SPECIAL REPORT

THE INTERNET
and Public Sector Agencies

REPORT NO 3 – JUNE 1996
THE INTERNET
and Public Sector Agencies

REPORT NO 3 - JUNE 1996

OFFICE OF THE AUDITOR GENERAL

4th Floor Dumas House
2 Havelock Street
West Perth WA 6005
Telephone: (09) 222 7500
Facsimile: (09) 322 5664
E-mail: oagwa@iinet.net.au
WWW: http://www.iinet.net.au/~oagwa/
Our Vision
To lead in performance auditing.

Our Mission
Under the auspices of the Auditor General, auditing will provide Parliament with that information necessary to enhance public sector accountability.

The Office of the Auditor General is a customer focused organisation and is keen to receive feedback on the quality of the reports it issues.
SPECIAL REPORT - THE INTERNET AND PUBLIC SECTOR AGENCIES

This Report has been prepared consequent to examinations conducted under section 80 of the Financial Administration and Audit Act 1985 for submission to Parliament under the provisions of section 95 of the Act.

Such examinations are an integral part of my Office's overall Performance Auditing Program and seek to provide Parliament with assessments of the effectiveness and efficiency of public sector programs and activities, thereby identifying opportunities for improved performance.

D D R PEARSON
AUDITOR GENERAL

June 19, 1996
## Contents

- **Preface** 1
- **Executive Summary** 2
  - Background 2
  - Overall Findings 3
  - Recommendations 4
- **Introduction** 5
  - Background 5
  - Examination Focus and Approach 8
- **Benefits of the Internet** 10
  - Background 10
  - Findings 11
  - Good Practice 13
- **Balancing Risks and Costs** 14
  - Justification 14
  - Risk Assessment 15
  - Costs 18
- **Managing Information** 21
  - Information and Records Management 21
  - Publishing Requirements 23
  - Currency of Information 25
- **Providing Security** 28
  - Physical Mechanisms 28
  - Logical Mechanisms 32
  - Monitoring 34
  - Internal Policies 35
- **Establishing a Management Framework** 37
  - Technical 37
  - Agency 38
  - Government 40
  - Conclusions 41
  - Recommendations 42
- **Appendix 1: Good Practice Summary** 43
- **Glossary of Terms** 47
- **Performance Examinations Reports** 50
Preface

This special report presents the findings of a performance examination into Internet usage across Western Australian public sector agencies. Its primary aim is to identify the issues affecting efficiency and effectiveness faced by agencies that connect to, and/or publish on, the Internet. As part of that process, ways to reduce potential risks are identified and ‘good practice’ statements developed. These statements are relevant for the situations found, but will need to be regularly reviewed in light of the dynamic nature of the Internet.

The use of the Internet by agencies is a relatively recent phenomenon. This examination takes a snapshot view of current usage and practices and ways of minimising the risks that public sector agencies face. It also seeks to identify the gains that agencies have made from usage of, and/or establishing a presence on, the Internet.

Much discussion surrounds both the benefits to be gained from using the Internet and the risks that such usage can pose. Twenty two agencies were examined and their experiences in using various services of the Internet, including publishing, were gathered. The size of an agency was not a factor in whether they were selected for review, although all agencies selected had one thing in common — they are listed in the Western Australian Government’s Home Page on the World-Wide Web.
Executive Summary

Background

The Internet is growing at a phenomenal rate, and is attracting more and more involvement from both government and business alike as they seek to improve service delivery and extend the reach of those services. Public sector use of the Internet both here, interstate and overseas has also increased dramatically, especially in the past 12 months. The relative ease with which it is possible to connect to and use the Internet means that even small agencies are able to quickly reap some of the benefits on offer in this new medium.

As with any new initiative it is important that agencies assess whether the potential benefits offered through using the Internet are of sufficient value to justify paying the associated costs. Ideally, agencies should aim to achieve productivity enhancements through improved communications, information access and research. Improvements can also be offered in service delivery. This includes making services and information available to audiences who may not normally be able to have access to them. It may also be possible to reduce publishing costs by making some material available primarily on the Internet.

Along with benefits, there are also risks. The risks draw attention to the need to protect public and agency information from unauthorised or inappropriate use and access. The ability to publish public sector information via the World-Wide Web raises new issues regarding electronic publications within a duty of care framework.

The Information Policy Council (established by the Premier to provide an appropriate policy, standards and advisory framework in the areas of Information, Information Technology and Telecommunications) has issued policies that encourage agencies to establish connections to public networked information services, publish information for use by clients, and to expand customer services. The policies also require that adequate security measures are implemented and the appropriate use of Internet services be determined before a connection is established.
Executive Summary

Overall Findings

Even though agencies have identified many benefits associated with using the Internet, the extent to which these benefits are being realised is still largely unknown. While several of the agencies examined in this review are able to demonstrate benefits already achieved, most are not yet in a position to identify or quantify them.

As might be expected, security issues dominate the risks that agencies are assessing before connecting to the Internet. This is reflected in the rapid growth of an access control mechanism called a ‘firewall’ installation where agencies establish a direct connection to the Internet. Unfortunately, the policies that underpin such installations as these are lagging behind. Although most agencies had developed the necessary content for these policies, few had moved beyond the draft stage.

One area that needs more attention is the legal exposure an agency faces from establishing a publishing presence on the Internet. This includes issues such as copyright, defamation, privacy, inappropriate use, coordination across agencies of the information published, and information accuracy.

Policies relating to electronic publishing and the management of information in both agencies and the public sector as a whole lag behind developments in the area and actual practice. As more and more agencies use the Internet, and their policies and practices become more diverse, this may lead to problems. In addition, without adequate direction and management, this area of Internet usage has the potential to cost more than anticipated. Resources may be rapidly consumed as the need to keep ever increasing amounts of information accurate and current is focused on.
Executive Summary

Recommendations

- Agencies should establish an Internet Management Framework that:
  - applies the appropriate good practices presented; and
  - considers the possible benefits of Internet usage and assesses their relevance to the agency's function and operations.

- The Public Sector Management Office should, as part of their coordination role in setting policies and standards:
  - determine how best to coordinate the information presented on the Internet across agencies;
  - develop and maintain good practice guides on Internet usage; and
  - facilitate the establishment of a register (via the Internet is an option) of appropriate security and advisory services.
Introduction

Background

The Internet is essentially a global network of connections linking many computers together. Its origins lie with United States military computer networks of the 1950s and 1960s. With the increasing use of computers by the defence forces, the need to share information and messages through network connections became obvious. One of the limitations that then existed with network topography was that damage to any of the facilities connected to the network would severely disrupt network communications for the rest of the facilities. Therefore, it was necessary to find a way to ensure that if any of these sites were damaged in any way, that the rest of the network would function normally. The solution found was the start of the Internet.

Because some defence research in the United States is undertaken by universities, it soon became desirable to have the universities connect to the military network, then known as ARPANet. This led to the widening of its use to the academic population. As these students moved into industry and government, they took with them the desire to continue to benefit from such a network and the original ARPANet grew into the Internet, now used throughout the world by people and organisations.

The major Australian link to the Internet was, for many years, AARNet (Australian Academic and Research Network) which was established in 1989. The day to day management of AARNet was taken over by Telstra in 1995, with most Internet services now provided by resellers of the Telstra service.

Figure 1: Western Australia can communicate with most countries via the Internet
This figure is illustrative only.

Source: OAG and Corel
Introduction

The Internet has grown at an exponential rate over the past year. Estimates of size relating to the Internet can never be accurate as its growth to date has been so rapid and there is no centralised control or coordination. Indicative figures suggest that there are more than 50 million users worldwide via more than two million computers in over 150 countries. Australia has one of the highest per capita Internet user populations in the world.

This increasing usage, the lack of control of what is available on the Internet, and how it is increasingly affecting people and organisations around the world has led to much media and government attention. Discussions range from whether this is the much touted ‘Information Superhighway’ to whether laws should be applied to its content and use.

Regardless of any concerns that people or governments may have, the Internet continues to grow at an astounding rate. This rate is being contributed to by public sector agencies the world over, including those in Western Australia (WA). A survey conducted by Information Technology Watch (then part of the Department of State Services) during the second half of 1995, found that of 79 public sector agencies canvassed, 76 per cent already had connections to the Internet with the remainder all planning to connect — the majority of those within six months. Of those with a connection, more than two-thirds used the World-Wide Web.

The Internet comprises a number of services, the most common being:

- electronic mail (e-mail);
- mailing lists;
- transfer facilities for text files, software, and pictures (FTP – File Transfer Protocol);
- search tools for finding information;
- newsgroups (that act like a bulletin board or forum for specific topics);
- connection facilities between specified computers (Telnet); and
- the latest facility, which is generating most of the recent rapid growth, the World-Wide Web.

The World-Wide Web is a public access search and retrieval system that provides graphical document information on the Internet. Estimates suggest that there are more than 100 million pages of information on the World-Wide Web, and that a new page is being added every four seconds.
Introduction

Figure 2: Western Australian Government Home Page

The Government’s Home Page on the World-Wide Web provides links to a wide range of other public sector information services.


During the last quarter of 1995, the WA Government Home Page was launched on the World-Wide Web. This provides, among other things, a reference to individual agency home pages that have been published on the World-Wide Web.

Agencies are actively encouraged to have a presence on the World-Wide Web and provide links to the WA Government Home Page. For most of the agencies with a presence on the World-Wide Web it is early days, with the initial aim having been to establish that presence. In the first quarter of 1996, more than 25 agencies were providing home pages. By the end of the second quarter, this figure is expected to double. There is also an increasing emphasis being placed on publishing documents (reports, policies, standards, guidelines, legislation and general agency information) via an agency’s home pages.

Agencies connect to the Internet by either establishing a connection from their own server to Telstra or by using a service provider, usually via dial-up facilities. Bureau Services (part of the Department of State Services) presently operates as a provider to which agencies may be linked directly rather than by dial-up facilities.
Implementation of a government wide digital network, the Common Digital Network (CDN), is planned to be phased in during 1996. This aims to rationalise existing agency networks and progressively migrate to a whole-of-government managed service supporting the business needs of all agencies. Agencies will need to assess the likely impact provided by this initiative on their connections to the Internet.

**Examination Focus and Approach**

The examination’s aim was to identify the issues facing public sector agencies in their use and management of the Internet, and to determine good practices that are beneficial in most situations. This will help to ensure that any such moves are conducted in the most efficient and effective manner possible. Twenty two agencies that used the Internet in some way were selected.

The examination addressed Internet issues under an Internet Management Framework that can be depicted as follows:

![Figure 3: The Internet Management Framework](source: OAG)

Sound policies and guidelines are the key to good management of Internet activities.

Source: OAG
The main issues examined relate to:

- benefits of the Internet;
- balancing risks and costs;
- managing information;
- providing security; and
- establishing a management framework.

A common list of questions derived from public sector policies and guidelines, and other literature describing sound Internet management practices, was used to interview each agency. In addition, each agency's Home Page on the World-Wide Web was tested against these guidelines and against applicable technical standards. Where relevant, the agency's own policies and guidelines were assessed for their contribution to good practices. Specific tests of individual agency physical and logical security controls were not performed.

Valuable contributions were also provided by the Public Sector Management Office (primarily through the then Strategic Information and Information Technology Unit), an academic specialising in Internet and security issues and a consultant specialising in Internet 'firewall' implementations.
Benefits of the Internet

Background

A fundamental premise behind any business decision is that some benefit will be derived. That benefit may be financial, provide a competitive advantage, improve service delivery or be consistent with a wider business direction. In order to determine the success of the decision, the expected benefits need to be known.

There are many potential benefits for an organisation in connecting to the Internet. Rapid and easy contact may be established and maintained with people around the world by using services such as electronic mail (e-mail) and mailing lists; computer files and software may be transferred using services such as FTP (file transfer protocol); information may be shared and acquired using services such as gopher, the World-Wide Web (WWW), and Wide-Area Information Services (WAIS); conferencing between parties anywhere in the world may be achieved via services such as Chat and Internet Relay Chat (IRC).

These benefits can, and should, be used in a number of ways. Productivity can be enhanced by using the Internet to improve communications, information access and research. Service delivery can be improved, or provided to audiences that would not normally have access. Printing and publishing costs can be reduced if information is provided using the World-Wide Web. The latest, and any new, information can be provided faster than any other method to the widest possible audience for a very low cost.

Some benefits of the Internet will grow over time such as the move to have agencies establishing a presence through publishing of their Home Page. When the majority of agencies have a presence established, the customer starts to benefit from single point access to government services. In this particular area, it may be desirable to examine the potential to structure the information content by service, rather than just by agency. This will enable people to find what they are looking for without having to know which agency deals with the information they want. It will also enable any changes to agency roles to be as transparent as possible.

Other benefits are more specific and provide potential for real value being added to the services agencies receive and provide. Whatever the benefits, they must be identified and measured in order to conclude whether they have been achieved and the value that was gained from them. While this assessment may not be easily achieved, the analysis should nevertheless be performed.
Benefits of the Internet

The many services available on the Internet, and the experience of many people using them, means that it is easy to develop a list of anticipated benefits to justify using the Internet. Many of these will be difficult to quantify. As such, it is important that achievements are monitored to provide management assurance that the benefits are real. A justification, for example, claiming improved customer service delivery may not be relevant if the majority of intended customers of an agency are unlikely to have access to the Internet.

Of course, these benefits do not manifest themselves simply by connecting to the Internet. As with any process, they must be managed if the benefits are to be maximised or realised at all. Achieving these benefits will almost certainly affect operations not directly concerned with the Internet, and as such must be managed with the overall costs and benefits to the organisation in mind.

Findings

Half the agencies surveyed reported being satisfied with the benefits gained from their experiences with the Internet. The other half were optimistic about the potential for further gain. Many agencies expressed caution, however, since they were in the early stages of Internet usage. The agencies believed that the following specific benefits had already been achieved or were likely to be achieved:

Enhancing Service Delivery

- having access to a wider customer base to deliver services with more current information;
- ability to market services world-wide;
- improving exposure to customers particularly overseas;
- ability to target specific customer groups;
- being able to provide information 24 hours per day 7 days a week;
- making information available to clients who have difficulty calling in; and
- lowering of geographical boundaries both within the State and overseas.
Benefits of the Internet

Reducing Costs

- reducing the level of customer inquiries by phone, mail and front desk visits;
- reducing publishing costs by making electronic versions of documents available;
- being able to conduct surveys at lower cost; and
- having a zero marginal cost for each additional information recipient.

Improving Operations

- greatly expanded research capabilities in considerably shorter time frames;
- generally improving communication and the speed of communication with peers and experts wherever they may be;
- better opportunity to provide their own staff with information (Intranet);
- more efficient contact with regional staff;
- getting quicker, better solutions to software problems by being able to directly access suppliers’ databases overseas and downloading fixes to software (also reduces reliance on consultants); and
- earlier receipt of new software releases.

Even though some 70 per cent of the agencies reviewed were monitoring their usage of the Internet in some way, less than 15 per cent were in a position to link this to the benefits they may be receiving. This lack of evaluation of benefits being realised suggests that most agencies perceive the benefits they are achieving rather than know that they have achieved them.

Agencies reported that one of the main uses and benefits of the Internet lay in research with 60 per cent reporting a high level of use for that purpose. This use of the Internet is common to many of its users. It is important to note, however, that care must be exercised when using any information that is located. While much of the information is accurate and relevant, a significant proportion of it should not be relied on without further investigation and analysis. As the number of people who are not skilled in research use the Internet both for searching for and disseminating information, care must be exercised in the use of such information.

Industry predictions indicate a significant potential use of the Internet for electronic commerce. A major stumbling block for many organisations has been concern regarding security over the transfer of financial transactions. Only a few agencies
Benefits of the Internet

indicated an interest, at this time, in the possible future use of the Internet for that purpose. When the security concerns are sufficiently addressed, many benefits are likely to be realisable by agencies taking advantage of new ways of operating via electronic commerce.

Good Practice

- Determine anticipated gains from Internet usage and presence and measure achievement of these.
- Monitor gains made by others for applicability in an agency’s own environment.
- Share ‘success’ stories with other agencies.
Balancing Risks and Costs

JUSTIFICATION

Background

Any purchase by an organisation, or any change in policy or procedures, should be prompted by some sort of improvement. In the case of a public sector agency, the need to implement a change could arise from being better able to meet government or public requirements, improving program delivery, reducing costs, or improving overall efficiency and effectiveness.

Identifying what to introduce or change, why it is necessary, and how it will be paid for is the role of a business case. It is also important to determine how the organisation will know whether the expected benefits have accrued from the decision, and how and when this review will take place.

In the case of Internet usage or presence, costs can be low in the early stages and only tend to rise when more comprehensive security measures are implemented or when substantial amounts of information of a volatile nature are published, taking extra resources from other organisational operations. Low initial costs allow trials to be readily conducted, with costs being absorbed into existing budgets before more significant expenditure justifications are developed. Low initial costs also lead to the possibility of Internet connections being established without the knowledge of senior management.

Findings

Many agencies were found to be trialing Internet usage to ascertain the benefits to themselves and their clients. Four broad categories of justification were used by the agencies reviewed. More than 35 per cent of agencies had put a justification to the Executive management of their organisation. Over 25 per cent had costs included in, but not readily distinguishable from, their overall computing budget with a similar amount covering costs as part of their normal service delivery. The remainder had primarily set up a presence on the Internet consistent with the encouragement of agencies to have a Home Page set up on the World-Wide Web.
Balancing Risks and Costs

While agencies generally publish material on the Internet only for external customers, 20 per cent were found to be using, or in the process of developing, the same technology to provide access to information within their organisation, — often referred to as the Intranet. Given the early stages of Intranet considerations, the examination found little real evidence that agencies are actively looking at which internal work practices could be re-engineered with this method of internal service delivery.

Good Practice

◆ Decide in advance why the Internet is going to be used, who is going to use it and for what purpose. Use this information in the risk assessment process.

◆ Consider the opportunities for using both the Internet and the Intranet.

◆ Consider re-engineering internal work practices in association with Intranet usage.

◆ Decide on the acceptable cost level and desirable benefits to be achieved and review the project against these criteria at appropriate intervals.

RISK ASSESSMENT

Background

Risk management is a significant factor affecting the operations of both the public and private sectors. Risk identification and assessment should be undertaken before any decision is taken about acquiring new resources, implementing new practices, or changing existing ones. The results should form part of the analysis and justification process, thus ensuring that all factors can be comprehensively evaluated. If this process is not performed, unidentified risks with unintended consequences could affect the outcome.
Balancing Risks and Costs

The Internet poses its own unique set of risks, and these can vary considerably. Each service subscribed to on the Internet poses different risks and costs, and so should be separately assessed to determine whether the cost of minimising that risk is warranted. This should form part of an overall risk management framework that also takes into account the level of expertise available to an agency.

Along with any other organisational endeavour, the Internet exposes the agency to both financial and legal risks. Financial risks, such as the service costs, the costs of service disruption or information corruption, are better understood and more widely experienced than legal risks. The Internet can significantly broaden the areas where an agency faces legal risks. These legal issues, such as copyright infringement, defamation, privacy and general legal liability arising from provision of out-of-date or incorrect information, also need to be considered during the assessment process.

An agency that only publishes basic information through a third party does not need to go through as extensive an exercise as one that allows access by all staff to all Internet services. Nevertheless, there is a real need to assess what risks are associated with Internet use, particularly with direct connections to it.

As with any new business opportunity, many Internet Service Providers have established themselves in Western Australia. Whether this large number will continue to operate remains to be seen, however there is a risk that this may not be so if rationalisation occurs in the industry. If an agency chooses to use a service provider, and then use their systems to establish an Internet presence, they will need to assess the viability of the provider. There are also other important considerations, covering issues such as integrity, confidentiality, and the security arrangements at the provider’s site. In order to minimise the impact that such changes in service provider would have, consideration should be given to registering a domain name (see Glossary) for an agency. This would enable the agency to change providers with as little impact as possible on the agency’s clients and operations.
Balancing Risks and Costs

Findings

Figure 4: Risk Assessment Undertaken

Source: OAG

Just over 30 per cent of agencies had undertaken a specific risk assessment exercise in relation to their Internet usage. A further 50 per cent had considered some of the risks during their decision making process, such as deciding on the type and configuration of their security systems. The remainder primarily had a presence publishing on the Internet rather than using its other services.

It is also important to consider who is managing the operations and therefore the risks. In nearly 75 per cent of cases, responsibility for managing Internet usage (maintaining a connection, providing access to services, and monitoring security) rested with the Information Technology group in an organisation. In 20 per cent of cases responsibility was shared — across Information Technology, user areas and/or consultants. In one case the day-to-day management was completely outsourced. Outsourcing does not remove or diminish management’s ultimate responsibility for monitoring usage and information content.

All agencies felt that their corporate data was safe from unauthorised interrogation, corruption or loss through access via the Internet. Where risks had been considered, emphasis had been primarily placed on security issues.

More than 60 per cent of agencies reported some concern regarding the response time when using the Internet. There had been little attempt to address service provision issues through changes in service provider.
Balancing Risks and Costs

For those agencies where an ‘acceptable use’ policy was reviewed, specific consideration was usually found for the handling of software retrieved through the Internet. The issue of proper licenses for software will need ongoing monitoring.

Good Practice

- Undertake a risk assessment prior to implementing Internet connections and services.
- Review the risk assessments each time a change occurs — either in the Internet services used or in the risk minimisation processes.
- Address the issue of licensing of software downloaded via the Internet.
- Set up guarantees in the event of a provider failing or being taken over by another provider.
- Consider the level of expertise available within the agency.
- Seek assurances from Internet Service Providers that material published using their systems is safe from alteration by other subscribers to that provider or other Internet users.
- Consider registering the agency’s own domain name, so that changes in service provider do not affect references to the agency.

COSTS

Background

The cost of using the Internet varies widely, depending on how it is used. New expenditure will be incurred, some savings may be achieved, and in some areas the costs and savings may tend to cancel each other out. There are three potential areas of expenditure: establishing a connection, establishing an Internet presence on the World-Wide Web, and the ongoing maintenance of either or both. In any case, cost components are likely to grow as a greater need is seen by agencies to provide more staff and/or clients with access to the facilities of the Internet, and to expand the services provided on the Internet.
Balancing Risks and Costs

Additional cost considerations include the training of staff and provision of support facilities — both of which can influence staff productivity. Indeed, the issue of staff productivity is an important consideration. Without ‘appropriate use’ policies and close monitoring of the services used by staff, it is possible that productivity will fall when access to the Internet is introduced. Staff need to be informed of their responsibilities, and the risks to both themselves and their organisation, arising from inappropriate use of some Internet services.

Also as part of overall cost considerations, the agency’s operations should be reviewed and recognition given to the cost of not providing services via the Internet. All components of costs need to be incorporated into the justification case.

Findings

Only one agency was found to have had a specific Internet budget item. The others were equally split as to whether Internet costs formed part of the computing budget or part of the user budget. In most cases they were part of a service delivery budget rather than separately identifiable.

Nearly half the agencies reported initial establishment costs under $20 000. Nearly 30 per cent had initial costs in the $20 000 – $75 000 range. Two agencies reported all up costs exceeding $75 000. Over 15 per cent of agencies could not readily separate their initial Internet costs, since they formed part of their normal service delivery.

![Figure 5: Initial Set-up Costs](image-url)
Balancing Risks and Costs

In terms of annual maintenance costs, nearly half the agencies reported expenditure below $5,000. Nearly 30 per cent fell in the $5,000 – $10,000 range. Only one agency spent more than $10,000. The remaining 20 per cent of agencies could not readily separate these costs. Costs were mainly being monitored by the Information Technology group (65 per cent of cases).

![Pie chart showing maintenance costs distribution](image)

**Figure 6: Maintenance Costs**

Nearly 70 per cent of agencies provided some form of internal Internet training for staff. Half of the remainder provided training through external sources, with the balance providing no direct training opportunities. Some form of support to internal users of the Internet was available at all agencies with more than 75 per cent providing this themselves.

Just over 30 per cent of agencies reported some concern about the possible negative effect on staff productivity through the use of the Internet. Several agencies had limited the use of ‘newsgroups’ as a service as they considered it had a potential adverse effect on productivity.

**Good Practice**

- **Budget for expected initial costs of setting up Internet services and for their ongoing maintenance.**
- **Estimate any likely resource implications associated with ongoing Internet usage and presence.**
- **Consider the cost of not providing services via the Internet.**
Managing Information

INFORMATION AND RECORDS MANAGEMENT

Background

Information is one of the primary assets of any organisation. This is particularly so for public sector organisations. Without proper management, an agency faces the risk of making information available to unauthorised people, releasing information that is not current, or providing the wrong information entirely. There may also be legal ramifications such as breaching privacy legislation.

Publishing on the Internet is, in principle, no different than publishing in paper form. There are, however, some added risks that do not arise (at least to the same extent) in the traditional method of publishing. For example, it is much more difficult to contain any release of incorrect information. The access that the Internet grants means that many thousands of people may have seen it before a mistake is discovered. It is not possible to recover the copies. People may even unwittingly pass copies of this incorrect information on, so that something akin to a domino effect may arise. The Internet also introduces a somewhat new risk to this area. With the search capabilities available on the Internet, it is a simple matter for anyone to compare information released by two or more agencies on any topic. If this information is contradictory, the potential for damaging the credibility of an agency exists.

The same rules as those required for proper records management, archival procedures, version controls, duty of care and authorisations need to apply to information released via the Internet. These are easier to apply when control over information is consistent across an agency. It is considerably easier to bypass controls when publishing material electronically or making it available as attachments to mail. Copyright issues may have more of an impact, since it is easier to have plagiarism occurring because of the ease with which an electronic document can be copied and republished.

Control over information is more readily exercised when there is clear responsibility and accountability for that information. This can be achieved by coordinating control through a specific Information Officer role or designating a number of different information groups or owners each with their own point of control. On an
Managing Information

organisation wide basis there needs to be a clear understanding of how information (or data) is classified to ensure consistency in what information can be made available and to whom.

Findings

In 50 per cent of agencies an overall Information Officer role appeared to exist, with a further 25 per cent reporting a sharing of this role across several groups within the agency. There was some uncertainty about responsibility in the remainder of agencies. Less than 25 per cent of agencies were confident that they had a working data/information classification system in place, which is of concern in general terms, quite apart from the Internet. The degree to which such a need exists depends on the type of information being made available on the Internet but its absence makes it more difficult to get it right.

At least 35 per cent of agencies reported that material published on the Internet World-Wide Web did not come under normal records management and archival procedures. In most of these cases such material was an electronic copy of existing published information which did fall within such procedures. Nevertheless, several cases were identified where agencies may be exposing themselves to loss of trails of what they have published over time. From a legal point of view, this is particularly relevant where information is volatile and provides advice upon which people are likely to act.

Office of the Auditor General
Managing Information

Good Practice

- Allocate clear responsibility and custodianship for information management.
- Incorporate electronic publishing into records management and archiving procedures.
- Maintain version controls over electronic publishing.
- Classify data/information before determining what to publish.

PUBLISHING REQUIREMENTS

Background

The Information Policy Council has developed a policy regarding publishing on the Internet. It outlines a number of items for which agencies are accountable. These include: claiming Crown copyright; stating copying permission; indicating authorisation; and generally exercising a duty of care. Also listed as desirable in other guidelines are: indicating the size of documents; indicating date last updated; and providing disclaimer statements. These all form part of the desire to develop and maintain a coherent and organised structure to the public sector’s presence on the Internet. As more electronic publishing occurs, issues regarding intellectual property and ownership of information will arise.

Ease of use for customers is also of importance in developing Web pages. A balance needs to be maintained between attractiveness of pages and the length of time graphical work can take to download.

Ease of navigation through Web pages should be a prime design criterion. This needs to consider both the end customers’ point of view and any consistency of presentation desired across the public sector. The growing use of providing links within a site to other information increases the concern that some links may not always be working. This can cause frustration to users. The links should therefore be checked regularly.
Search engines are a facility on the Internet that allow people to quickly find information. They catalogue and index many millions of pages of information throughout the world. Finding an agency’s Web pages without using the WA Government’s entry is made easier by ensuring that they are registered with the major search engines.

Findings

![Publishing Requirements](image)

Figure 8: Publishing Requirements

Source: OAG

The examination considered the above publishing requirements only in relation to each agency’s Home Page. For that reason, some may not always be applicable to the Home Page but more relevant to subsequent published material. Half the agencies were found to have a copyright statement. Less than 20 per cent of agencies stated copying permission with less than 15 per cent providing an indication of authorisation. Some form of disclaimer statement was found on 25 per cent of pages with 50 per cent of agencies indicating a date last updated.

The integrity of links between Web pages and references was being checked to some extent by 70 per cent of agencies. During the examination, two instances were encountered where the link from the Government Home Page to an agency was not operational for at least three days. While the reason for the link not working...
Managing Information

in those cases was not identified at the time, it is indicative of the sort of frustration a user could experience.

Good Practice

As applicable, ensure that publications:

- claim Crown copyright;
- state copying permission;
- check copyright before publishing;
- provide disclaimer statements;
- state currency of information;
- state authorisation for publishing;
- indicate size of documents;
- minimise unnecessary graphics;
- include a link to the WA Government Home Page;
- register site with leading search engines;
- provide an option for customer feedback by e-mail or electronic form;
- monitor integrity of links; and
- provide ease of navigation.

CURRENCY OF INFORMATION

Background

A key accountability item for agencies under the Information Policy Council’s policy on publishing is “maintaining the currency and quality of published information”. This is consistent with the view that incorrect or out-of-date information can be worse than no information. As more and more agencies publish more and more information on the World-Wide Web, the issue of currency of information is likely to become of increasing concern. Aside from the aspects of providing a useable customer service, information that is not valid at the time of publication could leave an agency open to legal liability where incorrect advice is acted upon.
Managing Information

Maintenance of information published on the Web can produce an increasing load on agency resources if that information is complex, voluminous or volatile. That load needs to be considered during the justification process as it could add substantially to the overall cost of providing an Internet service.

A possible solution to these problems lies with automating the content and maintenance of Web pages. This should be given consideration if there is to be any substantial move to publishing electronically.

Findings

Figure 9: Currency of Information

Source: OAG

Four categories were identified in discussing the currency of information with agencies. A number of agencies (35 per cent) published only small amounts of information, usually not highly volatile, so found it relatively easy to ensure it was kept current. A similar proportion allocated responsibility to each of the areas within the agency that provided that information, thereby reducing the effort each had to undertake to maintain currency and accuracy. Ten per cent of agencies had automated the updating of their Web pages by passing information directly from their databases.
Managing Information

The remainder (20 per cent) reported that they already see this as a problem area because of resource constraints. Two agencies indicated that they had been unable to update some of their published information for more than a year because the resources required to do that were not available.

**Good Practice**

- Ensure information being relied on by clients is current and accurate or state an appropriate disclaimer.
- Automate updating of electronic published information where possible.
- Determine the resourcing load of maintaining ever increasing amounts of electronic published information before committing to it.
Providing Security

PHYSICAL MECHANISMS

Background

No single person or organisation has responsibility for managing the Internet. The actual physical connection to the Internet may be controlled, but the Internet itself is free from the influence of any organisation or public sector agency. This is both a benefit and a risk, and is one of the main reasons why organisations must take responsibility for managing their Internet connections.

In order to protect their information from alteration or improper use, agencies have traditionally controlled access to both it and their computer applications by using internal layers of security. These security measures restricted access to only those people who needed it to do their job. When it became possible to offer dial-up access to agency systems, extra levels of security were introduced. In order to gain access to agency systems with dial-up facilities, it would be necessary to have permission to use these facilities, and then to also have permission to view the data or use the software applications. These initiatives are essential to protect the integrity of public information and to ensure that privacy is protected. If an agency decided to connect their network to the Internet directly, there is yet another level of security that must be introduced in order to have adequate protection of data resources. It is essential that this path not be followed until the agency has carefully addressed the risks that need to be countered.

The Internet poses some special considerations regarding security of information and systems, as well as emphasising the need for security in general. The Internet has the potential to open an agency’s computing resources to the world. Without adequate security it is, in effect, extending any existing network to include unknown people and organisations in unknown locations on the Internet. ‘Hackers’ can attempt to gain access to computer systems and may choose to disrupt operations, corrupt information kept on the systems, or make the information available to anyone, anywhere.

When establishing a connection to the Internet, it is necessary to consider both how the connection is established and what services will be used when assessing security risks. It is now true to say that any Internet connection provides a potential...
way of accessing the computer being used by the agency, and therefore the agency’s network. All types of connections must be managed in order to minimise the possibility of outside parties gaining access to public and agency information. However, any perimeter type of security can be rendered ineffective if staff are permitted access to the Internet which bypasses the security system.

The first step is to develop and establish a sound security policy based on a risk assessment. This will then address the sorts of barriers that must be installed to prevent unauthorised communications between the agency’s computer systems and the Internet.

**Figure 10:** Standalone connections to the Internet
A standalone connection ensures that there is no direct link between the agency’s computer systems and the Internet.

Source: OAG and Corel
Providing Security

Figure 11: Firewall connection to the Internet

A ‘firewall’ helps to protect an agency from the dangers posed by the Internet.

A ‘firewall’ is a collection of devices that restricts data flow between computer networks according to a set of security standards. This can range from a one-way flow of data — such that nothing can enter a network, while anything can leave it — to an unrestricted two-way flow of information. Neither extreme would, in practical terms, be desirable, so firewalls are used mainly as access control devices. The most common approach is to permit any service unless expressly denied, rather than denying any service unless expressly permitted. The latter approach, however, is more desirable from a security perspective.
Findings

Figure 12: Physical Security Mechanisms
All agencies examined have some form of physical security associated with their Internet services.

Source: OAG

Some agencies operate their connection to the Internet via a separate standalone computer not connected to other computers. A few only have a publishing presence on the Internet which is accomplished via a service provider. Just over 30 per cent of agencies fitted into these categories. The risks that agencies in these classes face are fairly minimal, especially regarding agency data. Care should be taken that, having established a low risk Internet presence, progression to a higher risk scenario is not permitted without the requirement to undertake the risk assessment process.

The other agencies (70 per cent) used some form of physical computer security device or combination of devices to provide access control between their computers and those on the Internet. While firewalls can provide security in these environments, it is important to note that they are only effective if they are properly configured and managed.

All agencies saw Internet security as part of their overall Information Technology security responsibility. Nearly 75 per cent of agencies considered themselves solely responsible for security. The remainder reported some responsibility being shared with a service provider or consultant. In 50 per cent of cases, agencies reported they were satisfied that they were managing potential exposures as well as they could. The remainder considered their current security and use of the Internet did
Providing Security

not provide additional exposures. The confidence level regarding security was generally high, although 50 per cent of agencies reported limited internal expertise regarding Internet security.

At least 50 per cent of agencies reported potential for staff to dial-up direct from their desks. Such dial-up facilities are not Internet specific but provide an opportunity for controls to be bypassed. Logs of Internet access, for example, would not show such usage. Most agencies are relying on policy type controls to regulate this.

Good Practice

◆ Determine which security mechanism is warranted on the basis of costs, potential exposures, acceptable risks and the requirements of security policies.

◆ Use external expertise when considering mechanisms outside the field of internal expertise.

◆ Permit only those accesses and services specifically wanted rather than allowing all by default.

◆ Manage and monitor all security mechanisms.

LOGICAL MECHANISMS

Background

The security framework of an organisation relies on both physical and logical security. The physical components of the security framework mentioned above will almost always require a level of logical control.

Agencies will already have a system of layered security for their internal information systems based on passwords and access permissions. When connecting to the Internet, an agency must give additional consideration to addressing the specific risks that such a move exposes, usually through additional logical controls. Security measures need to protect against unauthorised access to, and disclosure of, information both from outside an agency and from within.
Providing Security

Findings

Authentication controls are designed to ensure that only people who should have access can access computer systems. In most cases, agencies rely on the use of user identification codes and passwords. The password is the important part of the security equation here, since it is fairly simple to find someone's user identification code. This means that people must ‘do the right thing’ to select and keep secret an appropriate password.

A higher level of access security removes this reliance on what someone knows, and places it on what someone owns. For example, one agency reported the use of dial-back modems — where the server will telephone the user’s computer and grant it access after being notified by a call from the user to signal they want access. Another agency used individually issued Identification Security cards that require synchronised codes to be entered before access is granted.

Another option to protect data while it is in transit on a network or the Internet is to use encryption. Although no agency reported this option as a standard mechanism for users to implement, about 20 per cent either used some form of encryption available in software packages already installed, or through the use of encryption at the modem. Individuals within agencies can, and some do, encrypt their own information content.

Good Practice

- Re-affirm the principles of good password use.
- Consider additional authentication methods beyond passwords where exposures warrant.
- Evaluate the need for encryption mechanisms.
MONITORING

Background

Developing security policies and implementing the resulting physical and logical security mechanisms are not the only tasks that must be undertaken. With the rapid improvements in technology, all security features need to be constantly managed and monitored to ensure they are still relevant and still working as intended. Some of this monitoring requires that usage of the Internet be logged and reviewed. Monitoring the systems will enable the detection of attempts to breach the security of the firewall, identify inappropriate use by staff, and assist a review of the appropriateness of security policies. However, as mentioned earlier, where staff have individual dial-up access to the Internet, monitoring of such access may not be possible.

Monitoring also extends to ongoing checks for computer viruses. These viruses are readily transmittable via the Internet. In some forms viruses are embedded in data, where it may not be possible to detect them until after they are activated.

Findings

All agencies reported that virus checking software was used, at least at the personal computer level. Some agencies also reported that virus checking took place at the network level.

Usage logging was common although this was primarily for statistical purposes. The evaluation procedures for the logs were still being developed in some agencies. A few agencies use an independent third-party to provide active monitoring of their firewall facilities.

The extent to which agencies evaluate the usage of the Internet by their staff appears to depend largely on the number of staff who have access to the Internet, and the extent of the services they use. In 40 per cent of agencies, less than ten staff had access to the Internet — a number of these sites had only one standalone computer available for access. Less than 30 per cent of agencies had more than 50 staff with Internet access available and these agencies tended to perform more evaluation of
Providing Security

usage. One agency reported that evaluation of usage had led to one group of users having access removed since their usage pattern was not consistent with their work requirements.

In two cases, the evaluation of logs had revealed unsuccessful attempts to gain unauthorised access through the firewall. Warnings from security groups such as AUSCERT regularly advise of the latest attempts to break through security and which software weaknesses are being exploited. Only 25 per cent of agencies reported subscribing to such security groups.

No agency reported actively monitoring electronic mail, although at least one provided the option to automatically store important messages.

**Good Practice**

- Log, monitor and evaluate uses of the Internet.
- Use up-to-date virus checkers at all potentially exposed components.
- Subscribe to reputable security advisory services.
- Warn staff in advance when deciding to monitor or store electronic mail messages in line with privacy considerations.
- Consider attacks where viruses are embedded in, for example, e-mail data when evaluating security measures.

**INTERNAL POLICIES**

**Background**

Policies form the cornerstone of any control mechanism. Security policies in particular provide the basis for any form of security an agency wishes to employ. Such policies must be clear, disseminated to all parties and enforced. Policies in relation to the Internet need to cover both what is coming in and what is going out and build on existing network and security controls. They need to stipulate what is permitted and concentrate on protecting the public information assets. Agency
Providing Security

and Public Sector image should also be a factor considered. When a strong policy is implemented together with well managed physical and logical controls, security can begin to become effective.

Existing policies covering backup and disaster recovery need to incorporate the elements associated with the Internet. To develop these policies, an agency’s internal network documentation must be up-to-date. The design of controls needs to consider input from all functions in an agency that can affect security.

Findings

A site security policy (including drafts) incorporating Internet usage was reported at 70 per cent of agencies. The remainder (generally smaller agencies) were unsure as to the extent any policies specifically covered their current or proposed Internet usage. Several agencies had policies established in advance of the Internet services being provided.

Good Practice

- Incorporate additional requirements generated by Internet connection in site security policies and procedures.
- Maintain accurate documentation of internal networks.
- Ensure that the appropriate functions (such as security and communications networking) within an agency have input when designing security controls.
Establishing a Management Framework

TECHNICAL

Background

Technical standards are applicable to a whole range of issues associated with the Internet. For this examination, the only standard specifically checked for all agencies was that applicable to information published on their Web pages. To enable any user to read published Web pages, such pages are ‘marked up’ using a specific language (referred to as HTML — Hyper-Text Markup Language), that is recognised by the Web browser software used as a World-Wide Web navigation aid which is used to read those pages. Standards apply to that language, although these have been slow in keeping up to date with the need to publish attractively presented Web pages and provide ease of use. By far the most popular Web browser in use around the world is Netscape Navigator. This recognises the HTML international standard but also provides its own extensions to that standard to allow for more scope in publishing.

Findings

As part of the analysis of agencies' home pages, they were validated against the applicable HTML technical standard. Three different validations were applied, with no agency's Home Page fully meeting any of these standards despite some agencies stipulating this requirement when outsourcing the development of their Web pages. For most Internet users this deficiency is not likely to cause any problems, but agencies need to keep their likely clients in mind and the types of Web browsers they may be using. A failure to adhere to the standards may mean that while one browser ‘interprets’ what is meant correctly, another will not, and information will be lost. The overriding presumption by most agencies is that users will have Netscape Navigator available as their Web browser, which does work on their Web pages, despite the fact that one of the validation tests failed was against Netscape's own standard.
Establishing a Management Framework

As there are other Web browsers likely to remain in the market place, the best assurance that all clients will be able to read an agency’s World-Wide Web pages is to ensure that the underlying HTML standards are used.

Good Practice

- Know who and where (in general terms) your customers are and their likely use of Internet facilities.
- Comply with the appropriate mark-up language standards applicable to Web publishing.

Agency

Background

Each agency needs to develop their own policies and guidelines outlining how they will cope with the issues that are likely to affect them. These will form the basis of the framework of control that management should be able to rely on to meet their accountability responsibilities.

A range of issues need to be addressed by agencies when dealing with Internet usage and presence. This range will vary depending on the services subscribed to on the Internet, the way those services are provided and the method used to gain access to those services. The issues to be addressed range from usage by staff — to access security — to information content control. The critical first step however is that internal policies and guidelines, such as ‘Acceptable Use’ policies, are available to address these issues. Any subsequent measures employed will have limited value if they are not part of policy. Also vital to the ongoing relevance of policies and guidelines is an audit process in place to ensure that they are being adhered to.
Establishing a Management Framework

Findings

Nearly 75 per cent of agencies were found to have some form of policy or procedures dealing with Internet usage. The majority of these were still in the draft stages. Some agencies were found to have quite comprehensive policy statements covering the range of issues associated with their use or planned use of the Internet. A number required signed application forms for usage that incorporated agreement to such conditions as ‘Acceptable Use’. Less than 20 per cent of agencies had not yet considered the legal and ethical issues relating to published information, although these tended to be agencies in the early stages of publishing information.

About a third of agencies were satisfied that their audit of procedures would be adequate. A similar amount (35 per cent) were unsure of that adequacy, with the remainder not having a process in place to audit their procedures for relevance and adherence.

Electronic Commerce which involves using the Internet for financial transactions, was under preliminary consideration at only a few agencies. Of the agency policies that were reviewed, only one specifically included reference to this method of doing business.

No specific attempt was found to nominate an official Internet spokesperson for an agency in their policies (such as an Incident policy) — this is currently a growing issue overseas.

A few agencies have procedures in place, or were considering them, for the charging of fees, or allocating of costs, to their various cost centres making use of Internet services.

Good Practice

- Provide clear policies and guidelines for staff on the conditions of use of the Internet.
- Update existing policies relating to security, publishing and information management to incorporate the changes brought about through Internet usage and presence.
Establishing a Management Framework

GOVERNMENT

Background

The framework under which all the above issues should be gathered are the policies, standards and guidelines set by central agencies and by the agencies themselves. Also applicable are any technical standards that need to be followed in using the facilities of the Internet. Without this framework in place, attempts to separately address the issues raised have limited chance of success. Indeed, in many cases, the only safeguard is adherence to the control framework itself.

The Information Policy Council has published two policies dealing with the use of, and presence on, the Internet. These are:

◆ Connecting to and use of Internet or other Public Networked Information Services.
◆ Publishing on Internet or other Public Networked Information Services.

During the course of this examination, the State Supply Commission released a User Guide, under Contract 026A1996, for the “Supply of Internet and Internet Related Services”. This guide provides assistance in selecting services relating to the Internet in the areas of Service Provision, E-Mail, Web Development and Consultancy. Its adoption was not considered during this examination since agencies had not had an opportunity to use the panel contracts.

The Public Sector Management Office (PSMO) has made some draft guidelines available to agencies. These include the series on ‘AARNet Usage and Security Guidelines’ that have been published as drafts for some eighteen months. Also available from PSMO are ‘Internet Publishing Guidelines’. These were updated during the course of this examination. The Joint Network Security Working Party, operating on behalf of two focus groups of the Information Policy Council, are drafting their ‘Internet Security Policy’ that agencies will need to consider when it is published.

The rate of change in opportunities and risks through the Internet is rapid. Existing policies and guidelines need constant updating. Somewhat paradoxically, the Internet itself is the likely source for the most up-to-date advice available.
Establishing a Management Framework

Findings

All agencies were aware of the published Information Policy Council policies, with 50 per cent being aware of one or more of the drafts. The extent to which agencies adhered to the responsibility requirements raised in those policies varied. These are addressed in more detail in the other sections of this report. At least half the agencies felt more detailed direction from Government would be of benefit to them. No correlation was found between this latter group and the level of awareness of the draft guidelines by agencies.

Smaller agencies in particular had more difficulty in keeping up with changes to the Internet environment, primarily because of their lower level of resources and expertise. The ongoing availability of good practice guidance will be of specific benefit to them.

Good Practice

- Adhere to the responsibility requirements contained in the Information Policy Council policies wherever applicable.
- Maintain an awareness of emerging guidelines based on changes to the Internet environment.
- Monitor key Internet advisory services for notifications of security problems and changes to relevant standards and guidelines.

Conclusions

There has been a lot of activity in the public sector pertaining to the Internet. Many agencies are connecting to the Internet, and at an increasing rate. While most agencies perceived benefits from the Internet they are not yet able to quantify them.

Some agencies are already having difficulty resourcing the maintenance of accurate and up-to-date information published on the Internet. These resourcing issues need to be examined before agencies formally move to disseminate information in this way.
Establishing a Management Framework

The risk assessments that have been performed have been aimed at security issues whereas potential legal exposures from published information have received little attention. This area will need to be addressed at both agency and public sector-wide levels before matters arise that force them to be addressed.

Policies and procedures on Internet usage and associated information management are lagging behind agencies’ moves to join the Internet.

The current state of involvement on the Internet by public sector agencies means that it is important to develop policies and guidelines that are relevant across agencies, as well as placing the onus on agencies to examine their own operations and develop relevant policies.

Recommendations

🔹 Agencies should establish an Internet Management Framework that:
  - applies the appropriate good practices presented; and
  - considers the possible benefits of Internet usage and assesses their relevance to the agency’s function and operations.

🔹 The Public Sector Management Office should, as part of their coordination role in setting policies and standards:
  - determine how best to coordinate the information presented on the Internet across agencies;
  - develop and maintain good practice guides on Internet usage; and
  - facilitate the establishment of a register (via the Internet is an option) of appropriate security and advisory services.
Appendix 1: Good Practice Summary

Policies, Standards and Guidelines

- Adhere to the responsibility requirements contained in the Information Policy Council policies wherever applicable.
- Maintain an awareness of emerging guidelines based on changes to the Internet environment.
- Monitor key Internet advisory services for notifications of security problems and changes to relevant standards and guidelines.
- Provide clear policies and guidelines for staff on the conditions of use of the Internet.
- Update existing policies relating to security, publishing and information management to incorporate the changes brought about through Internet usage and presence.
- Know who and where (in general terms) your customers are and their likely use of Internet facilities.
- Comply with the appropriate mark-up language standards applicable to Web publishing.

Business Case, Costs and Benefits

- Decide in advance why the Internet is going to be used, who is going to use it and for what purpose. Use this information in the risk assessment process.
- Consider the opportunities for using both the Internet and the Intranet.
- Consider re-engineering internal work practices in association with Intranet usage.
- Decide on the acceptable cost level and desirable benefits to be achieved and review the project against these criteria at appropriate intervals.
- Undertake a risk assessment prior to implementing Internet connections and services.
- Review the risk assessments each time a change occurs — either in the Internet services used or in the risk minimisation processes.
- Address the issue of licensing of software downloaded via the Internet.
- Set up guarantees in the event of a provider failing or being taken over by another provider.
Appendix 1: Good Practice Summary

- Consider the level of expertise available within the agency.
- Seek assurances from Internet Service Providers that material published using their systems is safe from alteration by other subscribers to that provider or other Internet users.
- Consider registering the agency’s own domain name, so that changes in service provider do not affect references to the agency.
- Budget for expected initial costs of setting up Internet services and for their ongoing maintenance.
- Estimate any likely resource implications associated with ongoing Internet usage and presence.
- Consider the cost of not providing services via the Internet.
- Determine anticipated gains from Internet usage and presence and measure achievement of these.
- Monitor gains made by others for applicability in an agency’s own environment.
- Share ‘success’ stories with other agencies.

Security

- Incorporate additional requirements generated by Internet connection in site security policies and procedures.
- Maintain accurate documentation of internal networks.
- Ensure that the appropriate functions (such as security and communications networking) within an agency have input when designing security controls.
- Determine which security mechanism is warranted on the basis of costs, potential exposures, acceptable risks and the requirements of security policies.
- Use external expertise when considering mechanisms outside the field of internal expertise.
- Permit only those accesses and services specifically wanted rather than allowing all by default.
- Manage and monitor all security mechanisms.
- Re-affirm the principles of good password use.
- Consider additional authentication methods beyond passwords where exposures warrant.
Appendix 1: Good Practice Summary

- Evaluate the need for encryption mechanisms.
- Log, monitor and evaluate uses of the Internet.
- Use up-to-date virus checkers at all potentially exposed components.
- Subscribe to reputable security advisory services.
- Warn staff in advance when deciding to monitor or store electronic mail messages in line with privacy considerations.
- Consider attacks where viruses are embedded in, for example, e-mail data when evaluating security measures.

Information Management

- Allocate clear responsibility and custodianship for information management.
- Incorporate electronic publishing into records management and archiving procedures.
- Maintain version controls over electronic publishing.
- Classify data/information before determining what to publish.
- As applicable, ensure that publications:
  - claim Crown copyright;
  - state copying permission;
  - check copyright before publishing;
  - provide disclaimer statements;
  - state currency of information;
  - state authorisation for publishing;
  - indicate size of documents;
  - minimise unnecessary graphics;
  - include a link to the WA Government Home Page;
  - register site with leading search engines;
  - provide an option for customer feedback by email or electronic form;
  - monitor integrity of links; and
  - provide ease of navigation.
Appendix 1: Good Practice Summary

- Ensure information being relied on by clients is current and accurate or state an appropriate disclaimer.
- Automate updating of electronic published information where possible.
- Determine the resourcing load of maintaining ever increasing amounts of electronic published information before committing to it.
# Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication controls</td>
<td>Controls used to identify and confirm a user is authorised to gain access.</td>
</tr>
<tr>
<td>Common Digital Network (CDN)</td>
<td>The proposed government wide digital network aiming to rationalise existing agency networks with a view to progressively migrate to a whole-of-government service supporting the business needs of all agencies.</td>
</tr>
<tr>
<td>Computer virus</td>
<td>A computer program that could damage the information held on a computer, or adversely affects its performance.</td>
</tr>
<tr>
<td>Data/Information classification</td>
<td>Identifying what data (or information) can be accessed by whom in line with confidentiality, privacy etc. Also applies to who can authorise release of data/information.</td>
</tr>
<tr>
<td>Dial-up</td>
<td>Connecting one computer to another using a modem and a telephone line.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>A unique reference name for a group of computers. For example, a Department of Strategic Services could have a domain name such as dss.wa.gov.au</td>
</tr>
<tr>
<td>Download</td>
<td>To transfer information or computer files (including software) from a remote computer to your local computer. (see File Transfer Protocol)</td>
</tr>
<tr>
<td>Duty of care</td>
<td>Accountability that includes ensuring information published is accurate, up-to-date and does not breach privacy laws.</td>
</tr>
<tr>
<td>Electronic commerce</td>
<td>Undertaking business transactions using computer systems (such as purchase orders generated by one system for transfer to another).</td>
</tr>
<tr>
<td>Electronic mail (e-mail)</td>
<td>Messages that are sent to another person using a computer network.</td>
</tr>
<tr>
<td>Electronic publication</td>
<td>A publication produced for electronic distribution. Its format matches as closely as possible to any paper versions that exist.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Scrambling information in such a way that only those with an encryption key can view it. It is used to securely transfer information and files.</td>
</tr>
<tr>
<td>File Transfer Protocol (FTP)</td>
<td>One method of transferring files from one computer to another using a network or dial-up connection.</td>
</tr>
<tr>
<td>Firewall</td>
<td>A collection of components placed between two networks that control network traffic flow.</td>
</tr>
<tr>
<td>Home Page</td>
<td>The primary or main World-Wide Web page for an individual or organisation.</td>
</tr>
</tbody>
</table>
### Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML</td>
<td>Hyper-Text Markup Language. A subset of Standard Generalised Markup Language. This controls how the information on a Web Page is presented, and what elements to include. The information is interpreted by a Web Browser.</td>
</tr>
<tr>
<td>Incident policy</td>
<td>Policy covering responsibilities and actions in the event an incident occurs e.g. hacker corrupts agency data.</td>
</tr>
<tr>
<td>Information Officer</td>
<td>The person who has responsibility for managing the information controlled by an agency.</td>
</tr>
<tr>
<td>Internet</td>
<td>A network connecting many millions of computers around the world. It is more a set of protocols rather than an entity. No person or organisation is responsible for or controls the Internet.</td>
</tr>
<tr>
<td>Internet Service Provider (ISP)</td>
<td>A company that has established a permanent connection to the Internet, and then sells time on its system to subscribers, who in turn gain access to the Internet through the ISP.</td>
</tr>
<tr>
<td>Intranet</td>
<td>A system that uses the same tools and software as the Internet, but restricts access to members of a particular organisation.</td>
</tr>
<tr>
<td>Link</td>
<td>On a Web Page, clicking on a coloured and/or underlined word or picture (the link) makes the Web Browser load the information it refers to. This is generally another Web Page. Also known as a hyperlink.</td>
</tr>
<tr>
<td>Log</td>
<td>A computer file containing historical information that is automatically recorded by the computer system. For example, records about system usage.</td>
</tr>
<tr>
<td>Mailing list</td>
<td>By subscribing to a mailing list, an e-mail message sent to one address can be automatically forwarded to everyone else who has subscribed to the mailing list. It is used so that people who are interested in similar topics can share information.</td>
</tr>
<tr>
<td>Modem</td>
<td>An acronym for Modulator-Demodulator. This is the device that enables a computer to communicate with another computer using a telephone line.</td>
</tr>
<tr>
<td>Newsgroups</td>
<td>A public area on the Internet containing many thousands of topic areas. Anyone can post messages to any of these groups without any restrictions. Also known as the Usenet.</td>
</tr>
</tbody>
</table>
**Glossary of Terms**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Re-engineering</td>
<td>Re-designing processes and procedures in an organisation, generally so that they are more closely aligned with the mission and vision. It may also be necessary to re-engineer processes and procedures to take advantage of new computer systems.</td>
</tr>
<tr>
<td>Search engine</td>
<td>A method of finding information on the Internet. For example, see <a href="http://www.altavista.digital.com/">http://www.altavista.digital.com/</a> By registering an agency's reference (the URL), a user has a better chance of finding out about the service being offered.</td>
</tr>
<tr>
<td>Server</td>
<td>A computer that contains information that can be accessed via a network (such as the Internet). It also serves as an access control system for users.</td>
</tr>
<tr>
<td>Telnet</td>
<td>A protocol that enables a user to conduct operations on a remote computer.</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator. This is effectively an address that enables a Web Browser to locate information (generally web pages) on the Internet. For an example, see the entry for Search Engine.</td>
</tr>
<tr>
<td>Version control</td>
<td>A system to ensure that the most recent version of an electronic document (such as a web page) is always in use and previous version contents can be derived.</td>
</tr>
<tr>
<td>Web browser</td>
<td>Software that allows a user to access information on the World-Wide Web.</td>
</tr>
<tr>
<td>Web page</td>
<td>Information that contains formatting that enables it to be viewed by a Web Browser.</td>
</tr>
<tr>
<td>World-Wide Web (WWW)</td>
<td>A system that enables information to be presented using formatting, graphics, and containing links to other information.</td>
</tr>
</tbody>
</table>
Performance Examination Reports

1993

Internal Audit in Selected Government Agencies
Child Care in Western Australia
Public Sector Travel
Corporate Card
Main Roads Properties
Mining Royalties

November 2, 1993
November 10, 1993
November 16, 1993

1994

Utilisation of School Facilities in the Metropolitan Area
Grants to Non-Government Organisations
Pastoral Leases
Records Management
Purchasing
Public Hospital Waiting Lists Information: Waiting Times - The Real Issue

March 24, 1994
May 11, 1994
October 19, 1994

Financial Assistance to Industry
Public Rental Housing
University Consultancy Services

November 3, 1994

1995

Legal Aid Commission
Police Department Operations Centre
Management and Control of Minicomputer-based Systems in Western Australian Government Agencies
Management of the Public Bank Account Investments
Value for Money in TAFE
Public Sector Travel
Corporate Card
Cabcharge Facilities
Hospital Emergency Departments
Contracting for Services
Public Dental Services

April 5, 1995
May 4, 1995
May 23, 1995
August 23, 1995
August 30, 1995
September 19, 1995
November 1, 1995
November 22, 1995
December 6, 1995

1996

Improving Road Safety

May 1, 1996