Information Systems Audit Report

Report 11– June 2013

Background

The Information Systems Audit Report summarises the results of the 2012 annual cycle of audits as well as other work completed by our Information Systems group over the course of the financial year. This year the report contains three items:

- Information Systems – Security Gap Analysis
- Application controls audits
- General computer controls and capability assessments

Information Systems – Security Gap Analysis

Ninety per cent of the agencies we reviewed had serious gaps in their management of information security when assessed against better practice international standards. Many of the agencies sampled are not adopting a strategic approach to identifying and assessing risks. In the absence of a strategic approach agencies may be wasting resources on areas of minimal risk while leaving critical areas exposed.

Application controls audits

This year we reported on the five applications at four agencies.

- **WA Police – Firearms Management System:** The Firearms Register and supporting systems have numerous weaknesses in the controls over data input, processing and reporting. As a result we have no confidence in the accuracy of basic information on the number of people licensed to possess firearms or the number of licensed or unlicensed firearms in Western Australia. In the absence of reliable information, WA Police are unable to effectively manage firearms licensing and regulation in WA.
- **Department of Finance – ProgenNET:** Overall ProgenNET is working properly with no significant control weaknesses identified. As a result we have confidence in the accuracy of information used to calculate lease charges and for the ongoing management of leases, tenants, landlords and other aspects of government office accommodation.

- **Health – Emergency Department Information System:** EDIS was found to be an effective application for managing workflows in the emergency department. However some control weaknesses were identified during the audit. These control weaknesses mean that staff could anonymously alter data relating to treatments provided and times of admission and discharge. We analysed data logs captured by the system over the last two years against data entered by staff and found no alterations had occurred.
- **Health – Hospital Morbidity Data System:** The Hospital Morbidity Data System (HMDS) was found to be operating as designed. However we found a few control weaknesses. The main weaknesses relate to the risk of unauthorised access to morbidity data. This can occur through insecure methods used to obtain and transfer data or because recommended software security updates are not implemented. While the system is working effectively, the identified weaknesses pose an unacceptable risk to the integrity and confidentiality of morbidity data and patient information.
- **Department of Mines and Petroleum – Royalties Online:** The Royalties Management System was found to be operating effectively. Only minor issues were identified during the audit and all where promptly dealt with by the Department and no longer pose any long term risk.

General computer controls and capability assessments

We reported 375 general computer controls issues to the 44 agencies audited in 2012.

From the 36 agencies that had capability assessments conducted only three were meeting our expectations for managing their environments effectively. Half of the agencies were not meeting our benchmark expectations in three or more categories.

Management of Changes and Physical Security were being managed effectively by most agencies, the Management of IT risks, IT security, Business continuity and IT operations need much greater focus.