VAGO has issued a new version of this better practice guide.

This document should be considered historical information only and is not representative of current better practice.

Managing internet security

GOOD PRACTICE

GOOD PRACTICE GUIDE

Auditing in the Public Interest

AUDITOR GENERAL
VICTORIA

Contents

Published by the Victorian Auditor-General's Office, Level 34, 140 William Street, Melbourne.
First published June 2004. Also published on <www.audit.vic.gov.au>

ISSN 1449–2733
ISBN 0 9752308 4 0

2004 : 3

Foreword

Many Victorian public sector agencies are now using the internet to improve the community's access to information and to deliver services to their customers. Their use of the internet for internal purposes also continues to grow. As it does, so does the need for effective internet security to provide a reliable and problem-free environment for users, and to safeguard agency data.

This guide, and the supporting check list, serves as a practical resource for chief information officers, business managers, information technology staff and audit committees, to help assess and improve their agency's internet security practices.

The guide sets out the main issues that need to be considered when assessing the effectiveness of security over an internet system. It provides a starting point for a planned and structured approach, at an "overview" level, to such assessments. As agencies will have their own particular security needs and procedures, they should also consult with vendors, relevant regulatory bodies and information security organisations to obtain further information about the particular requirements of their specific systems.

This guide has been developed by the Victorian Auditor-General's Office, drawing on work undertaken during recent audit examinations of internet security management across Victorian public sector agencies. Selected government departments and other agencies were also consulted during its development.

In producing the guide, we aim to raise awareness in all Victorian public sector agencies, including local government councils, of good practices to address internet security threats and risks. These practices should form part of the broader security arrangements over agency information technology (IT) systems, which should address both internal and external security threats and risks.

JW CAMERON

Auditor-General

About internet security

"Information is an asset which, like other important business assets, has value to an organisation and consequently needs to be suitably protected[1]."

The internet is the worldwide, interconnected communications phenomena of our time. Public sector agencies, like non-government organisations, increasingly rely on information technology (including internet technologies) to manage their operations and to deliver services to the community.

This reliance on, and the pervasiveness of, the internet increase the risks to agencies' data and IT systems. The main systems risks are:

- unauthorised access, use or alteration of agencies' systems and data
- denial-of-service attacks, resulting in an inability by users to access systems
- infection of systems and data by viruses or trojans
- defacement of agency websites and online systems.

Failure to effectively manage these risks can, ultimately, have wide-ranging consequences for agencies and their performance, including:

- a deterioration in the agency's reputation
- reduced public confidence in the agency's online services
- unauthorised disclosure, or alteration, of confidential or sensitive agency data
- breach of privacy requirements
- financial loss through online fraud
- financial loss by not having systems or data available for use by agency staff.

Internet security needs planning, expertise, continuous attention and a long-term commitment by agencies. The size and complexity of an agency's internet system and its components will affect the degree of security required. The need to integrate and manage disparate technologies and systems, rapid advances in technology and new security threats and risks, ensure that internet security will continue to be an important concern for all agencies into the foreseeable future.

"Any form of computer attack that occurs electronically, often remotely, and which has the ability to harm data confidentiality and integrity or system availability, represents one of the greatest threats that has emerged in parallel with our increasing levels of Internet connectivity and dependency on publically connected networks[2]."

---

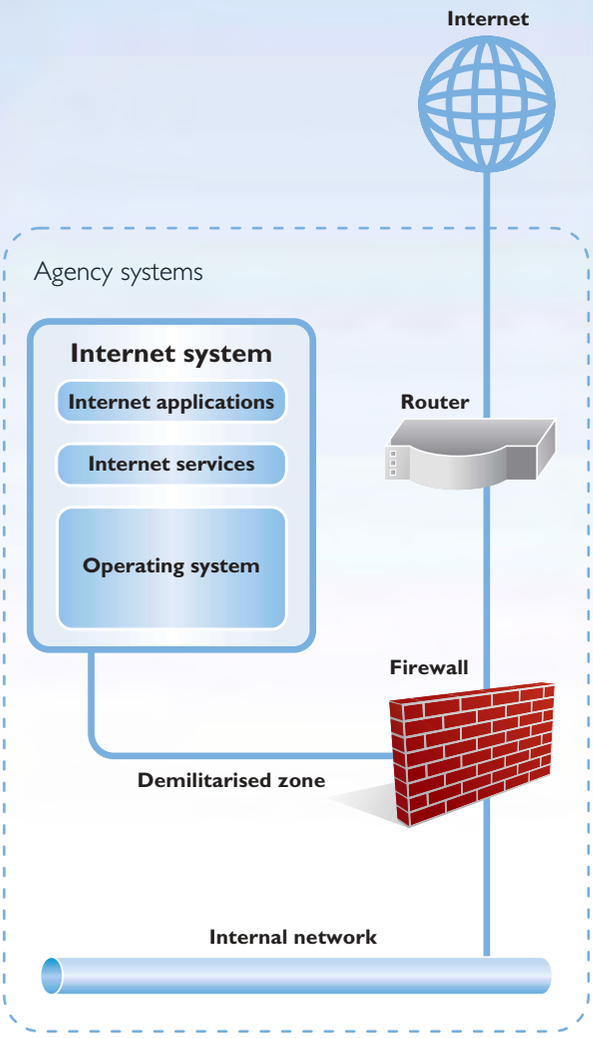
[1] Standards Australia, AS/NZS ISO/IEC 17799:2001 *Information technology - Code of practice for information security management*, 2001.

[2] AusCERT, *Australian Computer Crime and Security Survey*, 2004, p. 13. AusCERT is a computer emergency response organisation.

What are the key components of an internet system?

The **internet** is a collection of many computers connected via telecommunication networks throughout the world that communicate through a common language. The typical **internet system** comprises internet applications, internet services and an operating system, which connect to the internet. These systems allow external users to access an organisation's website, or transact business with an agency over the internet.

Figure 1: Typical internet system and its components



Internet applications are software that allow transactions to take place between external users and the agency (e.g. making payments or querying a database to obtain information).

Internet services are provided with the operating system (refer below) and allow an agency's internet system to interact with the internet. The main internet services are:

- a **web service** (such as Internet Information Server or Apache), which allows users to access the agency's internet system from the internet
- an **email service** (such as Microsoft Exchange or Lotus Notes), which allows agency staff to send and receive emails
- a **database service** (such as SQL or Oracle), which allows data to be stored and manipulated.

The **operating system** (such as Windows 2000 or Unix) is the base set of instructions to the computer that controls the screen, keyboard, applications and other devices attached to the system.

Typical **internet system components** include the following:

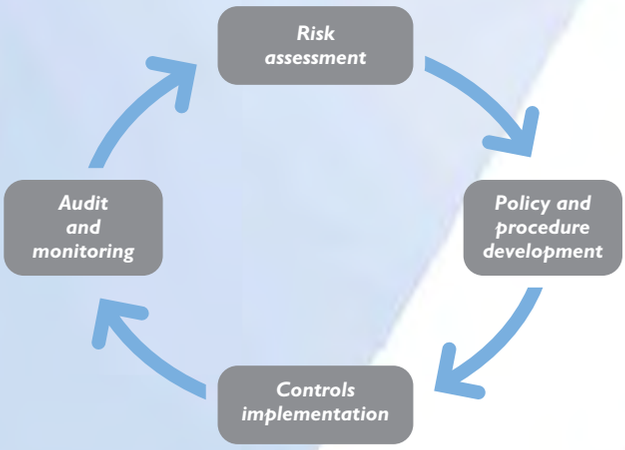
- a **router** - a special-purpose computer or software package that manages the connection between the agency firewall and a non-agency router connected to the internet
- a **firewall** - a combination of hardware and software that protects agency systems by forming a "fortress" between the internet, the agency's internal network and the agency's internet system
- the **DMZ** (known as the demilitarised zone) - a linkage between the internet system and the firewall that allows external users from the internet to interact with the agency's internet system
- the **internal network** represents all communications, databases, computers and applications used by the agency that need to be protected from access from outside the organisation.

Assessing internet security

The management of internet security is an iterative process. It includes the assessment of key security risks, the development of a policy and procedural framework to guide the management of these risks, the implementation of policy and procedures, and monitoring processes to ensure the effective operation of the established framework and procedures.

Figure 2 illustrates these important aspects of managing internet security. Each is further explained in the check list that follows. Because risks change over time, they need to be continuously assessed, policies reviewed and controls developed and updated. Auditing and monitoring are also not one-off, but ongoing activities. This means that the check list steps that follow require constant review and repeating over time.

Figure 2:
Key internet security management steps



Check list

Risk assessment
- Roles and responsibilities
- Risk management

Policy and procedure development
- Policy and procedures
- Outsourced agreements

Controls implementation
- Internet application security
- Backup and recovery
- Change management
- Perimeter defence
- Security hardening
- Antivirus procedures
- Email
- Encryption and authentication

Audit and monitoring
- Security and activity monitoring
- Audit

Risk assessment should include an assessment of the impact of loss or damage to organisational systems (and ultimately to agency operations), identification of the threats to those systems and determining the likelihood of those threats being realised. This analysis should assist in determining the level of security that should be implemented.

Policies and procedures should provide guidance on how to implement and maintain security in a controlled and structured manner within the organisation, and dictate what ongoing activities need to be conducted to ensure security is maintained. In addition, they should promote awareness of the importance of information security to staff.

Specific preventative **control procedures** should be implemented over the IT environment, information systems and data to reduce the likelihood of threats being realised. These should comply with organisational policies and procedures, and reflect the level of risk associated with the information system or data.

System and security-related activity should be continuously logged and regularly **monitored**. Incidents or exceptions should be investigated in accordance with organisational policies and procedures.

Audit processes should ensure that security controls mechanisms and policies comply with good practice and are actually being adhered to.

Agencies should compare their current practices against the check list in this guide. Where good practice is not being met, agencies should develop a course of action to address the relevant issue as well as provide a date when this action will be complete. Chief information officers and IT managers will likely be the appropriate staff to initially evaluate the organisation's practices, however, responsible business managers and audit committees should take an active role in following-up action items and target dates.

There is a growing body of literature about information and internet security. Key references can be found on the inside back cover of this guide.

Internet security check list

Risk assessment

Good practice	Good practice met	Action plan	Target date
Roles and responsibilities			
Roles and responsibilities for the security of the internet system and its components have been clearly defined, documented, approved and communicated. These should include responsibilities for security design, implementation and administration.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Staff responsible for the security of the internet system and its components have appropriate skills, experience and qualifications.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Staff responsible for the security of the internet system and its components are maintaining their skills/knowledge to keep them current.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Risk management			
Risks to the current or planned internet system and its components have been assessed and prioritised. **Risks** are the potential for damage to the agency's internet system and its components, and the likelihood of damage. Risk assessment should also include consideration of legal and regulatory risks such as non-compliance with the requirements of the Privacy Act and/or Spam Act. **Recognised standards** include AS/NZS 4360:1999: *Risk management* which provides guidance for establishing and implementing a risk management process.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Plans to mitigate or insure against prioritised risks have been developed and implemented.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Risks to the internet system and its components are periodically reassessed, and reprioritised as required.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		

Policy and procedure development

Good practice	Good practice met	Action plan	Target date
Policy and procedures			
An **information security policy** has been developed in accordance with **recognised standards.** The policy has been documented, approved and communicated throughout the agency. An **information security policy** can include the agency's general approach to information security, and general rules about what is allowed and what is not. **Recognised standards** include AS/NZS ISO/IEC 17799:2001 *Information technology - Code of practice for information security* management.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Internet security procedures consistent with the information security policy have been developed, documented, approved and communicated to relevant staff. **Internet security procedures** include step-by-step instructions about how to protect the internet system and its components.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Security incident procedures have been developed and documented. The procedures have been communicated to relevant staff, or throughout the agency, as applicable. **Security incidents** can include detection of unauthorised access to the internet system. **Security incident procedures** can include what to do when an incident occurs, who an incident must be reported to, and how it must be reported.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Policies and procedures are periodically reassessed to maintain their currency and applicability.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Outsourced arrangements			
If the internet system or its components are outsourced (in whole or part) to an external third party, the contract requires the party to mitigate or insure against assessed and prioritised risks.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Contracts with external third parties for outsourced services include the right to conduct independent audits of their operations.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Independent assurance is periodically obtained and evaluated by the agency on the effective operation of external party security procedures. **Independant assurance** can include the conduct of security audits of the third party, initiated either by the agency or the third party. The frequency and type of audits should depend on the assessed risk exposure to the agency.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		

Controls implementation

Good practice	Good practice met	Action plan	Target date
Internet application security			
If the internet system stores or transacts **confidential data**, users are **authenticated** before being granted access to that data. **Confidential data** can include information confidential to the agency or to internet users (such as personal or credit card details). **Authentication** can include entering a user name and password, or use of encryption techniques, to verify a user's identity. The extent of authentication procedures implemented should reflect the risks identified to the internet system.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Users can only access parts of the internet system they are authorised to access.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
A privacy policy and procedures have been developed, documented, approved and communicated throughout the agency, and to users as applicable. They include requirements for handling information used and stored by internet systems.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
If the internet system stores and transacts confidential data, the data is **securely stored.** **Secure data storage** can include requiring passwords for access, encrypting data, using file and directory access controls and locating data on another server.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Internet applications check automatically that all input data is in the correct format.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Backup and recovery			
Disaster recovery and/or business continuity plans have been developed, documented, approved and communicated. **Disaster recovery and/or business continuity plans** include steps that the agency will take if its internet system or components fail. The extent and complexity of the plans depends on the likely impact of the assessed and prioritised risks to the agency's operations.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Disaster recovery and/or business continuity plans are periodically tested and updated if required.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
A **backup** policy for the internet system and its components has been documented, approved and communicated to relevant staff. **Backing-up** is making a copy of data, system settings and software so that they are not lost if the originals become unusable.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		

Good practice	*Good practice met*	*Action plan*	*Target date*
Backup and recovery (continued)			
All data, internet applications and the operating system are backed-up in line with the backup policy.	*Yes* ☐ *In part* ☐ *No* ☐		
Backup media are stored in a **secure location**. Backup media are periodically relocated off-site to another location not close to the internet system. **Backup media** can include tapes, CDs, DVDs and removable hard disks. A **secure location** can include a locked, fireproof safe, as well as restrictions on who can access backup media.	*Yes* ☐ *In part* ☐ *No* ☐		
Backup media are periodically tested to ensure data can be recovered.	*Yes* ☐ *In part* ☐ *No* ☐		
Change management			
Change management policies and procedures to implement and modify the internet system and its components (and in particular for internet applications) have been developed, documented, approved and communicated throughout the agency.	*Yes* ☐ *In part* ☐ *No* ☐		
All changes to the internet system and its components (and, in particular, internet applications) are tested to ensure that they are secure before being implemented.	*Yes* ☐ *In part* ☐ *No* ☐		
Perimeter defence			
A firewall is used to separate the agency's internal network from the internet, and the firewall is correctly **configured.** **Configuration** is the process of adjusting the hardware and settings so that the firewall operates at maximum effectiveness.	*Yes* ☐ *In part* ☐ *No* ☐		
The internet system is placed within the demillitarised zone (DMZ) using an **access control device.** An **access control device** can include a router or firewall.	*Yes* ☐ *In part* ☐ *No* ☐		

Good practice	*Good practice met*	*Action plan*	*Target date*
Perimeter defence (continued)			
Firewall policies and procedures have been developed, documented, approved, communicated and implemented. **Firewall policies and procedures** can specify allowable communications to and from the internet and DMZ. Procedures can also cover changing firewall rules, upgrading firewall software and monitoring firewall logs.	*Yes* ☐ *In part* ☐ *No* ☐		
All changes to the configuration of the firewall comply with the agency's documented change management policy and procedures.	*Yes* ☐ *In part* ☐ *No* ☐		
Firewall rules are reviewed periodically to ensure that they are secure and comply with the firewall policy. **Firewall rules** define the specific communications that can pass through the firewall.	*Yes* ☐ *In part* ☐ *No* ☐		
Firewall logs are regularly monitored for security violations and incidents, using applications to identify high-risk connections and threats. Action is taken and violations and incidents reported in line with procedures. **Firewall logs** are the records of communications accepted or rejected by the firewall.	*Yes* ☐ *In part* ☐ *No* ☐		
Security hardening			
Good practice security configuration guides, specific to the agency's internet systems and components, have been followed. **Good practice security configuration guides** are provided by software and hardware vendors, and by reputable information security organisations, to help agencies secure specific internet services, operating systems and other components.	*Yes* ☐ *In part* ☐ *No* ☐		
The internet system only uses the minimum applications and operating system functions required by the agency, and other applications and functions have been removed.	*Yes* ☐ *In part* ☐ *No* ☐		
Applications that allow users to perform **powerful system functions** are not installed on the system or, when installed, their use is tightly controlled. **Powerful system functions** are functions that allow major changes to the way the system operates.	*Yes* ☐ *In part* ☐ *No* ☐		

Good practice	*Good practice met*	*Action plan*	*Target date*
Security hardening (continued)			
A password policy and guidelines have been developed and compliance is either system or manually enforced. This should aim to ensure that all passwords are sufficiently complex and are changed on first use and on a regular basis.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Security alerts relating to the internet system and its components are regularly received, reviewed and actioned by IT staff as applicable. **Security alerts** can include information about system vulnerabilities such as bugs in software or hardware, ways to fix the vulnerabilities and the ways that attackers are exploiting these vulnerabilities.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
The internet system hardware and related equipment is located in a secure area, and access to it is tightly controlled.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Patches and updates are tested and implemented as a high priority. **Patches and updates** are "fixes" for system vulnerabilities, bugs or configuration settings in software or hardware that are released by vendors.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Vulnerability scanning is periodically undertaken to identify and correct security weaknesses in the internet system and its components. **Vulnerability scanning** uses software to scan for known security flaws or weaknesses within a system.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Antivirus procedures			
A policy covering **viruses** and **trojans** has been developed, documented, approved and communicated. **Viruses** are applications that are designed to do something unexpected or undesirable to the internet system or its components. They are often spread from computer to computer, without user knowledge or permission. **Trojans** are applications that are hidden in legitimate applications and that open a virus or other destructive application when they are run.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
The internet system and relevant components have an antivirus application correctly installed, configured and activated to detect viruses and trojans.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
The antivirus application is automatically and frequently updated to minimise the risk of new viruses and trojans being undetected.	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		

Good practice	*Good practice met*	*Action plan*	*Target date*
Email			
An **email policy** has been developed, documented, approved and communicated. **Email policies** should establish clear rules for which files and software are allowed to be received or sent.	*Yes* ☐ *In part* ☐ *No* ☐		
Inbound and outbound emails are scanned to restrict access to viruses and unauthorised types of files. Viruses and unauthorised types of files are quarantined or rejected.	*Yes* ☐ *In part* ☐ *No* ☐		
Unsolicited bulk commercial email (spam) is identified, blocked and rejected.	*Yes* ☐ *In part* ☐ *No* ☐		
Attackers are "prevented" from sending emails through (bounced off) the agency's email service, to make it appear they originated from the agency.	*Yes* ☐ *In part* ☐ *No* ☐		
Encryption and authentication			
Where the internet system sends or receives confidential information, **encryption** and a **method of authentication** is used to protect individual privacy, and to establish the agency's identity. Secure Socket Layer (SSL) is a common method used to secure internet communications and authenticate the identity of organisations. **Encryption** is the scrambling of data in such a way that a secret code is needed to unscramble it. **Methods of authentication** can include a password or digital certificate.	*Yes* ☐ *In part* ☐ *No* ☐		
Encryption keys of 128 bit or greater are used to encrypt confidential communications. **Encryption keys** are the secret code that is used to scramble or unscramble data.	*Yes* ☐ *In part* ☐ *No* ☐		
If **digital certificates** are used, they are current and have been issued by a **reputable certificate authority.** A **digital certificate** is an electronic document used during a transaction that confirms the agency's identity. A **reputable certificate authority** is a trusted third party that verifies the identity of organisations and their websites, and issues a digital certificate.	*Yes* ☐ *In part* ☐ *No* ☐		
If digital certificates are used, they are securely stored and protected by passwords, and by **file and directory level security**. **File and directory level security** refers to controls over the rights of a user or system to access directories and files.	*Yes* ☐ *In part* ☐ *No* ☐		

Audit and monitoring

Good practice	*Good practice met*	*Action plan*	*Target date*
Security and activity monitoring			
Audit logs on the internet system and its components are generated, collected, and secured from tampering and unauthorised access. **Audit logs** are records of dates, times, incidents, actions and other events that have occurred on the internet system and its components.	*Yes* ☐ *In part* ☐ *No* ☐		
Audit logs are regularly backed-up.	*Yes* ☐ *In part* ☐ *No* ☐		
Audit logs are regularly monitored for security violations and incidents. Action is taken, and violations and incidents reported, in line with procedures.	*Yes* ☐ *In part* ☐ *No* ☐		
Intrusion detection applications are installed and operating on the internet system and its components. **Intrusion detection applications** inspect all communication and identify likely attempts to break into the system, or detect unauthorised access to system files.	*Yes* ☐ *In part* ☐ *No* ☐		
Audit			
A **security audit** has been conducted on the internet system and its components. A **security audit** is the step-by-step process to determine if the system is well-secured against attackers. The type of security audits can vary, and include: • compliance with information security policies and procedures • assessment of the configuration of an internet system or its components • testing of general computer controls.	*Yes* ☐ *In part* ☐ *No* ☐		
Security audits are conducted at a frequency influenced by the risk assessment (previously referred).	*Yes* ☐ *In part* ☐ *No* ☐		

Further references

Three important publications, with detailed guidance about information security practices generally, are:

- AS/NZS ISO/IEC 17799:2001, *Information technology - Code of practice for information security management*, Standards Australia, available at <http://www.standards.com.au>
- *Control Objectives for Information and related Technology*, IT Governance Institute, available at <http://www.itgi.org/>
- *Internet Delivery Decisions – A Government Program Managers Guide*, Australian National Audit Office, 2001, available at <http://www.anao.gov.au>. This guide includes a section on internet systems security and authentication for government programs.

Other useful references about information technology control, including internet security management, can be found at the following internet sites:

- <http://www.auscert.org.au> (Australian Computer Emergency Response Team, an independent not-for-profit organisation)
- <http://www.dsd.gov.au> (Defence Signals Directorate, an Australian federal agency)
- <http://www.agimo.gov.au> (Australian Government Information Management Office, Australian federal agency)
- <http://www.nist.gov> (National Institute of Standards and Technology, a USA federal agency)
- <http://www.sans.org> (SANS Institute, a research and education organisation, USA)
- <http://www.isaca.org> (Information Systems Audit and Control Association, USA)
- <http://www.owasp.org> (Open Web Application Security Project, a USA not-for-profit foundation).

The good practice check list included in this guide draws on these useful resources.

Good practice guides produced by the Victorian Auditor-General's Office

2004:1 Chief Finance Officer: Role and responsibilities

2004:2 Managing risk across the public sector

AUDITOR GENERAL
VICTORIA