

**Choose your engineering test:** Fire Pressure Blast

E-records patchy, audit finds

Chris Jenkins

OCTOBER 13, 2006

AN audit of three federal agencies has found a patchy approach to electronic record-keeping.

The audit, which examined the record keeping practices of the Attorney-General's Department, the Australian Electoral Commission and the Department of the Prime Minister and Cabinet, examined all facets of the agencies' archiving practices.

All three agencies used a mixture of paper-based and electronic systems. But the audit found electronic records caused particular problems, echoing findings from two previous reports.

"The records held in the majority of the electronic systems reviewed as part of the audit were not being managed in accordance with the entity's recordkeeping policy," auditors found.

Record keeping requirements were generally not considered in plans for new IT systems and systems not designed for record keeping were often being pressed into service for archiving.

A perennial issue in audits of government departments, user access control, was also flagged as a problem area.

"Audit testing of user access procedures and their implementation found that although appropriate procedures were in place in two entities, the procedures were not consistently implemented."

In addition, some systems did not define which functions a user would be given access to, while in other cases, the user accounts of employees that had left the agency had not been deleted.

"The ANAO considers that these practices compromised the information contained in system audit logs and the ability of the entity to trace the actions of users. It also meant that there was no record of users whose access had been terminated," the audit report says.

In addition, two of the three agencies audited did not keep sufficient record metadata to meet Commonwealth guidelines. In most cases, electronics records system security also fell short of mandated requirements.

"The ANAO found that, with one exception, no risk management plans or system security plans had been developed for the systems reviewed," auditors found.

"As a consequence, the entities did not comply with the relevant requirements of the Protective Security Manual and ACSI 33. "

This report appears on australianIT.com.au.
