Information Systems Audit Report

Report 2 – April 2009

This is the first year that we have reported the results of our annual IS audits as a stand-alone report.

The first item of the report raises some issues of concern and is a 'wake up' call to all government agencies that handle personal and sensitive information. The second item on general computer and application controls audits reinforces my concern that many agencies are continuing to ignore the importance of effectively managing their information systems.

IS Compliance Audit: Protection of personal and sensitive information

Background

Poorly managed databases containing personal and sensitive information can create significant security risks for the database owners and members of the public. The objective of this examination was to establish whether the controls in place at a selection of government agencies were sufficient to protect personal and sensitive information.

The examination approach was to first identify the personal and sensitive information stored within the agency. Then based on our assessment of the most significant risks and vulnerabilities, we tested the adequacy of the controls.

What the examination found…

There was a lack of fundamental controls in place to protect personal and sensitive information at the five agencies we examined. This meant there was a real and significant risk of inappropriate disclosure or access to the information held by those agencies. In numerous cases the agencies would have no way of knowing if data theft or manipulation had occurred.

Specifically we found:

- Three out of the five agencies lacked IT security policies. This indicates a lack of understanding of security requirements by senior management. This in turn means agencies were often operating without a full awareness of the threats and vulnerabilities posed to their IT environment. Nor did they have appropriate procedures or guidelines for staff on how to mitigate those risks.
- None of the agencies we examined were consistently applying simple administrative controls such as police checks or confidentiality agreements for staff dealing with personal or sensitive information.
- Computer network security was poor. Weaknesses we found included:
  - active network accounts for former employees of agencies
  - generic accounts that allow access to networks by unidentified individuals and that had no passwords or easy to guess passwords. In one agency, by using these accounts and guessing passwords, Audit was able to access almost 700 000 sensitive records via the Internet
  - network account and password details for generic accounts 'posted' on computer monitors
  - three agencies that were not logging or monitoring network use or unsuccessful log on attempts
  - three agencies that were not updating network operating software in line with vendor recommendations to address known security vulnerabilities.
- Fundamental weaknesses in the security controls for computer applications and databases. Specifically:
  - Two agencies were storing sensitive information using database applications that were grossly inadequate for that purpose. The applications had no password controls and a well known security weakness which allowed the initial log on screen to be bypassed providing full access to all information.
  - Four of the agencies had active accounts belonging to former employees. These types of accounts provide opportunities for misuse by insiders with minimal chance of tracing the individual responsible.
  - In two of the three agencies that used a specific database, system default database accounts remained active and set to their default password. Database vendors warn that security is most easily compromised by leaving default passwords unchanged for these accounts.

- In four of the five agencies examined we found a wide range of confidential documents and files saved to unsecured folders on network servers. In some of the agencies this meant that thousands of sensitive files and documents relating to members of the WA public could be viewed by anyone connected to the network.
- None of the agencies we examined had adequate controls to address the risk of portable USB devices such as thumb drives that can be easily lost or stolen, being used to transfer or store personal and sensitive information. We found several instances where USB devices were directly connected to computers used to store sensitive information.

General computer controls audits

Background

The objective of our general computer controls audits is to determine whether computer controls effectively support the confidentiality, integrity, and availability of information systems. The audits also involve assessing the adequacy of risk management and internal audit practices as they relate to computer processing environments.

We are also for the first time reporting the results from our use of capability maturity models. A capability maturity model is a way of assessing and benchmarking how well developed the established IT controls are compared to how well developed they should be.

What the examination found…

We reported well over 500 general computer control related issues to agencies in 2008. Of the 41 agencies we assessed using the capability model, we found that:

- Over 60 per cent had not established effective controls to manage IT risks, information security and business continuity.
- 46 per cent of agencies had not established effective controls for change management.
- 33 per cent had not established effective controls for management of physical security.

Computer application controls

Background

Each year we review a selection of key applications relied on by agencies to deliver services to the general public. Applications are the software programs used to facilitate key business processes of an organisation. Failings or weaknesses in these applications have the potential to directly impact other organisations and members of the general public. Impacts range from delays in service to possible fraudulent activity and financial loss.

What the examination found…

- Only one of the five business applications we reviewed was considered well managed with few control weaknesses. In total, we identified 30 control weaknesses of which: Security weaknesses made up 50 per cent of the control weaknesses. These included computer vulnerabilities such as easy to guess passwords, unauthorised user accounts and failure to remove accounts belonging to former staff.
- Data processing controls issues made up 33 per cent of our findings. Weaknesses in data controls put the integrity of information processed at risk.
- The remaining 17 per cent of issues related to operations, change control and business continuity controls.