



GC Communicate

3 weeks to go ... Next steps for your Local Authority!

With the Data Access Policy deadline of 31 March 2009 fast approaching, many local authorities are now completing the final iterations of their CoCo in preparation for final approval. We would like to thank every LA that is working very closely with the team to reduce the number of outstanding actions on their assessment in preparation for approval. Please do continue to work towards reducing the number of actions and to resubmit your CoCo for next assessment as soon as possible.

Please note that we are currently assessing a large number of CoCos, which has affected our assessment turnaround. If your CoCo is in for formal assessment please be assured that we will return it to you as soon as possible.



Do remember that if, upon receipt of the CoCo Assessment, an LA believes that there is a risk to their achievement of compliance by the required date, LAs should:

Write (from 151 Officer) to Philip Littleavon and Anna Smith

- Providing specific details of the issue in an action plan
- Providing commitment for the LA to achieve compliance by the proposed revised date

GC may convene a conference call with the LA to discuss the issue and decide the most appropriate course of action and will respond formally to the request.

Preparation for local configuration

In addition, those LAs that have received their RESTRICTED configuration dataset should book a slot with the Configuration Team on the earliest date possible to make best use of the available resources.

LAs that have reached a certain level of compliance will be contacted by our Configuration Team to book the consultant's support day to help with your local configuration. We have permission from OGCbs to complete this before full compliance so that LAs can be operational as soon after compliance with the CoCo as possible (simply re-activating the GCSx circuit). In preparation for this, please ensure that you:

- Complete your pre-configuration checklist and return to the team (RESTRICTED datasets will be sent to LAs as soon as they have reached the appropriate level of compliance)
- Plan to complete any local changes as early as possible, so that we can complete your local configuration in advance of 31 March 09 deadline (please do be as flexible as possible with dates rather than waiting until the last week in March)

Finally, please do raise any further issues with the team to gctech.team@dwp.gsi.gov.uk, and most importantly, please do stay in touch.

Anna Smith, Implementation Manager

Come and join Philip Littleavon speaking at:

**NWeGG Spring
Full Members Meeting**
18 March 2009
Liverpool

Mobile Government Conference
24 March 2009
QEII Centre - London



How secure is LA Remote Access?

Citizens rightly demand that personal data is properly handled and access controlled. Remote access and mobile media are particular challenges, in that they provide a 'soft underbelly' for physical and virtual attack on systems, such as hacking. Furthermore, we risk losing public confidence when we misplace or mishandle remote devices containing secure data. And yet, this way of working is fast becoming a necessity within Local Authorities.

Whilst local authorities have been, and are, innovative, CESA security standards have highlighted weaknesses. Prior to GCSx, councils were not assessed against industry standards for remote access. A secure system of remote access is part of the CoCo process (although the GCSx network does not technically impact on remote working).

The vast majority of Local Authorities are now acting positively to correct these weaknesses. Networks are assured and risk assessed against confidentiality, integrity and availability. In fact, the government data that is accessed across GCSx includes Impact Level 3 (IL3) Restricted data, e.g. DWP's CIS database.

CoCo compliance also demands dual factor authentication on remote network access, in order to reduce the threat of attacks against LAs. Normally this is a card or token based solution which confirms the user identity i.e. authenticates. It offers an additional assurance that users are who they say they are, and not just someone who has gained access to the system and passwords.

When data is accessed by remote systems, some



of this data may still be cached on the PC. This data is retrievable using specialist tools that can be deployed by unauthorised as well as authorised persons. Such a PC could cause considerable embarrassment, as a minimum if it falls into the wrong hands. This is one reason why CESA insists that PCs must be appropriately encrypted and consideration given to disposal.

Although there are thin client systems that claim not to leave information on PCs there are compliance difficulties if these are not correctly configured. There is a need for appropriate control at the end points where they sit outside the LA network.

A further risk is that the PC might not be maintained at the right patch level i.e. all operating system updates are applied. This could include essential security patches which would leave the PC (and hence the network) exposed if not properly controlled. This is not possible if the PC is owned by the individual rather than the organisation.

Remote working brings inherent risks which can certainly be mitigated through checks and balances, outlined within the CoCo process. GC presents an immediate opportunity to put those checks into place sooner rather later before it's too late.

What do you need to do next?

- Agree a plan for CoCo re-submission with the central support team.
- Schedule your free configuration visit
- Should your authority's circumstances change please keep in touch with the support team: gctech.team@dwp.gsi.gov.uk
- Monitor the Government Connect website & newsletters for updated information

If you were granted an exemption, keep working towards going live on the agreed date. This includes meeting the agreed actions, staying in contact with Government Connect if you have any questions and submitting your Code of Connection in time to meet your revised Go Live date.

If you are already live with GCSx and have any operational problems, please refer to annex i of the [operational support guide](#) or contact the service desk at 0800 505 3375 / it.servicedesk@tameside.gov.uk

Devon Trading Standards Special Investigation Unit

Devon County Council's Trading Standards Service maintains an environment for local businesses to compete on equal terms and ensures that consumers are not compromised by unfair or illegal trading practices. It fulfils its mission in collaboration with other agencies and stakeholders.



The Special Investigation Unit (SIU) sits within the Trading Standards Service and looks into complex cases of consumer fraud; supports and

champions investigations requiring specialist techniques; leads on the countrywide service response in relation to level 2 criminal activity; acts as a focal point for service improvement using intelligence, and as the single contact point for technical and service compliance with human rights legislation.

The SIU currently sends and receives information through post, fax and non-secure email. There are clearly associated risks and costs with each of these methods. GC Mail uses infrastructure provided by the Government Connect Secure eXtranet (GCSX) to deliver emails securely, integrating seamlessly with secure email systems in the wider Government Secure Intranet (GSi) community.

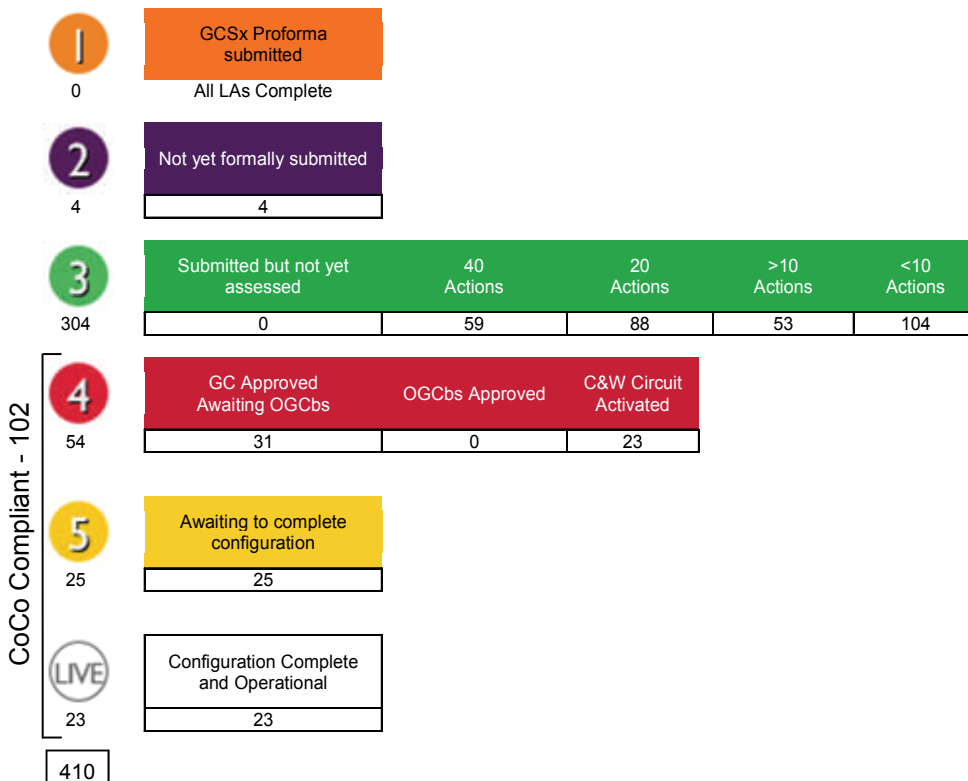
GC Mail is now the preferred communication option for many central government departments and agencies, and has been adopted as the standard by Devon Councils.

The SIU is exploring the following options using GC Mail:

- Sharing council tax, housing benefit and electoral roll data with Devon Councils (rather than via fax)
- Requests to Police regarding previous convictions
- Registering court cases for recording purposes
- VAT returns/references with HMRC
- NHS related campaigns
- Beating scams, counterfeiters and rogue traders through the exchange of sensitive information with cross-border councils



LA Connectivity Progress (as on 11 March 2009)



News from across the regions - ICT Policy Pack

The West Midlands LGA and the West Midlands Regional Improvement and Efficiency Partnership jointly provided funds to develop a pack of policies, to support local authorities in the region to secure compliance with their Government Connect Code of Connection.

A project manager was employed, to work with regional councils in developing the pack of policies. The pack is now complete and is freely available to local authorities to implement, as they see fit, locally.

[Download full pack and policies](#)

Contact GC:

CoCo Support: 0845 838 2945
gctech.team@dwp.gsi.gov.uk

Communications:
geeta.vara@dwp.gsi.gov.uk

General enquiries:
gc.info@dwp.gsi.gov.uk

