ITEM No.3

Audit Committee

6th March 2009

Information Security: ISO27001 Compliance Report

Report of Jim Cox, ICT Project Leader (Information Security)

Purpose of the Report

1 An ISO27001 Compliance Progress report dated 26th November 2008 was issued to the Chair of the Audit Committee in December 2008. This report provides details of the progress made since then, towards compliance with ISO27001 for its Information Security policies and procedures.

Background

2 In 2001, following the preparatory work done to avoid any possible Y2K disasters, DCC started work on putting in place Policies and Procedures that were compliant with British Standard 7799 (Information Security). The standard was upgraded to ISO 17799 and then renumbered to ISO 27001.

3 Risk Register Update

As was reported in November, a recent compliance assessment has highlighted the:

a) Need for a Risk Register revision to allow for an Asset Inventory update. This has been planned for February 2009 and will be performed in line with corporate risk management techniques, involving both the Corporate Risk Manager (David Marshall) and the Customer Services Risk Manager (Peter Lunn);

UPDATE: The revision of the Risk Register is nearing completion by the Customer Services Risk Manager and the ICT Project Team Leader (IS). The Corporate Risk Manager will then be involved in its sign off.

b) Sign-off of all IS documentation, by the IS Forum, so it can be posted on the Intranet IS page;

UPDATE: The IS Forum will be asked to sign off the Human Resources Arrangements, Operational Procedures and System Development and Maintenance documents at its meeting on Thursday 26th February 2009. These documents will then be added to those already available on the IS page of the Intranet. The Personal Information Security Policy is also due to be signed off on 26th Feb 2009, which will allow the outmoded Laptop Usage Policy and the Policy & Code of Practice for Use of the Internet & Email to be removed.

c) Sign-off, by the IS Forum, of Business Continuity test plans;

UPDATE: In line with National guidelines, the Business Continuity Plan has been renamed as the Business Contingency Plan. Unfortunately, no information has been received from the Service Representatives on the corporate Emergency Co-ordinators Group (chaired by the Civil Contingencies Unit) regarding the priority given to the re-establishment of services. This information was requested via the minutes of the last Co-ordinators Group meeting in December 2008. A draft copy of the Plan will be posted on the Intranet page marked "(under review)".

d) Revision of the Statement of Applicability as, and when, the Information Technology Infrastructure Library (ITIL) framework is deployed (as part of BSF);

UPDATE: Delays in the progress of the BSF project have meant that a revision of the Statement of Applicability has not yet been appropriate.

e) Endorsement of the IS Policy by the recently appointed Chief Executive.

UPDATE: George Garlick endorsed the IS Policy in December. A copy of the Policy will be available on the IS page of the Intranet from Monday 2nd March 2009.

4 Information Governance

Information Security is an integral part of Information Governance, along with Data Quality Assurance, Records management and Information Risks. The move towards ISO compliance has been made ensuring that all these elements have been considered throughout the process.

As part of a corporate initiative the following five top information security risks were identified:

- Theft of valuable/attractive assets
- System failure
- Disclosure of Council Information
- Unauthorised logical access
- Misuse of portable/personal equipment

Guidance to minimise each of these risks is provided in the IS documentation that has been produced; more specifically; the IS Manual, the Personal IS Policy, the Logical Access Policy and the Business Continuity Plan.

The recent corporate implementation of the MicroSoft SharePoint system has ensured that workflow techniques are available to ensure an automated end-to-end approach to Information Governance.

UPDATE: Progress made with the SharePoint development has been slower than expected due to the product's limitations. However, guidance obtained from external sources has moved the project along. This situation should not impact upon obtaining compliance with the ISO standard.

Recommendations and reasons

5 An IS training plan has been discussed with corporate HR, which is to be supported by an on-line IS system, ensuring all members of staff agree to abide by all relevant DCC IS policies and procedures. These policies and procedures, along with all other relevant IS documentation, are available on the DCC Intranet IS page.

UPDATE: Unfortunately, the server hosting the on-line IS system - CETIS – crashed and was irreparable. A replacement system is being sought which will meet the increased needs of the new Unitary Authority. A number of on-line training systems are already in use by DCC Services and the intention is to utilise one of them to host the IS information.

Investigating the options available will take some time, so it is unlikely that a system will be in place when the compliance assessment takes place in mid March 2009. However, if a decision has been made on the choice of system and an implementation/development plan agreed then the assessor might regard our situation sympathetically.

In order to ensure that DCC continues to move towards ISO27001 Certification, a full-time IS officer needs to be identified who can make sure that all the policies and procedures are maintained at an appropriate standard. This officer should report to a Chief Information Officer (or equivalent) based in central service support.

UPDATE: No full-time IS Officer has so far been appointed and it would appear that the structure for the new Unitary Authority contains no provision for one. The LGR Information Management workstream has already made a suggestion that this discipline would best sit in the Deputy Chief Executive's Office – along with the other disciplines associated with Information Governance.

Contact:	**Jim Cox**	**Tel:**	**0191 370 8638**

Appendix 1: Implications

Local Government Reorganisation
(Does the decision impact upon a future Unitary Council?)

The medium term aim is to gain advanced compliance for the new Unitary Council shortly before the ISO27001 standard is revised in 2010.

Finance

A Strategic Support Agreement with Sapphire Technologies costs approximately £20,000 annually.

UPDATE: The on-line system to house the IS information should cost approximately £2,000 per annum for support and maintenance.

Staffing

One member of staff is needed to ensure compliance with all policies & procedures developed.

UPDATE: It is likely that more than one full-time member of staff will be needed as the policies and procedures need to be reviewed and updated on a regular basis. Also, the on-line IS system will need developing and maintaining, especially when the ISO standard is reviewed and updated.

Equality and Diversity

All policies and procedures are developed for the benefit of all members of staff and are available on the DCC Intranet. Should they be needed, copies can be produced in Braille, large print and in a variety of languages.

Where appropriate, plain English is used.

Accommodation

N/A

Crime and disorder

The Information Security Officer at Aykley Heads Police Headquarters has been involved in the production and review of all policies and procedures.

The main purpose of producing the policies and procedures is to provide DCC members of staff with guidelines so that they can avoid situations where crime and disorder becomes an issue.

Sustainability

By ensuring the most efficient and effective use of ICT equipment, DCC staff can minimise the need to replace ageing hardware. Also, by protecting the same equipment - especially when teleworking - the working life of the hardware can be maximised.

When equipment does need to be replaced, DCC always strives to purchase the most sustainable products that meet the business needs of the user.

UPDATE: Disposal of ICT equipment is always done in the most environmentally friendly way.

Human rights

N/A

Localities and Rurality

By providing guidance on the most secure way of using ICT equipment when “out and about”, DCC is attempting to make sure services can be delivered locally, where appropriate.

Young people

The policies and procedures apply equally to young people as to all other classifications.

Consultation

All Services within DCC, as well as all District Councils, have been involved in the production of the policies and procedures - along with the ISO at the Police Headquarters (see Crime & Disorder above). Expertise from Sapphire Technologies has also benefited the project.

Health

The guidance included in the policies and procedures is designed to minimise any adverse effects of using ICT equipment.