OFFICE OF THE

Auditor General
of British Columbia

Management of the Information Technology Portfolio in the Ministry of Attorney General

OFFICE OF THE
Auditor General
of British Columbia

LOCATION:
8 Bastion Square
Victoria, British Columbia
V8V 1X4

OFFICE HOURS:
Monday to Friday
8:30 a.m. – 4:30 p.m.

TELEPHONE:
250 387– 6803
Toll free through Enquiry BC at: 1 800 663–7867
In Vancouver dial 660–2421

FAX: **250 387–1230**

E–MAIL: **bcauditor@bcauditor.com**

WEBSITE:
This report and others are available at our Website, which also contains further information about the Office: http://bcauditor.com

REPRODUCING:

The Honourable Claude Richmond
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Sir:

I have the honour to transmit herewith to the Legislative Assembly of British Columbia my 2001/02 Report 5: Management of the Information Technology Portfolio in the Ministry of Attorney General.

Wayne Strelioff, CA
Auditor General

Victoria, British Columbia
February 2002

copy: Mr. E. George MacMinn, Q.C.
       Clerk of the Legislative Assembly

table of contents

– continued

table of contents continued

auditor general's comments

This, my fifth report to the Legislative Assembly for 2001/02, contains the results of my Office's audit of how well the Ministry of Attorney General manages its information technology portfolio.

Information technology (meaning the use of systems such as computers and telecommunications to store, retrieve and send information) offers all organizations unprecedented opportunity to improve performance, reduce costs, and enhance both the range and responsiveness of their service delivery. Over the years, government has increasingly come to depend on information technology systems to carry out its wide range of activities. However, management and delivery of these systems is challenging—because, in both the private sector and in the government environment, many such projects fail to meet time or budget requirements and few of the resulting systems are ultimately capable of doing all they were intended to do. Many projects started are never even completed.

If government is to achieve its objectives as cost-efficiently as possible, information technology systems must be managed well. One way of doing this is by using an integrated approach known as "portfolio management." The portfolio includes everything related to the organization's information technology investments. The costs, benefits and risks of all information systems—proposed, under development, and operational—are scrutinized regularly, with the goal being to understand and manage the risks involved while maximizing the strategic benefits of systems investments as a whole. With this approach, information technology is seen as an investment opportunity, not as an expense, and attention is focused on tangible benefits that align with the organization's strategic goals.

The purpose of our audit was twofold. First, we wanted to bring the Legislative Assembly up to date about significant issues related to the Province's management of information technology portfolios today. Second, we wanted to provide all government organizations with a range of tools for evaluating how well they are managing

their information technology systems. To meet both of these aims, we chose one ministry, Attorney General, on which to focus. This ministry is responsible for the administration of justice in British Columbia. To support its work, it uses many different information technology systems that are large, complex and crucial to the organization's effectiveness. We used the portfolio management model for assessing how well the Ministry of Attorney General is managing its systems.

We were pleased to find that the ministry's senior executives are directly involved in overseeing the development and use of information technology in the organization. However, we also noted areas where improvements could be made, and we provide a number of recommendations related to how the ministry could better assess the value of proposed changes to its portfolio of systems and better manage risks related to delivery of new systems.

I encourage all government organizations to review these recommendations, as well as the tools we describe, and to consider using them to evaluate the management of their own information technology systems.

My thanks to all those individuals who cooperated with and assisted my Office during the course of our work, especially staff from the Ministry of Attorney General.

Wayne K. Strelioff, CA
Auditor General

Victoria, British Columbia
February 2002

❖   ❖   ❖
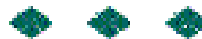
Review Team

Deputy Auditor General: Peter Gregory
Senior Principal: Endre Dolhai
Director: Ken Lane
Project Leader: Bill Gilhooly

❖   ❖   ❖
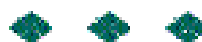
highlights
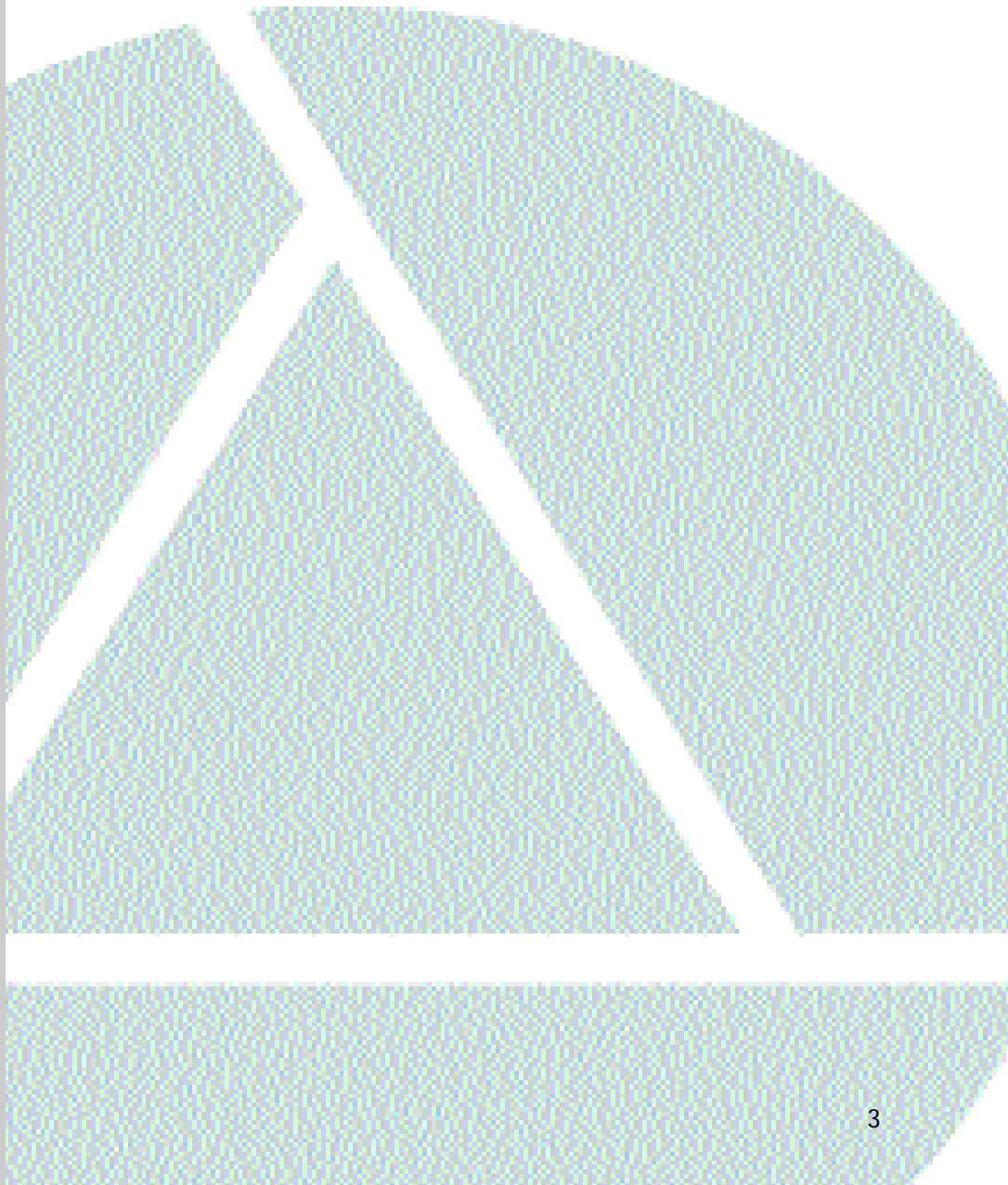
background

Information technology systems are essential for modern government, but hard to manage and deliver

Information technology is transforming all aspects of society and the economy, just as the steam engine, railroads, and electricity did in the past. Information technology's rapid pace of innovation is offering unprecedented opportunities for both government and commerce to improve performance, reduce costs, and enhance both the range and responsiveness of service delivery.

In order for information technology to help government improve, many challenges must be overcome. A disproportionate percentage of information technology projects, both public and private, fail to meet time or budget targets, fail to reach completion or, when completed, do not perform as they were meant to.

In the early stages of information technology, systems were built to automate manual processes; they did the same tasks as had been done manually (e.g., cheque processing), but did them more efficiently. Benefits were relatively simple to see and to measure. Developing such systems may have been technically difficult, but once their development was complete, they began delivering benefits.

Now, most information technology projects are designed to restructure work processes—to do things differently—or even to redefine the nature of the business—to do different things. Their expected benefits only materialize after existing business processes are re-engineered. Making such changes needs different skills and techniques from those used on the information technology project itself, and requires the involvement of many staff with a variety of responsibilities within the organization.

Information technology projects in government face additional obstacles. In the private sector, investment decisions about technology usually have a single agreed-on, measurable goal, such as return on investment. This is not the case in government organizations, where there are many stakeholders with differing and, sometimes, shifting goals and priorities.

Governments are also at a disadvantage in competing with the private sector to attract and keep the right mix and level of key staff to work on information technology projects. Mandatory standards and administrative policies further increase the complexities that ministries must consider in managing information technology.

Portfolio management offers an integrated approach to dealing with these problems

One response to these challenges which is gaining increasing acceptance is "portfolio management," an integrated approach to information systems. The "portfolio" includes everything related to deriving business benefit from information technology investments. The costs, benefits and risks of all information systems—proposed, under development, and operational—are scrutinized regularly, with the goal being to understand and manage the risks involved while maximizing the strategic benefits of systems investments as a whole.

The portfolio concept is grounded in the management principle that any significant investment requires careful stewardship to maximize its value and protect its integrity. This principle is well understood for traditional investment categories, such as real estate and equity investments, which are commonly managed as portfolios, allowing decision-makers to view their investments as a whole and to consider individual investments in context.

When all information technology systems and projects are included in a portfolio, the information technology "business" of the organization is understandable as a complete package. Systems and projects can be evaluated consistently, and management can more easily look for synergy among its information technology investments. Risks can be systematically considered: the risk/reward relationships of particular investments can be examined, and quantified to some degree, as can the overall risk profile of the portfolio.

Seeing information technology as an investment opportunity, not as an expense, focuses attention on tangible benefits that align with the organization's strategic goals. It enables an organization to select technology assets and projects that maximize benefits, and to favour the "must do" over the "nice to do."

Good portfolio management practice requires regular scrutiny of the portfolio. Once a year (often, as part of the annual budget cycle) is not enough. As circumstances

change, projects previously deferred can be reconsidered, or development projects found to be obsolete or too costly can be cancelled. Also, the portfolio approach borrows from financial management practice the compelling idea that even the best investments have a finite life: a good portfolio manager never acquires a new asset without thinking about the appropriate time to replace that asset with one that offers better value. This idea is even more important for information technology assets, which need periodic investments (e.g., software version upgrades) just to maintain their original value.

Portfolio management is being widely used today for information technology systems. It is at the heart of the Government of Canada's initiative to improve its information systems management. It is also being encouraged in the U.S. government as a best-practices approach. The State of Washington, which is seen as a leader in information technology management among U.S. states, has applied the portfolio concept, as have a number of well-known information technology consulting firms.

Audit Purpose and Scope

The purpose of this audit was to assess how well the Ministry of Attorney General managed its portfolio of information systems. This included examining how well the ministry evaluated the cost-effectiveness of the systems in its portfolio, and ensured that those systems align with and meet its needs. In the process of selecting the ministry, we first looked for ministries that have a significant number of major information systems—systems that are an essential part of delivering services of importance to the public and Legislative Assembly. We then selected ministries that appear to have in place the key organizational tools needed for managing an information technology portfolio. (Our purpose was to find a useful example so that other ministries and agencies could make use of our audit findings and apply them to their own circumstances.)

The ministry selected for detailed examination was the Ministry of Attorney General, which is responsible for the administration of justice in British Columbia (including operation of courts, prosecution of criminal offences, and provision of correctional services). It uses about 140 different information technology systems to support its work. Some are small and specialized and others (such as the CORNET system in the ministry's Corrections Branch) are large, complex and pivotal to operations. These systems are, in many cases, of critical importance to the ministry's effectiveness, because of

the particular significance of the information conveyed and contained in the justice system. The information in a land title, for instance, confers ownership and economic rights; the information in a court decision sets out whether an accused is jailed or goes free.

Our work focused on management practices in the ministry—in particular, those centred around the ministry's major information technology projects—during the 2000/2001 fiscal year. Thus, we examined the ministry before its functions were reorganized on June 5, 2001. Also, we looked mostly at systems that appear to be critical to the ministry's core business functions. We did not look at government-wide systems, as they are generally the result of management decisions made outside the ministry.

Our examination was performed in accordance with standards for assurance engagements recommended by the Canadian Institute of Chartered Accountants, and accordingly included such tests and procedures as we considered necessary in the circumstances.

We examined the ministry's capacity for governance, for decision-making, and for project delivery

Successful portfolio management in any organization requires three key elements:

- clear governance;
- informed, well thought out proposals for changes to the portfolio; and
- well-managed delivery of changes to the portfolio.

Clear governance: To successfully manage its portfolio, an organization must have a senior decision-making body that is able to oversee all significant information technology investments in the organization. This body (usually called a steering committee) is responsible for selecting the best information technology solutions to meet the organization's needs, and for overseeing successful delivery of these solutions.

In managing the portfolio, the steering committee must have help from information technology staff, project management staff, and project steering groups. It oversees delivery of individual projects, but does not take direct command of them. The latter is the job of the project (or program) sponsor, a senior executive who is responsible for seeing that the project and its associated benefits are successfully delivered.

Proposals for change: Making the right choices of portfolio additions that carry out new functions, or replace obsolete systems, lies at the heart of successful portfolio management. Invariably, there are more potential additions than there are resources with which to acquire them. Steering committees must decide not just whether proposals are worthwhile, but which are the *most* worthwhile, both on their own merits and when combined with the other parts of the portfolio.

For each proposal considered, portfolio managers must ask "how?" and "how much?" The "how" question is fundamental: how will this proposed system provide the benefit it is supposed to? Rare today is the information system that simply automates a manual process and can be plugged in to an organization without any other changes. Most systems require changes in human behaviour, skills or attitudes. Determining how these changes will be brought about is an essential part of any project proposal.

Answering the "how much" question requires quantifying (or at least describing in a consistent way) the benefits the system will provide and the costs—in dollars, in staff time, in disruption of other work—to provide them.

It is important to ensure that cost estimates recognize all the expenditures needed to deliver the benefit. This includes costs that may not be part of the project itself, but are necessary if it is to be successful (e.g., expenditures on user training), and maintenance costs throughout the life cycle of the system (e.g., for operating system upgrades). It is also important to consider non-financial costs. For example, will a worthwhile project monopolize an organization's scarce supply of project managers? Will it exhaust staff's ability and willingness to change the way they do business?

Delivery of changes: Developing a new or replacement information technology system is an out-of-the-ordinary event, one that requires skills and processes different from those used in day-to-day program delivery. It is, in fact, a project—an organized activity with a definite beginning and end, undertaken to create a unique product or service. There is a well-developed methodology, called project management, for carrying out such endeavours.

Two important aspects of project management are determining a project's scope (i.e., what it includes and what it will produce) and defining and managing its cost. A third aspect, risk management, involves managing the uncertainty

around future events and outcomes. (Experience has shown that unmanaged or unmitigated risks are one of the primary causes of project failure, especially in information technology projects.)

Risk can be thought of as a special kind of lens through which a portfolio is viewed, a lens that focuses attention on obstacles to success. The benefit of such focus is that, as a rule, what gets attention gets managed. It is important that risks not only be identified and analyzed before the decision is made to proceed with a project, but that they also be detected and managed during project delivery.

Overall Conclusion

We concluded that the ministry has an appropriate organizational structure for exercising senior management control over the information technology portfolio. This is an important foundation upon which to build an effective portfolio management system. However, to better manage its portfolio of information systems the ministry needs to improve its methods for assessing the value of proposed changes to its portfolio, align its information technology with its needs, and identify the significant risks of proposals and manage those risks during the life of the projects.

Key Findings

Governance: the ministry has set up an appropriate senior decision-making body

In our opinion, the ministry's Administration and Technology Committee—made up of senior executives and reporting to the ministry's executive committee— is an appropriate mechanism for overseeing information technology in the ministry. It also has an appropriate range of responsibilities, including developing and monitoring the ministry's technology plan, and reviewing and monitoring all significant projects related to technology and administrative change.

Decision-making: the ministry needs to improve the way it assesses the value of proposed changes to its portfolio

Three things are needed to assess the value of proposed information systems: good information on costs, good information on benefits, and effective, consistently-applied techniques for evaluating this information.

We found that the ministry has made several recent improvements in capturing dollar cost information. However, these had not yet been extended to capturing non-financial costs, nor to describing and, where possible, quantifying benefits. We also found that effective techniques of evaluation were inconsistently used. In particular, we noted that for many pre-existing major projects, analyses of the expected value of the projects were not clear or persuasive.

We recommend a basic but essential cultural change: recognizing that objective, information-based project evaluation is an essential precondition for success, and that investment decisions must focus on strategic payoffs for the ministry as a whole. (We also recommend improvements in technique, such as developing standard checklists of costs and benefits to be considered, and using evaluation aids such as the Balanced Scorecard.)

Project delivery: the ministry needs to improve its management of the risks related to delivering new systems

We found that, in general, insufficient attention is paid to risk at the inception of projects, and that monitoring and management of risk is ad hoc while projects are underway.

Finding appropriate techniques of risk management is not a problem: the ministry used them well on the Year 2000 project, and some ministry contractors are using them now. Again, we recommend that the prime focus for change be within the management culture. Specifically, the Administration and Technology Committee should recognize that risk management is one of its crucial roles, and should delegate administrative tasks whenever possible so it can focus its attention on risk questions.

The portfolio management maturity model provides a good guide for enhancing management of information technology

Getting better at portfolio management requires getting better at a whole set of techniques and attitudes at roughly the same time. For example, world-class portfolio evaluation tools are little use if the projects chosen cannot be delivered consistently on time and on budget. This idea—that improvement comes about through advances in the overall capability of an organization over time—has been formalized in the concept of portfolio management *maturity.*

The maturity metaphor originated with studies carried out for the U.S. Department of Defense on how to improve software development, to "help software organizations improve the maturity of their software processes…from ad hoc, chaotic processes to mature, disciplined…processes." The concept has since been extended to other areas of information technology, as well as to financial management and project management. Last year the U.S. General Accounting Office produced a maturity model for information technology investment management. We found it to be a good match for the portfolio concepts we outline in this report. We believe that the ministry, and other parts of government, would benefit from using the maturity model, as a guide to enhancing their management of information technology.

❖ ❖ ❖
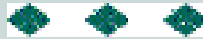
summary of recommendations

The ministry should maintain complete and organized information on the performance, value and prospects of each information technology system in its portfolio. (page 35)

The ministry should adopt standard industry practices for determining benefits and costs and weighing the merits of competing projects, and should use those methods consistently. (page 36)

The Administration and Technology Committee should ensure that the projects it approves clearly demonstrate net benefits that contribute directly to the achievement of the ministry's strategic goals. (page 36)

The ministry should carry out post-implementation reviews of all its significant information technology projects upon completion or termination of a project, and use the findings to improve its processes for managing its information technology portfolio. (page 36)

The ministry should develop formal guidance on risk management and reporting. (page 40)

The Administration and Technology Committee should make risk management one of its critical responsibilities, and delegate administrative duties whenever possible so that it has more time for risk management. (page 40)

The ministry should examine its information management using a portfolio maturity model such as that developed by the U.S. General Accounting Office. (page 40)
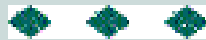
detailed report
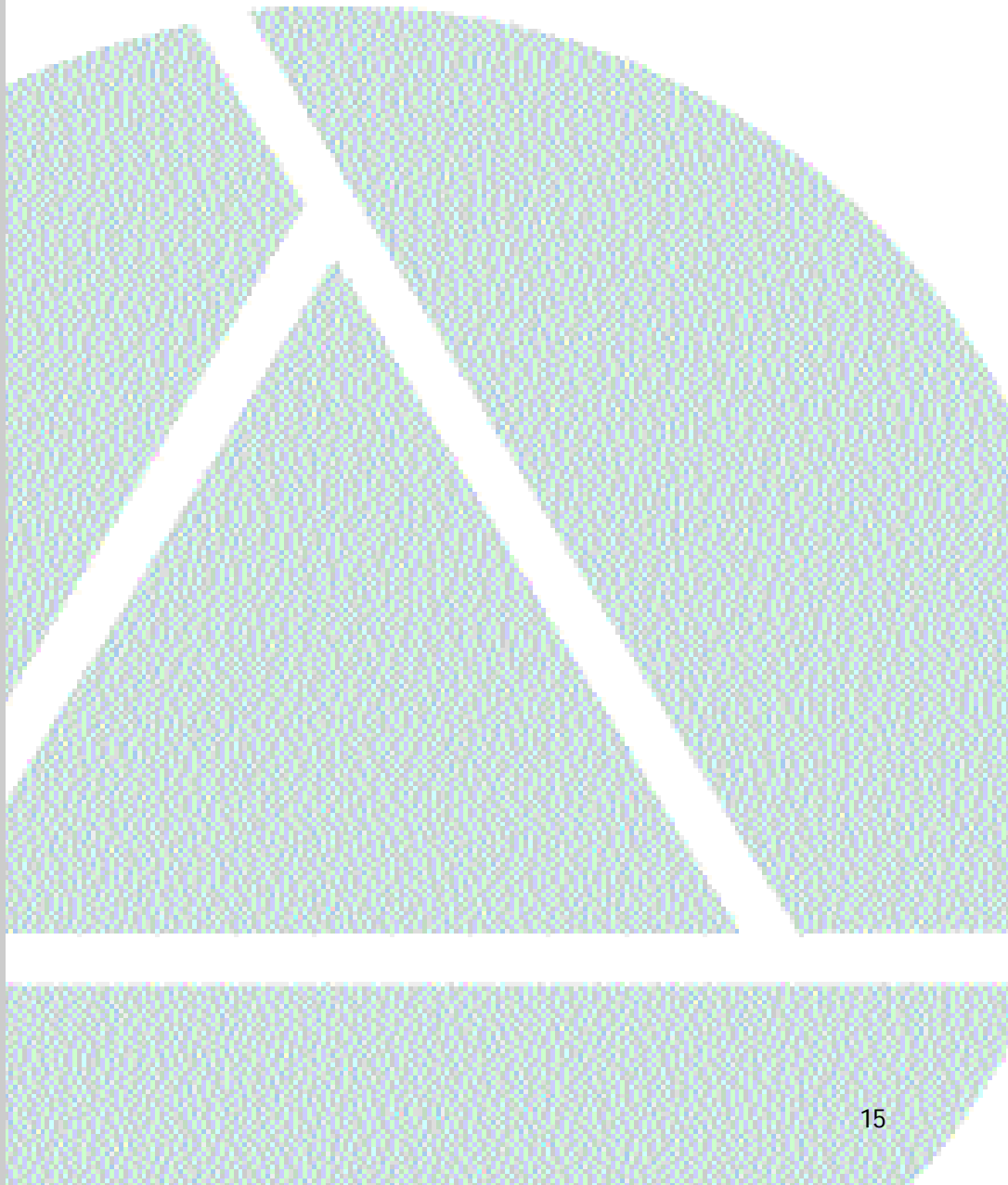
background

Obtaining value for money from information technology investments is difficult, especially for governments

Both the private and public sectors have become increasingly dependent on information systems to perform their most important activities. That dependence can be a problem, because the development of these systems often poses a number of difficulties. Some systems projects fail to meet time or budget requirements. Other systems, even when completed, do not perform as they were meant to.

To understand why is it so difficult to obtain value from information technology projects, it is useful to think of such projects as having evolved through several stages. An early stage was the automation of work—systems developed during this period did the same tasks as had been done manually (e.g., cheque processing), but did them more efficiently. Expected benefits were relatively simple to see and to measure. Developing such systems may have been technically difficult, but once they were up and running, they began delivering benefits.

Now, most information technology projects are designed to restructure work processes—to do things differently—or even to redefine the nature of the business—to do different things. Such projects are often as technically difficult as first-stage projects or more so. Furthermore, completion of an information technology project per se is now just an intermediate step. The expected benefits only materialize after existing business processes are re-engineered. Such changes need different skills and techniques from those used on the information technology project itself, and require the involvement of many staff with a variety of responsibilities within the organization.

Defining the goals for information technology projects is also harder than for early-stage projects. "Processing payroll more efficiently" is clear and measurable. "Improving management decisions through an executive information system" may provide more benefit to the organization than a new payroll system, but it is no easy task to define the benefit, decide whether it is worth the cost of achieving, and make sure it really is achieved.

In all of this, governments face particular challenges. For one, they do not operate with the same motives and purposes as the private sector, where investment decisions about technology often have a common denominator—namely, a bottom line, or return on investment. The disparate, even conflicting, goals and priorities assigned to government organizations make decisions about information technology investments difficult. Goals can even shift suddenly, with a change of government or with the introduction of new policies or programs.

Governments may also have disadvantages in competing with the private sector to attract and keep the right mix and level of key staff to work on information technology projects. Although some of these resources can be contracted from the private sector, it is important that a government still have its own core of people who have not only the technological skills needed to oversee projects, but also knowledge of the ministry's or agency's business.

As well, government entities are more likely than their private sector counterparts to have to conform to mandatory standards or policies regarding information technology. For example, ministries in British Columbia are expected to comply with government technology standards for hardware and software, follow specified procurement practices, and use specified accounting methods for capital amortization.

The purpose of such government-wide requirements is to ensure that government policies are delivered and administered consistently, with economy and efficiency. At the same time, however, such requirements can increase the cost and difficulty of ministry service delivery. For example, in the Ministry of Attorney General we noted that central requirements have resulted in:

■ significant time spent by the ministry's senior information technology steering committee working out the implications of new government capital amortization policies;

■ lengthening of the approval process for projects, creating slippage in schedules (often with an associated budgetary impact, especially if funding lapses); and

■ differences between the projects that the ministry may consider a priority and the projects that receive central agency approval for funding.

An American perspective on the difficulty of successfully delivering information technology projects in government is presented in the sidebar. We believe it summarizes the situation in British Columbia well.

Information Technology Risks Inherent in the Public Sector Environment

IT [Information Technology] innovation is risky business in every organization. Organizations of all kinds abandon IT projects because they fail to accomplish the objectives they were intended to meet. In both the public and private sectors, IT innovation is limited by several common risk factors. Government seems to have even more trouble than the private sector in successfully applying new technology. The public policy choices and public management processes that are part of government make it an especially difficult environment for IT managers. This environment adds several risks that are unique to the public sector. These layers of complexity present a daunting challenge to public managers who are responsible for choosing, funding, and building IT innovations.

Risks inherent in the public sector environment:

Extreme risk aversion

Government's business is public business. This means that most new ideas have to be implemented in full public view. An innovation-gone-wrong risks not only dollars, but the credibility of an agency and its leadership with legislators, executive officials, and the public. It's not surprising that government tends to rely on the "tried and true."

Divided authority over decisions

Executive agency managers do not have a clear line of authority over agency operations. Their decisions are circumscribed by existing law, the limits of current appropriations, a civil service system, other political constraints, and a variety of procedures mandated by both legislatures and the courts. These restrictions do not blend well with the complexities of managing a multi-million dollar IT project in a rapidly changing technical environment.

Multiple stakeholders

Government programs are characterized by a multiplicity of stakeholders who often have competing goals. Customers, constituents, taxpayers, service providers, elected officials, professional staff, and others all have some stake in most programs. Understanding how different choices may affect each stakeholder group helps to prevent unexpected problems.

One year budgets

Since most government budgets are handled on an annual cycle, uncertainty about the size and availability of future resources weakens the ability of government agencies to adopt new IT innovations successfully.

Highly regulated procurement

Most decisions to adopt emerging technologies are made through the traditional competitive bidding process, a one-shot technique that is ill suited to the experimentation and learning that should appropriately accompany such large investments. While the goals of competitive procurement are goals of integrity and fairness, the processes are often a source of problems and delays, especially when agencies write requests for proposals (RFPs) that depend on the limited information they have been able to gain from inadequate experience and research.

Many links between programs and organizations

Few government programs stand entirely on their own. Most are connected in some way to other programs in the same or other agencies, or with non-governmental entities. Sometimes the connections are explicit and formal. Often they are informal or unintended. Changing one program often means that some other program will be affected.

Source: *Making Smart IT Choices,* 1998, copyright, Center for Technology in Government, State University of New York at Albany, Albany, NY
        <http://www.ctg.albany.edu/resources/smartin.html>

Portfolio management is a way of focusing information technology efforts on achieving strategic goals

Portfolio management is an integrated approach to managing information systems investments. The portfolio concept is grounded in the management principle that any significant investment requires careful stewardship to maximize its value and protect its integrity. This principle is well understood for traditional investment categories, such as real estate and equity investments, which are commonly managed as portfolios. These portfolios allow decision-makers to view their investments as a whole, and to consider individual investments in context.

In information technology, a "portfolio" includes everything related to deriving business benefit from information technology expenditures. The costs, benefits and risks of all information systems—proposed, under development and operational—are scrutinized regularly, with the goal being to minimize risks while maximizing the return on systems investments.

Portfolio management is being encouraged as a best-practices approach to information systems management by the U.S. General Accounting Office and by other U.S. federal agencies such as the Office of Management and Budget. It is also at the heart of the Treasury Board of Canada's initiative to improve information systems management. And the State of Washington, which is seen as a leader in information technology management, has adopted the portfolio concept, as have a number of well-known information technology consulting firms.

The portfolio management approach increases:

- **Common understanding:** Senior managers, even without an information technology background, often have a good understanding of portfolio concepts from financial management, allowing information technology managers to "speak their language."

- **Coherence:** Because all information technology systems and projects are included in the portfolio, the information technology "business" of the organization is understandable as a complete package. Systems and projects are evaluated equally, and management can more easily look for consistency and synergy among its information technology investments.

- **Attention to payoffs:** Seeing information technology as an investment, not as an expense, focuses attention on the bottom line of each investment—namely, the tangible

benefits that align with the organization's strategic goals. This then enables the organization to select technology assets and projects that maximize benefits and favour the "must do" over the "nice to do."

- **Attention to risks:** With this approach, risks are systematically evaluated. For example, the risk/reward relationships of particular investments can be examined, as can the overall risk profile of the portfolio.

- **Responsiveness to changing conditions:** With this approach, evaluation of information technology assets happens consistently, systematically and frequently. Good portfolio management requires regular scrutiny of the portfolio. Once a year is not enough. As circumstances change, projects that may have been previously deferred can be reconsidered, or development projects found to be obsolete or ineffective can be cancelled.

- **Attention to life cycle:** The financial portfolio approach includes the notion that even the best investments have a finite life. Thus, a good portfolio manager never acquires a new asset without thinking about the appropriate time to replace the asset with one that offers better value. This idea is even more important for information technology assets, which need periodic investments (e.g. software version upgrades) just to maintain their original value.

Successfully managing an information technology portfolio requires a long-term perspective. Even though long-term success is the ultimate goal, portfolio managers must move forward one step at a time, evaluating success at each stage before taking the next step.

The ministry has a significant information technology portfolio to support its work

In Canada, provincial governments are responsible for the administration of justice, which includes operation of courts, prosecution of criminal offences, provision of correctional services, provision of law enforcement, and appointment of Provincial Court judges. They are also responsible for most areas of civil law.

In British Columbia, the Ministry of Attorney General carries out the administration and delivery of these justice services, spending over $1 billion to do so in 2000/2001. Its main branches, and the services they provided that year, were as follows:

- Community Justice—consumer services, crime prevention, victim assistance

- Corrections—adult custody (youth custody is managed by the Ministry of Children and Families), community corrections, family justice
- Court Services—court administration, liaison with judiciary, sheriff services
- Criminal Justice—Crown Counsel
- Land Title
- Legal Services—barrister and solicitor services to other ministries
- Liquor Control and Licensing
- Public Safety and Regulatory—criminal records review, film classification, gaming investigation, police service contracts, emergency programs, licensing of security guards and private investigators

As well, the ministry provides support to a number of specialized agencies, boards and commissions, such as the B.C. Human Rights Commission, the B.C. Board of Parole, and the Public Guardian and Trustee of British Columbia.

The Ministry of Attorney General has made use of information technology to improve the efficiency of its everyday operations (for example, in adopting information systems to manage its correctional facilities and maintain security within them). However, it has also come to rely on information technology in a much more fundamental way because of the particular significance of the information conveyed and contained in the justice system. The information in a land title, for instance, confers ownership and economic rights; the information in a court decision determines whether an accused is jailed or goes free. And such vital information does not reside solely in the ministry, but moves among a number of important groups, including the judiciary, the police, and the federal government (see Exhibit 1).

Therefore, in the case of the Ministry of Attorney General, the right information in the right format in the right hands is more than just good administrative practice: it is vital to the ministry's functioning. This makes the ministry's work in developing and maintaining information technology systems highly complex and demanding, both technically and in terms of meeting governance and accountability obligations.

In 2000/2001, the ministry budgeted $23 million a year to operate its information systems, and $12 million for information technology capital expenditures, and employed about 80 people in its Information Technology Services Division, along with

Exhibit 1

Ministry of Attorney General Major Business Areas and Information Flows
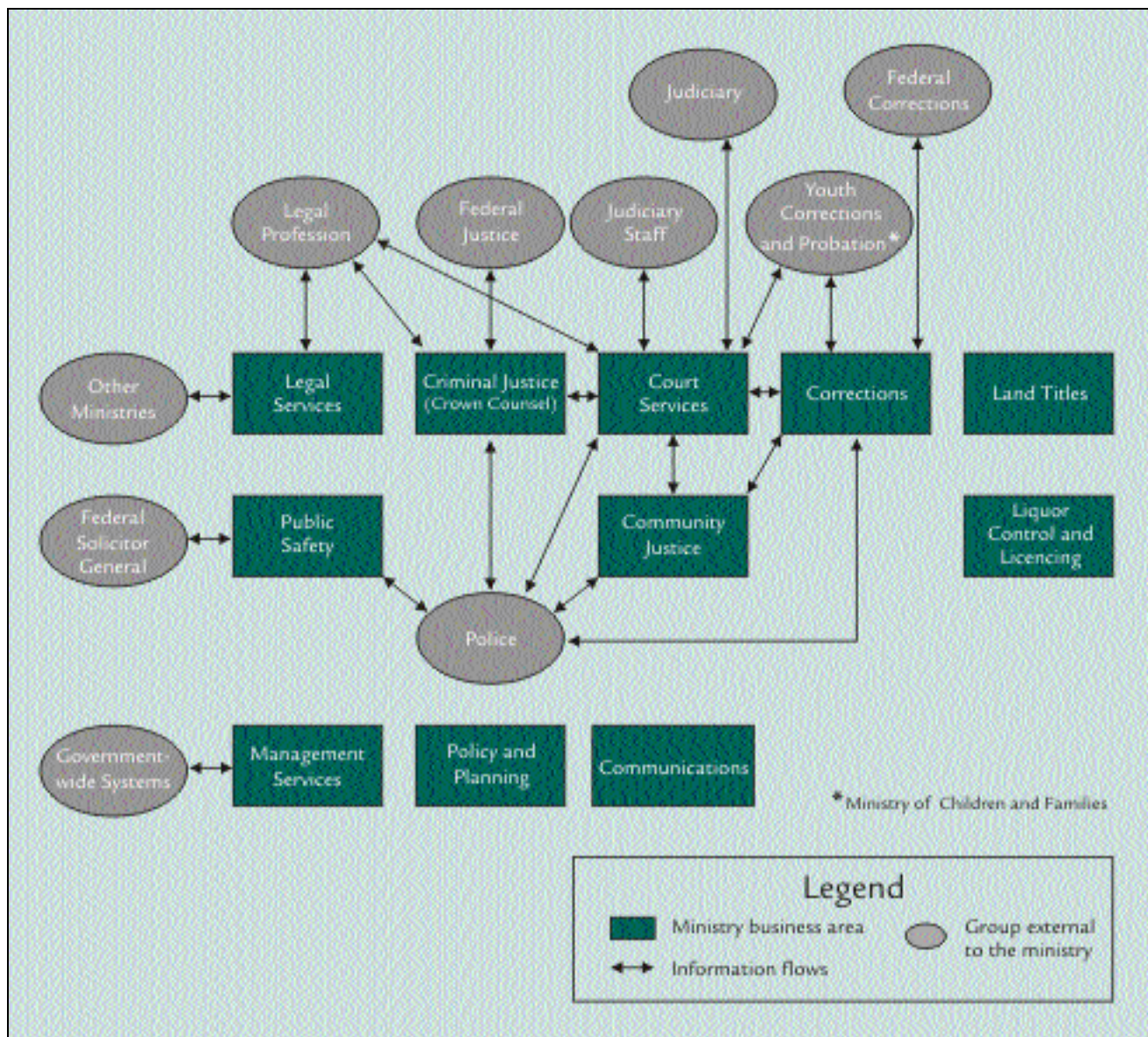
about 45 others who were directly involved in technology delivery but not in the division. A number of contractors are also engaged to provide information technology related services. The division reports to the Assistant Deputy Minister, Management Services.

In total, about 140 different information technology systems are being used in the ministry: some small and specialized, and others (such as the CORNET system in Corrections Branch) large, complex and key to the operations of the branch. Replacement or upgrading of many of these systems is either underway or being considered. Since good portfolio management is most important during such changes, we chose to focus our attention on the most significant systems currently undergoing change. We based our choice on:

■ the importance of the system to the ministry's core mandate;

■ the system's size (in terms of cost, personnel, number of locations, etc.); and

■ the system's complexity (in terms of scope, variety of users and stakeholders, etc.)

We ended up with a selection of 13 major systems (summarized in Exhibit 2.) At the time of our audit fieldwork, some of these were in their initial planning stages, some were under development, and four had been completed within the last two years. As well, in Appendix A we describe in more detail the JUSTIN project, because of its importance, its links to other major projects, and the way it illustrates the ministry's increasing skill in managing large information technology projects.

There are three key elements to successful portfolio management

Successful portfolio management in any organization requires:

■ clear governance and accountability;

■ informed, well thought out proposals for changes to the portfolio; and

■ well-managed delivery of new systems being added to the portfolio.

Clear governance and accountability

An organization must have a senior decision-making body that is able to oversee all material information technology investments in the organization. The main job of the decision-making body (often called a steering committee) is to continually adjust the portfolio. The goal is to optimize benefits to the organization by (1) selecting the best information technology solutions to meet the organization's needs, and (2) overseeing the successful delivery of these solutions.

Exhibit 2

Major Information Technology Systems Reviewed in the Audit

Name	Description	Project phase at beginning of year 2001	Major users
Integrated Justice Projects			
JUSTIN (JUSTice INformation System)	Tracks all criminal cases, linking police, court administrators, Crown counsel and others	Implementation	All parts of justice system
EJSP (Electronic Justice Services Project)	Will be similar to JUSTIN, but for civil cases	Planning	Lawyers, court administrators, judges
222 Main Vancouver Jail Project	Manages the remand centre/lock-up at 222 Main Street in Vancouver	In use	Police, Corrections Branch staff
CORNET (CORrection NETwork)	Tracks all aspects of prisoners in custody	In use	Corrections Branch staff, Ministry for Children and Families staff
Branch- or Agency-Specific Projects			
Electronic Filing System	Will allow electronic filing of land title documents	Planning	Lawyers, Land Title Branch staff
Aboriginal Law Research System	Supports treaty negotiations and land claims lawsuits	Initiation	Legal Services Branch staff, researchers
Project to replace COMET financial and trust accounting system	Will support the work of the Public Guardian and Trustee	Under development	Public Guardian and Trustee staff
Accounts Receivable and Collections system	Manages accounts receivable, and their collection, in courthouses	Initiation	Court Services Branch staff, Insurance Corporation of B.C., Government Agents
Liquor Control and Licensing Branch Systems Review	Will replace the existing licensing production system, and develop a compliance and enforcement system (this project results from a recent review of liquor licensing in BC)	Planning	Liquor Control and Licensing Branch staff
Public Safety and Regulatory Branch Combined Operational Systems	Will provide new operational support for Film Classification, Gaming Audit and Investigation Office, and Private Investigators and Security licensing offices	Planning	Public Safety and Regulatory Branch staff
Infrastructure or Other Ministry-Wide Projects			
Enterprise Data Warehouse	Will collect and analyze management information ministry-wide	Under development	Ministry executive, analysts
Leasing project	Upgrades and standardizes the ministry's information technology hardware	In use	All ministry staff
Year 2000 Project	Upgraded systems that, without modification, might not correctly have processed dates in the year 2000	Completed	All ministry staff

Source: Compiled by the Office of the Auditor General of British Columbia

To be effective, a steering committee must consist of senior executives and must itself report at a senior level. It must also have oversight over all the information technology activities of the organization.

In managing the portfolio, a steering committee must have help from information technology staff, project management staff, and project steering groups. It oversees delivery of individual projects, but does not take direct command of them. The latter is the job of a project (or program) sponsor, a senior executive who is responsible for seeing that the project and its associated benefits are successfully delivered.

Informed, well thought out proposals for changes to the portfolio

Before it can decide what to improve, an organization must know what it has in its portfolio. At the very least, it should know the name, location, ownership and brief technical specifications of each system. It should then add qualitative information that will help guide decisions about improving the portfolio—information that answers such questions as: How cost-effective is the system and how much longer will it continue to be so? Is it running out of capacity? Are its users satisfied?

Deciding what to improve also requires information about what is technically possible and desirable. In the information technology industry, rapid and disruptive change is the norm. The marketplace is constantly offering new ways or cheaper ways of doing things. An organization's managers must be constantly watching for technologies that will help them deliver their programs in a more cost-effective way (while avoiding dead-end solutions with short lives and so-called "bleeding-edge" solutions that offer more risk than reward to early adopters). Doing this job requires both knowing what technological opportunities are available and, more importantly, knowing whether they are adaptable to the specific needs of the organization.

Improvement to an information technology portfolio usually comes about by adding systems to carry out new functions or replace obsolete systems. Choosing these additions well lies at the heart of successful portfolio management. It is not an easy task because, invariably, there are more potential additions than there are resources with which to acquire them. The problem becomes not just deciding whether proposals are worthwhile, but deciding which are the most worthwhile. Deciding how to allocate the capital funds and other scarce resources available for acquiring new or replacement systems is a three-part process that involves:

- gathering information on benefits;
- gathering information on costs; and
- applying analytical tools to determine which proposals offer the best net value to the organization.

Benefits can take many forms: a solution to an existing problem; the necessary support for future business process improvement; or a way of meeting new statutory requirements. No proposed benefit is worthwhile, however, if it does not align with an organization's strategic goals. Projects that have good alignment increase the organization's ability to carry out its mission. They directly or indirectly support major strategies, conform to major policies, and focus on the organization's key missions, not on secondary activities. As well, they fit with other projects to form a portfolio—an optimized blended package of results that benefit the organization as a whole.

Rare today is the information system that simply automates a manual process, and can be plugged in to an organization without any other changes. Most new or enhanced systems require changes in human behaviour, skills or attitudes. Determining how these changes will be brought about is an essential part of any project proposal. For example, if an executive information system is being proposed, the portfolio manager must assess what steps are being taken to ensure that executives need and want the information it will provide, and whether they will use the information to make better decisions.

Benefits can be under-valued or over-valued if they are vaguely described. Consider the difficulty of evaluating systems that promise to "make [a process] easier," "provide better access to [specific information]," "create a strategic advantage," or "create a paperless environment." Without more concretely-defined benefits, decision-makers are at increased risk of approving projects that do not turn out to be worthwhile.

One way to deal with vagueness is to require the use of more precise language that allows the possibility of measurement. The mnemonic "MEDIC" is a reminder that words such as "better" or "enhanced" should be replaced by:

- **Maintained** (e.g., a level of service maintained),
- **Eliminated** (e.g., a function eliminated),
- **Decreased** (e.g., turnaround time decreased),
- **Increased** (e.g., revenue increased), or
- **Created** (e.g., a specific capability, one that contributes to strategic goals, is created).

Another way to deal with vaguely defined benefit proposals is to determine whether they are intermediate results that could in turn lead to desired outcomes. A formal way of doing this is to develop logic models that link inputs and processes with outputs and eventually desired outcomes. A less formal technique is to ask the question "so what?" whenever a vague benefit is described, and to continue doing so for each answer until linkages are clear from the proposed project right down to the real—and measurable—benefits.

Working out all the steps that are needed to deliver a benefit checks the completeness of a proposal and highlights places where costs will be incurred. Working out the steps between conceiving a project and realizing benefits from it is also essential for good risk management, which we discuss in the next section.

It is important to ensure that the estimated costs of a proposal are complete and include all those needed to realize the benefit, as well as those that will be incurred into the future. Cost tallies should include costs that may not be part of the project itself, but are necessary if the project is to be implemented successfully (e.g., expenditures on user training). They should also include maintenance costs throughout the life cycle of the system, such as operating system upgrades and software maintenance.

To estimate financial costs, methods such as life-cycle costing and total cost of ownership are useful. However, non-financial costs should be considered too. For example, will a worthwhile project monopolize a ministry's scarce supply of project managers? Will it exhaust staff's ability and willingness to change the way they do business? These costs have the potential to be as draining on an organization as those that deplete all the funds available for the project.

Effective methods for evaluating competing proposals for portfolio additions or changes focus on strategic benefits and weigh financial and non-financial costs. They also ensure that proposals are considered not in isolation, but as they affect the total portfolio. A number of good evaluation methods are available. Examples include the Balanced Scorecard, Information Economics, and the U.S. federal government standard model (which is based on Information Economics). Most use a scoring procedure that assigns numerical values to different categories of benefits and costs. All compare financial costs and benefits using discounted cash flow or other net present value calculations, which require the evaluator to have a realistic sense of how long the system being analyzed will continue to deliver value.

Mandatory projects (those required by law or policy) do not require much examination, since they must be carried out. Nevertheless, portfolio managers should still plan and manage these projects to ensure they are delivered as economically and efficiently as possible.

Not all project proposals should be evaluated in the same way. Projects that expand or enhance infrastructure, for example, should not be directly compared to service delivery projects. Doing so can result in infrastructure projects being neglected (because they rarely show quick payoffs when viewed in isolation) rather than being considered in light of the future opportunities they open up for the organization. However, it is also important to ensure that infrastructure enhancements fit within a well thought out technical architecture that is suited to the organization's mission and culture. Good practice in evaluating infrastructure projects is to first decide what percentage of resource investment should be allocated to infrastructure and what to projects that directly deliver service. Such an allocation is difficult to make, but strategically important. The projects in each category should then be evaluated against each other to determine how best to invest the available infrastructure funds.

Well-managed delivery of new systems being added to the portfolio

Adopting a new information technology system is an out-of-the-ordinary event for most organizations, one that requires skills and processes different from those used in program delivery. Project management is the discipline that has been developed for managing these events (see sidebar, p. 37).

Good project management is important for any kind of "one-off" activity, such as a building project or office renovation. And it is critical for information technology projects which, by their very nature, have a high risk of failure. This risk has two main sources, both alluded to above. The first is that technology is changing so rapidly that systems may never become fully productive and well used before they become obsolete. Second, even with a well-established technology, the process of fitting it to a particular organization—its processes, its culture, its technology platform—can be difficult.

The rest of this section of our report is devoted to reporting how well the Ministry of Attorney General met these three key requirements of portfolio management.

❖ ❖ ❖
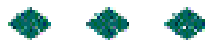
findings and conclusions

The ministry has an appropriate senior decision-making body

The ministry has a steering committee for information technology projects called the Administration and Technology Committee (ATC). In our opinion, the ATC is an appropriate mechanism for overseeing information technology in the ministry. It is made up of senior executives and reports to the ministry's executive committee. All branches are represented on it. The ATC also has an appropriate range of responsibilities: its key functions are to manage the deployment of technology and applications throughout the ministry, decide which information technology projects will be funded, and monitor all significant projects related to technology or business re-engineering. Exhibit 3 describes the ATC's mandate in more detail.

The ATC was established in the spring of 1998, replacing the Information Technology Steering Committee. Like its predecessor, the ATC has continuously improved its methods of work. For example, in response to changes in government's methods of amortizing capital investments, the committee now regularly receives and reviews information on the amortization implications of projects in its portfolio. As well, the ATC recently set up a technical sub-committee to aid it in its work. We believe this is a worthwhile improvement, one that should allow the senior committee to focus more of its attention on strategic issues, ensuring proposals are treated more consistently and project progress is better tracked. The ATC has also made good progress in ensuring that all relevant projects pass under its scrutiny.

One area of ambiguity requiring clarification, however, is the relationship between the committee and project steering committees which have members from outside the ministry. For example, the steering committee for the Electronic Justice Services Project (EJSP) includes representatives of the judiciary, and the electronic filing of land titles steering committee has representatives of the legal profession. The issue not clearly addressed is whether these project steering committees can set priorities, standards and spending directions for their projects that are at variance with the ministry's overall priorities, standards and directions. We recognize that this is an area where hard-and-fast rules may be problematic, but suggest that the ministry define more clearly the governance relationship between such steering committees and the ATC.

Exhibit 3

Excerpts From the Terms of Reference of the Administration and Technology Committee, B.C. Ministry of Attorney General

Mandate

[M]anage and guide the deployment of technology and applications throughout the Ministry and to periodically approve revisions to the Ministry's high level Information Resource Management Plan (IRMP). The Committee is also tasked with reviewing, monitoring and approving plans for significant administrative change and business reengineering and associated feasibility studies.

Objectives

[D]evelop and monitor a technology/information plan and process to facilitate the efficient and effective use of technology and the opportunities for business reengineering. In order to achieve this objective, the Committee will:

- [R]eview and approve updates to the Ministry's IRMP and associated Master Project Plan.

- [A]nnually establish the list of projects to be corporately funded from the Committee's development fund and, thereafter, to monitor progress and outcomes of each.

- Review and monitor all significant and crossbranch projects related to technology and administrative change.

- Review and monitor all significant business reengineering projects.

- Provide a forum to share information and foster new and innovative approaches to Information Technology/Information Management … and business reengineering in the Ministry.

Project Control

Prior to initiation, each information technology/IM or business reengineering project in excess of $100,000 or with crossbranch implications must have an associated Project Initiation Document (PID) completed and tabled at the Administration and Technology Committee.…A PID outlines the overall intent and scope of a project as well as estimating both internal and external resource requirements. These projects will include administrative reforms which are enabled by technology investments.

Source: "Terms of Reference, Administration and Technology Committee", April 28, 1998
(attachment to minutes of May 1999 ATC meeting)

We were also disappointed to find that one central government requirement with potential for encouraging good portfolio management has not been effectively applied. That is the requirement for ministries to periodically produce strategic information technology plans. Doing so would allow a ministry to think about its information technology in a more coherent and strategic way, and to contribute to development of a similarly coherent government-wide strategy. We concluded that the ministry's most recent (2000) such plan does not build upon and relate to the issues on which the ministry has actually been focusing its efforts. In other words, plan and activity are not aligned.

The ministry needs to improve its assessment of the value of changes to its portfolio

The ministry has a working knowledge of the systems currently in its portfolio

One prerequisite for managing a portfolio of assets is having an up-to-date description of those assets: their current value, their condition, and their expected value in the future. We were able to find reasonably current information about most of the ministry's information technology systems from two main sources:

- one-off inventories of systems at a point in time, produced for particular purposes; and

- analyses of the condition and value of current systems being considered for change or replacement, prepared as part of the due diligence for new project proposals.

An example of the first type of information is the system inventory prepared as a part of the ministry's successful effort to address anticipated Year 2000 problems. However, this inventory has not since been kept up to date. Nor has a similar inventory prepared for the ministry's 1994 Information Resource Management Plan.

An example of the second type of information is the 55–page "Current Situation Analysis Report" on the systems used by the Gaming Audit and Investigation Office, prepared in 1999 as part of the due diligence that eventually led to the decision to develop a combined system to meet the needs of the Film Classification, Gaming Audit and Investigation, and Private Investigators and Security licensing offices.

However, this system information is scattered throughout a large number of documents and files, many of which are not being maintained on an ongoing basis. In our opinion, such basic management information should be collected consistently, gathered in one place, and kept up-to-date—in other words, treated like a real portfolio. Since the ATC is the prime user of such portfolio information, we think it would be appropriate for the committee to take responsibility for the collection and maintenance of that information.

The ministry obtains sufficient information on opportunities for improving its portfolio

A critical fact about information technology is its rapid change. Hardware constantly drops in cost and increases in performance; new software and development tools stream

onto the market. We expected that the ministry would have an organized way of keeping track of these changes and of finding opportunities for using information technology to improve the organization's efficiency and effectiveness.

What we found was that, although the ministry does not have formal processes for searching out useful innovations, in practice it has enough informal ways of achieving that end, through the activities of operational branches, information technology staff, and information technology contractors.

Operational branches keep an eye on innovative ideas being tried in other jurisdictions, and watch for technological developments that are sufficiently mature and relatively low risk to be beneficial. Land Titles Branch did this in its examination of the use of electronic signatures. The branch researched various approaches taken in other jurisdictions to provide such signatures, and worked in cooperation with two other British Columbia government projects that were considering the idea too.

The ministry's information technology specialists are also active in searching for better technologies, and better ways of using or delivering those technologies. For example, before proposing that the ministry shift from buying to leasing personal computers, printers and servers, the specialists studied how well a similar shift had worked for the Ministry of Transportation and Highways.

Another source of information on innovations is contractors employed to develop new systems. They often bring fresh ideas from their work for the private sector and for other ministries. An example is the suggestion that video image capture technologies could be used to streamline the work of the Film Classification Office.

The ministry's methods of assessing value need improvement

We found that, for all significant project proposals, the ministry prepares justification documents in which it lays out expected costs and benefits. Before the ATC will consider any project, a standard project initiation document must be prepared identifying expected benefits. As well, the committee usually requires a cost and benefit analysis or a business case for significant proposals. The ministry also describes expected benefits in submissions to external approving agencies such as the Treasury Board Secretariat and the Information Science and Technology Agency.

However, in our opinion, evaluation methods have not been adequately developed or consistently applied. We did not find that the ministry had a standard method for describing costs and benefits, or for ensuring that the descriptions were consistent and of sufficient quality. Nor did we find evidence that the Administration and Technology Committee made consistent use of the cost and benefit information provided it.

For some projects we examined, the original benefits and value were never well articulated or supported. Several others were justified by arguments that harm would befall the ministry if the projects were not carried out, but in only two cases did we find these arguments persuasive.

We noted that several improvements have been made in recent months. Financial costs and benefits of all proposed projects are now assembled into a spreadsheet that shows both capital cost and operating impacts for five years. Non-financial benefits and costs, however, are not yet treated in a similar way. This is an important oversight, for we noted that most of the projects on the spreadsheet could not be justified solely on financial grounds.

We concluded that these weaknesses in delineating costs and benefits, and in making decisions based on that information, are of two forms: technical and cultural. The technical weaknesses can be solved relatively simply by requiring consistent use of standard methodologies such as:

- checklists of costs and benefits to consider;
- logic models to ensure completeness and relevance of costs and benefits;
- cost comparison tools (e.g., net present value); and
- evaluative techniques (e.g., the Balanced Scorecard, or Information Economics).

The cultural issues require an acceptance by the ministry that there is a problem—and a willingness to correct it by ensuring that evaluation is taken seriously.

We believe that this cultural difficulty is exemplified by the rarity with which the ministry conducts post-implementation reviews of completed projects. The purpose of a post-implementation review is to examine an investment after development is complete in order to validate actual investment results. The process of evaluation has two goals: (1) to examine differences between the estimated and actual investment costs and benefits; and (2) to extract "lessons learned" about the investment selection and control processes that can be used to

help improve these management processes. (Reviews should also be conducted for projects that were terminated before completion, to identify potential process improvements.)

Reviews provide the means to contribute to the repository of lessons learned and best practices. They assist in "wrapping up" the project and ensuring that everyone involved has an opportunity to understand their contribution to the project, and to contribute ideas for improving the delivery of future projects.

More profoundly, post-implementation reviews help reinforce an important truth: systems projects don't automatically deliver benefits, no matter how well the project is managed; benefits must be worked for once the systems are installed. Post-implementation review offers the chance to objectively understand the system's actual capabilities, and to plan out the further work (e.g. training, process re-engineering, further systems development) needed to make full use of those capabilities.

Post-implementation reviews are widely seen as a standard good practice in any project-based endeavour. For example:

- such reviews are a requirement for information technology projects conducted for the Canadian government; and
- the portfolio maturity model developed by the U.S. General Accounting Office (described in Appendix B of this report) sees the use of post-implementation reviews as a good indication of mature levels of portfolio management.

Also, in British Columbia such reviews are required by policy for major projects. The government's General Management Operating Policy (Section 8.4.4.4) states: "Ministries shall conduct a Post-Implementation Review on all major developments or enhancement projects within six months of project completion."

Despite this, we found few examples of post-implementation reviews in the ministry. Those we did find were cursory, and did not attempt to measure how well the project had achieved success relative to the originally stated intentions when the project began.

Recommendations

The ministry should maintain complete and organized information on the performance, value and prospects of each information technology system in its portfolio.

The ministry should adopt standard industry practices for determining benefits and costs and weighing the merits of competing projects, and should use those methods consistently.

The Administration and Technology Committee should ensure that the projects it approves clearly demonstrate net benefits that contribute directly to the achievement of the ministry's strategic goals.

The ministry should carry out post-implementation reviews of all its significant information technology projects upon completion or termination of a project, and use the findings to improve its processes for managing its information technology portfolio.

The ministry needs to improve the way it manages risk

Developing a new or replacement information technology system differs from the ongoing and repetitive operations of an organization. It is, in fact, a project—an organized activity with a definite beginning and end, undertaken to create a unique product or service. There is a well-developed methodology, called project management (see sidebar), for carrying out such endeavours.

A vital part of successful project management is risk management—that is, managing the uncertainty around future events and outcomes. Experience has shown that unmanaged or unmitigated risks are one of the primary causes of project failure, especially in information technology projects.

Risk can be thought of as a special kind of lens through which the portfolio is viewed, a lens that focuses attention on obstacles to success. The benefit of such focus is that, as a rule, what gets attention gets managed.

To be used successfully, risk identification and management must become part of the organization's culture. That means, for example, not just creating lists of known risks at the planning stage, but remembering to consider them further as the project progresses.

At the core of good risk management are four processes:

- **identification**, which entails carefully thinking through how the project will be carried out, and noting every place where problems with hardware, software, people or work processes could occur;

- **assessment**, which involves prioritizing risks according to their potential effect on the project's objectives;

A Brief Introduction to Project Management

Project management is the application of knowledge, skills, tools, and techniques to project activities in order to meet or exceed stakeholder needs and expectations. …. [It] invariably involves balancing competing demands among:

- Scope, time, cost, and quality.
- Stakeholders with differing needs and expectations.
- Identified requirements (needs) and unidentified requirements (expectations).

[Projects differ from the everyday operations of an organization] in that operations are ongoing and repetitive while … *a project is a temporary endeavour undertaken to create a unique product or service.*

Temporary means that every project has a definite beginning and a definite end. …Temporary does not necessarily mean short in duration: many projects last for several years.

Projects involve doing something which has not been done before and which is, therefore, *unique.* A product or service may be unique even if the category it belongs to is large. For example, many thousands of office buildings have been developed, but each individual facility is unique—different owner, different design, different location, different contractors, and so on. The presence of repetitive elements does not change the fundamental uniqueness of the overall effort.

Because the product of each project is unique, the characteristics that distinguish the product or service must be progressively elaborated. *Progressively* means "proceeding in steps; continuing steadily by increments" while *elaborated* means "worked out with care and detail; developed thoroughly." These distinguishing characteristics will be broadly defined early in the project and will be made more explicit and detailed as the project team develops a better and more complete understanding of the product. Progressive elaboration of product characteristics must be carefully coordinated with proper project scope definition…. When properly defined, the scope of the project—the work to be done—should remain constant even as the product characteristics are progressively elaborated.

It is important to note that many of the processes within project management are iterative in nature. This is in part due to the role of progressive elaboration in projects, i.e.: the more you know about your project, the better you are able to plan your project, as it is a gradual discovery process.

Source: Excerpted from *A Guide to the Project Management Body of Knowledge, 2000 Edition Exposure Draft,* 2000,
Project Management Institute , Newtown Square, PA

- **quantification,** which involves measuring the likelihood that these problems will occur and the effect they will have if they do occur; and
- **response planning,** which means deciding in advance what to do if particular problems occur.

Insufficient attention is paid to risk at the inception of projects

We expected to find that the ministry would first evaluate the risks around any proposed project, and then consider that information when deciding which projects to approve.

We found that the ATC has some methods for collecting information on the riskiness of a project proposal. It has a standard project initiation process for first assessing projects, and often funds feasibility assessments for significant new projects, reducing the likelihood that excessively risky projects will be approved. However, we did not find that risk information was considered in a consistent and meaningful way when decisions were made as to which projects would proceed.

However, we were pleased to find that ministry staff have recently used a risk assessment model developed by the state of California [see Appendix C] to assess the risks related to the ministry's major projects.

Monitoring and management of risk while projects are underway is ad hoc

We also expected to find a consistent and comprehensive process by which project teams would examine the risks facing their project, and report to the ATC on how they were responding to those risks. We did not find such a process being used consistently.

We did note that good risk management had been an integral part of the Year 2000 project, and had included both an assessment of where the risks were in relation to established criteria and a plan to actively manage the risks. Furthermore, regular reporting on risks was part of the control scheme required by the government's central Year 2000 project office. Many of the contractors carrying out ministry projects have their own detailed project management methods, including risk management. In our view, there are no technical obstacles preventing the ministry from carrying out good risk management on an individual project basis.

Changes are needed in both culture and techniques around risk management

Lack of policy on the matter seems to be partly the reason for the ministry's inconsistent attention to risk management. We found no detailed policy guidance on risk management for either ministry project managers or the ATC to follow. Central agency guidance is only cursory in areas of project and risk management. The ministry itself offers no specific policy for risk management with respect to projects. And, the mandate for the ATC does not mention risk management in its terms of reference.

Another problem seems to be that senior management attention is focused elsewhere. We concluded that the ATC devotes an excessive portion of its attention to cost management,

and thus has too little time to devote to project performance and risk management. At each meeting, it reviews information on which projects are slipping on their schedule and therefore not spending as fast as expected. Its practice in dealing with such slippage has been to reallocate unspent funds to previously unfunded projects, rather than to focus on getting the prime projects back on schedule.

We understand why the ministry needs to pay attention to cash flow, but believe that having this issue be a prime concern of the ministry's highest-level information technology steering committee sends the wrong message to staff about what is important. In our view, the ATC should delegate the management of cash flows (perhaps to the ATC working committee). It could then focus its own attentions on ensuring that the projects it approves offer the greatest strategic benefit to the ministry, that the risks surrounding these projects are managed, and that every attention is given to seeing that the projects do in fact deliver the benefits they promised.

When a number of projects are being carried out at the same time, the risks related to individual projects can have a compounding effect. For example, too many high-risk projects underway at the same time could strain an organization's supply of skilled project managers and demand more time and attention than its senior management have available. This emphasizes the importance of applying risk management at the portfolio level.

We examined the risk profile of the ministry's portfolio using two different, but complementary, risk assessment tools. We concluded that a disproportionate number of the ministry's major projects had high-risk characteristics, such as having multiple "customers" in the ministry involved in the project (e.g., Accounts Receivable and Collections, and Public Safety and Regulatory Branch Combined Operational Systems), or being reliant for success on the cooperation of others outside the ministry (e.g., EJSP and Electronic Filing System). Our point is not that the ministry should avoid risk—often, high-payoff projects are also high risk—but that it should know how much risk it can handle, and choose the mix of high-, medium- and low-risk projects that gives it the best set of payoffs within that risk constraint.

(Subsequent to our audit work, we were informed by ministry staff that the majority of the ministry projects not yet completed, including many that we considered high risk, have been cancelled or are on hold pending further review.)

Recommendations

The ministry should develop formal guidance on risk management and reporting.

The Administration and Technology Committee should make risk management one of its critical responsibilities, and delegate administrative duties whenever possible so that it has more time for risk management.

## The ministry could benefit from analyzing its "portfolio management maturity"

Our findings in this audit suggest to us that the Ministry of Attorney General (and other ministries) could benefit from using the idea of portfolio management *maturity*—the idea that organizational improvement is not a matter of individual hits and misses, but that it comes about through advances in the overall capability of the organization over time.

The maturity metaphor originated with studies carried out at Carnegie Mellon University for the U.S. Department of Defense on how to improve software development. The result was a model designed to "help software organizations improve the maturity of their software processes…from ad hoc, chaotic processes to mature, disciplined … processes." It was presented schematically as five levels of maturity, each building on success achieved at the maturity level below. The concept has since been extended to other areas of information technology, as well as to financial management and project management.

Last year the General Accounting Office (GAO), the independent auditor of the U.S. government, produced a maturity model for information technology investment management. This we found to be a good match for the portfolio concepts we outline in this report. We believe that the Ministry of Attorney General, and others, would find it useful to rate themselves against the GAO maturity model, as a guide to making future strategic enhancements to their information technology capability. (Appendix B provides more information on the model.)

Recommendation

The ministry should examine its information management using a portfolio maturity model such as that developed by the U.S. General Accounting Office.

❖   ❖   ❖
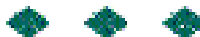
ministry response

Thank you for the report "Management of the Information Technology Portfolio in the Ministry of Attorney General" dated November 26, 2001. Please be formally advised that senior staff have carefully considered the overall findings and recommendations.

It is important to note the following points when reviewing the report and our formal response:

- *The field work for the report was conducted over a year ago, well before the reorganization of the former Ministry of Attorney General. The findings of the report remain applicable to the new Ministry of Attorney General including the Treaty Negotiations Office, and the Ministry of Public Safety and Solicitor General.*

- *The Administration and Technology Committee (ATC) referenced in the report remains a single, active committee in support of both ministries.*

- *It is important to note that government's move to greater shared service for information technology management, coupled with budget reductions, may impact the ministries' Information Technology Services Division's (ITSD) ability to respond fully to all recommendations.*

- *We agree that it is important to align systems projects with established organizational goals and objectives.*

The recommendations contained in the report provide a useful guide to strengthen information technology management in our ministries. Accordingly, the ministries' response to the audit recommendations is summarized below:

1. ***Recommendation: "The ministry should adopt standard industry practices for determining benefits and costs and weighing the merits of competing projects, and should use those methods consistently."***

   Ministries' action:

   The Administration and Technology Committee (ATC) will research and define "industry standard practices" in our government context, then extend the Project Initiation Document (PID) and project evaluation process to include a standardized summary of benefits and costs.

2. ***Recommendation: "The Administration and Technology Committee should ensure that the projects it approves clearly demonstrate net benefits that contribute directly to the achievement of the ministry's strategic goals."***

   Ministries' action:

   The Information Resource Master Plan (IRMP) will be an ATC funded initiative facilitated by ITSD.

ATC will enhance PID checklists to show how a project contributes to the respective Ministry Service Plan. Proposed project net benefits will be brought by proponents to ATC through the ATC working committee.

3. Recommendation: "The ministry should carry out post-implementation reviews of all its significant information technology projects upon completion or termination of a project, and use the findings to improve its processes for managing its information technology portfolio."

Ministries' action:

Ministries' project proposals will include a line item for funding for a post-implementation review (PIR) and include a PIR activity in project schedules and contracts.

ATC will endeavor to commission external post-implementation reviews.

4. Recommendation: "The ministry should develop formal guidance on risk management and reporting."

Ministries' action:

ATC requires regular project status reports from Project Sponsors.

ATC will conduct summary risk assessment reviews on all development projects at the beginning of each new phase of the project. ITSD has a computerized tool in place to assist with this task.

Major (high risk) projects will plan and budget for annual and/or mid-phase formal independent progress reviews. Major projects in our context are defined as those costing more than $1 million.

5. Recommendation: "The Administration and Technology Committee should make risk management one of its critical responsibilities, and delegate administrative duties whenever possible so that it has more time for risk management."

Ministries' action:

ATC has modified its procedure to consider management of project risk. Attendance at ATC by Assistant Deputy Ministers or their designates will be confirmed, and the profile of ATC will be reconfirmed by introducing a biannual report from it to the Joint Executive Committee. (The executive members of the Ministry of Attorney General, Treaty Negotiations Office, and the Ministry of Public Safety and Solicitor General meet regularly to discuss common issues in support of the ministries.)

6. Recommendation: "The ministry should examine its information management using a portfolio maturity model such as that developed by the U.S. General Accounting Office."

Ministries' action:

This subject will be one of the themes of the next IRMP report. The Ministries will consider their information management with respect to a maturity model.

7. Recommendation: "The ministry should maintain complete and organized information on the performance, value and prospects of each information technology system in its portfolio."

Ministries' action:

ATC will look for direction and assistance from the province's Chief Information Officer for moving to an inventory system. It will focus on defining 'performance', 'value', and 'prospects' and how this can be measured in an inventory system.

On behalf of the Ministries of Attorney General and Public Safety and Solicitor General, I thank you again for this work.

❖   ❖   ❖
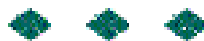
appendices
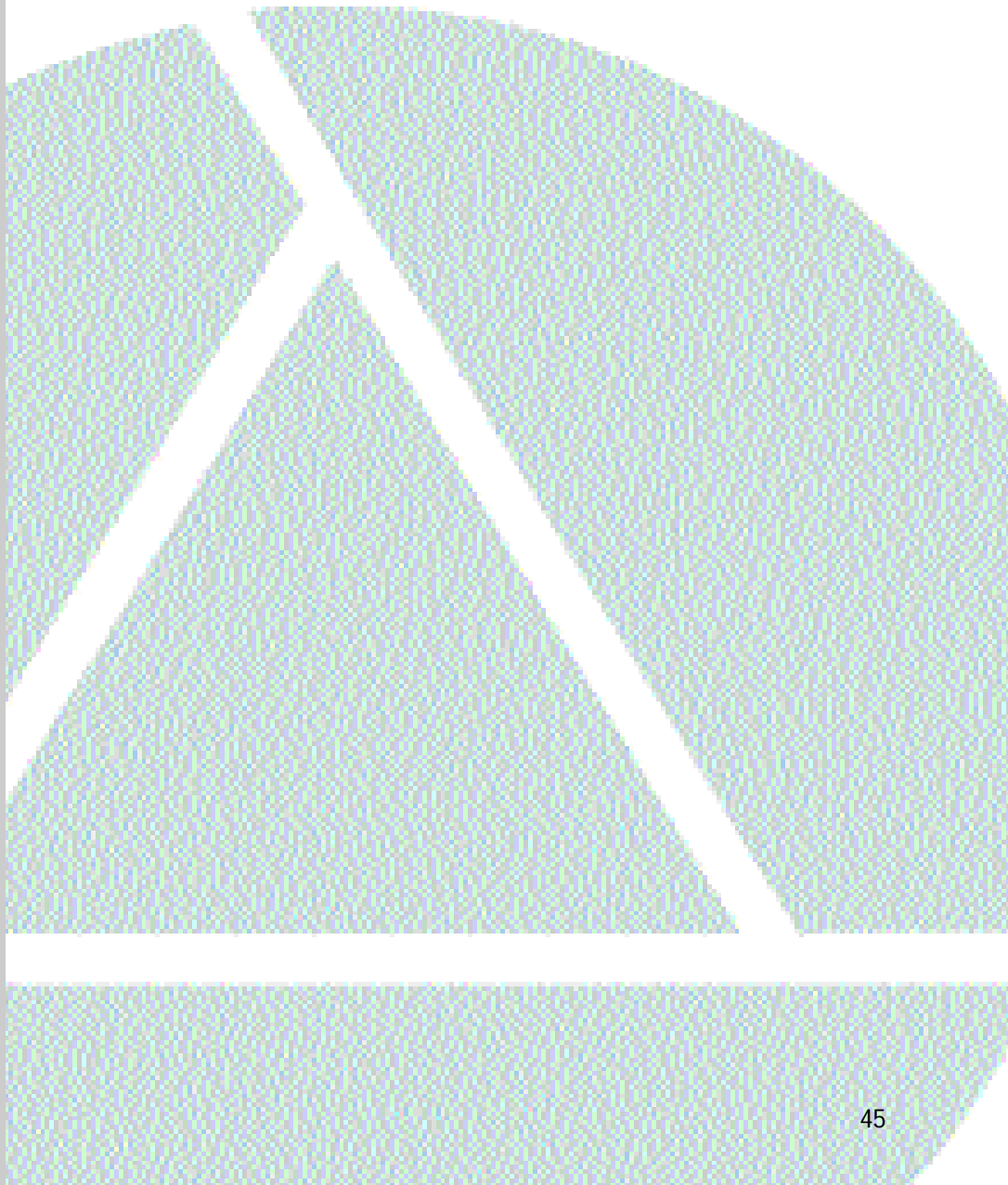
appendix a:

Justice Information System (JUSTIN)
—An Example of a Major Information Technology Project

Jurisdictions throughout North America are searching for ways to integrate their justice systems

As in other jurisdictions, participants in the British Columbia justice system—police, Crown counsel, court administrators, judges and Corrections staff—are separate but interdependent. Getting the proper balance between separation and interdependence is becoming increasingly important. Justice agencies throughout North America increasingly recognize the importance of integrating their information systems in order to share critical data, documents, images and key transactions. Integrated systems have the potential to improve the quality of information, and therefore the quality of decisions, by eliminating error-prone, redundant data entry. In addition, through the sharing of data between systems, integration typically improves the timely access to information, a critical factor in decisions such as setting bail. Moreover, integration enables the sharing of crucial information without regard to time or space. Multiple users can access the same record simultaneously from remote locations around the clock.

JUSTIN is an integrated justice information system

JUSTIN (JUSTice INformation system) is the largest and most important information technology project that the Ministry of Attorney General has undertaken. It supplies services to a number of key branches of the ministry, as well as linking to the judiciary and the police, and does so in locations throughout the province. Its development has taken some five years, and its out-of-pocket cost has been at least four million dollars. We have included this appendix to give the interested reader some sense of the complexity of major information technology projects.

JUSTIN is a database of information on almost every aspect of a criminal case, including police reports to Crown Counsel, Crown Counsel's case assessment and approval, victim and witness notification, court scheduling, document production, and judicial trial scheduling.

JUSTIN's information is *integrated:* information about a case is entered only once and is re-used by various agencies as the case moves from initiation through to disposition. This re-use of data throughout JUSTIN helps reduce staff time in recording and processing cases, and minimizes the possibility of errors due to re-entry of data. JUSTIN also provides *participant-based tracking.* This means that information entered about a participant (e.g., an accused, a witness or a victim) in one case can be re-used in subsequent cases.

JUSTIN has four main components: Report to Crown Counsel; Crown; Courts; and Judiciary:

■ The Report to Crown Counsel is the principal method of communicating the results of investigations between police and Crown Counsel. This module allows police to prepare an Report to Crown Counsel on a computer and electronically submit it to Crown Counsel. JUSTIN captures information about the progress of the case, including appearances, dispositions and orders.

■ Crown: This module allows Crown Counsel to examine the Report to Crown Counsel online when reviewing charges and preparing for trial.

■ Courts: This module tracks cases in Provincial Court (adult criminal, youth, and traffic cases) and Supreme Court (criminal cases). It automatically generates documents such as sentencing orders, documents compelling appearance in court, and prisoner release orders.

■ Judiciary: Using this module, trial coordinators select trial dates, check the availability of police and civilian witnesses, and maintain court room calendars. Notifications related to trials are immediately available to all concerned agencies.

In addition, JUSTIN has two specialized components. One, LEA (Law Enforcement Availability), tracks the shift cycles, vacations scheduled, and special assignments of police officers. Trial schedulers and court registry staff use this information to assist them in scheduling trials that require an officer's attendance. The other, CVWS (Crown Victim Witness Services), automates the identification and notification of victims and witnesses.

JUSTIN's expected benefits include:

Increased public safety

■ Police have immediate access to the complete criminal history of an accused, as well as to information such as warrants issued or cancelled, protection orders, firearms prohibition orders, and high-risk offender indicators.

■ JUSTIN maintains the names of all high-risk offenders in the province.

Better information quality

■ Crown Counsel can make better "charge approval" decisions, as they are able to see work that is pending in another Crown office or has been waived to other courts.

■ JUSTIN generates customized reports to provide administrators with accurate and timely statistics about cases and case volumes.

Reduced costs

■ Maintaining a single, province-wide system instead of many separate systems reduces costs and duplication of effort.

■ Electronic file transfer between agencies saves time and paper and reduces costs.

■ Online inquiry greatly reduces the need to locate physical files to answer queries.

■ Automatic production of documents such as the Report to Crown Counsel minimizes data entry effort, increases accuracy, and standardizes document formats.

Improved court scheduling

■ Police are able to indicate dates when they are not available for court, which allows trial schedulers to set trial times more accurately. This reduces police overtime costs and reduces the number of adjournments because of unavailability of police witnesses.

■ In consultation with trial schedulers, administrative judges are able to view all trials set in order to schedule sitting judges according to need at a specific time.

Developing JUSTIN has been a long and complex task

In the early 1990s, the ministry began a project called the Integrated Case Processing System (ICPS) to research, design and implement a province-wide, integrated justice information system. The ICPS project never reached the stage of developing a prototype, but the business knowledge gained was used as input to what eventually became the JUSTIN project.

Work on JUSTIN began in 1995. Late that year, pilot testing of the first component—Crown Counsel—began in the first test site, Kelowna. Work continued step by step until the system encompassed its full range of functions. The core software product, JUSTIN Version 1.02, was completed in May

1999. The budgeted cost of Version 1.02 from inception was $4.0 million. (However, this is not a complete measure of cost. In addition to this out-of-pocket cost, much staff time has been devoted to the design, specification, testing, training, project management and support necessary to make the initiative a success.) JUSTIN implementation was completed in July 2001, and the system is now installed in about 400 locations in the province.

❖ ❖ ❖
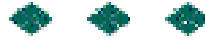
appendix b:

A Useful Portfolio Management Maturity Model

The portfolio management model presented here was developed by the U.S. General Accounting Office (GAO). It has five stages of maturity. Each stage builds upon the lower ones and enhances the organization's ability to manage its information technology investments.

The five stages are:

- Stage 1: Creating investment awareness—There is little awareness of investment management techniques. Information technology management processes are ad hoc, project-centred, and have widely variable outcomes.

- Stage 2: Building the investment foundation—Repeatable investment control techniques are in place and the key foundation capabilities have been implemented.

- Stage 3: Developing a complete investment portfolio—Comprehensive information technology investment portfolio selection and control techniques are in place that incorporate benefit and risk criteria linked to mission goals and strategies.

- Stage 4: Improving the investment process—Process evaluation techniques focus on improving the performance and management of the organization's information technology investment portfolio.

- Stage 5: Leveraging information technology for strategic outcomes—Investment benchmarking and information technology-enabled change management techniques are deployed to strategically shape business outcomes.

Stage 1 is characterized by ad hoc, unstructured and unpredictable investment processes. For example, in a Stage 1 organization, there is generally little relationship between the success or failure of one project and the success or failure of another. If an information technology project succeeds and is seen as a good investment, that is largely because of the exceptional actions on the part of the project team members and thus the project's success might be difficult to repeat. Investment and development processes that are important for success may be known, but only to isolated teams; this process knowledge is not widely shared or institutionalized.

The unpredictable nature of project outcomes means that even if an organization does recognize that a project is in trouble, it has only a limited ability to address and resolve the project's problems.

Additionally, a focus on project results in terms of business benefits is often missing in Stage 1 organizations. Most organizations with Stage 1 maturity have some type of project selection process in place as part of their annual budgeting activity. However, the selection process is frequently rudimentary, poorly documented and inconsistent.

The primary focus of **Stage 2** maturity is on attaining repeatable, successful investment control processes and basic selection processes at the project level. For an organization to develop a sound information technology investment process, it must first be able to control its investments so that they finish predictably within established schedule and budget ranges. An organization can begin by focusing on gaining control of its existing collection of projects, and following a disciplined process for tracking each project's cost and schedule milestones and improving project outcomes over time. Supporting these activities requires the creation of an inventory to ensure that the organization knows basic information about its information technology assets.

Stage 2 selection-related processes are designed to establish basic selection capabilities that can evolve into the more mature selection capabilities of Stage 3. Therefore, the organization also focuses on defining and developing its information technology investment boards, identifying the business needs or opportunities to be addressed by each information technology project, and using this knowledge in the selection of new information technology proposals.

Establishing a consistent, well-defined information technology investment portfolio perspective is the critical focus of **Stage 3**, along with maintaining mature control processes and initiating basic evaluation processes. Once new information technology proposals can be selected and developed on schedule and on budget (Stage 2), the organization needs to consider criteria for how it should develop an information technology investment portfolio—that is, not just a collection of projects but a conscious, proactive look at how the organization expends its limited resources on information technology, what beneficial impacts these investments have on the organization, and what alternative investments will better achieve the organization's mission.

An organization at **Stage 4** maturity is focused on using evaluation techniques to improve its information technology investment processes and portfolio, and on maintaining mature control and selection processes. A main tool for accomplishing this is the post-implementation review, which is conducted after an investment is completed and examines the outcome of the investment relative to its plans and expectations. This examination typically identifies lessons learned from the investment and improves the understanding of the key variables in its business case. Analyzing a number of such reviews serves as the basis for changing and improving the information technology investment processes.

Additionally, at Stage 4 the organization has the capacity to conduct information technology succession actions and thus plan and implement the "de-selection" of obsolete, high-risk, or low-value information technology investments.

At **Stage 5**, now that the organization has mastered its selection, control and evaluation processes, it seeks to shape its strategic outcomes by learning from other organizations, and by continuously improving the manner in which it uses information technology to support its business outcomes. A Stage 5 organization benchmarks its information technology investment processes against other "best-in-class" organizations and actively searches for breakthrough information technologies that will allow it to significantly change and improve its business performance.

Exhibit B.1 shows characteristics typical of each stage, organized to match the structure of this report.

Exhibit B1

Characteristics of Different Stages in the Portfolio Management Maturity Model of the U.S. General Accounting Office

Stage	Portfolio ownership	Portfolio management	Opportunities and project proposals	Project delivery	Systems in operation
5		Continually improve processes for using information technology to improve business outcomes; learn from "best-in-class" organizations	Search for break-through technologies that will significantly improve performance		
4		Use evaluation techniques such as post-implementation reviews to improve information technology investment processes			Plan and carry out deletion of obsolete, high-risk, or low-value information technology investments
3	Align authority of multiple steering committees	Define information technology invest-ment selection criteria; analyze proposals against criteria	Ensure proposals support ministry's mission and strategies	Deliver projects on budget and schedule, manage risks and benefits	
2	Define and develop information technology steering committee(s)	Establish basic selection criteria	Identify key business needs and customers served by proposal	Use disciplined process to oversee project cost and schedule; improve project outcomes over time; act successfully when project 'goes off the rails'	Maintain organized set of information on all systems
1		Use ad hoc and unpredictable selection process	Often lack focus on business benefits of proposals	Achieve success, sometimes, through one-off "heroism"; cannot consistently put projects "back on the rails"	Lack organized information on systems

Source: Excerpted from *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity/Exposure Draft,* United States General Accounting Office, report GAO/AIMD-10.1.23. To obtain the report, see the GAO website <http://www.gao.gov>.
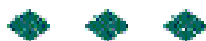
appendix c:

A Sample Risk Assessment Template

Assessing the risk of a project is a critical management responsibility, especially at the proposal stage of the project. A number of checklists and templates have been developed to guide risk assessment. The one we present here was developed by California's Department of Information Technology (a similar template is used by the State of Washington, which is considered to be a leading state for information technology management). It consists of 38 questions in five main categories. For each question, the checklist gives typical answers and assigns the answers a risk rating from 1 to 9, with 9 being the highest risk. (These ratings are averaged to determine overall risk levels for each of the major risk areas.)

Strategic Risk

1. To what degree is the project's purpose aligned with the agency's overall business strategy?

2. How clearly are the expected project outcomes defined?

3. Have metrics been established to verify the successful completion of each project phase?

4. To what extent are senior management committed to the project and its outcomes?

5. How severe would be the result of late delivery?

Financial Risk

6. What is the end-to-end expenditure that this project will require?

7. Are the cost/benefits clearly defined with a documented write-up?

8. Is there a clearly defined payback for this system?

9. What is the payback time for the project?

10. To what degree have existing expenditures met budgeted amounts?

11. Is the vendor well established in the business community with a strong financial background?

Project Management Risk

12. **Does the project management team have relevant experience?**

13. **To what extent has a workplan been developed for the entire project lifecycle?**

14. **To what degree have critical checkpoints and milestones been established for this project?**

15. **What is the total elapsed time of the project from start to finish?**

16. **Have scope changes occurred which appear to exert pressure on schedule demands?**

17. **To what degree have "open issues"' been tracked and included as part of ongoing management processes?**

18. **Is the project development team organized and deployed to a single location?**

19. **To what degree are the development and user skill requirements well defined?**

Technology Risk

20. **Is there a plan for ensuring that deliverables meet the need of the users?**

21. **Is there a system load test or other measures to ensure good system performance (i.e., measures to test response time, system efficiency, etc.)**

22. **How thoroughly have the technology options been evaluated?**

23. **What is the knowledge of the proposed technology environment?**

24. **Do the key technologies appear to be the appropriate foundation given the system design?**

25. **How many existing computer systems must the project system interact with?**

26. **To what extent will the new system enable de-installation of the existing system?**

27. **What is the vendor's ability to implement the technology?**

Change Management/Operational Risk

28. How is the acceptance testing plan being developed?

29. Is the current operations organization prepared to support the new system?

30. Is the proposed hardware/software environment in production already within the organization? (i.e., mainframe, client server, middleware, etc.)

31. How clearly defined are the system operating procedures (backups, restart/recovery, etc.)?

32. How severely would business be impacted by a system failure?

33. What will be the magnitude of change that the new system will impose upon the users?

34. Are department staff willing to accept this change?

35. Will staff numbers be reduced as a result of implementing the system?

36. Will multiple business organization units be affected by the new system?

37. To what degree are changes to the current business processes being managed?

38. What is the level of user involvement in the project?

An important idea underlying risk assessment templates such as this one is that relatively small changes in certain conditions can lead to much larger changes in risk. For example, note how the suggested risk ratings (shown in brackets) increase rapidly for the following key questions:

12. Does the project management team have relevant experience?

- Members of the project management team have experience leading projects of similar size and complexity. **(1)**

- Members of the project management team have had exposure to projects of similar size and complexity but not in lead roles. **(4)**

- Members of the project management team have had limited exposure to projects of similar size and complexity and generally lack detailed knowledge. **(7)**

- Members of the project management team have no experience with projects of similar size and complexity. **(9)**

33. **What will be the magnitude of change that the new system will impose upon the users?**

- **The new system will impose very little change, if any, upon the users. (1)**
- **The new system will change slightly the current daily operations of the users. (2)**
- **The new system will require significant changes by the users and will require training. (5)**
- **The new system will present an entirely new way for the users to complete daily operations. (8)**

34. **Are department staff willing to accept this change?**

- **Staff are well informed about the change and show strong enthusiasm. (1)**
- **Probably; staff seem enthusiastic but there has been no formal evaluation of their enthusiasm or detailed knowledge of the change. (3)**
- **Unclear; only limited or informal feedback from staff has been received. (5)**
- **No; firsthand feedback clearly indicates reluctance to the change. (9)**

Source: State of California Department of Information Technology website
<http://www.doit.ca.gov/SIMM/RAM/RAMQuestions.asp>.
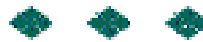
appendix d:

Office of the Auditor General: 2001/02 Reports Issued to Date

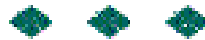*Report 1*

Managing Interface Fire Risks

Report 2

**Transportation in Greater Vancouver:
A Review of Agreements Between the Province
and Translink, and of Translink's Governance Structure**

Report 3

**Building Better Reports:
Public Performance Reporting Practices
in British Columbia**

Report 4

Monitoring the Government's Finances

❖   ❖   ❖

appendix e:

Office of the Auditor General: Performance Auditing Objectives and Methodology

Audit work performed by the Office of the Auditor General falls into three broad categories:

- Financial auditing;
- Performance auditing; and
- Conduct of business auditing.

Each of these categories has certain objectives that are expected to be achieved, and each employs a particular methodology to reach those objectives. The following is a brief outline of the objectives and methodology applied by the Office for performance auditing.

Performance Auditing

What are Performance Audits?

Performance audits (also known as value-for-money audits) examine whether money is being spent wisely by government —whether value is received for the money spent. Specifically, they look at the organizational and program elements of government performance, whether government is achieving something that needs doing at a reasonable cost, and consider whether government managers are:

- making the best use of public funds; and
- adequately accounting for the prudent and effective management of the resources entrusted to them.

The aim of these audits is to provide the Legislature with independent assessments about whether government programs are implemented and administered economically, efficiently and effectively, and whether Members of the Legislative Assembly and the public are being provided with fair, reliable accountability information with respect to organizational and program performance.

In completing these audits, we collect and analyze information about how resources are managed; that is, how they are acquired and how they are used. We also assess whether legislators and the public have been given an adequate explanation of what has been accomplished with the resources provided to government managers.

Focus of Our Work

A performance audit has been described as:

...the independent, objective assessment of the fairness of management's representations on organizational and program performance, or the assessment of management performance,

against criteria, reported to a governing body or others with similar responsibilities.

This definition recognizes that there are two forms of reporting used in performance auditing. The first—referred to as attestation reporting—is the provision of audit opinions as to the fairness of management's publicly reported accountability information on matters of economy, efficiency and effectiveness. This approach has been used to a very limited degree in British Columbia because the organizations we audit do not yet provide comprehensive accountability reports on their organizational and program performance.

We believe that government reporting along with independent audit is the best way of meeting accountability responsibilities. Consequently, we have been encouraging the use of this model in the British Columbia public sector, and will apply it where comprehensive accountability information on performance is made available by management.

As the performance audits conducted in British Columbia use the second form of reporting—direct reporting—the description that follows explains that model.

Our "direct reporting" performance audits are not designed to question whether government policies are appropriate and effective (that is achieve their intended outcomes). Rather, as directed by the Auditor General Act, these audits assess whether the programs implemented to achieve government policies are being administered economically and efficiently. They also evaluate whether Members of the Legislative Assembly and the public are being provided with appropriate accountability information about government programs.

When undertaking performance audits, we look for information about results to determine whether government organizations and programs actually provide value for money. If they do not, or if we are unable to assess results directly, we then examine management's processes to determine what problems exist or whether the processes are capable of ensuring that value is received for money spent.

Selecting Audits

All of government, including Crown corporations and other government organizations, are included in the universe we consider when selecting audits. We also may undertake reviews of provincial participation in organizations outside of government if they carry on significant government programs and receive substantial provincial funding.

When selecting the audit subjects we will examine, we base our decision on the significance and interest of an area or topic to our primary clients, the Members of the Legislative Assembly and the public. We consider both the significance and risk in our evaluation. We aim to provide fair, independent assessments

of the quality of government administration and to identify opportunities to improve the performance of government. Therefore, we do not focus exclusively on areas of high risk or known problems.

We select for audit either programs or functions administered by a specific ministry or government organization, or cross-government programs or functions that apply to many government entities. A large number of such programs and functions exist throughout government. We examine the larger and more significant of these on a cyclical basis.

Our view is that, in the absence of comprehensive accountability information being made available by government, performance audits using the direct reporting approach should be undertaken on a five- to six- year cycle so that Members of the Legislative Assembly and the public receive assessments of all significant government operations over a reasonable time period. We strive to achieve this schedule, but it is affected by the availability of time and resources.

Planning and Conducting Audits

A performance audit comprises four phases of a performance audit—preliminary study, planning, conducting and reporting. The core values of the Office—independence, due care and public trust—are inherent in all aspects of the audit work.

Preliminary Study

Before an audit starts, we undertake a preliminary study to identify issues and gather sufficient information to decide whether an audit is warranted.

At this time, we also determine the audit team. The audit team must be made up of individuals who have the knowledge and competence necessary to carry out the particular audit. In most cases, we use our own professionals, who have training and experience in a variety of fields. As well, we often supplement the knowledge and competence of our staff by engaging one or more consultants to be part of the audit team.

In examining a particular aspect of an organization to audit, auditors can look either at results, to assess whether value for money is actually achieved, or at management's processes, to determine whether those processes should ensure that value is received for money spent. Neither approach alone can answer all the questions of legislators and the public, particularly if problems are found during the audit. We therefore try to combine both approaches wherever we can. However, because acceptable results-oriented information and criteria are often not available, our performance audits frequently concentrate on management's processes for achieving value for money.

If a preliminary study does not lead to an audit, the results of the study may still be reported to the Legislature.

Planning

In the planning phase, the key tasks are to develop audit criteria—"standards of performance"—and an audit plan outlining how the audit team will obtain the information necessary to assess the organization's performance against the criteria. In establishing the criteria, we do not expect theoretical perfection from public sector managers; rather, we reflect what we believe to be the reasonable expectations of legislators and the public.

Conducting

The conducting phase of the audit involves gathering, analyzing and synthesizing information to assess the organization's performance against the audit criteria. We use a variety of techniques to obtain such information, including surveys, and questionnaires, interviews and document reviews.
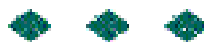
Reporting Audits

We discuss the draft report with the organization's representatives and consider their comments before the report is formally issued to the Legislative Assembly. In writing the audit report, we ensure that recommendations are significant, practical and specific, but not so specific as to infringe on management's responsibility for managing. The final report is tabled in the Legislative Assembly and referred to the Public Accounts Committee, where it serves as a basis for the Committee's deliberations.

Reports on performance audits are published throughout the year as they are completed, and tabled in the Legislature at the earliest opportunity. We report our audit findings in two parts: a highlights section and a more detailed report. The overall conclusion constitutes the Auditor General's independent assessment of how well the organization has met performance expectations. The more detailed report provides background information and a description of what we found. When appropriate, we also make recommendations as to how the issues identified may be remedied.

It takes time to implement the recommendations that arise from performance audits. Consequently, when management first responds to an audit report, it is often only able to indicate its intention to resolve the matters raised, rather than to describe exactly what it plans to do.

Without further information, however, legislators and the public would not be aware of the nature, extent, and results of management's remedial actions. Therefore, we publish updates of management's responses to the performance audits. In addition, when it is useful to do so, we will conduct follow-up audits. The results of these are also reported to the Legislature.