EDS Submission on the

Review of Management and Integrity of the Commonwealth's Electronic Information

18th December 2002

Contents

Introduction

This submission provides comments in the context of the recommendations made as part of the:

"Internal Security within Commonwealth Government Agencies"
The Auditor General
Audit Report No 12 2001-2002
Performance Audit
Australian National Audit Office

These recommendations are generally excellent in relation to the mechanics of traditional ***Information Security.*** Of the general recommendations made as part of paragraph 47, only 2 of the 7 general recommendations made relate to strategic approaches to ***Information Assurance.***

Critical security issues relating to the responsibilities of service providers within outsourced arrangements and the need for a proactive and iterative ***Information Assurance Model*** are not addressed. In this context EDS would like to comment on:

- **Stewardship and Strategic Sourcing** – The roles of Service Providers in an outsourced environment and the impact of strategic sourcing on this role.
- **Implementation of an Iterative Information Assurance Model** – the need for a comprehensive Information Assurance Model with particular emphasis on the continual validation and upgrade of information security measures

Stewardship and Strategic Sourcing

Information Management and Assurance organizations have two key players:

- **The Owner -** The actual owner of the information who has ultimate responsibility for the use of the data
- **The Custodian –** Holds the information in trust for the information owner and looks after the information on behalf of the owner for the use by all parties who are permitted legal access

In a Government context the Owner has been the Crown whilst a Custodian has been seen as an individual government agency or statutory body.

With the spread of outsourcing there has been a subtle change in these roles and a third role has developed, that of the information ***Steward***.

While the basic roles and responsibilities of Owner and Custodian remain the same, a Steward provides information management services and support to the Custodian organisation. The degree and extent of this support is determined by contractual arrangements between the outsourcing organisation (Custodian) and outsource service provider (Steward).

With Single Source Outsourcing arrangements a single point of responsibility exists between the Government Custodian and the Steward Prime Contractor providing for robust and stable Information Security management.

Strategic Sourcing, on the other hand, threatens this stability.

The concern around Strategic Sourcing within the realm of Information Security and Assurance relates to the potential for multiple points of responsibility and in turn multiple Stewards. With multiple Stewards there is potential for confusion with regard to who is the Steward for a particular item of information and their corresponding Information Security responsibilities.

EDS believes it to be a more sound approach to standardise responsibilities of Steward organisations across government outsourcing arrangements and for each individual Custodian organisation to assign the Stewardship role to a single organisation such as a prime contractor, or an internal group such as a contract management office.

With the emergence of the Steward role, the issue of security clearance of personnel within both the Custodian and Steward organizations has also arisen. The driver for appropriate clearance levels for individuals should be the specific risk to and sensitivity of information being held. It is important to examine this when setting clearance requirements. Anecdotal evidence suggests that where previous government employees have transitioned to outsource service providers, fulfilling virtually identical roles, there has been a requirement for higher levels of clearance than previously necessary.

An Iterative Information Assurance Model

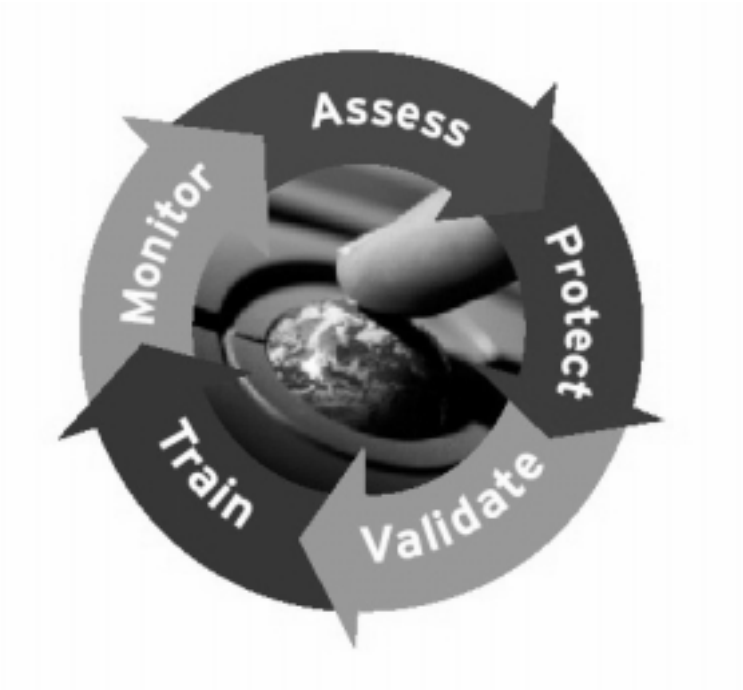
General recommendations have been made in the ***"Internal Security within Commonwealth Government Agencies"*** audit report around the need to ***adopt a structured approach to the management of Internet security*** and ***ensuring that appropriate risk assessments are conducted***.

These recommendations correctly identify the need for a structured model with clearly identifiable phases and an appropriate emphasis on risk assessment.

Given the high pace of change within the IT industry, EDS believes there is a need to further emphasise the iterative requirements of such a model.

Risks change over time. They are not static, an organisation's guiding principle should be that "***even if an organisation's infrastructure is secure today, it may not be tomorrow"***.

EDS' ***Information Assurance*** lifecycle is a structured and iterative model that includes five Information Assurance phases:



- **Assess –** Assessing, evaluates the security of the organisation (both physical and logical), identifying the assets to be protected, security vulnerabilities, and then recommending protective options for eliminating or mitigating security risks.
- **Protect –** Protecting, implements solid architectures, plans, and policies for integrating robust security practices enterprise wide that ensure maximum levels of security and productivity
- **Validate** – Validation, tests that the security mechanisms put in place during the protection phase adequately support security policies and address the risks and vulnerabilities identified during the assessment phase.
- **Train** - Training, ensures support personnel are appropriately trained and skilled in all Information Assurance service areas including industry-recognized certifications and Information Assurance programs.
- **Monitor –** Monitoring, provides a layered defence and includes in depth strategies to secure, monitor, protect, and manage your organization's critical business environment, including intrusion detection and response.

It is a fact that development, progress and change lead to the introduction of new risks and vulnerabilities at an alarming rate. New technologies are developed and implemented; new hardware and software platforms are installed, new business features, functions, and capabilities are created; organisational supply chains are extended. At the same time, the skill, sophistication and motivation of system hackers seems to be increasing. The critical challenge then, is to not only ensure continuous re-assessment of risk and the introduction of appropriate mitigation measures, but also to ensure that both existing and newly implemented security mechanisms are continuously tested. This emphasis on ***Iterative Verification***, which is often neglected in traditional security approaches, should be an important component of any rigorous approach to information security.

EDS Observations

EDS wishes to highlight the following aspects of Information Assurance that should be considered by the Government:

- **A single Steward role** be considered to provide a ***Unified Management Approach*** to Steward roles and responsibilities
- **A set of Steward roles and responsibilities** should be developed particularly in regards to outsource arrangements
- **A standardised approach to levels of clearance** be adopted driven by the risk and sensitivity surrounding the information held
- **An Iterative Information Assurance Model** be adopted with a particular emphasis on continual and proactive validation and risk assessment processes