

Audit and Scrutiny Committee

Dorset County Council



Date of Meeting	20 November 2008
Officer	Director for Corporate Resources
Subject of Report	Information security management – planned activity and progress
Executive Summary	<p>The report provides an overview of the programme of work to become compliant against the international standard for information security management (ISO 27001/2) for electronic information.</p> <p>The report also summarises other improvements, or planned improvements, to our information security management capability.</p>
Budget/Risk Implications	None specifically arising from this report. There are budget and risk implications arising for the work programme, which are being managed or monitored as appropriate by the Information Systems Strategy Group and Internal Audit.
Recommendation	That the Committee considers the work programme and progress made to date.
Reason for Recommendation	To support the Council's strategic aim of building a Council fit for the future.
Appendices	None
Background Papers	None
Report Originator and Contact	<p>Name: James Ailward Tel: 01305 221130 Email: j.a.ailward@dorsetcc.gov.uk</p>

1. Background

- 1.1 The Head of ICT Systems and Strategy presented a report on the subject of information security to the Committee on 15 January 2008, in the light of the well publicised losses of electronic information by government agencies. This report advised that the Authority should seek to become accredited to the International Standard for Information Security (ISO 27001/2).
- 1.2 It was noted that the level of investment required to become secure should be appropriate to the value of the information in question. It was also acknowledged that it was necessary to ensure that the importance of information security, and their resultant responsibilities, was understood by individual members of staff.

2. Progress towards ISO 27001

- 2.1 ISO 27001 for Information Security Management can be applied to any defined organisational or functional scope within an organisation. Attempting to apply this to the whole organisation for paper and electronic information is an enormous task.
- 2.2 Consequently, the Information Systems Strategy Group (the cross-directorate officer group responsible for overseeing strategic management of ICT matters) has commissioned work to become compliant to ISO27001/2 for all electronic information systems as a first step to becoming fully compliant across the wider Authority (if the business case stands for full accreditation). The ICT elements account for a significant proportion of the controls for the whole authority.
- 2.3 The outline work programme for delivering against ISO 27001/2 across the ICT function is as follows:

Planned activity	Completion date
○ Gap analysis by Internal Audit partner Deloitte	Complete
○ Review and creation of security policies, standards and guidance	December 08
○ Security incident management	January 09
○ Security awareness and training programme	January 09
○ Formal risk assessment	February 09
○ Baseline and implement risk controls	September 09
○ Initiate review and audit processes - formal 6 month review period	September 09

3. Other improvements achieved or planned

- Other activity has been implemented or planned to improve the secure handling of information since the report to the Committee in January of this year:
- 3.1 The County Management Team on 31 October 2008 approved a revision to the responsibilities of the Information Systems Strategy Group to encompass a strategic responsibility for development of a strategy and plan for the management of information – this includes compliance with data security obligations.
- 3.2 The Authority's Data Protection Officer has published several articles on Staffnet regarding issues of concern around the secure handling of personal or confidential

information. Further articles are planned in tandem with the ICT Security Officer.

- 3.3 Enhanced password security has been implemented across the whole council ICT network - longer passwords are now stipulated with more frequently and consistently applied password changes enforced.
- 3.4 A new range of remote working solutions provides an appropriate level of security compliant with the ISO 27001 controls, including encrypted hard discs, secure switching on of PCs, increased password security and secure connections back to the council network where required.
- 3.5 We are committed to becoming compliant with the level of security required to join the Government Connect Secure Extranet by the end of this financial year – this will allow secure exchange of information between local and central government agencies, and health, police and fire authorities.
- 3.6 We have a solution in place (called ShareFile) which allows the secure transfer of data files to 3rd parties without the use of email. This is in use in Exchequer Services and is being planned for introduction to Financial Services.
- 3.7 We have the Criminal Justice Secure Email service in place for Youth Offending and other teams - this is being rolled out currently across Adult Services and Childrens' Services directorates.
- 3.8 IT Services have engaged with Internal Audit in their review of information security measures both in place and planned, resulting from a letter from the Home Office to the Chief Executive.

Elaine Taylor
Director for Corporate Resources