



How to Decide to Use the Internet to Deliver Government Programs and Services



Internet Delivery Decisions

A Government Program
Manager's Guide



This component of the ANAO Better Practice Guide aims to help managers decide whether, and how best, to use the internet to deliver government programs and services.

It does not answer all the questions that internet delivery of government programs can pose. It is intended to help you make suitable decisions. It also points to other sources of information and advice.

The Guide contains various components to help managers make decisions about how best to use the internet. Each component has been written to be used alone. However, they are best read as part of the set of material. The components include:

- ▶ How to Decide to Use the Internet to Deliver Government Programs and Services;
- ▶ A Business Case and Cost-Benefit Analysis for Internet Use in Government;
- ▶ Designing and Maintaining Internet Sites for Government Programs;
- ▶ Costing Internet Service Delivery in Government;
- ▶ Monitoring and Evaluating Internet-Delivered Government Programs and Services;
- ▶ Internet Systems Security and Authentication for Government Programs;
- ▶ Legal Considerations for Government Internet Service Delivery;
- ▶ Privacy Issues, the Internet and the Government Manager; and
- ▶ How to Make Government Sites More Accessible.

Several government agencies with policy internet responsibilities have helped the ANAO produce this Better Practice Guide. Those agencies include the National Office for the Information Economy, the Attorney-General's Department; the Department of Employment, Workplace Relations and Small Business; the Office of the Federal Privacy Commission, Human Rights and Equal Opportunity Commission; and the Defence Signals Directorate. The work takes account of other agencies that have been in the forefront of internet use for service delivery.

This first component of the Better Practice Guide identifies:

- ▶ government policy and legislation relevant to making a decision to use the internet to deliver government programs and services; and
- ▶ questions you should answer when making your decision.

When you are familiar with government policy

When you know government policy towards internet use you will be better informed about making decisions on how best to use it to achieve the Government's objectives.

On 8 December 1997, the Prime Minister announced the Government's policy *Investing for Growth*. The statement included a plan to establish the Commonwealth as a leading-edge user of technology, including making all appropriate services internet-deliverable by 2001. Internet services were to complement—not replace—existing written, telephone, fax and counter services, and to greatly improve the quality, user-friendliness and consistency of those services.

In April 2000, the Government released *Government Online: The Commonwealth Government's Strategy*. This set out eight priority areas as follows:

- ▶ agencies to take full advantage of the opportunities the internet provides;
- ▶ facilitation of enablers such as authentication, metadata standards, electronic publishing and record keeping guidelines, accessibility, privacy and security;
- ▶ enhancement of government online services in regional services;



- enhancement of the impact of the Government Online initiatives on development in the Australian Information Technology industry;
- government business operations to go online;
- monitoring of best practice and progress;
- facilitating cross-agency services; and
- communicating with stakeholders.

The Government also defined a set of minimum online requirements or Online Information Service Obligations.

In November 2001, the Government endorsed a whole of government online portals framework to provide a customer-focused, coordinated approach to the Commonwealth's online presence. The framework describes the staged implementation of a number of portals identified on the basis of customer groups or subject matter areas. These portals will improve the reach of services to the customer groups that they are intended for, and facilitate linked transactions across agencies. They are intended to complement rather than replace existing and future agency and subject websites.

Three publications, issued by the Department of Communication, Information Technology and the Arts through the National Office for the Information Economy, detail government policy on internet use:

- *Government Online. The Commonwealth Government's Strategy;*
- *Commonwealth Electronic Procurement-Implementation Strategy; and*
- *Customer Focused Portals Framework.*

They are available at the following website—www.govonline.gov.au

Be informed about relevant legislation

Knowing the law means you can better deliver programs and services through the internet, by understanding the legal requirements and constraints. Two sets of laws are most relevant—administrative and program law.

Administrative law includes:

- the *Financial Management and Accountability Act 1997*, a framework for properly managing both public money and public property. It provides that Chief Executive Officers, who are responsible for their agencies, ensure that agency activities promote proper use of Commonwealth resources. Proper use means efficient, effective and ethical use. Program managers are responsible for delivering government programs consistent with this legislation. For more information, see www.dofa.gov.au/pubs/fmab/accountact.pdf
- the *Electronic Transactions Act 1999*. This Act clarifies the legal status of electronic transactions. It provides a regulatory framework that enables business and the community to use electronic communications in their dealings with government. For more information, see <http://law.gov.au/ecommerce>
- the *Human Rights and Equal Opportunity Act 1986*. The Human Rights and Equal Opportunity Commission is responsible for investigating complaints under this Act. For instance, in regard to access and equity barriers to government programs and services. For more information, see <http://www.hreoc.gov.au>

- ▶ the *Privacy Act 1988*. This Act details strict privacy safeguards which Commonwealth agencies must observe when collecting, storing, using and disclosing personal information. The Act also gives individuals access and correction rights in relation to their personal information. For more information, see <http://www.privacy.gov.au>

Program law

The second set of laws is legislation governing the objectives and delivery of particular programs. This legislation could be about immigration, health, defence, education or another specific area of public administration. Agencies also must take into account and implement Cabinet and Ministerial decisions establishing program objectives and service delivery mechanisms.

Taking Action

Understanding the requirements of these two sets of laws will help ensure your decisions are well informed. By understanding how such laws interact you will be better placed to judge the best way forward.

The Financial Management and Accountability (FMA) Act and subsidiary legislation set out the requirements here by providing that if compliance with the requirements of the regulations, Finance Minister's Orders, Special Instructions or any other law would hinder or prevent the proper use of those resources, the Chief Executive Officer must manage so as to promote proper use of those resources to the greatest extent practicable while complying with those requirements. Proper use means efficient, effective and ethical use. In addition, expenditure must be in accord with government policies. You must interpret the significance of the requirements of the FMA Act and subsidiary legislation for all forms of program delivery, including internet program or service delivery. This means reviewing legislation to identify any constraints to using the internet for program or service delivery.

Key Questions

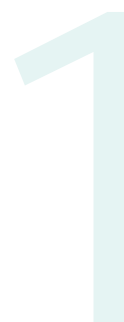
You must address several questions when assessing internet usage to deliver programs and services. Key questions are:

What services, if any, should be internet delivered?

It is important to note the difference between 'delivered' and 'deliverable'. Government policy requires all appropriate services to be deliverable through the internet, but not delivered as a sole means of delivery as this would exclude some clients.

Factors that program managers should consider and which are discussed in components of this Guide include:

- ▶ the importance of complying with government policy. Government policy requires all appropriate services being internet deliverable. It does not require delivering all services that way. You must decide what are appropriate services. Your decisions must be consistent with the relevant legislation.
- ▶ having sound reasons for internet program delivery. While government policy requires delivering appropriate services on the internet, it also requires managers to have efficient and effective program and service delivery. Therefore, in making your decision, you must know the costs and benefits of current and proposed electronic service delivery.



- ▶ identifying the target group for internet service delivery. Depending on the program's purpose, this could be all or some of the clients. Delivering some services through the internet, will mean you need a way to authenticate electronically your clients' identities. This has cost and time implications.
- ▶ internet delivery funding and costs. These include the immediate and likely recurrent costs to government, and the entry and recurrent costs to program clients. Who should and will pay those costs? Your decisions on an appropriate combination of staff and continuing staff training are other dimensions affecting costs. Cost estimation can include the cost of maintaining the existing means of program delivery. Maintaining dual means of program delivery increases the costs the agency faces when introducing the internet. Dual delivery systems may be required for a long time depending on the program's goals and its target group. The agency must ensure it can continue to fund dual means of program delivery if necessary.
- ▶ the value of a cost-benefit analysis in getting valid and reliable data showing that internet service delivery benefits outweigh costs. It is best to conduct a cost-benefit analysis before deciding to deliver a program through the internet, noting that not all costs and benefits are quantifiable. Agencies may more readily absorb any additional costs involving small programs. However, cost absorption will be more difficult for larger programs with many clients. Periodic review of the costs and benefits of internet solutions is advisable in view of the rapid changes in technology and client take-up rates.

How can you best use the internet to deliver government programs?

Programs and services are not necessarily delivered better when delivered through the internet. Knowing this is fundamental, because it will sharpen your understanding of both the advantages and limitations of internet service delivery.

You must be able to support your decision for using the internet. The Government has stated that it expected appropriate services to be internet-deliverable by 2001. A decision on delivering such services should be supported by an appropriate business case, setting out the costs and benefits to the agency, and identifying the agency's clients.

There are various ways to characterise government programs and services delivered by the internet. One way is to think of such service delivery in four stages.

- ▶ Stage 1 is a website that publishes information about the agency and its services to all internet users.
- ▶ Stage 2 allows any internet user to browse and interact with the agency's database or databases.
- ▶ Stage 3 includes the first two stages and permits users to enter information on the website, exchanging or transacting secure information with the agency.
- ▶ Stage 4 is the same as Stage 3, but in addition the agency, with the user's prior approval, shares that user's information with other government agencies.

These stages are described in more detail in ANAO Report No. 18, *Electronic Service Delivery, Including Internet Use, by Federal Government Agencies*. The report is available on the ANAO's website—<http://www.anao.gov.au>

You can place the program you intend to deliver, or currently deliver, in one of these four stages when defining your internet use. A program or service can be delivered satisfactorily at Stages 1 or 2, depending on the program's goals. It is not necessary for all programs to be at Stages 3 or 4. The program manager must decide at what stage of internet service delivery the program should be. Stages 3 and 4 can be the most costly for the agency and the most difficult to accomplish.

You should have current, appropriate privacy and data security policies and practices in place for internet sites.

You should take appropriate action to identify and minimise any associated legal liability for government, such as might be created if incorrect or misleading information on an agency's internet site lead to a user's financial loss.

Deciding on using the internet requires you to reassess the risks and control strategies used for service delivery. In general, the extent and cost of the security required increases as you progress through Stages 1 to 3. This is as organisations move from protecting their website from 'hacking' attacks, to the need for increased confidence in authenticating users, the need to protect agency data and ensure the integrity of web-based transactions.

Finally, you must decide, at an early stage, how best to monitor and evaluate internet service delivery. Such assessments can then improve service delivery and provide data for the cost-effectiveness of delivering by the internet.

Where to start?

There is no single best starting point for you to consider whether and how to deliver programs by the internet. However, one sensible starting point is talking to program managers who already deliver programs that way. They will probably be eager to share their positive and critical experiences in achieving program objectives using the internet. In addition, talk with agency information technology staff. These may share or have different views from program managers about delivering programs and services using the internet. By talking with program managers already using the internet and with information technology personnel, examples of sound and unsound uses of the internet can be identified.

The great majority of Commonwealth agencies have websites. Check to see whether and how your program is already included in your agency's website, even if it is only currently in the form of email addresses, links and embryonic Stage 1 information.

Use other websites for other programs, including those run by other agencies. By accessing those, you will soon become aware of websites that succeed from a user's perspective and those with limitations. However, generally speaking, it is not possible to assess the success of service delivery simply by accessing another website. It is just the most visible part of that service delivery.



Further Information

Further information about how to decide to use the internet to deliver government programs and services, and on how to deliver programs and services more effectively through the internet, is found in other components of this ANAO Better Practice Guide, called *Internet Delivery Decisions—A Government Program Manager's Guide*. The full list of components is:

1. How to Decide to Use the Internet to Deliver Government Programs and Services
2. A Business Case and Cost Benefit Analysis for Internet Use in Government
3. Designing and Maintaining Internet Sites for Government Programs
4. Costing Internet Service Delivery in Government
5. Monitoring and Evaluating Internet-Delivered Government Programs and Services
6. Government Internet Systems—Security and Authentication
7. Legal Considerations for Government Internet Service Delivery
8. Privacy Issues, the Internet and the Government Manager
9. How to Make Government Sites More Accessible

Printed copies of this Guide are available from the ANAO. Copies can also be downloaded from the ANAO website—<http://www.anao.gov.au>



A Business Case and Cost-Benefit Analysis for Internet Use in Government



Internet Delivery Decisions

A Government Program
Manager's Guide



Development of a business case is an essential step in making decisions on whether to deliver government programs and services via the internet. Part One of this component of the Better Practice Guide outlines issues that influence preparing a business case to use the internet in government. Part Two covers developing a cost-benefit analysis to assist with decisions on using the internet.

Part One

Developing a Business Case

Developing a business case is the first step in considering delivery options for any output or program. It underpins the decision-making process and cost-benefit analysis. It can be the focus for any later evaluation or audit. Once action to achieve the output or implement the program begins, it should be possible to revisit the business case to consider whether the program delivered what it set out to deliver and whether it did so effectively and efficiently.

The business case should consider the program's suitability for online delivery and define your internet site's objectives. The detailed analysis in the business case should cover:

- ▶ the aims and objectives;
- ▶ the costs and available budget;
- ▶ the time for delivery;
- ▶ the mix of services (transactions) and information that is to be made available online;
- ▶ current systems that need to connect to the site—these are existing electronic systems that your agency uses to administer its program or administrative processes;
- ▶ new systems that need to be developed to deliver the service;
- ▶ the capacity of new and existing systems to be integrated and made accessible through an internet site;
- ▶ stakeholders for consultation; and
- ▶ expected benefits—both quantitative and qualitative.

It is important to define at the outset what you want to achieve. Consider what online experience you want your clients to have, and define what will be your measure of success. This can be done quite simply at first—for example, it might be a simple requirement such as:

- ▶ Clients should be able to find out about how they can get help under the XYZ program.
- ▶ Tender documents should be available online together with updates.
- ▶ Clients should be able to apply for assistance under a government program using an electronic form.

or it might be a list of requirements such as

- ▶ Clients should be able to:
 - find Australian Business Numbers;
 - apply for an XYZ licence online; and
 - sign up holders of the XYZ licence to receive a regular electronic newsletter.
- And I want to be able to survey our clients to find their opinions about the XYZ regulations.

Obviously these lists would become much more complex in relation to highly functional sites with many transactions and features and which involve linkages between agencies.



Measures of success include the efficiency and economy that is gained from putting the service online. Therefore, program managers should develop performance indicators and associated targets early. These would be statements such as:

- a move from paper-based to online delivery with x savings; or
- x proportion of transactions are online at a cost of y per transaction.

Your business case should involve a cost-benefit analysis. How and when to conduct a cost-benefit analysis is described in Part Two of this component of the Guide.

Developing a business model

After developing the business case, develop a business model. This involves selecting the method to set up and oversee a project to build your internet site and manage it long term. It involves considering the mix of agency staff and/or contracted service providers who will implement your site and then maintain it.

It may also involve considering partnerships with technology providers who would want to invest their own resources in developing your site in return for a share in the revenue generated by transactions on the site. In this case, appropriate contractual and governance arrangements to ensure fair and transparent processes for selecting potential partners will be essential, as well as ensuring the Government's intellectual property, privacy issues and control of the site are assured. Most importantly, any arrangements put in place need to be capable of being dismantled when the contract ends so site and transaction management can be brought within the agency or passed to a new contractor.

The choice of business model will depend on such issues as:

- available financial resources;
- availability of staff in the agency with skills in managing internet sites;
- the degree of agency control over the site that is required or desired and the frequency of updates;
- time frame to establish the site;
- length and complexity of the program the site will support;
- how committed and involved senior agency managers are—this will strongly influence staff allocation from across the agency to help develop and maintain your site if you establish a devolved site maintenance arrangement; and
- interest from potential partners/contractors to invest in your project.

Agencies with well-developed information technology infrastructure are likely to have their own staff with skills and capacity to develop simple sites or to manage contractors who construct or develop the internet site.

Involving your IT administration representatives early in decisions about the business model is important. They can ensure the specifications for any new internet sites or transactions are compatible with the agency's existing infrastructure.

Contracting out may be the best method of ensuring a high quality product, however, it raises a number of important issues such as:

- the need to manage contract processes effectively to ensure the government gets value for money;
- costs can be high and difficult to control—especially with large, complex sites; and
- continuing website maintenance by external contractors can be expensive and affect your flexibility to frequently change the site.

Part Two

Cost-Benefit Analysis

Introduction

This component of the ANAO Better Practice Guide provides information about issues that need to be considered when you as manager of a government program are sponsoring or conducting a cost-benefit analysis of internet service delivery (ISD) options.

It is in two sections. The first section explains what cost-benefit analysis means, while the second section considers when to use a cost-benefit analysis for internet service delivery.

There are many Commonwealth publications on cost-benefit analysis. In effect, all the same steps need to be undertaken. Cost-benefit analysis is described more fully in the following publications of the former Department of Finance.

- ▶ *Introduction to Cost-Benefit Analysis for Program Managers; and*
- ▶ *Handbook of Cost-Benefit Analysis.*

This Guide aims to:

- ▶ briefly summarise the cost-benefit analysis steps; and
- ▶ highlight key issues to consider when conducting a cost-benefit analysis of ISD options.

Another relevant component of this Guide is titled *Costing Internet Service Delivery in Government*.

What is a cost-benefit analysis?

A cost-benefit analysis is:

- ▶ a way of organising information to aid decisions about resource allocation;
- ▶ a quantitative tool that systematically assesses the merits of a range of options; and
- ▶ a framework for identifying and quantifying the costs and benefits of decision and for analysing the data in a systematic way.

While the cost-benefit analysis framework provides rigour to evaluating service delivery options, it is only a guide and forms part of the decision making process. It is advisable to identify unquantifiable benefits and costs, such as benefits accruing to society from government policy towards online service delivery.

The aim of a cost-benefit analysis

The aim of cost-benefit analysis is to inform decisions on:

- ▶ the costs of alternative ways of delivering a service;
- ▶ estimates of the size of a project;
- ▶ whether a project should be undertaken; and/or
- ▶ whether a current project should be continued, changed or ceased.

How to go about a cost-benefit analysis

1. Determine the scope, objectives and business needs

Accurate determination of the scope, objectives and business needs is critical to the success of a cost-benefit analysis. The better the understanding of the business needs, the easier it is to identify options, costs and benefits.



The project scope can be categorised into one of four stages of internet service delivery defined in the component of this Better Practice Guide titled, *How to Decide to Use the Internet to Deliver Government Programs and Services*. These stages define websites as:

- ▶ Stage 1 is a website that publishes information about the agency and its services to all internet users;
- ▶ Stage 2 allows any internet user to browse and interact with the agency database(s);
- ▶ Stage 3 includes the first two stages and permits users to enter information on the website, exchanging or transacting secure information with the agency; and
- ▶ Stage 4 is the same as Stage 3, but in addition the agency, with the user's prior approval, shares that user's information with other government agencies.

2. Identify the constraints

Constraints may be legal, financial, policy, organisational or marketplace driven. Identifying constraints and considering alternatives ensures options are feasible.

Constraints to address in a cost-benefit analysis on internet service delivery may include:

- ▶ market or target group readiness-is the market or target group ready/able to utilise the services. This goes to the heart of service delivery cost effectiveness, i.e., is this the right product or service for the right target group at the right cost;
- ▶ take-up rate or target group acceptance of new technology-this affects the cost of continuing current services while the take-up rate of the new service matures; and
- ▶ changes in versions of software-will the marketplace or target group be able to keep up with new versions, patches and bug fixes?

3. Identify the alternatives

Options need to be explored, including the maintenance of any existing non-internet means of program delivery option. Understand how each of the options will affect your organisation in the future. All options need to take account of government policy.

Current program or service delivery option should be considered the 'base case'. In a later stage, when comparing the costs and benefits of each option, these costs and benefits are measured incrementally against this base case.

4. Identify costs and benefits

The costs may include:

- ▶ capital expenditures;
- ▶ operating and maintenance costs;
- ▶ staff costs;
- ▶ materials;
- ▶ research and development;
- ▶ opportunity costs; and
- ▶ environmental health and other social costs.

Benefits may include:

- ▶ better, more cost-effective service delivery;
- ▶ the avoided costs-being the costs of the existing or conventional program or service delivery option;
- ▶ additional revenues generated;
- ▶ productivity savings; and
- ▶ environmental, health and other social benefits.

Specific costs and benefits of the different stages of internet delivery are listed in the section addressing each of the stages later in this component.

5. Quantify the costs and benefits

Costs do not always involve expenditure. Opportunity costs need to be included in the cost-benefit analysis. For example, an opportunity cost of a resource such as land is measured by the value of its 'next best use', i.e. in a more traditional development project. Where we owned a parcel of land and were considering building an office, the opportunity cost of the land would be the market value of the land not the original purchase price.

In the case of an internet service delivery, if the two viable options were:

- ▶ Option 1—to build a complete new data base and supporting programs; or
- ▶ Option 2—to enlarge and enhance a current system, then;

In assessing the options the market value (if any) of the current system's operations (if saleable) would be an opportunity cost associated with the second option if the system had no other business use. If the system was still required it would not be an opportunity cost.

When looking at quantifying opportunity costs on internet service delivery, you need to understand the full cost and ramifications the project might have, and factor in to the cost of the internet project the cost of utilising existing and new capacity such elements as:

- ▶ the network infrastructure—what level of consumer take-up use will the network support and at what level might it need upgrading;
- ▶ computer storage capacity; and
- ▶ hardware and software requirements (including bandwidth).

You may also need to consider the costs of running existing service delivery systems in parallel with internet service delivery. Not all potential clients will have access to technology and the internet.

Quantifying benefits may be more difficult and frequently related to improved service delivery. You still need to quantify the benefits (savings) from ceasing/reducing the existing service delivery. Assessing what these benefits are and when they are achievable will depend on overcoming some of the issues raised earlier in Section 2 of this component—Identify the Constraints.

Another benefit to quantify is the potential saving in agency functions of assessing or processing forms. These savings may reflect more accurate information provision on the website and/or the way forms are completed on line, such as immediate rejection of incomplete forms.

Addressing the potential for better quality information from clients helps form the basis for quantifying the benefit. When existing service delivery ceases, the cost of that former service delivery would form the basis of the benefits for the new service delivery.

Another component of this Better Practice Guide is titled, *Costing Internet Service Delivery in Government*. The Attachment to that component lists costs associated with internet service delivery in government. The Attachment may be used when quantifying the costs and benefits of any decision to use the internet in government. Also useful is a separate ANAO Better Practice Guide, *Building a Better Financial Management Framework. Defining, Presenting and Using Financial Information*.

6. Calculating the Net Present Value

Knowing the timing of when the cost and benefits occur is extremely important. A cost-benefit analysis takes into account the Net Present Value (NPV) of the options. The NPV calculates the value of future operations in today's money.



Basically this step requires subtracting the cost from the benefit for each period. A discount factor is applied for each period. This recognises money received now can be invested and converted to larger future amounts. The current discount rate is in the order of 8–10 per cent. The Department of Finance and Administration can provide further information about discount rates.

An example NPV for development of a government internet service may look like:

| | | Year 1 | Year 2 | Year 3 | Year 4 | Total |
|--|-----------------------------------|--------|--------|--------|--------|-------|
| Benefits | ► Revenues | 25 | 25 | 50 | 70 | 170 |
| | ► Cost reduction of prior service | nil | 75 | 150 | 150 | 375 |
| | ► Other benefits | 40 | 40 | 40 | 40 | 160 |
| | ► Total | 65 | 140 | 240 | 260 | 705 |
| Costs | ► Capital | 65 | 25 | nil | nil | 90 |
| | ► Development | 70 | 40 | nil | nil | 110 |
| | ► Ongoing | 20 | 30 | 30 | 30 | 110 |
| | ► Total | 155 | 95 | 30 | 30 | 310 |
| Result = benefit – cost | | –90 | 45 | 210 | 230 | 395 |
| NPV—discount factor of 10% accumulating each year, applied to the yearly result i.e. estimate of today's value | | –90 | 41 | 170 | 168 | 289 |

7. Perform sensitivity analysis

Assessing future benefits, costs and discount rates cannot be done with certainty. While this deals with 'most likely' values, you need to adjust the values of the key variables up and down and measure the impact of these adjustments on the NPV.

The key variables are usually time, capital and continuing costs. The time of the project and therefore the capital required are often extremely important variables. Failure to meet the timing of delivery can alter the cost-benefit analysis outcome significantly.

The example in the previous section assumed developing and completing the new system in Year 2, winding up the old service by the end of Year 2. If time delays meant the new service was not delivered until Year 3 and the development cost increased due to the longer period of development, then there may be a reduction in benefits of 75 and 150 and an increase in costs of say 40. This could change the NPV of this option from 289 to 67. This may be less than the NPV of a different option which is less exposed to variables that may affect the time of delivery.

The performance of sensitivity tests will help us draw a picture of the range of likely outcomes given the adjustments to the variables.

8. Consider equity issues and intangibles

A typical cost-benefit analysis will aggregate costs and benefits without regard to individual equity. Government service delivery needs to address individual equity issues. Addressing these may have a cost, particularly when considering the market or target group's readiness for (and potential take-up rate of) internet service delivery. Not all clients will have access to, or the ability to use,

technology and these clients will need to be serviced in other ways. The cost of servicing clients using multiple delivery modes will need to be considered.

A separate component in this Guide addresses access and equity issues more fully.

Use of Cost-Benefit Analysis

Use a cost-benefit analysis for internet service delivery when:

- ▶ developing a new or replacement internet service;
- ▶ restructuring a service delivery which may be better delivered online; and
- ▶ reassessing how a service is delivered online.

Periodic review of the costs and benefits of internet solutions is advisable in view of the rapid changes in technology and client take-up rates.

As mentioned above, in the component of the Better Practice Guide titled, *How to Decide to use the Internet to Deliver Government Programs and Services*, four stages of internet service delivery are defined. To determine when to use a cost-benefit analysis, this Guide refers to those four stages.

Stage 1—A website that publishes information about the agency and its services to all internet users

This stage involves placing mostly static information about the agency, its programs and services on a website. This information is available to anyone with internet access and the World Wide Web (www). Clients access information using a web browser although viewing tools such as Acrobat reader are also commonly used.

Information can be presented in a simple text/graphic browser-ready format (simplest) or larger amounts of information may be published on the website in a downloadable file format suitable for viewing offline, e.g. portable document format (PDF). This type of internet service delivery has characteristically infrequent upgrade (say monthly), lack of sensitivity and privacy of information, and would be replicated in the non-internet domain as brochures, annual reports, general publications, corporate plans, press releases and the like.

Commonly, the information placed on the website is published in hard copy as well. Due to the relative simplicity of this stage, costs are modest. Other than general security of the website which will be shared across all programs, no special security features are required. Risk of information corruption is minimal as is the likelihood of a serious security breach. Initial development costs might include:

- ▶ collecting and organising the information;
- ▶ layout and design;
- ▶ developing web pages and links to information sources (minimal programming) although converting documents to PDF involves a little additional cost over simple browser-ready text/graphics but it may also involve some accessibility problems;
- ▶ artwork/graphic licences (if required);
- ▶ advertising and/or marketing of the service;
- ▶ periodically updating the information;
- ▶ costs of hosting the information on the website (shared with other programs);
- ▶ information backup; and
- ▶ depending on the location of the website, (internal or external host), there may be modest data communications costs for the uplift and download of information to and from the website.



As the website information in the stage commonly comes from previously published information, the costs of this use of the internet is in addition to, but trades on, the costs of publishing the original information. Indeed, the materials may be sourced from the printer or graphic designer at no cost from those previous hard copy projects.

This level of internet service delivery is unlikely to need extensive cost-benefit analysis. Costs are usually modest, easily contained and managed. However, sufficient analysis will ensure the project costs are known and controllable. Benefits tend to be intangible and therefore somewhat difficult to quantify other than those gained from advertising the agency's services and providing basic agency information.

Stage 2—A website that allows any internet user to browse and interact with the agency's database or databases

This stage allows clients to access more substantial public information resources held in agency databases. Clients use a web browser to interact with the website using a web browser but, commonly, agencies need to develop a specific database client interface to help clients access the database information. The client interface usually has simple search and retrieval utilities.

Due to the public nature of the information, security and privacy are still not a major concern other than general protection of the website. Depending on the type and volume of the information contained in the databases, a dedicated database application server may be required. Clients will enter the website and (seamlessly) access the database application server when extracting information.

Depending on the agency's network infrastructure, some security will be required to prevent the client from accessing other servers on the network. This level of security is still fairly basic as the website and client interface can be structured to call up the required database information from the application server without allowing the client direct access to the database records. All database records should be read only, but will be able to be downloaded by the client.

Costs might include:

- ▶ Stage 1 costs;
- ▶ database development (including design, programming, testing and implementation);
- ▶ software licensing;
- ▶ storage requirements and capacity planning (for large volumes of information);
- ▶ application server operation and maintenance;
- ▶ security—simple firewall from other network resources;
- ▶ maintenance and update of the information; and
- ▶ development and testing of the web-based database client interface.

The benefits from this type of facility are in the enormous volumes of information clients can access efficiently.

At this level of internet service delivery, the nature of the agency program, the amount of information available, current delivery modes and the like will mostly determine whether to conduct a formal cost-benefit analysis. It is advisable to proceed to a cost-benefit analysis so that decisions can be taken having regard to the estimated costs and benefits of the project.

Stage 3—A website that allows user client interaction with agency databases and exchange of sensitive information

This stage allows a much higher level of access to information and exchange of information between clients and hosts. Typically, the information traded will require higher security and privacy.

It will be important for the facility to have a comprehensive client authentication process to ensure that the clients alone access the information they are entitled to access. Read/write access is usually provided to the database records. All client activity will need logging to ensure an adequate audit trail. Transmitting sensitive information may also require encryption to protect that information while in transit. The risk of data corruption and interception is higher for these types of services and this will translate into higher costs for the security and protection of the information.

As an interactive database application of this kind is complex, it will involve much higher development, operation and maintenance costs than those in Stage 1 and 2: e.g. additional user acceptance testing is needed, particularly for clients with disabilities. In addition this stage requires greater emphasis on marketing and advertising the service, including client training. Given the more personalised nature of the service, more intensive market research is needed into the client groups' ability and willingness to use the service. There may also be costs in developing and distributing client items including information brochures, software media and instructional materials. A client support Help Desk Service might be needed.

In relation to security, a more comprehensive security risk assessment is needed as well as more complex and costly security measures. Security and access control, including security firewalls, access gateways, authentication services and the like need considering. Similarly, privacy requirements will add to costs. With clients having read/write access, greater emphasis must be placed on client verification and identification, data validation, virus protection and the like.

At this level of internet service delivery, a cost-benefit analysis will be of much assistance. Developing sophisticated interactive services can involve high costs. Projects of this kind need to be carefully targeted and managed. A cost-benefit analysis will provide some of the base information required so a full business case can be developed.

Stage 4—This stage is the same as Stage 3 but in addition the agency, with the user's prior approval, shares that user's information with other government agencies.

Stage 4 is an extension of the interactive applications developed in Stage 3. In this stage, the agency may seek benefits from integrated transactions, for example, where a user's change of address request is updated as one integrated transaction rather than a series of separate transactions.

This should benefit both users (clients), who only need to make one request, not multiple requests to different agencies. Agencies are less likely to have input errors, because they can, subject to privacy conditions, use the same 'source data'. How government agencies review, examine, extract or otherwise use that information can be determined on a client based level or on a broader client group level.

The range of costs for developing the client/host applications will be the same as in Stage 3. However, establishing integrated transaction capabilities with other agencies may involve additional costs.

This activity will require an additional level of authentication, security and privacy depending on the nature of the information exchanged. Costs will also be influenced by whether other agencies access the information or whether large volumes of data are sent to the other agency. Interactive use of data commonly involves higher costs, while simple periodic transmission of large volumes of data is less costly.

Security and privacy requirements are paramount in delivering and using this service. Refer to both of these components in this series. Program managers must understand their obligations under relevant privacy legislation. This will include declarations to clients on why the data is collected and how it is used and whether it may be transmitted in full or part to other agencies.

You should conduct a cost-benefit analysis at this level of interaction and service delivery.



Further Information

Further information about how to decide to use the internet to deliver government programs and services, and on how to deliver programs and services more effectively through the internet, is found in other components of this ANAO Better Practice Guide, called *Internet Delivery Decisions—A Government Program Managers Guide*. The full list of components is:

1. How to Decide to Use the Internet to Deliver Government Programs and Services
2. A Business Case and Cost Benefit Analysis for Internet Use in Government
3. Designing and Maintaining Internet Sites for Government Programs
4. Costing Internet Service Delivery in Government
5. Monitoring and Evaluating Internet-Delivered Government Programs and Services
6. Government Internet Systems—Security and Authentication
7. Legal Considerations for Government Internet Service Delivery
8. Privacy Issues, the Internet and the Government Manager
9. How to Make Government Sites More Accessible

Printed copies of this Guide are available from the ANAO. Copies can also be downloaded from the ANAO website—<http://www.anao.gov.au>

April 2001



Designing and Maintaining Internet Sites for Government Programs

3

Internet Delivery Decisions

A Government Program
Manager's Guide

To help you understand the online environment for delivery of government programs and services, this component of the ANAO Better Practice Guide outlines the similarities and differences of online and conventional environments. It identifies some key questions for program managers, and the first steps in building an online program.

Things about online services that are the same as conventional service delivery media

Online service delivery is similar, in many ways, to other forms of delivery. Online delivery is usually designed to achieve a variety of your own agency's tasks. In this sense, the internet is no different from other media, just more immediate and more public.

Reliability

Like any form of communication or transaction, you want your internet service delivery to give consistent and reliable results. While it might promise faster, cheaper transactions, the most important goal is still to deliver on time, every time the correct services, such as providing information to users or identifying the eligibility of potential clients of government programs.

Audience groups

The way in which your services are delivered online may be different, but you will still need to target particular groups, for particular purposes. Those services must reach the right people with a message they can both understand and use. The internet environment should help you meet the needs of particular groups.

Things about the online environment that are different

There are some important differences that must be understood, and managed, when delivering services online. Some of these are listed below.

Global reach

The internet can potentially reach billions in an instant. Whatever you put online publicly for an Australian audience is as easily accessed in most areas of the world. Much of the time, people outside your target group will not visit your website, but it is important to remember that online content is public, which generally is its purpose.

This global reach also means that if you make a mistake you might suffer from it on a very large scale. One mistake could take a team of people weeks, if not months, to resolve.

Success (or failure) is fast

The internet is an almost instantaneous medium. This means that whatever you do will appear almost immediately (there are important exceptions to this-see inset following). This can be a major strength if you want to get information out very quickly or at a specific time. It can also be a problem if you make a mistake.



Time delay problems

Because of the way the internet and individual browsers work, there may be a delay in getting your updated information to users. There are two main types of delay. One is the slowness of some internet servers and Internet Service Providers (ISPs) to update their information. This particularly applies to ISPs using 'proxies' which collect and store frequently used information for local use. These are usually updated regularly and most will check for new information within 24-hours.

The second problem is the computer browser loaded on the hard disc of individual computers. This may store old information indefinitely, but will present it as current. This can cause old information to appear weeks or even months later. Ensure your staff are aware of the problem pending a technical solution. It is vital to keep your IT specialists and any call centre staff aware of any problems so that they can help both you and your staff with possible technical solutions.

Other specific problems may exist. For example, when moving your website it may take up to a week for other services, servers and systems to acknowledge this change and reflect the correct information to users.

Content keeps changing and must be current

The internet changes from one second to the next and is never the same twice. Users know and understand this. On the positive side this means that any changes you make will be accepted as part of the process.

However, there is very low or even zero tolerance of out of date material. If the information or transaction options you offer are out of date your credibility will suffer badly. Experience suggests this is a real challenge. A small but visible notation of the date and time the site was updated can increase user confidence. Websites are readily developed, but it is harder to provide continuing resources to maintain and refresh sites. It is like having out-of-date brochures as the only resource to give away at a front counter.

Audience attention span is brief

With the internet you will have no more than a few seconds to attract and hold the attention of your client. A slow loading graphic, a screen full of text or just no clear indication of what to do next, is likely to lose your client's attention.

Clients may not be 'web literate'

Because the internet is new, user skills vary widely. You shouldn't make assumptions about what your clients can or can't do.

The internet is passive

For all its dynamism, the internet remains a passive medium. The user must seek out information; it does not project itself into their daily activities in the same way as a television advertisement or a targeted letter. For this reason your information must be easy to find and clients need a good reason to go looking for it.

Audiences are harder to know

Visitors to internet sites are usually anonymous, unlike visitors to a front desk or even the names on a mailing list. Determining 'who is visiting' what areas and what they are making of that experience can be more difficult.

It is essential to adopt some of the techniques now being developed to understand and monitor internet audiences. See the component on Privacy in this series. It recommends stating how you will determine who is visiting and suggests, in part,

our service provider makes a record of your visit and logs the following information for statistical purposes—the user's server address, the user's top level domain name, eg. .com, .gov, .au, .uk etc.), the date and time of the visit to the site, the pages accessed and documents downloaded, the previous site visited and the type of browser used. No attempt will be made to identify users or their browsing activities...

First steps—is my program suitable?

Your program's suitability for online development will depend on what is delivered, the budget and the nature of the clients or customers it affects. There would be little value in placing transactions online if your clients are known not to have access to computers or the ability to interact with them. This is why it is important to develop a business case for your decision, requiring knowledge of the costs and benefits of the proposed initiative. Other components in this Better Practice Guide show you how to develop such a business case and to estimate the costs of internet usage to your agency.

Even if you decide your program cannot be delivered online, it is desirable to make available online any documents describing the program. It is also desirable to detail the agency's program activities, in the public interest, thus assisting intermediaries who may influence your clients. There is now a widespread expectation that information about government activities and programs will be available on the internet even if it is not yet possible to carry out all transactions.

Putting a program online can create a large amount of electronic commerce resulting in a large amount of additional business for your agency. Make sure that resources are allocated to handle any likely demand resulting from your site activity.

Identify client needs and define the functions you want to include on the site

Developing a program online requires the same disciplines and research that are needed to develop any other program or service. Understanding client needs, behaviours and demographic characteristics is fundamental to developing a successful internet-based service.

Visitors to internet sites are usually anonymous, unlike visitors to a front desk or even the names on a mailing list. The internet changes from one second to the next and is never the same twice. Users know and understand this.

3

Decide whether the site is a one-off location to obtain information (such as an address for further information available during a short-term advertising campaign), or whether it is intended to attract clients and encourage them to return for repeated transactions. In the latter case, pay more attention to creating 'stickiness'—sign and features that make the site attractive and easy to use and encourage clients to come back.

Online service delivery facilitates highly focused client services. It also provides the opportunity to better manage the client relationships. Interactive features and personalisation can tailor services to explicitly or implicitly expressed client needs and provide important information to the program administrator. If done well, internet services can remove the need for the client to understand the different levels of government or the levels of organisation within agencies.

Consequently, building an online program is not an information technology issue alone. It requires substantial contributions from people with expertise in communication and the program's subject matter. They advise the project team and control the look and content of the site and ensure that it provides the services specified. Such specialists play an important role in ensuring the quality of the information and the online experience, that the site suits its intended audience and serves the program's needs.

Consider whether additional client-focused features are to be provided such as:

- ▶ online feedback;
- ▶ discussion forum/chat facilities;
- ▶ advanced search facilities; and
- ▶ personalisation or customisation features to allow clients to arrange the internet page to suit themselves, express interest in particular types of information or collect and store links to frequently used services and information.

If you do decide to incorporate these features, it is necessary for you to develop a clear idea of how you want to use these facilities to manage the relationship with your clients. What outcomes do you need or expect? Are you going to be responsible for developing content for the site and ensuring its continued relevance and quality?

Market research may be required to discover such information as:

- ▶ client needs;
- ▶ client preferences and behaviour; and
- ▶ the level of online capability of the targeted group and the technology available to them.

You can expect that intermediaries such as lawyers and accountants are likely to have more up to date, powerful computers available to them than, say, unemployed people in rural areas, though this expectation can change quite quickly. For example, there is evidence that a large number of small businesses upgraded their computer systems ahead of the implementation of the Goods and Services Tax in July 2000.

Draw up a specification

Whether you decide to use internal resources or external contractors to design and build your internet site, you will need to develop a specification for the site that describes the features and functions that you expect your staff or the contractors to provide. You will then need to assess proposals to deliver these features, and whether or not they are feasible in the light of your time-frame, budget and priorities. It may be necessary to plan for your site to be implemented incrementally—with basic features at the start but developing more complexity and sophistication in later developments.

These specifications will form part of a Request for Tender (RFT) or Request for Offer (RFO) document if you are seeking external contractors to do the work for you. An RFT or an RFO should include details of your existing or preferred infrastructure and should set out your requirements.

The specification must provide details of a timeline with identifiable milestones. An RFO/RFT may seek contracts based on time and materials or a fixed price but it is important that the payment structure relates to identified stages in the project.

Some questions to consider?

What technical infrastructure will maintain the site?

Whatever its complexity, the site needs to be founded on software and hardware that provides appropriate useability, stability, reliability and client accessibility. Using databases can simplify site management by publishing information to several places on your site simultaneously and managing hyperlinks and metadata efficiently. Such software can be developed 'in house' or purchased and customised. Developing or buying software can be expensive and requires careful evaluation.

Software vendors have a number of different models for estimating the costs of applying their software to management of government internet sites. These may be based on the expected number of visitors to the site, flat licensing fees or partnership arrangements with developers where there is a share in the revenue from transactions.

What transactions are planned and how sophisticated is the programming needed?

Developing transactions also requires thoroughly assessing the interactions necessary between your systems and those of other agencies. Careful attention to security, privacy and interoperability issues are major concerns. Does this duplicate any other service? Has another agency built a similar solution adaptable to your needs without starting from scratch?

Will the site offer downloadable forms (to posted or emailed back to the agency) or are they completed and processed by an electronic transaction?

It was a requirement that, by 1 December 2000, all forms for public use must be available online, to be downloaded and/or electronically completed. The degree of interactivity will depend on the number of likely transactions and the kind of online experience you want clients to have. It will be most convenient for clients to complete their transaction as one action but if there are very few clients this may not be practical.



Should electronic payments be included online?

This issue depends on the relationship between your site and the agency's accounting infrastructure. Security arrangements would need to ensure safety for client details during transactions and that funds generated find their way into the agency's accounting infrastructure. Risk management, including fraud controls, would be essential.

Should all or some of the content only be available to a restricted group—if so, what are the security requirements?

An example of a secure network is the Department of Employment, Workplace Relations and Small Business Extranet that supports the Job Network. It is only available to Job Network members and provides a secure environment for a range of transactions including financial ones. At the centre of the administration of the government's services to the employment market, it requires the highest standards of security and privacy.

Is a separate domain name required, different from the agency's corporate web address?

The same considerations as to brand recognition of business names and logos apply here. Sometimes it is better to use your agency's web address and provide a path to a new sub-site if the web address is an obvious one or is well known to your potential clients. You should also consider the effect of managing a proliferation of domain names and whether your clients can locate your site easily.

Will the program site have a distinctive, separate look and capabilities different from the agency website, or carry the same look-and-feel as the agency's corporate website?

This is a matter of choice based on how necessary it is to identify your new program separately from the agency's mainstream activities. In designing internet sites it is important to maintain a consistent look, feel and navigation structure for a site so it is accessible and credible.

What are the accessibility issues, and how will they be managed?

Accessibility issues are discussed in a separate component of this *Better Practice Guide How to Make Government Sites more Accessible*.

Will the site be linked to other sites with similar subject matter or form part of a government information channel or portal?

The Business Entry Point is a current example of a government portal for the business community. From the 3rd Quarter 2001, a range of further customer-focused portals will enable easy interaction with government for specific customer groups and customers looking for specific subject areas. It may be appropriate to set up links to such portals or other government sites with a similar customer group or subject matter.

How is metadata best managed on the site?

Metadata is information about the pages on your site that flags them for discovery by search engines. Implementing a business classification scheme for metadata will ensure metadata is applied consistently across your site. Monitor each piece of site information to ensure it remains up to date and relevant. As information dates or is no longer required, remove it from the site and archived it in accordance with the Australian Archives' standards.

Metadata is information about the pages on your site that flags them for discovery by search engines. Implementing a business classification scheme for metadata will ensure metadata is applied consistently across your site.

If the website is part of Government Online, you must be aware of the need to apply, and meet, the relevant government standards (for example, messaging standards). Talk to your IT adviser about this.

Building your online program

Following development of your business case and having decided that your program is suitable for online delivery, it is necessary to move to the implementation phase. Form a project team of your staff or contractors. They will require a project leader and personnel from within the agency to help develop the project.

Building the program requires considering the following issues:

- ▶ developing a project plan and timetable, having regard to the costs of the initiative. Another component of this Better Practice Guide provides guidance on estimating the costs of agency use of the internet for program or service delivery;
- ▶ buying and maintaining hardware and software and integration with the agency's information technology infrastructure. This will require expert advice, consultation and close cooperation with the information technology providers to your agency;
- ▶ providing access to the agency's information technology systems to construct the necessary systems and implement them;
- ▶ Internet Protocol (IP) authentication and domain name registration-to allow your site to be correctly registered and discoverable on the World Wide Web;
- ▶ risk assessment and risk management strategies;
- ▶ arrangements for placing authorship and publishing of content on the site;
- ▶ arrangements for security, passwords and encryption and their administration and protection behind the agency's firewall;
- ▶ adequate documentation of the site and its administrative structures to ensure that it can be understood and administered by staff or contractors not involved in its initial development;
- ▶ arrangements for collecting data are needed so the agency can collect and analyse usage numbers and patterns, to enable program evaluation and improve service delivery. Such arrangements may involve using a cookie. A cookie is a mechanism that allows an entity to store its own information about a user on the user's own computer. Such mechanisms may have privacy implications. For that reason, refer to the Privacy component in this Better Practice Guide for guidance on arrangements for collecting data for program evaluation and service delivery improvements;

- ▶ quality assurance—ensuring that the quality of the information and services on the site is maintained. This involves ensuring firstly that documents published on the site are factually and legally correct but also involves ensuring that the site functions correctly. Also, that links and features function as intended and the appearance of the site is consistent with the intended audience;
- ▶ developing standards for the site—to ensure a consistent look, feel and operation of the site;
- ▶ an audit record to support the site—a system must record when information is placed on the site and when it is removed, for audit purposes;
- ▶ a system to add metadata to the site—metadata is indexing information that enables documents to be easily discovered by search engines;
- ▶ change management arrangements to ensure that staff are aware of the new site and those involved in its management receive adequate training;
- ▶ useability testing of the site before information or transactions are released to the site; and
- ▶ complying with, or exceeding, the minimum requirements specified in the Government Online Strategy, specifically concerning:
 - security
 - privacy
 - authentication
 - metadata
 - electronic record keeping
 - publishing guidelines
 - accessibility
 - online information service obligations (OISO).

NOIE's *Guide to Minimum Website Standards* at www.govonline.gov.au/projects/standards is a quick guide to the main elements of the minimum website standards.

Continuing site management

The program needs support and maintenance based on the site's expected life. Program managers must be aware of the need to apply resources to periodically update the site, revise its look and feel and to introduce more advanced functionality.

From the beginning it is important to identify the people with responsibility for site maintenance and its infrastructure. The allocation of these responsibilities should be negotiated with your information technology Advisers because you will require services from a range of people who set up and maintain the infrastructure of the agency—including domain name registration, firewall maintenance, servers, audit, collection of statistical data and so on.

The program needs support and maintenance based on the site's expected life. Program managers must be aware of the need to apply resources to periodically update the site, revise its look and feel and to introduce more advanced functionality.

To avoid prematurely releasing information on the site, it is usual to have separate server environments where development and testing of site content is possible before it is finally released for public access. Such safeguards would prevent an instance of an important document such as a budget paper being released prematurely and are important risk management considerations.

An efficient method of publishing to the site is necessary to ensure authors who need to place information on it have convenient access. For a small, simple site it may be sufficient for a small team to have publishing access. For a larger agency it would be desirable for several authors across the organisation to have that capacity. This allows information to be published as it comes to hand, ensuring the site is fresh and relevant. A bottleneck could be created if too few authors can publish material.

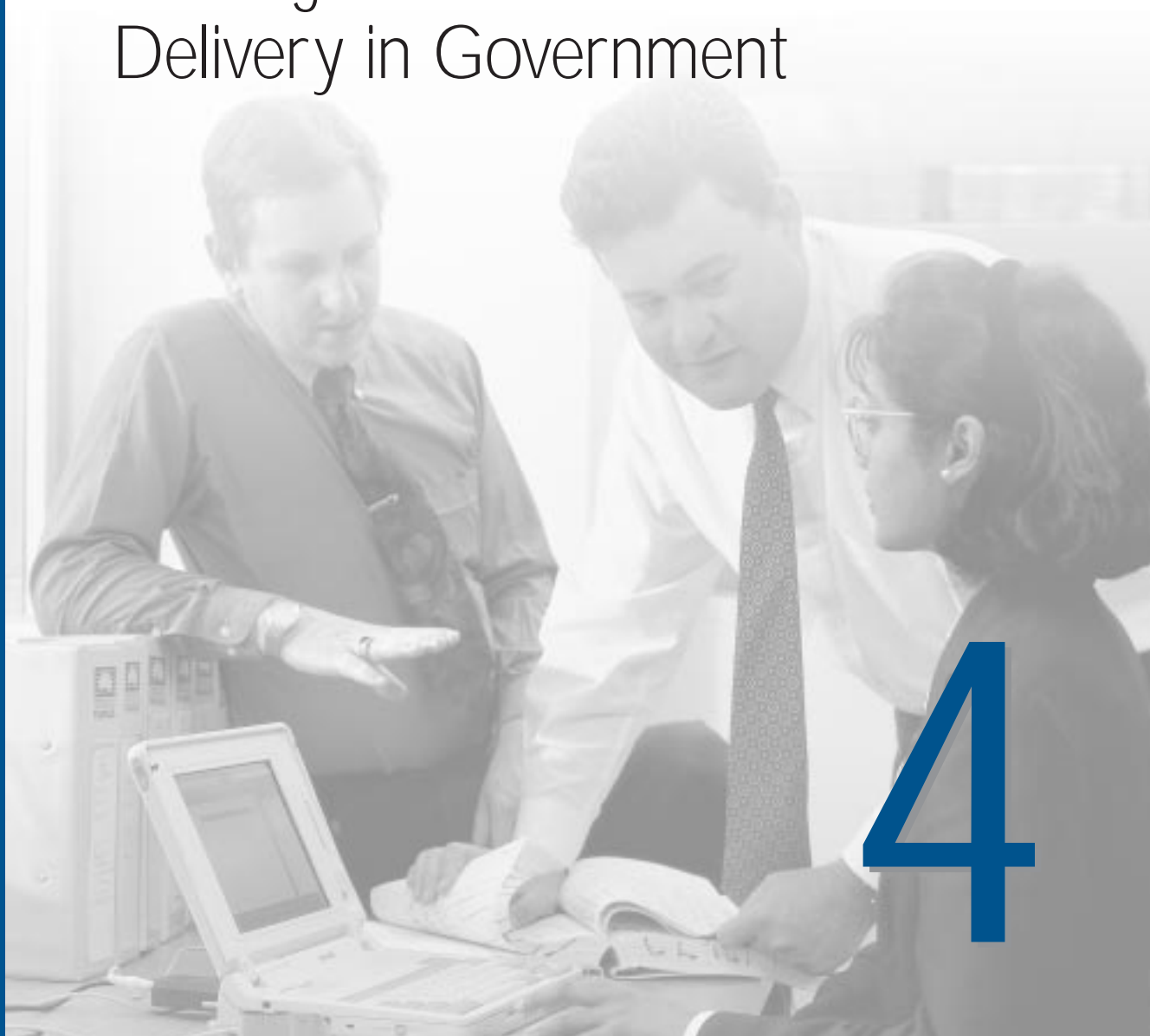
One model is to set up a network of 'web coordinators' who have access to the relevant websites relating to their organisational unit's activities. These coordinators are trained to prepare information and documents for publishing and they can access the development and test environments. A centralised web management team then:

- ▶ provides consultancy services;
- ▶ undertakes more advanced features and services;
- ▶ ensures quality control; and
- ▶ has the necessary authorisations to release material into the production or open domain.

Finally, you may find NOIE's Better Practice website helpful. Its address is www.govonline.gov.au/projects/strategy/better_practice



Costing Internet Service Delivery in Government



4

Internet Delivery Decisions

A Government Program
Manager's Guide



Understanding service delivery costs is fundamental to good government program management. Without this knowledge you, as a program manager, are not equipped and informed to improve service quality, lower costs or provide the range of services clients require. This component of the ANAO Better Practice Guide provides advice on how to estimate the costs of delivering government services using the internet. Other relevant information is in another component of this Guide titled *A Business Case and Cost-Benefit Analysis for Internet Use in Government*. The ANAO has also published a Better Practice Guide *Building Better Financial Management Support. Functions, Systems and Activities for Producing Financial Information*. That Better Practice Guide includes a component on costing systems. Its principles can be applied to the costing of internet service delivery in government.

Like any service delivery method, costing internet service delivery depends very much on defining all the contributing processes and activities, understanding how these generate costs, and then determining component costs to determine a total service cost.

Fundamental questions you need to answer through a costing process are:

- which components contribute to the internet service delivery and how;
- which of these components add value to overall service delivery and which just add costs; and
- what resource costs contribute directly to the service delivery.

By fully understanding and costing the components of an end-to-end service delivery chain, you can then determine the following:

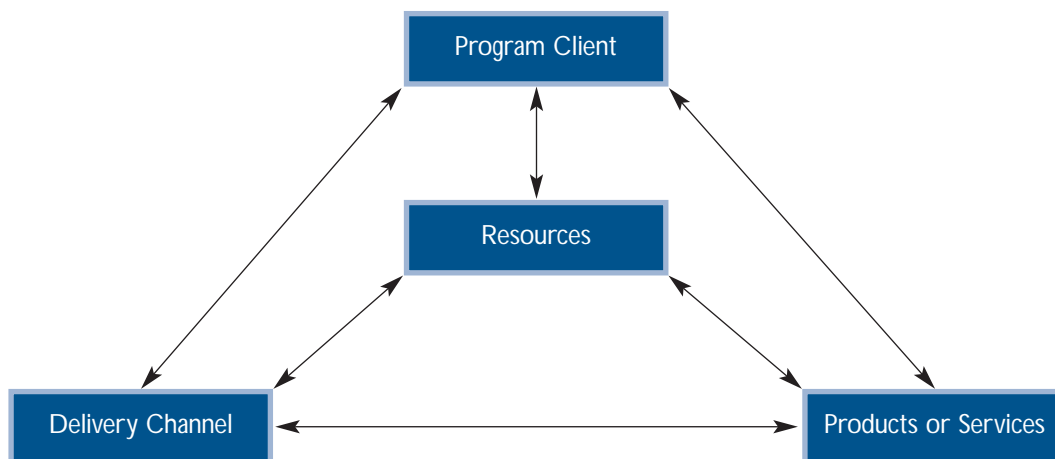
- is the program cost effective? i.e. is the program delivering the right outcomes to the right target group for the right cost?
- what is the appropriate level of funding required for this program?
- what is the appropriate price to charge for the services being delivered?
- whether to provide the services in-house or to source them from outside;
- what are the costs of introducing changes to the program or the savings from reducing or ending an existing service?
- how agency overheads are distributed across the service for budgeting/accounting purposes;
- basic rules for funding staff levels associated with changes in service levels or new policy/savings proposals; and
- performance benchmarks for effectiveness, efficiency and productivity.

Like any service delivery method, costing internet service delivery depends very much on defining all the contributing processes and activities, understanding how these generate costs, and then determining component costs to determine a total service cost.

How to identify the end-to-end service delivery

There are some logical steps to determine the processes and applications used in the service that need costing. To find what constitutes the totality of a government service that you deliver, establish the relationships between four key areas:

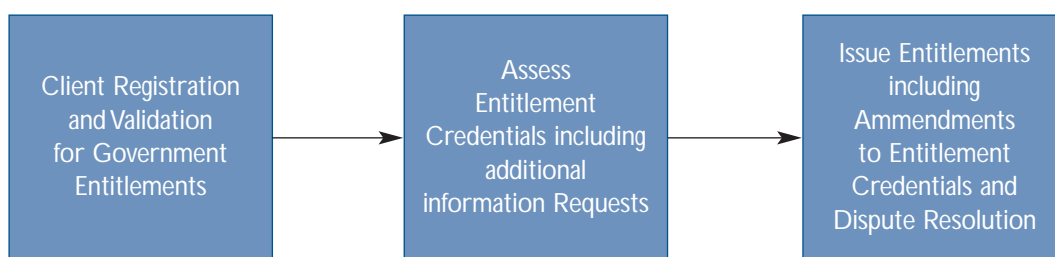
- clients;
- delivery channels;
- products and services; and
- available resources.



This end-to-end service delivery model acknowledges how clients influence the specifications, design and resources for the mechanism (such as the internet) which delivers the government service as well as the exact nature of what is delivered and its quality.

To determine the totality of end-to-end internet service delivery by government, you need to establish where client interaction starts, through to the concluding action in delivering the service or product to that client. By identifying the intervening activities and processes, their portion in the total cost of end-to-end service can be assigned.

A simple illustration of end-to-end service involves:



Each 'major process' has supporting activities and tasks to progress service delivery under its particular business rules, procedures and controls. The factors and answers are as individual as the program being delivered.

Fully costing a service or product means identifying all activities and the associated resource costs in each major process. Using the simple example, the starting point for the end-to-end service is the first time a client interacts with the agency and engages program resources. This may be an initial inquiry, or an application to receive the government service being delivered.

Each 'major process' has supporting activities and tasks to progress service delivery under its particular business rules, procedures and controls. The factors and answers are as individual as the program being delivered. As a generic example only, some supporting activities for the first process ('Client Registration and Validation for Government Entitlement') might include:

- ▶ process inquiries;
- ▶ receive applications;
- ▶ validate data; and
- ▶ complete registration.

Such steps involve specific tasks to ensure service delivery meets required service level requirements and system processing rules. Generally speaking, it is only necessary to cost service delivery to activity level (as this is normally the lowest level where resource use is logically captured, either through workloads processed or by recording staff effort). To cost service delivery below this level you need specific work measurement techniques that provide lower level volume counts (perhaps manually) and staff time recording at the task level.

Within the appropriate activities, identify when and what interactions occur with the internet system and what supporting or administrative tasks occur. Typically interactions occur through:

- ▶ processing client requests (i.e. operating the application); and
- ▶ reporting and monitoring.

The cost of activities which related to duplicated services during a changeover period also need to be identified. These costs are included in the overall costing but identified separately.

A more specific example of an end-to-end internet service delivery systems are the systems municipal or city councils use to process building or land development applications. This service involves:

- ▶ providing development conditions, regulations and/or rules;
- ▶ application lodgement, including data verification;
- ▶ applicants monitoring application progress;
- ▶ the council notifying affected persons;
- ▶ public access to all necessary data for consultation (including requests for additional data);
- ▶ lodging application objections and disputes; and
- ▶ notifying decisions.



What costs should internet service delivery costing include?

Costing service delivery involves identifying all the real costs in providing the service over a nominated period of time, for example, six monthly or annually. This normally requires the ability to confine the program or service delivery costs to an identifiable cost centre or number of cost centres within the agency's accounting system, and usually consists of all the program's staff and operating expenditure.

Attachment A has typical cost categories or cost pools associated with internet service delivery. These are only indicative and should guide relevant costs determination, but there may be other costs to take into account. Where organisations have a policy on capitalisation of software, split these internet costs between operating and capital expenditure.

How to link direct costs to service delivery components

Now the total direct costs of internet service delivery are identified, apportion these costs against all the identified process activities involved in that delivery. This can be an important step in developing a business case for internet service delivery. Another component of this Better Practice Guide can provide further advice on this matter. The component is called *A Business Case and Cost-Benefit Analysis for Internet Use in Government*.

Your own experience and the expertise of financial management staff can identify the basis for cost allocation by:

- the principal actions which influence total program costs; and
- what activity measures exist to help the cost attribution process.

Commonly, the labour/staff-time effort involved in each of the major processes is identified and estimated. Alternatively, where more disaggregated costings are required, assess the time and effort involved in each activity in the service delivery. This is usually expressed as a percentage by activity/process as the basis for direct cost attribution.

Resource accounting, or performance measuring, systems may provide information for more accurate cost attribution. This will allow specific cost assignments based on actual usage for certain activities that exclusively consume those costs.

In the 'building development' application example of end-to-end service delivery, total service delivery cost would be broken down into the costs of each described activity. You would need to determine how each activity uses resources in the end-to-end service before allocating any shared costs to each activity.

Costing service delivery involves identifying all the real costs in providing the service over a nominated period of time . . .

These often involve understanding component costs. For example, when allocating computing costs to each activity, you need to know each component of that 'computing' cost, such as server, communications and software costs. Then ensure that cost allocation matches resource use.

Cost accuracy for each activity then depends on the information you have concerning staff usage and other resources in the internet service delivery.

How to attribute overhead costs to the service

In terms of internet service delivery, overhead costs are usually those costs which other parts of the organisation pay for services and/or equipment that contribute to the activities.

Attributing these costs to activities is generally driven by either staff time or resource consumption (where 'consumption' can be reasonably assessed). Allocating an overhead by staff time requires allotting cost in proportion to individual staff time contributed to the activity.

Allocating resource costs based on consumption requires a different approach. A proportion of the resource cost is allocated to activity based on the percentage of resource consumption by that activity. For example, an activity which consumes 30 per cent of a server's capacity should be allocated 30 per cent of the cost of that server. This rule obviously applies to shared resources only. Where the resource is dedicated solely to the program, then 100 per cent of its cost is applied to the service regardless of use.

When allocating overheads, be aware items such as property costs associated with staff may be allocated on a staff time basis while the property costs associated with the computer room may be better allocated on a proportional use basis. Organisational overheads (such as participating in planning meetings with a Deputy Secretary) should not be included.

Attributing overheads is not an exact science and requires assumptions based on current business practices. These assumptions need consistent recording and application, and revision as costing information improves.

Conclusion

Government reforms have developed a framework which require you to operate, through devolved management, under the financial regulatory and accountability provisions of the Financial Management and Accountability (FMA) Act. This Act requires department heads to '*promote the efficient, effective and ethical use of Commonwealth resources for which they are responsible*'. Together with other recent government reforms such as accrual based accounting, you now manage under an environment that is focused on:

- ▶ information about the full costs and benefits of new and existing services;
- ▶ service output or product, services delivery management and those receiving services; and
- ▶ measuring the cost and quality of activities to provide services so 'best practice' assessments are possible.

As explained in the start of this component of the Guide, your decision-making about internet service delivery in government will be better informed once you understand what resource costs directly contribute to the service you deliver. Consequently, when costing government internet service delivery it is important to ensure you:

- understand the end-to-end service being costed;
- understand the costs associated with the service;
- link the costs to each component of the service delivery based on resource use;
- ensure that all appropriate overheads are included; and
- as information improves, revisit the original assumptions underpinning the costs—(service delivery costs are often underestimated, particularly regarding system development and maintenance).

Attachment—A

Costs Associated with Internet Service delivery

| Cost Category | Accounting Location |
|--|--|
| Direct Staff <ul style="list-style-type: none"> ▶ Salaries ▶ Overtime ▶ penalty/shift payments ▶ allowances ▶ any other direct salary related expenditure | Generally located in identified program cost centre(s) |
| Staff Overheads <ul style="list-style-type: none"> ▶ Comcare premiums ▶ long service provisions ▶ superannuation payments ▶ leave loadings ▶ separation payments, etc | Generally located in identified program cost centre(s) |
| Direct Administrative ('Operational' or 'Supplier' expenditure) <ul style="list-style-type: none"> ▶ travel ▶ postage ▶ office equipment & stores ▶ fuel, light & power ▶ consultants/contractors ▶ training ▶ advertising & recruitment ▶ computer consumables (other than identified internet expenditure) | Generally located in identified program cost centre(s) |
| Desktop/Communications (Direct) <ul style="list-style-type: none"> ▶ telephone charges ▶ internal voice and data transmission charges ▶ desktop charges | May be centrally charged through a corporate cost centre, then attributed to a program |
| Property (Direct) <ul style="list-style-type: none"> ▶ lease payments ▶ accommodation services ▶ security, etc | May be centrally charged through a corporate cost centre, then attributed to a program |
| Human Resources (Corporate Overhead) <ul style="list-style-type: none"> ▶ payroll processing ▶ corporate development/training ▶ EEO, OH&S, Workplace Relations, etc | May be centrally charged through a corporate cost centre, then attributed to a program |



| Cost Category | Accounting Location |
|---|--|
| Office Services (Corporate Overhead) <ul style="list-style-type: none"> ▶ mail room ▶ records management systems, etc | May be centrally charged through a corporate cost centre, then attributed to a program |
| Internet <ul style="list-style-type: none"> ▶ database development including design, programming, testing & implementation ▶ application maintenance (including client interface)—software upgrades, patches and bug fixes ▶ maintenance and operation of application servers ▶ hardware and software refresh/upgrade ▶ maintain and operate security firewalls, gateways, and authentication services; encryption services ▶ data validation, audit logging and review ▶ data communications costs (internal and external infrastructure) ▶ backup and continuity planning and operation (including testing) ▶ storage and capacity planning and operation ▶ application administration including client additions, deletions, password and identification services ▶ operating help desk and client support services ▶ education and training ▶ marketing and advertising ▶ Privacy legislation ▶ other legislative expenditure such as <ul style="list-style-type: none"> —legal advice (including risk analysis) —liability insurance | May be centrally charged through a corporate cost centre, then attributed to a program OR Located in identified program cost centre(s) |

Further Information

Further information about how to decide to use the internet to deliver government programs and services, and on how to deliver programs and services more effectively through the internet, is found in other components of this ANAO Better Practice Guide, called *Internet Delivery Decisions—A Government Program Managers Guide*. The full list of components is:

1. How to Decide to Use the Internet to Deliver Government Programs and Services
2. A Business Case and Cost Benefit Analysis for Internet Use in Government
3. Designing and Maintaining Internet Sites for Government Programs
4. Costing Internet Service Delivery in Government
5. Monitoring and Evaluating Internet-Delivered Government Programs and Services
6. Government Internet Systems—Security and Authentication
7. Legal Considerations for Government Internet Service Delivery
8. Privacy Issues, the Internet and the Government Manager
9. How to Make Government Sites More Accessible

Printed copies of this Guide are available from the ANAO. Copies can also be downloaded from the ANAO website—<http://www.anao.gov.au>

April 2001



Monitoring and Evaluating Internet-Delivered Government Programs and Services



Internet Delivery Decisions

A Government Program
Manager's Guide

This component of the ANAO Better Practice Guide outlines questions and issues about monitoring and evaluating your internet service delivery. It will be helpful whether you are planning or already delivering government programs and services online.

Internet service delivery refers to government information and transactions that are available through government internet services. Email, websites, internet transactions and feedback are all part of this process.

Monitoring and evaluating overlap. While monitoring is likely to occur in short time cycles, addressing immediate problems, evaluation occurs in longer time cycles and is more extensive.

Monitoring

Three steps to successfully monitoring internet programs and services

A fundamental starting point is that you are clear about the objectives of your program and service, and that you measure your performance against those objectives.

Step 1

Look at your service delivery from a user's perspective.

Step 2

Establish performance measures and reporting to keep you informed in a timely and accurate way. You should always have a reliable 'picture' of how your internet service delivery is performing.

Step 3

Establish processes for making rapid and correct changes or additions to service delivery.

Step 1: Service delivery from a user's perspective

The internet is a new way to reach clients, with the promise of targeting the needs of particular groups, delivered with less cost and greater efficiency (in terms of time). However, creating the vehicle to do this effectively is a technical and organisational challenge.

The central aspect of successful internet service delivery is 'designing it in' at every stage, as a systematic approach to clients and users. Asking, '*How are the clients for these online services likely to use them? How will they benefit?*' is essential.

Start by listing each online service provided by your program. Then specify, for each of them, the particular client groups who will access the services. This 'map' will guide your monitoring and evaluation work, so that you do not shift the focus completely to your own processes.

There are a few simple, diagnostic questions about users which also keep the focus on delivering services to clients.

What questions and language are clients likely to use in accessing services?

The jargon of a government agency can easily creep into online environment structures. For example, a client may want to know more about getting help with a tree-planting plan, but if they are confronted with labels such as 'Grants Allocation Unit', 'Reafforestation Division', and 'Timber Products Evaluation Panel' they are unlikely to find information which assists their own tree-planting plans. It can also reduce client confidence in using internet service delivery.

How does the online delivery 'fit' in the everyday context of your clients?

When you have listed your services and clients, think about client use of services, everyday, in their own locations. As online environments become more sophisticated, it will be possible to adapt online environments to the thinking and uses of particular groups. At this early stage, thinking about the context and purposes which clients bring to their online uses will prevent some major mistakes being made. For example, business clients may access sites from handheld devices and graphics-heavy pages may be a disincentive in provided timely information and service delivery.

Techniques such as market testing or useability testing can highlight problems early. The Commonwealth Department of Employment, Workplace Relations and Small Business has established a useability laboratory where individuals are asked to do a 'test run' of web pages and online information. The problems encountered are addressed by making changes to improve language, information and navigation.

Are there problems in finding information or completing transactions?

The list of services and clients can also highlight the major areas of a website likely to be accessed. In a testing phase, it will be important to do a 'run through' for each of these main areas of predicted use. Barriers to easy access should be removed at this stage (note, these are 'functional barriers', not 'security' barriers). More information about this matter is contained in another component of this Better Practice Guide titled *Internet Systems Security and Authentication for Government Programs*.

If you are regularly getting incorrect or incomplete responses to your forms or questionnaires, this indicates that users may be having problems with the layout, wording or sequence of questions on the online form.

It is worthwhile to ask some people who typify your target audiences to try out your interface and give informal feedback about how it works. A full evaluation should certainly include testing the website from the perspective of your major target audiences.

The Department of Finance and Administration, in administering the www.fed.gov.au website, regularly analyses the site's log files to identify where users are having difficulty locating material. Analysing and learning from these 'failed' searches helps improve the service.

Is the response time satisfactory?

Slow-loading and uninformative graphics are one of the main causes of poor service delivery. Your office may be hooked into a fast connection, but many of your clients have to contend with poor quality links and older computers which cannot handle slick-looking graphics the way you can. If the users are paying by the minute or working from a public library where access is limited, they are likely to have a very negative reaction to your 'state of the art' presentation.

Step 2: Performance measures and reporting

Once you fully understand your online presence and your clients, you should define an adequate set of measures and information to keep you informed about your online delivery process.

Regular reviews

Depending on the purpose and nature of your online presence, you should create a system of regular reviews. For example, you may want to audit online content every six months, but check critical details (such as phone numbers, dollar amounts or important external links) every week, daily or even hourly. Some of the review process can be automated.

Reliability checks

Online delivery should be reliable and the information up to date. You may wish to set standards or parameters such as:

- ▶ never be offline for more than a minute;
- ▶ have ready-to-run backup systems;
- ▶ all critical changes made within 30–minutes; and
- ▶ less urgent changes made within 24–hours.

Generating web statistics

A number of companies offer website statistical packages to monitor site use. It is important to define a small set of information that is generated regularly and is directly useful. Present the statistical information in a useful format such as time-series graphs and pathway maps, for example:

- ▶ measuring unique visitors (rather than, or as well as, 'hits');
- ▶ measuring the main pathways around the site;
- ▶ measuring most used pages, and downloads;
- ▶ record where users come from (this is usually captured in relation to domain names); and
- ▶ measures of 'successful' visits.

See the component on Privacy for more information on appropriate ways to do this.

Collecting other feedback

Users who have experience—good or bad—of your online service, may pass on that information in other ways. The next step may be to find a person to speak to. This may mean a call to a call centre or (if available) a visit to your front counter. If you do not monitor these sources, potentially valuable feedback that begins something like: *'I tried looking for this on your website but...'* may be lost.

If you can detect and fix a commonly experienced problem at the source (for example, a hard to find website button), you might save yourself many thousands of phone calls or personal visits—and have much happier customers.

An online monitoring system should collect information from all available 'offline' sources. These might include:

- ▶ call centres;
- ▶ email from other sources;
- ▶ front desks; and
- ▶ anecdotal comments.



Consider having online feedback options, especially for new online products and services, so these opportunities are captured and channelled to the monitoring team, and you, quicker.

Step 3: Making changes to service delivery

The essence of online service maintenance is ensuring changes are both fast and accurate. To achieve this, particularly if you have a large volume of changes, you will need a reliable and efficient process.

Don't leave it to the technician

A very common mistake is to push through changes which leave an IT person making critical decisions about content. This is dangerous and unfair. The technician's job is to keep the system running smoothly. It will be somebody else's task to decide what should go online, where and how it should be placed. Plan for these decision makers to be available, either in person or by phone, when major changes go online. And remember, site upgrades are often done in the early hours of the morning (to minimise down time for clients during daylight hours).

Create a process

Create a system of 'sign-offs' so each person approves and passes on a proposed change. A simple change process may involve a series of action and sign-off steps that look something like this:

- ▶ factual error on website page detected by users and reported by front counter staff;
- ▶ page author notified, makes necessary change;
- ▶ graphic designer incorporates change in design;
- ▶ IT technician loads change on website; and
- ▶ author checks online.

Set time targets

Time targets should be set. An urgent and important change might be required within 30 minutes. Every agency will have a different set of change requirements, but 'urgent', 'normal' and 'low' priorities might be appropriate to most. Make periodic checks with your IT manager that 'urgent' isn't the most common priority. This may reflect poor management by authors or sections who expect the IT area to then perform miracles to satisfy service goals promised at CEO level or higher.

After clearly defining processes and setting targets, it is important to record and monitor the actions, timing and what is achieved. Over time, documenting the changes and time cycles involved in online delivery maintenance becomes a valuable tool (e.g. for assessing major overhauls or bottlenecks).

If you are regularly getting incorrect or incomplete responses to your forms or questionnaires, this indicates that users may be having problems with the layout, wording or sequence of questions on the online form.

Evaluation

Systematic evaluation assesses how effectively online delivery matches client service with program objectives. The evaluation process uses information gained in monitoring, and adds user research and other special measures.

Evaluating online delivery

Online delivery changes the way services are designed, communicated and made available. It also changes the relationships you have with clients, and what you can know about them. For these reasons, you need a different approach when evaluating your service delivery effectiveness using the internet. The key questions to ask about such an evaluation are:

- ▶ Why evaluate internet service delivery?
- ▶ When do I conduct it?
- ▶ How do I design such an evaluation?
- ▶ Who do I involve in the process?
- ▶ How do I use the results to improve services to clients?
- ▶ How do I best manage the evaluation process?

Why evaluate internet service delivery?

Good practice demands that government services be systematically evaluated, so that outcomes for client groups can be known, and judgements made about the program's effectiveness in fulfilling objectives. Evaluation usually describes outcomes, and also includes measures which can be used as benchmarks and tracked over time.

Evaluation is very important for internet service delivery, especially in its early days. The online environment dramatically changes relationships with client groups, depending on their access to the internet, and their comfort with using it. On the one hand, clients who are skilled users can seem more immediate. They will use email responses to be vocal in their praise or blame, or to raise questions. On the other hand, there are clients of government services who are distanced or even alienated by internet service delivery. The effectiveness of the services themselves, as well as the impacts of new ways of informing, communicating and conducting transactions must all receive systematic scrutiny.

The other strong reason for evaluation is that of cost. Assumptions have been made about the efficiencies which internet service delivery should create. Evaluation seeks to document the realities, which may not live up to expectations. Program staff as well as clients may have a very different story about the effectiveness of online delivery.

When do I conduct an evaluation?

Allow for an evaluation phase, in outline, when the project starts. Think about what you will want to know and how the results can improve services. Establish a timetable, work schedule and a budget for this.

It is an advantage to have initial discussions with those who will conduct the evaluation, because simple ways of collecting information throughout the project can be 'built in'. This is not always possible, especially if external assessors are involved.



Most program evaluations occur after operating long enough to see consistent patterns and results. Consequently, evaluations often occur at the end of a service cycle, or a watershed such as a policy review.

When services are delivered in new ways, such as the internet, an additional, early evaluation is sometimes advisable. This does not replace the major evaluation, but is useful to make early revisions.

Two kinds of early evaluation, can help adjust services for more effective client service delivery:

Formative or front end evaluation

Formative evaluation is the research undertaken before implementing internet service delivery. It is sometimes called front end evaluation or needs analysis. Formative evaluation can be an inexpensive and effective way to proceed when:

- ▶ direction or structure is needed at the outset;
- ▶ a clear understanding of client needs is needed; or
- ▶ it is important to understand how clients use particular media.

Formative evaluation is not program-focussed, but examines clients needs and circumstances as well as the resources and media needed.

Preliminary evaluation

This can be conducted in the test stages of a program, or a short time after it has been implemented. Preliminary evaluation analyses different indicators of program progress and produces an early assessment. It is particularly effective for highlighting content or systems that don't work, or identifying unexpected uses of internet resources. It uses information already available, e.g.:

- ▶ web statistics;
- ▶ fault reports;
- ▶ email feedback; and
- ▶ additional research which might include:
 - analysing content such as language, images;
 - short surveys to particular client groups; and
 - telephone interviews to explore complaints or unexpected events.

Preliminary evaluations are usually focus heavily on diagnosing and resolving possible problems. They do not usually give a representative or comprehensive overview.

The National Library of Australia conducted a preliminary evaluation of its new online resource, Pictureaustralia.org.au. The methods involved analysis of the design and images, testing 'trails' and pathways which particular users might follow, and analysing web statistics and email responses.

This website analysis was in a test phase before launch.

The evaluation prompted many changes which made the site easier for different users to follow. The amended site adopted alternative contents and sequences. Additional material was added to explain site functions more clearly and appeal to a wider users group.

How do I design an internet service delivery evaluation?

One of the best ways to plan an evaluation is to ask, *'how do I want to use the results of the evaluation?'* If results will guide subsequent developments and add further client groups, you will need a full account of how services were used: what worked, what didn't and why. The descriptive information and accounts from clients themselves is most useful.

On the other hand, if the results are purely for overall government reporting, it is just as important to produce statistics that are accurate and representative for the group as a whole.

Mixed methods

In practice, evaluation results are used in several different ways. For this reason, it is a good idea to design an evaluation process which produces different kinds of information, by using a mix of methods.

Descriptive methods such as interviews or client focus groups highlights the 'voice' of clients.

Email feedback complements this, but should not be used in isolation because it reflects one group who are probably more comfortable with online communications.

Web statistics and surveys produce summary measures which show patterns over time.

Fault reports, reports from team members and feedback from 'counter staff' describe the everyday realities of service delivery.

Independent audits, and content and navigation analysis apply specialist skills to test the site and suggest improvements. Audits for accessibility by people with hearing disability or vision problems will also be important—(more information about this matter is in the Better Practice Guide component titled *How to Make Government Internet Sites More Accessible*).

Assessed together, all of these different information sources can diagnose problems, raise questions and suggest improvements. A single evaluation is likely to combine four or five different approaches which best address the question of program effectiveness. Most evaluations will include performance indicator measurement.

Performance indicators

Whatever the evaluation methods used, it is important to define performance indicators appropriate to the original objectives. Performance measures give a 'snapshot' of program progress. Important outcomes are represented as numbers and statistics giving trend information. These should be divisible as information for different client groups, and analysed for differences according to sex and age, or other factors.

For most programs or services there will be features which can be counted, not just described, and these form the core performance indicators. When designing a survey, it is useful to include questions which create performance measures from client information, and then compared with other internally generated performance indicators such as the numbers of successful online transactions or visits to information pages.



Stages of evaluation

Evaluation usually involves a number of steps. One suggested approach is:

1. Use web statistics, fault reports and systematic feedback from counter staff to draw a picture of service delivery from an internal perspective. Questions covered may include:
 - What website pages have attracted most use?
 - What is the completion rate of internet transactions?
 - What services or content have attracted criticism and why?
 - Where do most inquiries come from (this can usually be answered in terms of country or type of organisation)?
2. Get descriptive feedback from clients, in their own words. Use email feedback as well as qualitative measures such as interviews or focus groups. Questions covered may include:
 - What services have been most used/appreciated?
 - What services have been under utilised?
 - What content has attracted criticism/comment?
 - What additional services have been requested?
3. Design measures such as a survey which draw on the perspectives of those delivering programs, as well as clients. Use some of the language of clients to seek more systematic and representative answers from them. Questions covered may include:
 - What use have clients made of services?
 - How frequently have services been accessed?
 - How satisfied are clients with particular services?
 - What improvements do clients suggest?
 - Which clients are 'missing' or have not been reached?

Who do I involve in the evaluation process?

The short answer is use people who are external to the program team and who have skills in defining and measuring human behaviour and the specialist skills you require. Some agencies have evaluation specialists; others have social scientists or business analysts.

There are also external consultants with experience in evaluating government programs.

Always deliver the evaluation in close cooperation with the program team. Its design should reflect the particular objectives, priorities and outcomes of the services delivered.

How do I use the outcomes of evaluation to improve services?

It is vital that evaluations are put to use. Over time, applying the results should also create a culture of continuous improvement. Ways to use the outcomes include:

Track improvements

If evaluations are well designed, they can be repeated regularly to identify improvements for clients. This is very gratifying for teams who have worked hard in a novel and complex environment.

Consult others

At the beginning of an evaluation it is wise to consult with the major groups involved in designing and maintaining the internet service delivery and find out what their questions are. It is often possible to address different kinds of issues in an evaluation, by using combined methods as outlined above.

Communicate your results

Reports should give examples and details. Write them in a way that communicates with the different intra-agency groups involved in service improvement. It is a good idea to write a summary report for senior management, then include a range of reports based on the different methods.

If external consultants are engaged for part or all of an evaluation, it is important to discuss with them the kind of reporting which will be most useful, and how it is likely to be used.

How do I manage the evaluation process?

Managing an evaluation will take time. It should be considered a major task rather than an 'add-on'.

The best way to manage an evaluation is to see it both as a project management task, and as a communications task. Some simple keys to success include keeping people informed about:

- ▶ the overall objectives;
- ▶ what has been achieved to date;
- ▶ what the next stages are; and
- ▶ what is likely to happen.

All these engender greater support than short notice of some 'intrusion' into their working day.

Using external consultants

If you use external consultants, they will need comprehensive briefings in the initial stages, and advice and liaison about internal contacts and procedures. Presentations by such consultants, once evaluation ends, is a chance to further constructively discuss the results with those who have supported the work. Managers should also make a short report available to staff through intranets.

External participants who have responded to surveys or taken part in other ways are also pleased to hear of results.

In conclusion: The advantages of monitoring and evaluation

When online government services are developed or changed, setting up processes to monitor them day to day and evaluate their effectiveness seems just another task, and perhaps a less urgent one.

However, these activities are where the central purpose of the whole enterprise is tested, namely providing high quality government services to clients with optimum use of public resources.

Monitoring and evaluation will enhance the quality of your work from the beginning and assure you of its progress and success. Reports will communicate your increasing confidence and achievement to others. Monitoring is not an 'end process', but the returning link in the chain of continuous improvement which makes internet service delivery by government better and more effective.





Internet Systems Security and Authentication for Government Programs

6

Internet Delivery Decisions

A Government Program
Manager's Guide



This component of the ANAO Better Practice Guide provides advice on how to address security and authentication issues when delivering government programs and services via the internet.

Understanding how to implement best practice security in any online or internet services you may operate, particularly websites, is essential for government services online. Good online security maintains consumer confidence in these online services and it also protects the integrity of government information systems. Better online security also helps evolve better government online services.

Security rules cannot adopt a 'one size fits all' approach. Agencies operate in a variety of environments, have different missions, may face different risks, and may also have access to varying levels of expertise or resources. Implementing online security guidelines is ultimately a matter for good judgement by your agency as you apply the requirements to your particular circumstances and make appropriate risk assessments.

There are various ways to characterise government programs and services delivered by the internet. As indicated in other components of this Guide, one way is to think of such service delivery in four stages.

- ▶ Stage 1 is a website that publishes information about the agency and its services to all internet users;
- ▶ Stage 2 allows any internet user to browse and interact with the agency database(s);
- ▶ Stage 3 includes the first two Stages and permits users to enter information on the website, exchanging or transacting secure information with the agency; and
- ▶ Stage 4 is the same as Stage 3, but in addition the agency, with the user's prior approval, shares that user's information with other government agencies.

Different types of site may have different but appropriate security requirements. Security requirements for a Stage 3 or 4 site are likely to be more extensive than those of a Stage 1 site.

Note that clear minimum responsibilities exist which set a baseline of practice and standards compliance. This baseline should apply to all types of government online activity. You should also be aware of the six monthly Government Online reporting requirements, which require you to report security standards compliance. Current Commonwealth standards in this area relate to:

- ▶ **protection** of Commonwealth online systems and information assets;
- ▶ **detection** of incidents and vulnerabilities;
- ▶ **reaction** to address and resolve online security issues or incidents as they emerge; and
- ▶ **authentication** of the parties to online transactions.

Security rules cannot adopt a 'one size fits all' approach. Agencies operate in a variety of environments, have different missions, may face different risks, and may also have access to varying levels of expertise or resources.



The attached checklist is intended to guide you through effectively implementing these standards. You can complete it yourself, or in cooperation with your IT manager.

- Supporting information for this checklist is at: <http://www.dsd.gov.au/infosec>

Applying the checklist to your circumstances will help you better protect the security of both your data and systems. Applying it will also help reveal security problems associated with your program delivery online. It should also identify action needed to address these problems.

Protection *(Essential for Stages 1–4)*

Some high profile security incidents in Australia and overseas are a reminder of the vulnerabilities of governmental and other online and IT systems, and the real risks to which agencies (and their customers and partners) may increasingly be exposed as agencies move more of their activities online.

When considering how to effectively protect Commonwealth information interests and manage online security risks within your organisation, be aware that there are a number of Government-mandated online security rules and standards which require mandatory compliance, including fulfilling a number of reporting requirements. You need to be aware of these rules and standards and how to apply them to your agency's online activities. The principal ones include:

Privacy Act: *The Commonwealth Privacy Act 1998* mandates agency compliance with a set of 'Information Privacy Principles' that apply to Government websites, specifically:

- Principles 1–3 which cover maintaining privacy in the storage and use of personal information, and
- Principle 4, which mandates that record keepers ensure that records containing personal information are protected by adequate security safeguards.

Amplifying on these Principles is a detailed set of Guidelines issued and maintained by the Federal Privacy Commissioner that cover agency obligations in regard to website security and privacy.

- More information is in another component of this Better Practice Guide titled *'Privacy Issues, the Internet and the Government Manager'*, and at: http://www.privacy.gov.au/issues/p7_2.html

Protective Services Manual (PSM). The PSM—maintained by the Protective Security Coordination Centre within the Attorney-General's Department—is the Commonwealth's top-level framework for physical, information and personnel security. The PSM outlines the standards the Commonwealth demands for securing its resources and safeguarding its functions, including managing security risk; personnel security; and physical security. The PSM requires agencies to devise an Information Systems Security Policy and implement an Information Systems Security Plan. PSM compliance is mandatory for Commonwealth agencies.

- More information is available from: <http://www.sac-pav.gov.au/pscc/psm.html>

Australian Communications—Electronic Security Instructions (ACSI 33).

ACSI 33—maintained by the Defence Signals Directorate (DSD)—provides the formal basis for agencies to develop and implement effective IT and website security practices. It is a detailed guide to what agencies should do and how they should do it, with specific reference to network security, website security, email security and other components. As with the PSM, ACSI 33 compliance is also mandatory for Commonwealth agencies.

- More information is available from: http://www.dsd.gov.au/infosec/ACSI_33/acsi_index.html

When considering how to effectively protect Commonwealth information interests and manage online security risks within your organisation, be aware that there are a number of Government-mandated online security rules and standards which require mandatory compliance, including fulfilling a number of reporting requirements.

Gateway Certification Guide. DSD also administers the Gateway Certification Guide, which ensures the security of Commonwealth agency links or 'gateways' to the internet, especially where firewalls are used. Agencies seeking DSD certification of their gateway facility can use the Gateway Guide to check the requirements that they must fulfil. It is strongly recommended that agencies adhere to these provisions.

- ▶ More information is available from: http://www.dsd.gov.au/infosec/ACSI_33/HB8.html

Public Key Infrastructure. There are also existing mandated requirements—administered by the National Office for the Information Economy (NOIE)—that all Commonwealth agencies use Gatekeeper accredited products and services when implementing online security systems which use Public Key Infrastructure for authenticating businesses or individuals online, and communicating securely with them.

- ▶ More information is available from: <http://www.govonline/projects/publickey/Gatekeeper.htm>

FedLink: Fedlink—administered by NOIE—is a system to ensure communications between agencies are protected and secure. Effective from early 2001, Commonwealth agencies are required to use FedLink unless they have in place secure communications network arrangements that are commensurate with FedLink.

- ▶ More information is available from: <http://www.fedlink.gov.au>

Third party service providers: Operating Commonwealth agency online services may involve non-Government third parties or intermediaries—such as external web hosts, application service providers, web developers or other service providers. To protect the integrity of these services and apply a base level of security across the online infrastructure agencies use, Commonwealth agencies are required to ensure, from March 2001, that any non-government service providers or intermediaries that are materially involved in Commonwealth online service delivery comply with existing Commonwealth online security standards such as the PSM and ACSI 33, and/or other Commonwealth guidelines as they may evolve.

- ▶ More information is available from: <http://www.govonline.gov.au/projects/standards/security.htm>

CEO warrants: Reflecting the importance the Commonwealth attaches to protecting the privacy and security of online information, agency CEOs are also now required to warrant their compliance against all of the Commonwealth security standards above as part of their regular Government Online reporting framework responses.

- ▶ More information is available from: <http://www.govonline.gov.au/projects/standards/security.htm>



Detection *(Essential for Stages 1–4)*

Implementing detection measures is as necessary as having protection measures. Without the ability to detect security incidents, it can be difficult to assess whether protection measures are adequate, mitigate risk, and collect performance information that may be useful to help manage online security better.

Detection means the ability to identify, record and analyse inappropriate, incorrect or anomalous activity on an information technology based system. These incidents may, for example, include attempts to intrude into a secure area of a website, attacks aimed at obtaining site passwords, attacks aimed at stealing sensitive information from a system, or 'hacking' into a website and defacing the home page. Examples of all of these incidents have been recorded against Commonwealth agencies.

A system to detect such intrusions should be an important component of an agency security policy or plan. ACSI 33 provides advice to program managers on the goals, design and implementation of intrusion detection systems. Intrusion detection tools and techniques are important to organisations with an online presence in much the same way as virus checking software. These tools and techniques include firewalls, intrusion detection systems, logging and regularly auditing activity on important systems, and system integrity verification tools. Program managers should note however that effective detection is not just a technology issue—active 'hands-on' site management is also an essential component of incident detection.

- More information: http://www.dsd.gov.au/infosec/ACSI_33/acsi_index.html

Reaction *(Important for Stages 1–2 and essential for Stages 3–4)*

Having the means to detect and the tools to protect your systems is not enough. You need the capacity to react effectively and appropriately to security issues or incidents as they emerge. Protection, detection and reaction are the three keys to operating any effective online security system.

When a security incident occurs, you need to understand how to respond, and ACSI 33 provides clear procedures. Appropriate responses include:

- establishing the cause of any security incident, whether accidental or deliberate;
- the action to be taken to recover and minimise the exposure to a compromise; and
- how to prevent a recurrence.

How your agency will accomplish this should be described in a documented Incident Response Plan, which all agencies should develop.

The PSM states that the Defence Signals Directorate should be notified of any significant incident involving a security breach in a Commonwealth Government computer system. DSD may then help analyse the incident, identify remedial measures to remove the exploited vulnerability, minimise the likelihood of future compromise, and perform an overall assessment of the organisation's system security safeguards. Formal incident reporting should be undertaken using the established Information Security Incident Detection, Reporting, and Analysis Scheme (ISIDRAS), details of which are available from <http://www.dsd.gov.au/infosec>

ISIDRAS is not a substitute for referring criminal activity to the Australian Federal Police (AFP). Unauthorised access to a Commonwealth computing system is an offence under the Crimes Act, as is using a Commonwealth facility to obtain unauthorised access to any computing system. Agencies should define in their Incident Response Plan which type of incident should be reported to the AFP.

From early 2001, all Commonwealth agencies are required to participate in additional incident reporting and security mechanisms, co-ordinated by NOIE and DSD, which supplement ISIDRAS reporting. This system may monitor a wider range of low and medium level security incidents, and facilitate exchanges of security information, solutions and advice between agency security professionals and online managers.

- ▶ More information is available from: <http://www.govonline.gov.au/projects/standards/security.htm>

Authentication *(Essential for Stages 3–4)*

Establishing a degree of trust or confidence about the identity of parties involved in an online transaction with government is essential in many circumstances. This is called 'authentication'. You should be aware of authentication issues because they can run hand in hand with issues regarding prevention, detection and reaction. Protection, detection and reaction may be less effective if authentication is not part of the security framework around a website or online service. Whether authentication is required for your online application will depend on the type of government service you provide, the type of information you need to protect and your assessment of security risk.

Where a high degree of assurance is needed, electronic authentication technologies such as digital signatures (generated using 'public key' technology) can reliably authenticate parties. Public Key Infrastructure (PKI) can ensure:

- ▶ a transmission received or sent by an agency, is from who it says it is from (**authentication**);
- ▶ a transmission has not been changed in transit (**integrity and confidentiality**); and
- ▶ that neither party can deny that it was sent or received (**non-repudiation**).

PKI and digital signatures are the acknowledged foundation and assurance for conducting electronic commerce and other business transactions.

Within the Commonwealth government, where an online application uses strong, digital-signature-based authentication then compatibility with the Gatekeeper framework is mandatory.

- ▶ More information is available from:
<http://www.govonline.gov.au/projects/publickey/Gatekeeper.htm>



**COMMONWEALTH AGENCY
WEBSITE AND INTERNET SYSTEM SECURITY CHECKLIST**

WEBSITE OR ONLINE RESOURCE URL: (eg <http://www.yoursite.gov.au>).

.....://.....

Please indicate

or

GENERAL

1. Responsibility for online security and site compliance with Commonwealth security guidelines is part of the duty statement of an officer on the agency team responsible for website management.
2. An Agency Security Plan has been prepared, according to the PSM and ACSI 33 guidelines, that describes necessary security mechanisms and security procedures that apply within the agency, and this website or online system (including all of the key services that are involved in delivery of this site—e.g. DNS, firewall, databases, internet link) is included in that Plan.
3. Agency website managers are aware of the appropriate DSD security contacts and established incident reporting systems, so that when a incident does occur, they know who to report it to, and how.

SECURITY AUDIT OR REVIEW

4. A formal Threat and Risk Assessment has been performed against this site in the past 12 months by an appropriately qualified body or agency.

PRIVACY

5. The site has a prominent privacy statement making clear what information the site collects and how it will be used, and warranting that any information collected will be securely protected from unauthorised disclosure.
6. The site privacy statement complies with all the online Privacy Principles developed by the Privacy Commissioner.

GOVERNMENT CLASSIFIED INFORMATION

7. If or where Government Non-National Security Classified information (e.g. In-Confidence, Protected) is made available on this website or online system, then only DSD approved security products that have been evaluated under the Australasian Information Security Evaluation Program (AISEP) have been used; and/or the aggregated security mechanisms and procedures are suitable for the adequate protection of the data (refer to the PSM, ACSI 33, and DSD).
8. There is no National Security Classified information available on this website or online system.

Please indicate
 or

ENCRYPTION AND AUTHENTICATION

- 9. If or where this website or online system makes use of a Public Key based encryption or authentication technology, that technology meets the mandated Commonwealth Gatekeeper standards and is sourced from Gatekeeper accredited suppliers.
- 10. If or where this website or online system uses strong, digital-signature-based authentication to identify or authenticate business customers online, the system uses the Australian Business Number (ABN) as the identifier and the Gatekeeper compliant ABN-Digital Signature Certificate as the authentication tool, as is mandated for Commonwealth agencies.

EXTERNAL HOSTING/SERVICE PROVIDERS

- 11. All non-agency external third parties (e.g. web hosts, outsourcers, web developers, telecommunications providers, payment gateway providers) with a substantial role in the delivery of this site or online service, or the handling of sensitive site information, have been accredited according to AS 4444, or can demonstrate compliance with Commonwealth security guidelines such as ACSI 33 or the PSM.
- 12. Where non-agency external third parties play a role in directly managing or updating the site, systems are in place within the agency (e.g. Service Level Agreements with suppliers, contract conditions) to ensure effective protection of the confidentiality of site data, preservation of site security, and best practice site management.

SYSTEM AUDITING

- 13. A detailed audit and activity log (web server, proxy, login attempts etc.) collection and review system is in place on this website and associated internet systems.
- 14. Online system audit or activity logs are scanned, analysed and archived regularly.
- 15. Incident analysis is performed and recorded where suspicious activity may be evident.
- 16. The agency is a participant in an established incident reporting system.
- 17. Systems and procedures are in place to report suspicious or damaging activity to DSD or appropriate authorities under the incident reporting framework.

INTRUSION DETECTION

- 18. Intrusion detection and/or network monitoring systems are in active operation on this website.

INFORMATION PROTECTION

- 19. Where information about individuals or businesses (including email addresses) is collected by, or available from this online system or website, appropriate measures are in place to securely store and protect this information.



| | Please indicate <input type="checkbox"/> or <input type="checkbox"/> |
|--|---|
| 20. Access control, authentication and protection mechanisms are in place on sensitive elements of this agency system or website. <i>These mechanisms may include:</i> <ul style="list-style-type: none"> ▶ IP address or Domain Name access restrictions; ▶ Proxy server access controls; ▶ Restrictive file/directory permissions; ▶ Security measures on data bases behind firewalls; ▶ User authentication of website visitors and users; and ▶ Encryption used for authentication, confidentiality or integrity. | |
| 21. Systems are in place to detect unauthorised changes to website data and key system configuration files. | |
| 22. Systems are in place to capture and report illegal, unusual and unexpected input to the web server or other online system elements. | |
| 23. Regular backups of site content and key system data are performed, and stored securely. | |
| 24. A disaster recovery plan for the site has been prepared and tested, which includes planning for recovery from a serious website security breach. | |
| CHANGE CONTROL | |
| 25. Relevant system changes are reviewed and tested from a security perspective before implementation. | |
| FIREWALLS/SANITISATION | |
| 26. A formal sanitisation and checking process is employed when information is transferred from the internal network to the website in order to guard against leakage of sensitive information. | |
| 27. Firewall(s) are in use to control access to the website or internet system, from external and sensitive internal systems, and to also block unauthorised transmissions from the site. | |
| 28. Any firewall(s) in use on sensitive system elements has been certified by DSD or an appropriately qualified organisation. | |
| 29. Firewall(s) in use are actively maintained and monitored, and the latest updates, patches etc. are applied. | |
| ADDITIONAL WEB SERVER FUNCTIONALITY | |
| 30. If or where this online system or website uses active server content or technologies (such as CGI scripts, ASP, PHP, Java servlets, Cold Fusion, or Server Side Includes) appropriate measures are in place to identify, and then remove or control the vulnerabilities these technologies may introduce into the site or online system. | |
| 31. If or where this online system or website provides an ability to query or display information from a database product (such as SQL Server, Oracle, DB2, Access), appropriate measures are in place to identify, and then remove or control the vulnerabilities this functionality may introduce into the site or online system. | |

| | Please indicate <input checked="" type="checkbox"/> or <input checked="" type="checkbox"/> |
|---|---|
| 32. Any additional online functionality or internet services (such as telnet, email, FTP, chat, NNTP, LDAP directory services) offered by this website or internet service are identified, appropriately authorised, protected and managed, under the same security arrangements that apply to the core services of the site. | |
| 33. Agency site management has audited or scanned this website or online service for the most common vulnerabilities introduced into an online system, where technologies such as active server content, databases or other internet services may be made available. Site management has taken remedial action to address any vulnerabilities identified. | |
| SITE 'HARDENING' | |
| 34. On this website or online system, no software or services other than those required to deliver the core functionality of the site are installed. | |
| 35. On this website or online system, sample code normally installed as part of the default setup of the web server and/or operating system has been removed. | |
| 36. On this website or online system, development tools are not installed, or if installed, are appropriately secured. | |
| 37. On this website or online system, remote administration tools or web pages are not installed or active, or if installed or active, are appropriately protected with, for example, IP address or domain name restrictions on their use, or access is only made available via an authenticated encrypted session. | |
| 38. On this website or online system, there is a procedure in place to ensure that vendor security patches/updates for key system software components (the web server, operating system, database, middleware etc) are regularly applied. | |
| 39. On this website or online system, passwords are changed regularly, and there are clear guidelines in place for password selection and usage for all systems involved in delivering the service, including advice to staff not to disclose passwords to unknown and/or third parties. | |
| 40. Administrative access (physically and electronically) to the externally visible or key elements of this website or online system (e.g. the 'live' web server or the firewall) is tightly restricted. | |

Upon completion, please store this document in a secure location. Please do not send it to NOIE—retain it for your own records and action.



National Office for the Information Economy,
Government Online group.
<http://www.govonline.gov.au>
Contact information:
Steven Byrne—steven.byrne@noie.gov.au
Jim Aked—jim.aked@noie.gov.au



Defence Signals Directorate, Information Security Group
<http://www.dsd.gov.au/infosec>
Contact information:
DSD Infosec Group—assist@dsd.gov.au
Telephone — 02 6265 0197

Further Information

Further information about how to decide to use the internet to deliver government programs and services, and on how to deliver programs and services more effectively through the internet, is found in other components of this ANAO Better Practice Guide, called *Internet Delivery Decisions—A Government Program Manager's Guide*. The full list of components is:

1. How to Decide to Use the Internet to Deliver Government Programs and Services
2. A Business Case and Cost Benefit Analysis for Internet Use in Government
3. Designing and Maintaining Internet Sites for Government Programs
4. Costing Internet Service Delivery in Government
5. Monitoring and Evaluating Internet-Delivered Government Programs and Services
6. Government Internet Systems—Security and Authentication
7. Legal Considerations for Government Internet Service Delivery
8. Privacy Issues, the Internet and the Government Manager
9. How to Make Government Sites More Accessible

Printed copies of this Guide are available from the ANAO. Copies can also be downloaded from the ANAO website—<http://www.anao.gov.au>

April 2001



Legal Considerations for Government Internet Service Delivery



Internet Delivery Decisions

A Government Program
Manager's Guide



This component of the Better Practice Guide identifies legal issues associated with deciding whether to deliver a government program or service via the internet. It describes Australian laws applying to electronic service delivery, and addresses the question of how the *Electronic Transactions Act 1999* affects contracting.

The internet (or 'online environment') is a recent phenomenon, often characterised as allowing people to work (or interact) faster and more efficiently. This rapid development means it can be easy to overlook basic legal principles that govern the way commercial and government transactions have traditionally been conducted.

Commonwealth agencies that provide information and deliver services online need to be aware of the legal risks they may inadvertently expose themselves to. For the most part, laws that apply to paper transactions and traditional forms of communication apply to electronic transactions. For example, agencies need to respect defamation and intellectual property when publishing on the internet.

Characteristics peculiar to the online environment may increase these legal risks. The speed at which contracts can be formed electronically, for example, means that you may not always have adequately considered the issues or obtained sufficient legal advice before committing to a contract.

Agencies must therefore be alert to the range of legal issues when using the internet to deliver services and provide information. This component is not intended as comprehensive legal advice and you are encouraged to seek separate legal advice on issues specific to your work area.

How do I identify the legal issues?—conduct a legal risk analysis

If your agency intends to provide services and information online, you should conduct a legal risk analysis at the same time—and perhaps even before—you begin to think about delivery methods and design features. A legal risk analysis can be conducted by in-house legal advisers or other legal service providers. Consulting other agencies may also help identify actual and potential legal issues.

A legal risk analysis should be conducted in much the same way that a security risk analysis or economic risk analysis is conducted, that is,

- ▶ think about the consequences of the risk becoming a reality;
- ▶ assess the likelihood of this happening;
- ▶ consider the potential seriousness if something were to go wrong;
- ▶ identify what could go wrong—risk identification; and
- ▶ devise and implement risk mitigation strategies for each risk.

Some very useful guidelines for managing risk in the Australian Public Service are set out in the Australian and New Zealand Risk Management Standard published by Standards Australia (AS/NZS 4360:1999—Risk Management).

Resource management is an important consideration when assessing how to manage your legal risks. Section 44 of the *Financial Management and Accountability Act 1997* requires Chief Executive Officers to manage agency affairs in a way which promotes proper use of the Commonwealth resources for which the Chief Executive Officer is responsible. The Act defines 'proper use' as meaning 'efficient, effective and ethical use'. At this time, the relationship between this Act and legislation such as the *Electronic Transactions Act 1999* (the *Electronic Transactions Act 1999* is discussed in detail below) has not been tested in court with regard to program delivery on the internet.

You are encouraged to seek separate legal advice on the relationship between these different laws.



If your agency intends to provide services and information online, you should conduct a legal risk analysis at the same time—and perhaps even before—you begin to think about delivery methods and design features.

A legal risk analysis must take into account two important considerations; the potential and actual legal risks and opportunities represented by the online environment, and the Australian legal framework.

So what are the legal opportunities and risks represented by the online environment?

The opportunities offered by the online environment are well known and widely publicised. Online technology is convenient, relatively cheap and quicker than other forms of communication. It can be accessed from home or office 24-hours a day. It assists in bridging the perceived, if not actual, distance between government and the public. Online technology enables Australians to access government services and information quickly and directly. Indeed, Australians are among the highest per capita users of the internet worldwide.

Increasing the speed with which information can be accessed and transactions concluded, as well as increasing the range of people who can access information and services, can increase risk exposure. In particular, the key risk for a Commonwealth body providing services and information online is liability.

In order to identify the legal risks that can arise in the online environment you should think about what activities can be carried out online. The two most important activities in relation to government are providing services and disseminating information. Liability can arise in relation to both activities in a variety of ways:

- ▶ breach of specific Australian law, including discrimination, privacy, defamation and intellectual property laws;
- ▶ misleading and deceptive conduct;
- ▶ incomplete or inaccurate processing of information;
- ▶ ineffective or inappropriate authentication mechanisms; and
- ▶ security failure and breaches.

Legal Risk Mitigation—Disclaimers

One way you may wish to mitigate your risk and limit liability is by including a disclaimer on your home page. The disclaimer may refer to information on your site and linked sites. The disclaimer must be in a prominent position so that visitors to the site have a reasonable chance of seeing it.

The disclaimer does not absolve an agency of its responsibility for maintaining the accuracy of information displayed on its site. You should get legal advice when drafting a disclaimer in order to ensure it is appropriate for the purposes of the particular site.

What Australian laws apply generally to electronic service delivery?

Australian laws regulate the way information is collected, used, disseminated and stored. These restrictions apply equally to the online environment as they do to other forms of communication including written communications and speech.

The *Privacy Act 1988* and *Copyright Act 1968* are two good examples of the way in which laws apply to the online environment in much the same way as they do in the paper environment. You need to be familiar with both pieces of legislation to deliver services online in a way that complies with both government policy and the law.

Privacy

People have legitimate concerns about the legal certainty, security, authentication and privacy of electronic commerce. They need to be assured of who is collecting their name, address, telephone number, credit card details and any other information they disclose on the internet and that this information will be secure and accurate. They also need to be informed about how that information will be used, to whom it may be disclosed and for what purposes. Specific information on privacy issues for government managers is covered in the separate privacy component of this Guide. A brief summary of the Commonwealth legal framework for privacy protection follows.

The Privacy Act

Federal Government agencies are already required by law to inform people with whom they deal of these matters whether such dealings are conducted face to face, by mail or online. The 11 Information Privacy Principles (IPPs) in the *Privacy Act 1988* (the Privacy Act) govern the collection, storage, security, use and disclosure of personal information as well as access to, and correction of, such information by the individual concerned.

If you are conducting any business online you must ensure that you abide by the IPPs in the Privacy Act in your online activities. For example, you must ensure that your website privacy statements clearly set out your agency's policy and practice in relation to the online handling of personal information. System interfaces should be designed so that the only personal information that is solicited online is that which is necessary for the particular transaction. You are also required to ensure appropriate levels of data security.

The Privacy Act currently applies to Commonwealth and Australian Capital Territory (ACT) Government agencies and has some application to the private sector in respect of tax file numbers and the credit reporting industry.

Private sector privacy law

Recent legislation passed by Parliament will result in most private sector organisations being subject to privacy standards when handling personal information. The *Privacy Amendment (Private Sector) Act 2000*, which amends the Privacy Act, will come into effect on 21 December 2001. The new private sector privacy legislation establishes a co-regulatory privacy scheme for the private sector. It sets out legislative privacy standards called the National Privacy Principles (NPPs) and enables private sector organisations to develop privacy codes. For the Office of the Federal Privacy Commission to approve a privacy code, it must incorporate the NPPs or set out obligations that are at least equivalent. While the NPPs cover the same matters as the IPPs, there are differences.



The new private sector privacy legislation does not affect how the Privacy Act currently applies to Commonwealth agencies. However, some agencies that have exemptions under the Privacy Act due to their commercial activities may be brought within the private sector scheme. Also, there are special provisions directed at outsourcing government services to ensure that contracting agencies include privacy clauses in their contracts. Such clauses should ensure contractors are subject to the IPPs not the NPPs in respect of any personal information they handle on behalf of the Commonwealth.

You should be aware of these provisions if your internet service delivery uses private sector contractors.

Further information about the Privacy Act

For more information about the private sector privacy legislation and a compilation of the Privacy Act incorporating the amendments, refer to the component in this Better Practice Guide titled *Privacy Issues, the Internet and the Government Manager*. Also refer to the Attorney-General's Department website: <http://www.law.gov.au/privacy/>. The Information Law Branch of that department can answer queries concerning privacy.

Copyright

Copyright is a type of property right that is designed to give authors control over certain of their original works. Copyright protects a range of material including those commonly found on websites such as:

- ▶ written material (text, charts, tables);
- ▶ artistic works (graphics, icons, photographs, plans);
- ▶ computer programs;
- ▶ musical works;
- ▶ films (including moving images); and
- ▶ sound recordings.

Copyright owners have a number of rights in relation to their material. For example, they can control the reproduction and publication of their material. Others who wish to use the material in these ways must seek the permission of the copyright owner. However, there are some exceptions (e.g. fair dealing for the purposes of research or study) that allow others to reproduce copyright material without permission.

If you are conducting any business online you must ensure that you abide by the IPPs in the Privacy Act in your online activities. For example, you must ensure that your website privacy statements clearly set out your agency's policy and practice in relation to the online handling of personal information.

The Commonwealth's copyright

The Commonwealth owns copyright in material produced by its employees in the course of their employment. It also owns copyright in material produced under its direction or control, however, this can be varied by agreement. Ownership of copyright is an issue that you should consider when negotiating contracts for website development with external service providers.

Copyright notices

In Australia, copyright protection is automatic and no registration is required. It is not necessary to include the copyright symbol (©) on material in order for it to be protected by copyright. However, in some overseas countries, to qualify for copyright protection it is necessary that works bear the copyright symbol in a prominent place. It would therefore be prudent for Commonwealth publications (including websites) to include a copyright notice. The standard notice for Commonwealth websites is as follows:

© Commonwealth of Australia 200_ [year website released]

This work is copyright. You may download, display, print and reproduce this material in unaltered form only (retaining this notice) for your personal, non-commercial use or use within your organisation. Apart from any use as permitted under the Copyright Act 1968 all other rights are reserved. Requests for further authorisation should be directed to the Manager, Legislative Services, Department of Finance and Administration, GPO Box 1920, Canberra ACT 2601 or by email to Cwealthcopyright@dofa.gov.au

Using copyright material

'Government use' provisions in copyright law allow the Commonwealth to use copyright material belonging to others without their permission. However, this is on the condition that the material is used for the services of the Commonwealth and that the Commonwealth notifies the copyright owner and pays royalties for the use. The Commonwealth has entered into royalty agreements with societies that act on behalf of owners of copyright in written work and music. When using work that is not covered by these agreements, Commonwealth agencies will need to notify the copyright owner and negotiate a royalty.

Linking to other websites

Linking to other websites may raise copyright issues, particularly when material from another site is displayed in a frame on the website. It is advisable that you seek permission from the copyright owner of another site before linking to that site. It may also be advisable to use a disclaimer in relation to the content of the other site.

As the content of sites outside your agency's control may change without notice, include this in your risk assessment.

Further information about copyright

Further information about copyright is available from the Attorney-General's Department's Intellectual Property Branch (ip_branch@ag.gov.au or tel (02) 6250 6655) and the department's publication *Copyright Law in Australia: A Short Guide* (<http://www.law.gov.au/publications/copyrightaus97.htm>)



Information about administration of Commonwealth copyright (including copyright notices) is available from the Department of Finance and Administration (www.dofa.gov.au/infoaccess)

The Australian Copyright Council also provides information about copyright and the internet (<http://www.copyright.org.au>)

What Australian laws are specific to online service delivery?

The electronic commerce legal framework

In addition to laws about collecting, publishing and storing information, you should also be aware of laws specific to the online environment. An important part of the Government's Online Strategy is establishing a legal and regulatory framework for electronic commerce. The Government has committed itself to a light-handed, technology neutral framework to support and encourage business and consumer confidence in the use of electronic commerce.

The Electronic Transactions Act 1999

The *Electronic Transactions Act 1999* (the ETA) began on 15 March 2000 and represents a major step in meeting the Government's online service delivery commitment. Broadly speaking, the ETA removes existing legal impediments that may prevent a person using electronic communications to satisfy obligations under Commonwealth law. The ETA generally gives business and the community the option of using electronic communications when dealing with government agencies.

The ETA allows business and the community—your clients—to transact electronically with you and each other and in so doing to still satisfy Commonwealth legal requirements. It establishes the basic rule that, for the purposes of a law of the Commonwealth, a transaction is not invalid because it took place by means of an electronic communication. Specifically, four types of requirements under a law of the Commonwealth can now be satisfied using electronic communications—a requirement to:

- give information in writing (section 9);
- provide a signature (section 10);
- produce a document (section 11); and
- retain or record information (section 12).

The implications of the ETA for you are:

- where a person is required by law to give you information in writing, to provide a signature or produce a document, that person may choose to do so electronically;
- you can specify conditions that a person must meet if they wish to transact electronically with you but if those conditions are met the electronic communication will have the same legal status as a paper based communication;
- while members of the public and business are encouraged to enter the information economy by communicating electronically, they are not compelled to do so and must consent to receiving electronic communications from you; and
- you must accept electronic communications that comply with any IT requirements you have specified.

To determine the ETA's impact on your work in the short term you need to look at what laws the ETA applies to. The ETA is being introduced in two phases. The first phase began on 15 March 2000 when the ETA began. The second phase will begin on 1 July 2001. The ETA applies to 'laws of the Commonwealth' as defined in the ETA. Until 1 July 2001 a law of the Commonwealth is a law specified in the Electronic Transactions Regulations. After 1 July 2001 all Commonwealth laws will fall within the operation of the ETA except where a law has been expressly exempted.

In order to comply with the requirements of the ETA and government policy you must:

- ▶ decide whether legal requirements in legislation you administer to produce or retain information or provide a signature can be met electronically. After 1 July 2001 the ETA will apply to all laws you administer unless your laws are specifically exempted from the operation of the ETA.

The ETA does not operate where other, more specific, Commonwealth laws make provision for online service delivery (see section 9(3), 10(2) and 11(4)). However, enactment of specific legislation should only be considered where particular concerns mean that it is not appropriate to rely on the general provisions in the ETA.

- ▶ put in place IT systems and policies to manage these types of transactions. The ETA does not oblige you to accept electronic communications without qualification. The ETA allows your agency to specify IT requirements-including electronic signature requirements-to ensure that your clients are communicating with you in an appropriate way.
- ▶ notify your clients of your IT requirements so they can communicate electronically with you. Public notification of these requirements is critical to successfully implementing the ETA and may include publicising your IT requirements on your website, identifying your email address on your letterhead or sending information leaflets to your actual and potential clients.
- ▶ put in place electronic records management systems to ensure electronic records are managed with the same diligence as you would manage paper records. Electronic records are subject to requests under the *Freedom of Information Act 1982*.

Further information—the ETA

For further information about the ETA visit the Attorney-General's Department electronic commerce website at <http://www.law.gov.au/ecommerce> or email the AGD ecommerce mailbox at ecommerce@ag.gov.au

How does the Electronic Transactions Act affect contracting?

There is no general rule in Australian law that requires contracts to be in writing. However, written evidence of a contract may be required in some circumstances through the operation of (usually) State or Territory legislation such as legislation giving effect to the Consumer Credit Code.

The States and Territories have agreed to enact a Uniform Electronic Transactions Bill (the Bill) which is essentially identical to the Commonwealth's ETA. The Bill will apply to all laws of the jurisdiction in which it is enacted. This means that in situations where you use both Commonwealth and State or Territory law, you need to be aware of both the Commonwealth's ETA and the law in the relevant State or Territory. For example, whether a State or Territory has enacted the Bill will assist in determining whether contracts can be formed electronically in that jurisdiction.



At the time of publication New South Wales, Victoria, South Australia, Tasmania, Northern Territory and the Australian Capital Territory have enacted the Bill. Western Australia has introduced the Bill into their legislature. Queensland is expected to enact the Bill in the course of this year.

The ETA and the Bill establish the basic rule (set out in section 8 of the Act and section 7 of the Bill) that a transaction will not be invalid or unenforceable simply because it took place by means of an electronic communication. This will operate to ensure that, as a general principle, contracts can be formed by the use of electronic communications. Section 9 of the Act (replicated in section 8 of the Bill) ensures that legislation imposing writing requirements for certain types of contracts can be satisfied by the use of electronic communications.

The Uniform Electronic Transactions Bill makes clear in its definition of the term 'transaction' that it includes contractual transactions. Therefore, generally speaking, contracts may be made using the internet.

There are particular issues concerning the formation of a contract where goods and services are offered online that may not be present in more traditional forms of commercial transactions that are usually recorded in a physical document and evidenced in a physical transaction. These include evidencing the existence of a contract, determining whether a contract has been made and proving the terms of the contract.

There is very little case law regarding the creation of contracts online in Australia. For example, it has been argued that users clicking on an 'I agree' button when ordering goods over the internet can be deemed sufficient to bind the user to a contract. While this is becoming an increasingly popular practice, there is no legal certainty regarding the way such agreements will be interpreted by a court. Therefore, there is an element of risk involved in using this method of contracting that you should consider when deciding whether to conduct transactions online.

You should give particular attention to the uncertainties concerning the formation of contracts online. Your staff need to be warned to take care and to obtain legal advice before entering into contractual commitments by email.

There are particular issues concerning the formation of a contract where goods and services are offered online that may not be present in more traditional forms of commercial transactions that are usually recorded in a physical document and evidenced in a physical transaction.

Conclusion

If you are currently, or contemplating, delivering services and providing information online in accordance with the Government's Online Service Commitment, you need to:

- ▶ be aware of the legal issues that can impact on the way information is presented, agreements are made and services provided online;
- ▶ involve legal advisers in the design and delivery of services and information online;
- ▶ conduct a legal risk analysis;
- ▶ consider the ways in which the *Electronic Transactions Act 1999* and the Government's Online Service Commitment will affect on the way you do business;
- ▶ develop a comprehensive privacy policy that is prominently displayed on the website;
- ▶ comply with guidelines for online privacy;
- ▶ consider limiting liability through the use of disclaimers;
- ▶ keep up to date with new laws affecting electronic commerce; and
- ▶ take advice on the impact of current and new laws on your operations.

Further Information

Further information about how to decide to use the internet to deliver government programs and services, and on how to deliver programs and services more effectively through the internet, is found in other components of this ANAO Better Practice Guide, called *Internet Delivery Decisions—A Government Program Manager's Guide*. The full list of components is:

1. How to Decide to Use the Internet to Deliver Government Programs and Services
2. A Business Case and Cost Benefit Analysis for Internet Use in Government
3. Designing and Maintaining Internet Sites for Government Programs
4. Costing Internet Service Delivery in Government
5. Monitoring and Evaluating Internet-Delivered Government Programs and Services
6. Government Internet Systems—Security and Authentication
7. Legal Considerations for Government Internet Service Delivery
8. Privacy Issues, the Internet and the Government Manager
9. How to Make Government Sites More Accessible

Printed copies of this Guide are available from the ANAO. Copies can also be downloaded from the ANAO website—<http://www.anao.gov.au>

April 2001



Privacy Issues, the Internet and the Government Manager



Internet Delivery Decisions

A Government Program
Manager's Guide



This component of the ANAO Better Practice Guide identifies privacy issues that program managers must consider when deciding whether to deliver a government program or service via the internet. Part One of this component, prepared by the Office of the Federal Privacy Commission, includes the Federal Government websites guidelines mandated in 'Government Online: The Commonwealth Government's Strategy' released in April 2000. Part Two includes guidelines on workplace email, web browsing and privacy.

Part One

Guidelines for Commonwealth Government World Wide Websites¹

Introduction

The purpose of these guidelines is to assist agencies to adopt best privacy practice and comply with the Privacy Act in respect to their websites. When agencies are considering their web strategies and if personal information may be transmitted, published, solicited and collected using the internet they need to consider the relevant privacy implications. It is the responsibility of agencies to ensure that their website implementation complies with the Privacy Act and addresses the privacy concerns of net users.

It is not possible in this document to provide advice that will cover all possible agency website implementations. If you need further advice please contact our Office at privacy@hreoc.gov.au or phone the IT Standards Section on (02) 6247 3449.

Background

Several online surveys have indicated that Privacy is a major concern of net users. These surveys indicate several concerns including a lack of transparency regarding the use and disclosure of personal information by websites, the tracking of individual's activities at websites and concerns about the security of their information in the internet environment. It is widely considered that the public needs to trust that their privacy will be protected before they make significant use of the internet for services such as Internet Commerce and Electronic Service Delivery.

Openness

Privacy statement or policy

In response to these concerns many websites now include a Privacy Statement or Policy which states what information is collected about individuals when they visit the website, how it is used and if it is disclosed. This is now considered to be best practice.

Guideline 1

Agency websites should incorporate a prominently displayed Privacy Statement which states what information is collected, for what purpose and how this information is used, if it is disclosed and to whom and addresses any other relevant privacy issues.

¹ These privacy guidelines also apply to ACT Government websites.



Clickstream data and cookies

The Privacy Act defines personal information as ‘...information about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.’ Some information collected by website hosts about individuals visiting the site will not in itself identify the individual. This is sometimes called ‘clickstream data’ and consists of information automatically collected and logged due to the nature of the communications protocols. The following text from the Federal Privacy Commissioner's website Privacy Policy sets out the click stream data collected.

Our service provider makes a record of your visit and logs the following information for statistical purposes—the user's server address, the user's top level domain name (e.g. .com, .gov, .au, .uk etc.), the date and time of the visit to the site, the pages accessed and documents downloaded, the previous site visited and the type of browser used. No attempt will be made to identify users or their browsing activities except, in the unlikely event of an investigation, where a law enforcement agency may exercise a warrant to inspect the service provider's logs.

Even though clickstream data may not in itself identify individuals, and so may not be personal information as defined in the Privacy Act, it is recommended, in the interests of transparency that website Privacy Statements and Policies state what clickstream data is collected.

Cookies can also be used to track individuals' activities on websites. Like clickstream data, cookies may not conform to the Privacy Act definition of personal information, however many net users consider cookies to be intrusive. If a website uses cookies it is recommended that the Privacy Statement or Policy state that they are used and for what purpose.

Collecting personal information using websites

Some agencies may collect email addresses when individuals email the agency using the website. Agencies may also use electronic forms to solicit personal information related to the agencies' functions. This will become more widespread as agencies employ the internet for Electronic Service Delivery. Where agencies solicit and collect personal information using their websites, they must comply with the collection **Information Privacy Principles (IPPs 1–3)** of the Privacy Act.

IPP 1. (1) requires the collector to only collect personal information for a lawful purpose, directly related to the function or activity of the collector and that the collection be necessary for or directly related to that purpose. IPP 1. (2) requires that personal information not be collected by unlawful or unfair means. IPP 3 makes similar requirements for when the collector solicits personal information. To comply with the collection principles agencies should not collect or solicit personal information using their websites which would be unlawful, unnecessary or unrelated to their functions and collection should not be unfair or unreasonably intrusive.

IPP 2 requires that agencies provide notice to individuals where any personal information is solicited from the individual concerned. The notice should cover all those matters addressed by IPP 2, namely the purpose for which the information is being collected (including if the information is to be published), the legal authority for the collection if it is authorised or required by or under law and any usual disclosures made by the agency.

An example of part of a Privacy Statement for a site that collects email addresses is below.

We will only record your email address if you send us a message. It will only be used for the purpose for which you have provided it and will not be added to a mailing list. We will not use your email address for any other purpose, and will not disclose it, without your consent.

Guideline 2

Agencies that solicit or collect personal information using their websites must comply with IPPs 1–3. Agency website privacy statements should include a statement regarding this collection which complies with IPP 2. Where an online form is used to collect personal information the statement should be on the same page as the form or prominently linked to it.

Security

IPP 4. (a) requires record keepers to ensure that records containing personal information are protected by such security safeguards as are reasonable in the circumstances to take against loss, unauthorised access, use, modification, disclosure and other misuse. Agencies must ensure that their internal networks and databases which contain personal information are sufficiently protected from unauthorised access using their website and any internet connection. Firewall technology is often used to protect internal networks from the web. The Defence Signals Directorate issues guidelines and provides advice for Federal Government agencies on security.

When agencies solicit or collect information from individuals using electronic forms or email they should make it clear to the individual the risks associated with using the internet as the transmission medium and notify the individual of any other options there are for providing the information. For example, the individual may prefer to use the telephone or provide a response on paper.

If any security measures, such as encryption, are provided information regarding these should be provided to the individual. For example, the agency may include a hyperlink to a brief statement about internet security and, if they use encryption, to a statement about the product used and the level of protection it provides.

Guideline 3

If personal information is collected using an agency website this should be done by sufficiently secure means. Individuals should be provided with alternative means of providing personal information to the agency, other than using the website. The Privacy Statement should address security issues where appropriate.

Publication

Generally Available Publications (GAP)

The **definition of a record** in section 6 of the Privacy Act excludes a Generally Available Publication (GAP). A GAP is defined in the Privacy Act as a *...publication that is or will be generally available to members of the public*. Most websites are accessible to anyone with web access. If a website is accessible to the public then it fits the Privacy Act definition of a GAP. Some websites may be protected cryptographically and accessible only to users with a key or password (these are sometimes called extranets or virtual private networks) and other websites may exist within an agency or organisation and only be accessible to staff (sometimes called intranets). Sites such as these, which are not generally available to the public, are not GAPs.

While not prevented by the Privacy Act, the web publication of GAPs (not originally published on the web) can raise privacy concerns. Agencies should carefully consider the appropriateness of:

- ▶ placing GAPs which contain personal information on the web, as this information may be exposed to a much wider audience than originally intended; and



- ▶ publishing on the web, personal information which was collected for inclusion in a less widely available publication.

Agencies should also be aware that the Privacy Act applies to any disclosures or publications of personal information they hold in their records regardless of whether the same information is included elsewhere in a GAP. Therefore agencies should not disclose or publish their records of personal information on the web simply because the same information is made publicly available in another form. Another option may be to de-identify or remove personal information from the document before publishing it on the web.

Publishing Personal Information on a website

Agencies may publish personal information if it is collected for this purpose and if the collection complies with the Privacy Act. If the personal information was not collected for inclusion in a publication, it may only be published if allowed by one of the exceptions to IPPs 10 and 11 (which, respectively limit the use and disclosure of personal information). IPP 10. 1(a) allows the use of personal information for another purpose if the individual concerned has consented to the new use. IPP 11. 1(b) allows disclosure of personal information where the individual concerned has consented to the disclosure. It is important, where consent for publication is sought, that it is **informed** consent.

The individual should be given to understand that if their personal information is published on the web then it will be accessible to millions of users from all over the world, that their information can be searched for using an identifier such as the individual's name and that their information can be copied, and used by any web user. Most importantly, the individual should be made aware that once their personal information has been published on the web, the agency has no control over its subsequent use and disclosure.

While there are other exceptions in IPPs 10 and 11 which may allow the publication of personal information on the web these circumstances seem unlikely. Agencies should seek advice from the Office of the Federal Privacy Commission if these circumstances arise.

The staff of Federal Government agencies are entitled to the same protection, afforded by the Privacy Act, as agency clients. However, IPP 10. 1(e) allows the publication of personal information if this is directly related to the purpose for which the information was obtained. The web publication of information about certain staff such as the agency head, senior officers and contact or media officers may be directly related to the purpose for which the information was obtained and therefore permitted by IPP 10. 1(e). IPP 11 would permit disclosure of such details where the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that their personal information would be widely disclosed (see IPP 11. 1(a)). Staff in senior positions, or positions of public contact, would probably normally expect their contact details to be publicly available in some form. These staff members should be advised if their personal information is to be published on the web.

Other staff, however, may not expect their personal information to be published on the web or in another form. There have been instances where agencies have published entire staff telephone lists on their websites.

It is easy to download or print an entire staff list that is made available on the web. The publication and easy accessibility of this information may place staff at risk of receiving unsolicited email (spam) and unwelcome attention from a range of people and organisations.

Publishing a staff list on the web, may place staff in a position where they are subject to scrutiny by people with whom they would not normally choose to share their personal information.

The individual should be given to understand that if their personal information is published on the web then it will be accessible to millions of users from all over the world, that their information can be searched for using an identifier such as the individual's name and that their information can be copied, and used by any web user.

The publication of information such as staff classifications may make the information even more interesting to third parties as the salary range associated with these classifications is publicly available information.

There may also be dangers to particular staff in publishing their personal information on the web. Individuals may be placed at risk of harassment particularly if their work involves contact with members of the public. For personal safety reasons individuals may not wish that their work contact details be published.

There may also be instances where personal information is incidentally or accidentally published on the web. Personal information may be included in documents which are published on the web. It is recommended that documents are carefully checked before being published on the web and any unnecessary personal information removed.

Guideline 4

Where agencies are considering the publication of personal information regarding individuals on the web they should be sure that this complies with IPPs 1–3 and 10 and 11.

Guidelines

Openness

Guideline 1. Agency websites should incorporate a prominently displayed Privacy Statement which states what information is collected, for what purpose and how this information is used, if it is disclosed and to whom and addresses any other relevant privacy issues.

Collection of Personal Information using the website

Guideline 2. Agencies that solicit or collect personal information using their websites must comply with IPPs 1–3. Agency website privacy statements should, include a statement regarding this collection which complies with IPP 2. Where an online form is used to collect personal information the statement should be on the same page as the form or prominently linked to it.

Security

Guideline 3. If personal information is collected using an agency website this should be done by sufficiently secure means. Individuals should be provided with alternative means of providing personal information to the agency, other than using the website. The Privacy Statement should address security issues where appropriate.

Publishing Personal Information on a website

Guideline 4. Where agencies are considering the publication of personal information regarding individuals on the web they should be sure that this complies with IPPs 1–3 and 10 and 11.

The Human Rights and Equal Opportunity Commission welcomes feedback or comments. If you have any questions or comments please send these to: privacy@hreoc.gov.au



Part Two

Guidelines on workplace email, web browsing and privacy

Introduction

The use of the internet by governments and organisations has raised concerns about the privacy of staff email and web browsing activities. Despite the fact that they are using government or corporate equipment and networks staff may consider that their emails and web browsing activities are private. In some cases access controls and security features of a network (passwords etc.) give the user an illusion of privacy and they may not be aware that their browsing activities and email content can be scrutinised. It may not be understood that the purpose of access controls is to prevent unauthorised access.

The purpose of these Guidelines is to recommend steps that organisations can take to ensure that their staff understand the organisation's position on this issue through the development of clear policies.

This document is directed to organisations in both the public and private sectors. For agencies in the Commonwealth and ACT governments the transparency and openness the Guidelines are based on the Information Privacy Principles (IPPs) and are strongly recommended as constituting compliance with the *Privacy Act 1988*. For private sector and other organisations not covered by privacy legislation the Guidelines are recommended as good privacy practice.

Information and communications technology in the workplace raises questions about the supervision of its use. This technology includes email and access to the internet. The computers and internal network involved are controlled by the organisation and management has the responsibility for issuing instructions as to their proper use.

Without clear instructions the proper use of email and web browsing may not be clear to many in the workplace. Good practice suggests that management spell out clearly their expectations and permitted practices to employees. These Guidelines are designed to assist in the development of good practice. If you need further advice please contact the Commission at privacy@hreoc.gov.au or phone the IT Standards Section on (02) 6247 3449.

Background

Privacy expectations in the workplace

It is clear that most staff do not expect to completely sacrifice their privacy while at work. Their organisation may provide them with an office, a locker or filing cabinet to which they possess keys and also access to the computer network including storage space for their files. Typically their access to the network and computer systems will be by password control. They may be encouraged or required to use non-obvious passwords and to change them frequently. Their personal password gives them access to their files, email account and to web browsing. This may give the impression that no-one can access their files or monitor their activities on the network. Some staff may not be aware that system administrators are usually able to access everything on the network.

The technical realities of email use and privacy

Most email is insecure. It should be regarded as insecure unless it has been encoded or encrypted. Email is often compared to a postcard in that anyone who receives it can read it. Email may also be read if it is stored on servers during transmission.

Emails are hard to destroy. Many people think that if they delete their email it is gone forever. This is not so as most electronic documents are backed up and recoverable.

Logging. Most software used to operate networks, including web servers, mail servers and gateways, logs transactions and communications. These logs will normally include the email addresses of senders and recipients of email and the time of transmission. The content of emails themselves would not normally be logged but may be stored on mail servers. Similarly, web server logs record information on the sites that people visit. The keeping of these logs is usually necessary for the routine maintenance and management of networks and systems. System administrators are also capable of reading the contents of emails sent and received by the corporate network.

Jurisdiction and legal issues

Private sector

The Office of the Federal Privacy Commission receives many inquiries regarding the privacy of workplace email and web browsing activities. It is apparent from these calls that there is a general expectation, by staff, that law exists which protects their privacy in the workplace. There is no general constitutional or common law right to privacy in Australia.

However, the Federal Government intends to introduce 'light touch' privacy legislation to cover the private sector which will be based on the National Privacy Principles for the Fair Handling of Personal Information. It is expected that this legislation will apply to staff emails that contain personal information other than 'employee records' in certain circumstances. The private sector legislation may also apply to logs of staff web browsing activities.

Public sector

The Information Privacy Principles in the Privacy Act apply only to Commonwealth and ACT Government agencies. Within the Privacy Act jurisdiction, emails which contain personal information are records for the purposes of the Privacy Act. While Information Privacy Principles (IPPs) 1–3 cover the collection of personal information, IPPs 2 and 3 apply only to the collection of personal information where it is solicited and therefore do not apply to logging scenarios where information is logged automatically.

IPP 1 applies more generally to collection and can be applied to logging. It requires that personal information be collected for a lawful purpose that is directly related to a function or activity of the collector, that the collection is necessary for or directly related to that purpose and that collection shall not be by unlawful or unfair means. If staff were not made aware of the logging of their network activities, then this could be considered to be unfair. Therefore, network users should be made aware of the logging practices of the organisation.

IPPs 10 and 11 may apply to email that contains personal information. IPP 10 limits the use of records of personal information for purposes other than for which it was obtained. IPP 11 limits the disclosure of records of personal information. Emails which contain personal information may only be disclosed where one of the exceptions in IPP 11.1 (a) to (e) apply.



Developing a Policy

Some inquiries to the Office of the Federal Privacy Commission involve scenarios where management has announced that staff may only use email and web browsing for work related purposes and that all email and web access logs will be monitored for compliance with this position. As the organisation has responsibility for its computer systems and networks, it has the right to make directions as to its use.

Informing people about the personal information that is collected, held and what is done with it is an important privacy principle. The Federal Privacy Commissioner encourages organisations to develop in consultation with staff a clear privacy policy in relation to staff use of computer networks, particularly with regard to the use of email and the internet. It is recommended that the policy clearly set out the proper and permitted use of the network, including internet email and web browsing. This policy may form part of a general IT usage policy or a separate privacy policy dealing with email and internet use. Such an approach is likely to result in a policy that staff understand and accept.

Guidelines

The following Guidelines are provided to assist organisations to develop policies or improve their existing policies.

- 1. The policy should be promulgated to staff and management should ensure that it is known and understood by staff. Ideally the policy should be linked from a screen that the user sees when they log on to the network.**

Consultation with staff may also be useful. A consultative process can engender an understanding by management of the sorts of legitimate activities staff are using email and web browsing for and increase the understanding by staff of the possible risk to the organisation associated with improper email and internet use.

- 2. The policy should be explicit as to what activities are permitted and forbidden.**

While it is for each organisation to determine what it considers to be appropriate usage of its system, to simply say that all activity must be 'work-related' may not be clear. There may be scope for guidelines outlining what personal use of email both within the organisation and externally, to other organisations, is appropriate. Other activities may be specifically prohibited, e.g. the use of email to harass, flame (to send abusive email) or defame or disclose information, or to transmit pornography.

The issue of appropriate usage may be harder to define in respect to web browsing. It may not be possible to tell if a web page is relevant until it has been read. The operation of web search engines can result in surprising and irrelevant search results. Links on websites may also be misleading. Discussion with staff on the issue of work related web use might help to clarify this issue. Where an organisation determines that usage is to be work related only, it should clearly spell out what it considers to be work-related and not work-related.

The policy should refer to any relevant legislation. In the Commonwealth public sector this would include the Privacy Act, the Archives Act, the Freedom of Information Act, the Crimes Act, the Public Service Act, Regulations and the Australian Public Service (APS) Code of Conduct. APS Regulations provide that employees must use Commonwealth resources in a proper manner and behave in a way that upholds the APS values and the integrity and good reputation of the APS. For more information on the *Public Service Act 1999* please visit the Public Service and Merit Protection Commission website.

The Sex, Race and Disability Discrimination Acts and workplace relations law apply in both the public and private sectors. In particular, employers (please refer to the 'Employers' Page on the Human Rights and Equal Opportunity Commission website.) should be aware of their obligations under these Acts to protect their employees against sexual harassment, racial vilification and other forms of unlawful discrimination which could occur through email and internet use. The Corporations Law may also be relevant as well as state and territory statutes.

3. The policy should clearly set out what information is logged and who in the organisation has rights to access the logs and content of staff email and browsing activities.

Staff email boxes will normally contain the emails they have sent and received. Back-ups and archives may also contain copies of emails that have been deleted by the user. As well as the actual content of messages, the date and time the message was transmitted, received and opened and the email addresses of the sender and recipients will normally be recorded.

With web browsing the Uniform Resource Locaters (URLs) or website addresses of sites visited, the date and time they were visited and the duration of site visits may be logged. Normally, access rights to staff mail boxes and logs would be restricted to those with the responsibility for administering the system. Such access should be as limited as possible and who has access rights should be clearly set out in the policy. The policy should outline in what circumstances IT staff can legitimately access staff emails and browsing logs.

The policy should also indicate, in general terms, under what circumstances an organisation will disclose the contents of emails and logs. Many organisations will only do this on the production of a legal authority.

- 4. The policy should refer to the organisation's computer security policy. Improper use of email may pose a threat to system security, the privacy of staff and others and the legal liability of the organisation.**
- 5. The policy should outline, in plain English, how the organisation intends to monitor or audit staff compliance with its rules relating to acceptable usage of email and web browsing.**
- 6. The policy should be reviewed on a regular basis in order to keep up with the accelerating development of the internet and IT. The policy should be re-issued whenever significant change is made. This would help to reinforce the message to staff.**

Conclusion

While it is acknowledged that access to staff emails and browsing logs by system administrators may be required in certain circumstances, it is unlikely that pervasive, systematic and ongoing surveillance of staff emails and logs should be necessary.

Organisations are encouraged to foster an environment where staff are assured that the privacy of their communications will be respected as long as they abide by the organisation's stated policy.

Balancing the legitimate interests of organisations and staff may be difficult and this balance may vary in different organisations. Policy or practice which leads staff to believe that their privacy in the workplace is not respected may be regarded as intrusive and oppressive and have a negative impact on morale and productivity.





How to Make Government Internet Sites More Accessible



9

Internet Delivery Decisions

A Government Program Manager's Guide

This component of the ANAO Better Practice Guide provides advice on how government managers can make government internet sites more accessible. It explains the reasons for making sites more accessible and describes the meaning of accessibility. It also sets out how program managers can confirm that their program's sites are accessible. Some better practice sites are also identified.

Why do Commonwealth internet pages need to be accessible?

- ▶ *because that's what often best suits the clients (or 'service users')*

For anyone who uses the online services, accessibility means better service at times and places which suit them. This is most important for clients with a disability, but more accessible services make access easier for everyone.

Remember, disability is not always a physical limitation. A client with agoraphobia (a fear of crowds or open spaces) may find a trip to a shopfront office an impossible challenge.

- ▶ *because it is efficient and effective to make internet based services accessible*

Internet based information products and services, when properly set up, can significantly reduce the expense and time spent using products such as Braille and audiotape to reach Australians with disabilities. It can reduce the need for inefficient paper products.

Accessible design makes it easier for everyone in the community to get better and faster access whether they have a disability, including:

- ▶ most home users, who do not have cable or ISDN internet access speeds;
 - ▶ lower income, rural or older users with even slower connections, slower modems or less than state of the art equipment; and
 - ▶ increasing numbers of users of non-PC internet devices, including hand-helds (Web Application Protocol devices, or WAPs) and mobile phones.
- ▶ *because the Government has decided that Commonwealth internet services must be accessible*

On 21 March 2000, the Government adopted accessibility requirements for Commonwealth sites. This is part of the Government online strategy, requiring:

- ▶ all Commonwealth departments and agencies to see their sites meet the World Wide Web Consortium's (W3C) accessibility standards from 1 June 2000;
 - ▶ all new/contracted site work to include accessibility benchmarks from 1 June 2000; and
 - ▶ all Commonwealth sites to meet W3C standards by 1 December 2000.
- ▶ *because the Disability Discrimination Act requires accessibility*

The *Disability Discrimination Act 1992* requires government bodies to provide equitable access to people with disabilities.

Commonwealth websites (and others, including commercial sites) risk exposure under the Act to complaints from anyone claiming disadvantage by lack of access. The Act requires equal access for disabled people, where it can reasonably be provided.

While other service providers may argue that providing access would 'involve unjustifiable hardship', this defence is not acceptable when administering Commonwealth laws and programs.



For anyone who uses the online services, accessibility means better service at times and places which suit them. This is most important for clients with a disability, but more accessible services make access easier for everyone.

What does accessible mean anyway?

In terms of government programs and services, accessible means available to clients in formats which are easily available, easy to use and appropriately targeted at the potential audience. For example, it might include providing:

- ▶ audio links for blind clients;
- ▶ pop-up screens and TTY (teletype) access for deaf clients; and
- ▶ translations for key languages for non-English speaking background clients.

Users who cannot see, or cannot easily read print (e.g. those suffering retinal pigmentosa, or RP), or cannot distinguish colours, or hear, can receive and exchange information through the internet as readily as other users if sites and services are designed to be accessible.

In particular, blind or vision impaired people can use screen reader software and a range of programs and devices to receive web page content in speech or Braille. People who cannot read written English -due to learning or literacy difficulties or language differences-can also benefit from this ability of the internet to deliver material in different formats.

But what does accessible really mean?

The W3C standards have been government's benchmark for accessibility for Commonwealth Government sites: (see also the Human Rights and Equal Opportunity Commission's [HREOC] advisory note on Disability Discrimination Act compliance at www.hreoc.gov.au/disability_rights/standards/www_3.html). Government has set the W3C's Priority 1 'checkpoints' as a first stage and required Commonwealth bodies to comply.

The selected priority one checkpoints within the W3C guidelines are:

In General (Priority 1)

- ▶ provide a text equivalent for every non-text element (e.g. via 'alt', 'longdesc', or in element content). This includes: images, graphical representations of text (including symbols), image map regions, animations (e.g. animated GIFs), applets and programmatic objects, ascii art, frames, scripts, images used as list bullets, spacers, graphical buttons, sounds (played with or without user interaction), stand-alone audio files, audio tracks of video, and video.
- ▶ ensure that all information conveyed with colour is also available without colour, for example from context or markup.

- ▶ clearly identify changes in the natural language of a document's text and any text equivalents (e.g. captions).
- ▶ organise documents so they may be read without style sheets. For example, when an HTML document is rendered without associated style sheets, it must still be possible to read the document.
- ▶ ensure that equivalents for dynamic content are updated when the dynamic content changes.
- ▶ until internet products allow users to control flickering, avoid causing the screen to flicker.
- ▶ use the clearest and simplest language appropriate for a site's content.

And if you use images and image maps (Priority 1)

- ▶ provide redundant text links for each active region of a server-side image map.
- ▶ provide client-side image maps instead of server-side image maps except where the regions cannot be defined with an available geometric shape.

And if you use tables (Priority 1)

- ▶ for data tables, identify row and column headers.
- ▶ for data tables that have two or more logical levels of row or column headers, use markup to associate data cells and header cells.

And if you use frames (Priority 1)

- ▶ title each frame to facilitate frame identification and navigation.

And if you use applets and scripts (Priority 1)

- ▶ ensure that pages are usable when scripts, applets, or other programmatic objects are turned off or not supported. If this is not possible, provide equivalent information on an alternative accessible page.

And if you use multimedia (Priority 1)

- ▶ until internet delivery products can automatically read aloud the text equivalent of a visual track, provide an auditory description of the important information of the visual track of a multimedia presentation.
- ▶ for any time-based multimedia presentation (e.g. a movie or animation), synchronise equivalent alternatives (e.g. captions or auditory descriptions of the visual track) with the presentation.

And if all else fails (Priority 1)

- ▶ if, after best efforts, you cannot create an accessible page, provide a link to an alternative page that uses W3C technologies, is accessible, has equivalent information (or functionality), and is updated as often as the less accessible (original) page.

Where do I get more information?

Refer to the *W3C Web Content Accessibility Guidelines* and accompanying *Techniques for Web Content Accessibility Guidelines 1.0*. The full checkpoint list including Priority 2 and 3 Guidelines is also available.

In addition to its World Wide Web Access, see the *Disability Discrimination Act Advisory Notes HREOC* published in December 1999.



DOFA's *Guidelines for Commonwealth Information in Electronic Formats* also include discussion of accessibility issues.

That's too much information—can you put it more simply?

A useful easy reference guide to some major issues is provided in the *W3C Web Access Initiative's Quick Tips for Accessible Websites*:

- ▶ Images and animations. Use the alt attribute to describe the function of each visual.
- ▶ Image maps. Use client-side MAP and text for hotspots.
- ▶ Multimedia. Provide captioning and transcripts of audio, and descriptions of video.
- ▶ Hypertext links. Use text that makes sense when read out of context. For example, avoid 'click here'.
- ▶ Page organisation. Use headings, lists, and consistent structure. Use a cascading style sheet for layout and style where possible.
- ▶ Graphs and charts. Summarise or use the longdesc attribute.
- ▶ Scripts, applets, and plug-ins. Provide alternative content in case active features are inaccessible or unsupported.
- ▶ Frames. Use NOFRAMES and meaningful titles.
- ▶ Tables. Make line by line reading sensible. Summarise.
- ▶ Check your work. Validate. Use tools, checklist, and guidelines at www.w3.org/TR/WAI-WEBCONTENT

How do I check if my pages are accessible?

The Bobby program (available free at www.cast.org) can give an automatic check. This should highlight major access problems. However, automated checking is not a full substitute for human judgment and human user experience in any thorough assessment of effective accessibility, and broader issues of 'useability'.

- ▶ In all cases, and as early and extensively as possible, you should invite and act on user feedback.
- ▶ Consider more formal testing of accessibility and useability using consumer test groups (research has indicated that effective tests can involve as few as five users).
- ▶ Consider using consultant or employee internet experts with disabilities during site design and testing.

Users who cannot see, or cannot easily read print (e.g. those suffering retinal pigmentosa, or RP), or cannot distinguish colours, or hear, can receive and exchange information through the internet as readily as other users if sites and services are designed to be accessible.

Frequently asked questions (FAQ)

Does accessibility mean I can't use innovative or attractive design?

No. There is obviously a role for attractive visual design in ensuring that sites reach and serve their intended audience. Many people (including some people with disabilities) receive some information more effectively through graphic forms than through words. Accessibility does mean that, as far as possible, users can choose how they get the information from your page.

Does accessibility mean I need to maintain several versions of my site?

Some Commonwealth sites appear to have effectively managed several accessibility issues (as well as long download times for graphic-heavy pages) by implementing text only equivalent sites. A smaller number have implemented the W3C preferred approach, with one accessible version (but different versions of particular elements or pages where necessary). There are several reasons to adopt the single accessible site approach:

- ▶ a single accessible version will benefit all users. Work on 'accessibility' issues can provide a simpler, clearer, better site. Also, parallel ('text') versions may not cover all your site's accessibility issues because:
 - a text only version may still be inaccessible (for example because of errors in using frames,); and
 - scripts to create a text version will not automatically render accessible versions of graphics, multimedia or formats such as Portable Document Format (PDF).

Is PDF accessible?

PDF does not, in itself, accord with accessibility guidelines. It is, however, widely used by the Commonwealth and other Australian governments. This is only acceptable if sites either:

- ▶ test each PDF file to ensure it converts effectively to accessible formats (text or HTML) and provide links to conversion options developed by Adobe Inc (see <http://access.adobe.com>) to address accessibility issues with this format; or
- ▶ provide accessible alternative versions directly on site (preferred).

PDF is, at least in its origins, essentially a graphical format, which presents access problems for people who cannot see and who are relying on screen reader software to convert text into speech or Braille.

The W3C Web Content Accessibility Guidelines recommend:

When inaccessible technologies (proprietary or not) must be used, equivalent accessible pages must be provided...Converting documents (from PDF, PostScript, RTF, etc.) to W3C markup languages (HTML, XML) does not always create an accessible document. Therefore, validate each page for accessibility and useability after the conversion process... If a page does not readily convert, either revise the page until its original representation converts appropriately or provide an HTML or plain text version.

The proprietors of PDF have recently published a White Paper on PDF accessibility which includes guidelines for PDF accessibility. These emphasise the need for providers of documents to check that their work converts effectively.



If document providers check their documents convert effectively, by converting them to accessible formats, then such text or HTML alternatives are little extra effort to put online alongside the 'authentic' PDF version. Consequently, users aren't required (from their viewpoint, 'penalised') to do the conversion and undergo additional effort, expense or delay, together with the uncertainty of whether conversion will in fact be effective (rather than jumbled text and junk symbols, as seen on converted PDF files from a number of Commonwealth sites).

Can I use frames?

Several Commonwealth Government sites use frames as a convenient way to navigate. An example is using side bar menus in a constant screen position while the user scrolls through document content in another frame.

However, not everyone uses or can use browsers which support frames. Frames can present particular barriers for screen readers—who, for example, may not be able to find their way out of the first frame encountered to view the rest of the site.

The *Web Content Accessibility Guidelines* does not disbar frames. They require that frames should not prevent navigation by users who cannot see the whole page or use frames, and that a 'no frames' option should be provided. Frames are, after all, intended to improve navigability and presentation, rather than to make it difficult or impossible.

The Guidelines provide detailed advice on techniques to ensure that frames do not disable accessibility. Many of the Commonwealth sites which use frames do not comply with these requirements.

Can I use video, pictures, music and sound bytes?

Yes, but ensure that you provide a text description of the picture, video or sound track, and provide transcript and/or captioning of dialogue wherever possible.

Can I use animation and moving elements?

Yes, but you must provide an accessible alternative. Shockwave, flash animation and moving text are not accessible to all users. Also consider why you need to use these formats on a Commonwealth site.

Fixing the whole site will take time—where do I start?

Sites must comply with the priority one guidelines as soon as possible, thereby complying with government policy. This should not prove as hard as it looks once a start is made.

The following suggested order of priority for achieving compliance with at least the Priority 1 guidelines is based on advice from a leading commentator on web page useability:

- ▶ home page;
- ▶ all new pages;
- ▶ any pages required for completing important transactions on line;
- ▶ highest traffic pages;
- ▶ pages particularly relevant to users with disabilities; and
- ▶ other pages.

Not everyone uses or can use browsers which support frames. Frames can present particular barriers for screen readers—who, for example, may not be able to find their way out of the first frame encountered to view the rest of the site.

Can you give some examples of better practice sites?

Several Commonwealth agencies have achieved significant progress in accessibility (although further accessibility or useability improvements may be possible). These include:

- ▶ the Australian Taxation Office at www.ato.gov.au;
- ▶ the Federal Court of Australia at www.fedcourt.gov.au; and
- ▶ the Office of Disability within the Department of Family and Community Services at www.facs.gov.au

Can you give examples of current problem areas?

Here are some problems identified in HREOC's December 1999 audit of Commonwealth sites, in addition to the problems with frames and PDF already discussed:

- ▶ a page providing important information on a major government initiative used Shockwave animation. It was invisible (black) to users without the Shockwave program. An alternative (text) version was prominent on the front page, but not accessed from all pages within the site. For example, no text informed users who came directly to these pages that Shockwave was needed to read this otherwise 'black page', or that a text alternative existed and how to find it.
- ▶ on one Commonwealth department's homepage tested, alternative text was missing for image map hot spot links and for several images serving as links, including the image link given to the Prime Ministers' home page.
- ▶ on one Commonwealth department home page the image link for the department's contact details had alternative text saying only 'image'. Many links on the same page had alternative text saying 'click to go'—but go where, was not specified.
- ▶ on one major agency site most pages passed automatic checking with the Bobby program, but on checking manually (as recommended by Bobby and by the World Wide Web Consortium Guidelines) for whether the alternative text gave sufficiently meaningful information, 'click here' was found as the alternative text given for numerous links. Click here for what?
- ▶ on another department's site the alternative text for the main menu map read 'picture'.
- ▶ a number of tested Commonwealth sites provided audio files but appear to have overlooked providing text equivalents.
- ▶ several pages tested had dynamic content (such as a number of different headlines popping up or running across the page in turn) which was not reflected, or only partially reflected, in the static alternative text provided.



- ▶ in some cases a text home page had been provided which passed Bobby testing for accessibility, but most pages linked from there on failed for the common reasons of lack of alternative text for images and image map hot spots. Accessibility means more than access to the home page.
- ▶ a number of sites had text only versions, but provided links to these only from the bottom of the front page. For users of screen readers and speech output, this may involve sitting through (and perhaps paying for) minutes of listening to, and being puzzled or annoyed by, a synthesised voice intoning statements such as 'clearpixel.gif', 'spacer.gif', 'transspacergif', and so on as the system reads the names of decorative image files.



Internet Delivery Decisions

A Government Program
Manager's Guide

© Commonwealth of Australia 2001

ISSN 1036-7632

ISBN: 0 642 44227 4

COPYRIGHT NOTICE

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth, available from AusInfo. Requests and inquiries concerning reproduction and rights should be addressed to:

The Manager,
Legislative Services,
AusInfo
GPO Box 1920
Canberra ACT 2601
or by email: Cwealthcopyright@dofa.gov.au

Internet Delivery Decisions A Government Program Manager's Guide

Government policy is to establish the Commonwealth as a leading-edge user of technology, with all appropriate government services internet-deliverable by 2001. Internet services are to complement—not replace—existing written, telephone, fax and counter services, as well as improving the quality, availability, responsiveness and consistency of those services. It is clear that government agencies' use of the internet will continue to evolve in response to government policy, the needs of the programs' clients, and in response to developments in information and communications technology.

In 1999, the Australian National Audit Office (ANAO) conducted a cross-portfolio review of how government agencies were implementing Commonwealth policy on internet use. The results were tabled in Parliament on 15 November 1999 in Audit Report No. 18 of 1999–2000 entitled *Electronic Service Delivery, Including Internet Use, by Federal Government Agencies*. The audit's conclusions included affirmation of the importance of promoting good practice in service delivery by the internet.

The ANAO subsequently decided to produce a Better Practice Guide to help program managers use the internet effectively when delivering government programs and services. Program managers were the target audience because Audit Report No.18 1999–2000, indicated they were less well catered for, in terms of guidance, than Information Technology managers.

The Guide identifies key questions and issues for managers when deciding whether, and how, to use the internet. Delivering government services by the internet does not of itself guarantee a better service than more conventional delivery. The Guide was also produced to assist managers already using the internet to improve their service delivery. By more adequately informing program managers about the questions they should ask and issues they should consider, this Guide aims to better equip those managers to make effective choices in conjunction with their IT managers rather than attempt to answer all the questions and resolve all the issues at any point in time in this constantly changing environment.

The Guide will also be used by the ANAO as a basis for establishing audit criteria in reviewing agency performance in internet service delivery. This was a major catalyst for our involvement in developing and coordinating its preparation.

Each part of the Guide has been prepared as a standalone document but can also be used as part of a complete set of guidance material. The information in this Guide can also be used to complement agency Chief Executive Officer's instructions and other internal guidance.

Several agencies have helped produce this Better Practice Guide and well deserve our grateful appreciation. Their cooperation and input have been most valuable. As well, we have relied on specialist private sector consultants for some components of the Guide. Thanks to all concerned.

Following its publication, the Better Practice Guide will also be placed on the Australian National Audit Office's Homepage—<http://www.anao.gov.au>



P.J. Barrett
Auditor-General
April 2001

Contents and Primary Contributors

| | |
|--|-----|
| Foreword by the Auditor-General | iii |
| Contents and Primary Contributors | v |
| Glossary of terms | vi |

| Component/No. | | Page |
|----------------------|--|-------------|
| 1 | How to Decide to Use the Internet to Deliver Government Programs and Services: Australian National Audit Office. | 1.1 |
| 2 | A Business Case and Cost-Benefit Analysis for Internet Use in Government: KLA Australia. | 2.1 |
| 3 | Designing and Maintaining Internet Sites for Government Programs: Department of Employment, Workplace Relations and Small Business. | 3.1 |
| 4 | Costing Internet Service Delivery in Government: KLA Australia. | 4.1 |
| 5 | Monitoring and Evaluating Internet-Delivered Government Programs and Services: UserInsite. | 5.1 |
| 6 | Internet Systems Security and Authentication for Government Programs: Defence Signals Directorate. National Office for the Information Economy. | 6.1 |
| 7 | Legal Considerations for Government Internet Service Delivery: Attorney-General's Department. | 7.1 |
| 8 | Privacy Issues, the Internet and the Government Manager: Office of the Federal Privacy Commission. | 8.1 |
| 9 | How to Make Government Sites More Accessible: Human Rights and Equal Opportunity Commission. | 9.1 |

Terms and terminology used in this Better Practice Guide concerning the internet and internet service delivery:

| | |
|--------------------------|--|
| ACSI 33 | Australian Communications—Electronic Security Instructions 33 maintained by the Defence Signals Directorate. |
| Biometric Authentication | 'electronic fingerprinting'—verifying that the person or entity is who they say they are. |
| Clickstream data | some information website hosts collect about individuals visiting a site will not in itself identify that individual. This is sometimes called 'clickstream data' and consists of information automatically collected and logged due to the nature of the communications protocols. |
| Client | this term can have one of two meanings in this publication. The term 'client' can denote a program (such as a web browser) which requests web pages from servers. A client may also mean a person or organisation accessing and receiving government services and information. |
| Cookie | a cookie is a short piece of data, not code, which is sent from a web server to a web browser, on the user's machine, when the browser visits the server's site. The cookie is stored on the user's machine as data, but it is not an executable program. Cookies can track individuals' activities on websites. Like clickstream data, cookies may not conform to the Privacy Act definition of personal information. Many net users consider cookies as intrusive. If a website uses cookies it is recommended that the Privacy Statement or Policy state that they are used and for what purpose. |
| Domain name | a name given to a host computer or site on the internet. |
| Download | the action of transferring information from one computer to another. Broadly speaking, websites <i>upload</i> information (make it available on the internet) where people can <i>download</i> it. |
| FAQ | Frequently Asked Questions. A common feature on websites, where the most common questions have been answered. |
| Firewall | a security buffer which tries to isolate and protect a network from external threats. |
| Frames | a specialised use of HTML, creating a series of windows ('frames') for navigating a site. |
| FTP | File Transfer Protocol. Determines how files are transferred. |
| Gateway | a system which allows two incompatible networks to communicate. |
| Host | a system or computer with permanent internet connection, or subservient computers. |
| HTML | HyperText Markup Language. |
| HTTP | HyperText Transfer Protocol (a protocol which looks for a 'web address'). |
| Internet Protocol | the standard coding which systems use when communicating on the internet. |

| | |
|------------------|--|
| Hyper text | (also, 'hyperlinks') a system which contains links (often as underlined, coloured text) which helps users navigate through available material online. |
| IT | Information Technology |
| Intranet | generally, a network behind a firewall; in terms of government ISD, the agency's own internal computer network. |
| ISD | Internet Service Delivery. |
| ISDN | Integrated Services Digital Network, commonly used for dedicated lines. |
| ISDRAS | Information Security Incident Detection, Reporting and Analysis Scheme. |
| ISP | Internet Service Provider. |
| LAN | Local Area Network. A collection of computers which can interact, such as within an agency, and often behind a firewall. |
| Megabyte | a measure of the quantity of data (a million bytes). Sizes include kilobyte (Kb), Megabyte (Mb), Gigabyte (Gb) and Terabyte (Tb), in increasing order of size. |
| Metadata | information which describes data; information contained 'invisibly' within internet items which flags their contents to search engines. |
| Modem | a device which converts digital signals into analog telephone transmissions (mod ulation) and decodes them (dem odulation). |
| NOIE | National Office for the Information Economy. |
| PDF | Portable Document Format. A proprietary Adobe format which can allow people to view a document even though they do not have the program which originally created it. |
| Portal | generally, an interface to another system or mainframe; also used to describe links between intranet and internet sources. Also, one of the Customer Focused Portals, forming part of the Commonwealth Government's initiative to improve accessibility to online resources. |
| Protocol | a set of communication rules defining how computers send information to each other. |
| PSM | Protective Services Manual maintained by the Protective Security Coordination Centre within the Attorney-General's Department. |
| Server | a program or computer that services other programs or computers. |
| Service provider | a company providing a connection to the internet (also, ISP). |
| TCP/IP | Transmission Control Protocol/Internet Protocol. A set of protocols that control data transfer between computers. |
| URL | Uniform Resource Locator. |
| WAP | Web Application Protocol—handheld or mobile devices with internet capability. |
| www | World Wide Web. |

