is complimentary to standard anti-virus products which in many, but not all, cases will stop the code being transferred if the system has been configured correctly.

Achieving Compliance with GSi Code of Connection (CoCo) with Lumension Solutions

CoCo Requirements (ISO 27001 cross-reference)	How Lumension Addresses CoCo Requirements
Personal Firewalls	
2.21 : (ISO 27001 11.4.6)	As 2.7.1
2.21.1 : (ISO 27001 12.4.1)	As 2.7.1
2.21.2 : (ISO 27001 11.4.6)	As 2.7.1
Macros	
2.22 : (ISO 27001 10.4.2)	Lumension Endpoint Protection can allow granular access to executables and can also whitelist macros and scripts if required.
2.22.1 : (ISO 27001 10.4.1)	As 2.7.1
Removable Media	
2.23 : (ISO 27001 10.4.1)	<p>Lumension Data Protection by default denies access to all devices to provide the highest level of security. Therefore all removable media including: CD/DVD, USB Drives, External Hard Disks, Floppy Drives, Bluetooth connected devices and more are denied connection to a protected endpoint.</p> <p>Access can be granted by user or group via Microsoft Active Directory or Novell E-Directory and one of Lumension Data Protection's major assets is the granular levels of access that can be provided. For example one user could be granted access to all devices, whereas another could be allow to use only a serial numbered USB key for their particular job role.</p> <p>Lumension Data Protection can also force encryption using an AES 256 bit algorithm on both CD/DVD and USB removable storage. If required this can be configured such that the data can be shared with non-Lumension users by means of a passphrase, with no product installation or administrative rights required on the non-Lumension managed endpoint.</p>

CoCo Requirements (ISO 27001 cross-reference)	How Lumension Addresses CoCo Requirements
<p>2.23.1 : (ISO 27001 10.4.7)</p>	<p>Once an approved removable media device has been connected, Lumension Data Protection simply allows the operating system to access the device as normal, enabling typical anti-virus products and Lumension Endpoint Protection to ensure no virus-laden files can be transferred or accessed by the user.</p> <p>Where necessary Lumension Data Protection can also apply granular file type filters to ensure only approved file types are transferred either to or from the approved removable media. This becomes most useful with devices such as digital cameras, to allow only the import and export of image files. The file filters are content and header-based to ensure a simple file re-name does not allow the transfer of unapproved data.</p>
<p>E-Mail</p>	
<p>2.24 : (ISO 27001 10.4.1 & 10.4.2)</p>	<p>As 2.7.1</p>
<p>2.24.1 : (ISO 27001 10.4.1 & 10.4.2)</p>	<p>As 2.7.1</p>
<p>2.24.2 : (ISO 27001 10.4.1 & 10.4.2)</p>	<p>As 2.7.1</p> <p>Lumension Data Protection can also provide this functionality for removable media.</p>
<p>2.24.3 : (ISO 27001 10.4.1. & 10.4.2)</p>	<p>As 2.7.1</p> <p>Lumension Data Protection can also provide this functionality for removable media.</p>
<p>2.24.4 : (ISO 27001 10.4.1 & 10.4.2)</p>	<p>As 2.7.1</p> <p>Lumension Data Protection can also provide this functionality for removable media.</p>
<p>2.24.6 : (ISO 27001 10.4.1 & 10.4.2)</p>	<p>As 2.20</p>
<p>2.24.7 : (ISO 27001 7.2.2)</p>	<p>As 2.7.1</p>

Implications of Non-Compliance

Some organisations may not fully meet all the mandatory controls of the GSi Code of Connection either at the time of connection or during some point during the lifetime of GSi service being provided. This will result in the connection being assigned the following status:

- » Compliant – All mandated controls are in place.
- » Minor non-compliance – Partial implementation of a minority of the mandated controls.
- » Major non-compliance - Failure to implement a mandated control or only partial implementation of a significant proportion of mandated controls.

Major non-compliances will follow a documented escalation process of four escalation points. If an organisation does not achieve compliance within this process, sanctions may be applied. Sanctions may include, but are not limited to:

1. Enforced audit against the GSi Code of Connection
2. Restriction of available bandwidth
3. Restriction of available Internet facing protocols (e.g. no access to the WWW)
4. Restriction of available intranet protocols (e.g. use of mail only on the GSi)
5. Disconnection of a particular part of the Customer's service (e.g. a non compliant application or third party connection)
6. Disconnection from the GSi

Conclusion

Lumension's approach significantly reduces the cost and difficulty of achieving CoCo compliance and reduces the risk of policy drift by ensuring that systems maintain a trusted state. Lumension also enables organisations to effectively protect against unknown threats to systems and data through:

- » Regularly automated scanning and remediation of operating system and applications vulnerabilities and insecure configurations.
- » Policy-based enforcement that enables only trusted applications to execute and thus preventing malware and zero day attacks
- » Policy-based enforcement of removable device usage and data encryption that enables only trusted devices to be accessed by only trusted users, and if necessary allows only trusted file types into the system.

About Lumension

Lumension, a global leader in operational endpoint security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets.

Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, and Reporting and Compliance offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year.

Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Virginia, Florida, Luxembourg, the United Kingdom, Spain, Australia, India, Hong Kong and Singapore. Lumension: IT Secured. Success Optimized. More information can be found at www.lumension.com.



Key Steps to Ensuring CoCo Compliance

Quantify your risk of unmanaged USB Devices

with *Lumension*® Device Scanner Pro



Identify unwanted applications

with *Lumension*® Application Scanner



Assess your security posture

with *Lumension*® Vulnerability Scanner



Protect Your Vital Information Today

Protect Your Data

with *Lumension*® Endpoint Security Suite

Free Trial Offer



Manage Your Critical Risk Today

Manage Your Critical Risk

with *Lumension*® Vulnerability Management

Free Trial Offer

