

Unclassified

PUMA/SBO/RD(2001)1



Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

18-May-2001

English - Or. English

**PUBLIC MANAGEMENT SERVICE
PUBLIC MANAGEMENT COMMITTEE**

**PUMA/SBO/RD(2001)1
Unclassified**

MANAGEMENT OF LARGE PUBLIC IT PROJECTS: CASE STUDIES

**22nd Annual Meeting of Senior Budget Officials
Paris, 21-22 May 2001**

For further information, please contact Jens KRISTENSEN
Tel: 33-1 45 24 18 35; Fax: 33-1 45 24 17 06; E-mail: jens.kristensen@oecd.org

JT00107998

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

English - Or. English

TABLE OF CONTENTS

CANADA	3
DENMARK	29
FINLAND	323
FRANCE	365
IRELAND	68
NORWAY	71
NEW ZEALND	88
POLAND	128
SWEDEN	134
UNITED KINGDOM	143
UNITED STATES	173

CANADA

INTRODUCTION

This report has been prepared by the Enhanced Management Framework Division of the Chief Information Officer Branch, Treasury Board of Canada Secretariat, in support of the OECD project on Management of Large Information Technology (IT) Projects in the Public Sector.

The OECD project aims at finding out what it takes for governments to secure success in their management of large public IT investments, and what lessons can be learnt from past failures. It addresses the issues of governance, monitoring and risk management of such projects.

This country report is structured into four sections. Section 1 provides a synopsis of the general institutional framework put in place by the Canadian Government to improve the success rate of Information Management/Information Technology (IM/IT) investments. Section 2 of the report contains a number of case studies which provide actual examples of successes and failures, while Section 3 identifies the key lessons learned from recent projects on how failures can be avoided and success facilitated. Finally Section 4 contains references to further material on the management of large public IT projects.

1. GENERAL INSTITUTIONAL FRAMEWORK

1.1. *Background*

The Canadian Government is committed to delivering its programs and services more efficiently and effectively through the use of information technology. In 1994 the Treasury Board Secretariat published a "Blueprint for Renewing Government Services Using Information Technology". Since that time, the development and rapid growth in use of the Internet has revolutionised approaches to IM/IT usage. The government recognises the need to adapt its services to the new technology. In the October 1999 Speech from the Throne, the government made a commitment to having all of its information and services on-line by 2004. The government's goal is "to be known around the world as the government most connected to its citizens, with Canadians able to access all government information and services on-line at the time and place of their choosing".

However, for some time now, failures of major information technology investments and key systems development projects have raised concerns for the achievement of service improvement through information technology. In 1995, in recognition of these concerns, the Treasury Board Secretariat (TBS) carried out a review of 25 significant government IM/IT projects, with a total estimated cost of \$2 billion. The review identified business, project management, risk management, and human resource issues influencing the outcome of these projects.

Also in 1995, the Auditor General of Canada, as part of his annual review of government, studied four large systems development projects, with a combined value of \$490 million, underway by government departments, and found that only one of the four was being managed effectively in terms of the risks associated with the project.

The report described the results of these reviews, and also quoted private sector research (the Standish Group's CHAOS research) indicating that the likelihood of large multi-year systems development initiatives being completed on time, within budget and with the desired functionality (what the system should do for its users) in the public and private sectors was extremely low. In 1994, the chance of a project developed by a Fortune 500 company coming in on time and within budget was only 9%. At that time 31% of IM/IT projects surveyed by the Standish Group in both the private and public sectors were cancelled before completion. Subsequent CHAOS research shows that higher proportions of projects are being completed successfully, but the proportion cancelled has remained about the same.

The focus of reviews by the Treasury Board Secretariat and the Auditor General was on large IM/IT projects. These may be defined by a number of criteria, for example:

- with a value over \$10 million.
- taking 18 months or longer to implement.
- involving extensive business or organisational change.
- involving significant new technology and/or technical complexity.
- requiring implementation in numerous and widely dispersed locations, or across more than one organisation.

However, it was evident that the conclusions emerging from the reviews of large IM/IT projects were applicable to projects of all sizes in this area. These reviews led to a re-examination of the government's policy and procedures for the management of systems development projects, and ultimately to a new focus on the management of IM/IT investments in general: portfolio management.

1.2. Enhanced Management Framework for IM/IT (EMF)

In 1996 the Treasury Board Secretariat developed the Enhanced Framework for the management of IT projects, which has since evolved to become the Enhanced Management Framework for IM/IT (EMF). The objective of the EMF is to help departments improve management of their IM/IT projects and the success rate of their IM/IT investments. Departments were directed to apply this framework to all projects that have a significant information management or technology component, regardless of size. The EMF was designed to ensure that government information technology projects fully meet the needs of the business functions they are intended to support, deliver all expected benefits and are completed on time and on budget.

Subsequently the EMF has expanded from focusing solely on project management disciplines to include portfolio management, which addresses the overall management and governance of IM/IT investments. This helps improve the strategic use of IM/IT investments through a stronger alignment with business directions and priorities.

EMF enhances the government's ability to manage its IM/IT investments, successfully deliver IM/IT projects, and minimise risks. It provides for a more effective, efficient and successful management of IM/IT allowing for optimal selection of high-return IM/IT investments, balanced decision-making, comprehensive risk management and successful delivery of projects.

EMF is an integrated management model that includes processes and key practices for executives, as well as for business and project managers. The framework is supported by a set of principles, best practices, methodologies, tools, templates, handbooks, guides, and standards.

The conceptual model above shows the components of the EMF, and the way in which they are related. EMF is based on four guiding principles:

1. Alignment of IM/IT investments with business strategies;
2. Establishment of clear accountabilities for managing IM/IT investments;
3. Development of corporate project management disciplines; and
4. Identification and management of risks on a continuous basis.

EMF addresses two broad areas: portfolio management and project management. Portfolio management stresses the importance of aligning business planning with an integrated IM/IT strategy. This strategy should set priorities and budgets for the organisation's IM/IT investments as a whole, allowing it to assess and successfully manage projects, existing operations, enhancements and innovative pathfinders. Within this context, organisations should review their IM/IT investments and – based on this review and available funds – select those investments that will deliver optimal value. EMF also promotes the application of project management disciplines to all approved initiatives, as well as the implementation of risk and performance management throughout the entire process.

The implementation and the institutionalisation of EMF across government is led by an Implementation Council – a government-wide partnership with representatives from 28 departments, the Office of the Auditor General, and central agency functional areas like policy, risk, audit and procurement. The EMF Division within the Chief Information Officer (CIO) Branch of TBS, is a centre of excellence assisting departments in their EMF implementation efforts. In partnership with the Implementation Council, it develops the framework, rolls out well-researched solutions and toolkits, promotes and shares the best practices, conducts symposia and workshops, addresses policy issues, and provides leadership, advice and support.

Alliances have been formed with leading international standard setting organisations, United States government agencies, professional associations, educational institutions, and central agencies. Special Interest Groups are created to facilitate sharing of experiences, best practices, and lessons learned on specific subjects and issues such as risk and process improvement. *Ad-hoc* working groups are set up to help develop specific solutions, including templates, tools, guidelines and methodologies.

Details on the EMF and its range of solutions can be obtained from http://www.cio-dpi.gc.ca/emf/EMFIndex_e.html.

Since September 1997, all new projects submitted by departments for approval by the Treasury Board Secretariat have had to conform to the model of “best practices” outlined in the Enhanced Management Framework. In addition, the Secretariat applied the appropriate principles from the Framework to all Year 2000 projects.

1.3. Procurement philosophy

The government has adopted an innovative approach to buying goods and services to help ensure the success of complex IT acquisition projects, traditionally characterised by significant risk. The approach is called Benefits Driven Procurement (BDP), focusing on results, the benefits that the government – but also

its suppliers – must gain from each acquisition project. BDP is a philosophy more than a method, although its aims are achieved through very methodical means. Although developed to solve problems with information technology acquisitions, the BDP has a broad application and is relevant to a wide range of high-risk procurement endeavours.

The BDP approach is designed to avoid the pitfalls that beset many complex projects – the delays, cost overruns and end results that often fall far short of expectations. It is a new concept for today's new era of rapid-fire technological change, competitive marketplaces and pressures on governments to be more efficient and effective than ever before.

BDP addresses many of the problems related to traditional procurement approach by focusing on the overall outcomes rather than setting detailed blueprints for suppliers to follow.

The other key distinguishing feature of BDP is thorough and rigorous front-end planning to remove or mitigate potential problems in the procurement process. Both the front-end planning and the management of the entire acquisition life cycle are based on four elements: *i)* a solid business case; *ii)* risk analysis; *iii)* clear delineation of accountabilities; and *iv)* a compensation structure closely tied to the supplier's performance.

Additional information on the Benefits Driven Procurement is available from: http://www.cio-dpi.gc.ca/emf/solutions/Procurement/Procurement_e.html.

1.4. Funding

The majority of government IM/IT projects are funded from the budgets of their sponsoring departments. Departmental budgets are established and approved by Parliament through the government's Budget and Estimates process.

Certain IM/IT applications used by more than one department, typically financial management and human resource management systems, are designated Shared Systems. The CIO Branch of the TBS oversees the whole Shared Systems Program, including the acquisition of system licences for multi-departmental use. Each system is managed by a Cluster Group made up of representatives from each department that uses the system. The Cluster Group is responsible for managing the common maintenance and enhancement of the core system, although departments can still make their own individual enhancements to the core. The activities of the Cluster Group are generally funded from individual departmental budgets, by contributions from the cluster member departments.

In some cases, government-wide IM/IT initiatives, applying to all departments, are funded centrally. These initiatives are normally administered by TBS, and departments can get access to funding via a Treasury Board submission (as described in the next section) demonstrating how their proposed expenditures meet the objectives of the government-wide initiative. A current example of a government-wide initiative is the Strategic IM/IT Infrastructure (SII) Initiative. This is an interdepartmental program that will design and deliver a common information technology and policy foundation to government departments and agencies. It will act as the backbone for Electronic Service Delivery and will support key service improvement initiatives such as Government On-Line.

Departments receiving funding from Treasury Board Secretariat for IM/IT projects as part of a government-wide initiative are normally required to set up a Memorandum of Understanding (MOU) with TBS, which sets out the objectives of the projects and identifies how project success will be measured. The MOU specifies how often and in what form departments must report back on project progress to TBS, so that the value obtained for the funds disbursed can be monitored.

1.5. *Decisions and Assessment*

It is government policy that all IM/IT and capital projects, with a total estimated cost above the level that the sponsoring Minister of the department concerned can approve, must be approved by Treasury Board (the Committee of Government Ministers set up to review and approve expenditures). This applies even when the project is funded from the department's authorised budget. Approval is sought by the preparation of a Treasury Board Submission, which is thoroughly reviewed by officials in the Treasury Board Secretariat before being submitted to Treasury Board Ministers.

All projects submitted for approval must be supported by documentation that adequately describes the full scope of the project including the associated management framework. All submissions relating to IM/IT are reviewed by the Portfolio Management Division (PMD) of the CIO Branch, in a business-team setting to ensure that they represent an effective and efficient solution to the operational needs as set out in the department's defined priorities or in the Long-term Capital Plan. PMD also reviews compliance with the EMF to help departments and agencies meet their projected budget and scheduled timeframes.

The approval process normally consists of two stages: Preliminary Project Approval (PPA) and Effective Project approval (EPA). Departments normally request PPA when the initial project planning and identification phase is completed but before the project definition phase starts. The formal Treasury Board approval process may be tailored to individual projects and departments, depending on the nature of the risks involved in those projects.

The requirements for PPA are as follows:

- Proposal: It must list all authorities being sought from the Treasury Board, including:
 - the cost objective for the project definition phase.
 - any other objectives deemed to be sufficiently critical to require specific authority by the TB.

Supporting documentation, consisting of the following:

- A background section identifying the program's scope and requirements and providing justification that it relates directly to the department's or agency's goals and responsibilities.
- Indicative budget and total project cost estimates (total cost and annual cash flow) for the overall project.
- An overall project schedule which should provide an estimated schedule of milestones, a work breakdown structure, and a sequential implementation plan for all products/releases.
- The project management approach.
- The Enhanced Management Framework Questionnaire (used to assess that all appropriate elements of the framework have been addressed).
- The Project Charter.
- A Business Case.
- A summary of comprehensive cost-benefit and options analyses.
- A risk assessment and mitigation strategy.
- A Human Resource plan.

- A Communications plan.
- An outstanding issues section.
- Gating of the project (if it is large enough to warrant it).
- Other objectives, such as:
 - Schedule objective
 - Performance objective
 - Procurement strategy.

Under certain circumstances, PPA may be deemed unnecessary. This is acceptable so long as all the conditions required for PPA are met within the EPA submission.

The EPA submission must include the above PPA requirements, and in addition:

- Any updates to the PPA documents.
- Substantive budget and total cost estimates (total cost and annual cash flow) for the overall project.
- Full details of any agreements associated with the project.
- Explanations for any variances between PPA and EPA schedules, costs etc.

After receiving Project Approval, departments have reporting obligations to the Treasury Board Secretariat. These follow the “gating” concept. Gates are significant completion events or quality milestones, placed at key points in the project life cycle. Gates assess either the quality of the products produced so far, or the adequacy and completeness of the process to date, and can only be “passed” if the products or process meet a predefined performance standard. Gates may take the form of technical reviews, risk assessments, completion of documents, demonstrations or test cases, or project audits. Gates are identified in a project’s plan/schedule, and a gate review is required to formally “pass” each gate.

If, at a gate review, the gate’s criteria have not been met, it is possible that a significant change in project direction may be necessary. The project should not continue “as is” unless each gate is passed.

Once projects are completed, audits are normally carried out by departmental review branches, which report directly to senior management. On a government-wide basis, projects of significant scope and/or cost may be reviewed by the Auditor-General of Canada. Large and/or long-term projects may be subject to audits while still in progress.

1.6. Management Models

As is evident from the preceding sections, the central agency (Treasury Board) is responsible for setting overall departmental budgets, approving individual IM/IT projects where they are of sufficient size, and monitoring expenditures and project performance on an overall basis. Otherwise, individual departments are completely responsible for managing their own IM/IT projects. The only exception is in the case of government shared systems, where the departments have established cluster groups to carry out joint management of common system maintenance and enhancement projects.

The Enhanced Management Framework describes a governance structure that is to be used government-wide and by departments to select and manage IM/IT projects. This governance structure satisfies the key factors for project success as identified by the Standish Group research: early agreement on project

requirements; commitment and involvement of the user community; and commitment, attention and decision-making by top executives. A sound governance structure is expected to help government avoid typical project failures.

The EMF governance structure consists of four elements: planning and governance at the portfolio level; a business case; a project charter; and a review schedule tied to gates for each project.

Planning and Governance at the Portfolio Level identifies the organisation's process for selecting, prioritising, and monitoring each project in the context of the organisation's overall objectives and business priorities.

The Business Case puts the investment decision in a strategic context and identifies the business objectives and options that will affect both the decision and the investment itself. It provides the information necessary to decide whether a project should proceed. It provides an analysis of all the costs, benefits and risks associated with a proposed investment and with the reasonable alternatives to the proposed investment.

The Project Charter is a signed agreement between all stakeholders that defines the objectives, roles, responsibilities and level of participation of each stakeholder.

The Review Schedule tied to Gates establishes in the project charter the project review gates, the major decision points of a project – to continue or walk away. For each gate, the deliverables for that review, the type of review, the stakeholders responsible for reviewing each deliverable and the appropriate approval authorities must be defined.

Stakeholders in the governance structure are:

- Business Program executives and Information Technology executives responsible for strategies, priorities, and decisions.
- Business Program managers who implement information technology solutions in their program delivery value chains.
- Information Technology process support teams who provide the common standards and infrastructures for projects.
- Information Technology project teams who need an action-ready project infrastructure so that they can concentrate on delivery of the business solution.

1.6.1. Departmental Management Model

A typical governance organisation structure for a large department comprises a hierarchy of committees and working groups with specific responsibilities. One such department has the following structure.

Information Management Committee (IMC): a committee of Assistant Deputy Ministers responsible for IM/IT project approval and policy setting; reports to the departmental Business Board (the senior decision-making body).

Business, Information and Technology Alignment Sub-Committee (BITASC): a Director General/Director-level committee which identifies business and IM/IT support requirements of the various branches, and is

responsible for ensuring the development of IM/IT plans, policies and practices in support of business and technology integration.

Infrastructure Sub-Committee (ISC): a Director General/Director-level committee responsible for identifying and co-ordinating IT support infrastructure objectives for the department, and assessing impacts of new technology developments/changes.

These committees are supported by a variety of lower-level committees and working groups addressing areas such as the Internet, security, architecture, and office automation.

The use of sub-contract staff on government IM/IT projects is increasingly common, either working in project teams alongside government employees, or independently. It is more and more difficult for departments to retain highly specialised IT staff in the face of strong demand for resources from the private sector. The rapid development of new technologies can render knowledge and experience obsolete after only a short time, and the cost of constant updating of knowledge is high. It is recognised that with outside staff working on the delivery of IM/IT projects, the importance of thorough application of the principles and practices of the Enhanced Management Framework, especially as regards user ownership and involvement, is even more critical.

1.6.2. Central Agency IM/IT Governance

A number of other committees and individuals operate within TBS to give advice and guidance on IM/IT projects.

TIMS (TBSAC Information Management Subcommittee): TIMS is a sub-committee of the Treasury Board Senior Advisory Committee (TBSAC), comprising several Deputy Ministers (heads of government departments). TIMS mandate is to provide leadership in the search for better service to the public and improved productivity through the use of IM/IT. This senior management committee represents the business end-users of information technology, and can ensure that the government's strategies for the deployment of IM/IT (including the EMF) meet government-wide requirements from a business perspective.

Government Chief Information Officer (CIO): The CIO is responsible for determining and implementing a strategy that will accomplish government's IM/IT goals. The role of the CIO includes:

- providing leadership, co-ordination and broad direction in the use of IT.
- facilitating enterprise-wide solutions to horizontal IT issues.
- serving as technology strategist and expert advisor to Treasury Board Ministers and senior officials across government.

ACIM (Advisory Committee on Information Management): ACIM provides advice to the CIO and TIMS on IM/IT issues. ACIM members are heads of IM/IT from large departments. ACIM, chaired by the CIO, provides feedback to the EMF program to ensure that the EMF continues to be aligned with government strategic objectives. ACIM members promote and fund the use of the EMF within their departments.

IMB (Information Management Board): IMB was recently set up by TBS with members from senior management across government. It is chaired by the CIO and has a mandate for making decisions and overseeing the adoption and implementation of a government-wide IM/IT infrastructure. The IMB reviews

and approves proposals from departments seeking central funding for projects that contribute to this objective.

2. CASE STUDIES

2.1. *The 1995 Auditor General's Report*

The first of the cases referred to in this section is the 1995 Report of the Auditor General of Canada, referred to in the first section of this paper. The report was entitled "Systems Under Development – Managing the Risks", and identified some of the problems (and some of the successes) the government had in managing large systems development projects at that time, and presented some recommended solutions. This section covers the major points of the report.

Audit scope

The audit examined four major systems then under development. These systems were chosen for review because: *a)* they were complex, long-term initiatives that would take several years to implement; *b)* they would either affect the infrastructure of government, or have an important impact on the operational capabilities of a department; and *c)* they represented a significant investment on the part of the government.

The findings of the audit were presented under three main headings: project management and monitoring; the nature of large IT projects; and environmental factors.

Project management and monitoring

The audit found a number of management-related weaknesses associated with the introduction of the systems. These were as follows:

- Inadequate analysis of underlying business issues: for example, major projects had been launched without full understanding of the complexity of the business environment, and without resolving the business issues which were the real root cause of the problems the system was intended to solve.
- Inconsistent support from management and project sponsorship: in fact the importance of the project sponsorship role was not widely recognised in government at that time.
- Lack of experience: in all four projects, project teams started out without sufficient experience of projects of similar size and complexity, and in some cases without experience of the associated technologies.
- Inconsistent user involvement and acceptance: in one of the projects, user involvement had been very effective, and as a result there was widespread support for the project among users at all levels. In another project user involvement was less well addressed, and the resulting system ended up with fewer users than expected. Other potential users had not been convinced to convert from their existing systems.

- A lack of effective ongoing monitoring of systems under development: projects were able to produce adequate status data, although this was not always possible right from the start of the project. However issues such as the currency and continued relevance of the business case for the system were not so well monitored.

The nature of large IT projects

The audit noted several factors related to the inherent nature of large multi-year, multi-million dollar information technology projects that influenced the risk of successful implementation. These were as follows:

- Project size: the risk of failure of a systems project increases disproportionately with increased size and complexity of the system. It is important to measure this before development starts. One method is Function Point Analysis. Any system containing more than 5 000 “function points” is considered complex; research had shown that any project of more than 10 000 function points had about a 50% chance of being cancelled before completion. The estimated size of the systems reviewed in the audit was between 14 000 and 16 000 function points (in one case after previous scaling down).
- Technical complexity: One of the four projects was based on a commercial software package. This should have reduced the complexity; however the extent of modification carried out to meet departmental needs significantly increased the complexity. The other three systems were custom-developed and had aspects that were technically very complex.
- Risk associated with uncertainties about functional requirements: in each of the four systems, the functional requirements had been articulated at the time the project had been approved and initiated. However, as all four projects progressed, it became clear that the original requirements needed to be either restated, refined or more clearly communicated. The impact of any uncertainty about requirements affects both project budgeting and project approval: the scope may have to be reduced to stay within budget. It was apparent from the audit that the nature of large, multi-year projects did not allow project sponsors to predict with confidence the ultimate cost of the project.

Environmental factors

The business environment within which the government operates is continuously changing. At the time of the audit, the number of changes and the pace at which they are occurring, both globally and within government, had sometimes outpaced the ability of systems developers to respond to them. The audit identified two key environmental factors, as follows:

- A changing business environment: for each system that was reviewed, the business environment, under which the initial decision to build the system was made, was no longer relevant. It is not possible to successfully implement large systems that take years to develop, in a situation where the business environment is continuously changing.
- Advances in technology: while some of the projects were under way, user expectations expanded dramatically in response to the availability of new and emerging technologies. The developers were not able to keep pace with these growing expectations.

Conclusions and recommendations

The audit identified many factors that affect the successful development and implementation of systems. Those considered among the most critical to the management of risks were:

- effective project sponsorship.
- clearly stated requirements.
- effective user involvement in and commitment to the project.
- the expertise and experience of resources dedicated to the project.

The auditors recommended that an integral component of any new approach must focus on the implementation of long-term information technology strategies through smaller, more manageable components, each of which provided an improved capability (efficiency and/or effectiveness) to the organisation.

Such an approach would provide certain key benefits:

- it would be easier to define more clearly requirements for a smaller component.
- requirements would be less likely to be affected by changes in business environment.
- more complete and accurate estimates of costs and schedules could be provided.
- it would be easier to obtain project resources with appropriate levels of experience.

Follow-up Reports

Since the 1995 report, the Auditor General has continued to review large government IM/IT projects, and has also followed up the status of those projects reviewed previously, as well as tracking the implementation and application of the Enhanced Management Framework. Four more major systems under development were reviewed in 1996, and three in-house projects in 1997. Follow-up reports were published in 1998 and 1999. By 1999, 16 out of 20 large departments had submitted plans to TBS for the implementation of the EMF, and most of the Auditor General's recommendations for corrective actions on individual projects had been acted on.

2.2. *Integrated Resource Management System (IRMS) Program*

The Integrated Resource Management System (IRMS) integrates human resources, finance and material management services for the Canadian House of Commons. Implemented within budget over a 14-month period, IRMS has fundamentally changed the way the House works by providing Members of Parliament and the Administration with single-window Intranet access to enhanced tools, services and information.

Objectives and scope

A 1997 review of the services and systems of the finance, material management and human resources functions of the House of Commons concluded that existing systems were limited in their long-term capability. The seven existing systems were stand-alone and centralised, requiring duplicate data entry and

data reconciliation. The age and limitations of the technology meant that essential requirements could not be met efficiently at reasonable cost.

Management identified the need for a new integrated management system that would: align and streamline finance, material and human resource management services; transform administrative staff from transaction processors to service providers; and provide clients (members and managers) with secure desktop access to timely, accurate and integrated information on budgets, purchases, assets and staff costs, plus information management tools.

The IRMS Program was supported by a sound governance structure led by two project sponsors. From the outset, a key to the program's success has been the active participation of both clients and functional users (*i.e.* management and staff of the finance, material management and human resource functions) in all stages from planning the overall strategy to implementation of sub-projects. More than 200 clients and users participated in extensive consultations, and many performed a variety of roles in individual IRMS projects.

Costs and benefits

IRMS was the largest investment made to date in people, tools and services for members and the institution. The business case projected the total cost to be \$13.6 million over five years. If the cost of maintaining the existing systems (\$5.4 million) is offset, the net new funding required was \$8.2 million. Planned savings were \$2.2 million in administrative costs.

Qualitative benefits delivered to date include: facilitating House-wide information management policy; building linkages between policies and procedures across functions; and making available tombstone information for a corporate web-enabled telephone directory. Members will enjoy single-window Intranet access to frequently used forms, and "next day" budget information. On-line ordering and payment for purchases is the next step.

Critical success factors

The impact of the IRMS program has been far-reaching in its effect on internal policies and procedures. Recognising the potential impact of these changes on people, the program plan set out a comprehensive strategy for managing change. This included targeted communications, training and user support plans. One priority was to provide a seamless transition from old to new with minimal disruption for members.

Management of the program required a special blend of experience and skill. The program was complex, requiring a huge operational transition from old to new systems of financial management, coding and fiscal year reporting. IRMS integrated the services, information systems and cultures of three previously discrete functions, and included many external players.

The governance of IRMS reflected the complexity of this challenge. Initially an *Ad-hoc* team of the House Management Forum was set up. Since then governance has shifted structure and focus to meet the program's evolving needs, from consultation, inclusiveness and dialogue, to the practicalities of implementation.

The responsibility for day-to-day management of IRMS has been shared, reflecting the scope of the challenge. An in-house manager provided essential knowledge about the House, its organisation, key players and management processes, program functions and requirements, while outside consultants offered technical and functional expertise in implementing large-scale systems.

Risk Mitigation Strategy

The IRMS program was regarded as a high-risk project. It involved a significant investment of resources over a number of years; and its scope was virtually unparalleled in the history of the House of Commons. Risk management was an essential component of the management process. The risk management strategy included the following major elements:

- The overall strategy identified risk management as a critical element of the program as a whole as well as for individual projects.
- A formal risk assessment was conducted of the IRMS Software Evaluation Project. It identified approximately 50 program risks, as well as appropriate risk mitigation strategies.
- A comprehensive business case review was undertaken of various options for achieving the objectives of IRMS. The review included a detailed assessment of the risks associated with each of four main options.
- Two Systems Under Development (SUD) reviews of the full IRMS program were conducted: during the planning phase; and during the analysis phase. The objective was to identify potential obstacles to the success of the program. The reviews prioritised risks and proposed appropriate mitigation strategies in four key areas: project management framework; implementation plan; data integrity and security; and change management, communication and organisational readiness.
- A comprehensive evaluation framework ensures ongoing assessment of the IRMS program.

By helping to avert problems before they occur, the risk management approach has resulted in significant savings for the program.

Project management plan

The IRMS management framework was based on the Treasury Board Secretariat's Enhanced Management Framework. The project management framework included detailed project plans, regular progress reporting, well-defined objectives and a formal risk management strategy. A change management process ensured that proposed changes to the IRMS implementation plan had to be documented and reviewed.

The program's governance framework established a clear accountability structure, specifying roles and decision-making responsibilities for each authority level. One of the strengths of the IRMS management plan was its emphasis on "up-front" analysis and planning, and careful review and assessment at key stages during both the planning and implementation phases. Decision-making approaches included the following:

- Development of a business case defining the system requirements and analysing the benefits to members and managers, as well as the risks and costs of four options for addressing current and future service and system needs.
- Analysis of software options including a detailed assessment of costs and benefits associated with suitable commercial software products, evaluation and selection of a systems integrator, and development of an implementation plan and budget.
- Analysis of the fit between the new system and user service requirements to ensure that user interests were identified and represented.
- A roll-out approach to implementation, beginning in functional areas and proceeding to House managers and then to members and their staff.

2.3. *SIGNET Renewal Project*

SIGNET 2000+ is the computing environment that allows the staff of the Department of Foreign Affairs and International Trade (DFAIT) and 11 other departments to exchange messages and access application tools at any of 158 Canadian government offices around the world. Delivered ahead of time and under budget, the success of its development and global deployment is attributable to excellent project planning and management, plus an effective industry/government partnership.

Objectives and scope

Late in 1998, testing confirmed that the existing 16-bit SIGNET platform was not Year 2000 compliant. This mission critical-platform supported all non-classified messaging (about 30 million messages annually) and applications serving some 8 500 users worldwide. The legacy system was no longer supported by the vendor. Quick, effective, and economical design and implementation of a replacement was essential.

Project challenges included:

- The team had 18 months from identification of the problem to select a product, design, develop, test, procure components, and implement the system at 158 locations around the world before the fixed deadline of the Year 2000 transition.
- The nature of business conducted in offices overseas required that SIGNET be updated with minimum disruption to their operations which included presidency of the UN Security Council and the Kosovo crisis.
- The global scale of the system, representation of foreign nationals among both users and technical staff, and mobility of staff in general produced special challenges including: enhanced security; remote administration and user access; single sign-on anywhere in the world; compatibility with data from 1 500 existing applications; training in several languages; and local alphabet support (including Russian, Chinese and Japanese).

Costs and benefits

The project had a budget of \$46 million, including engineering, replacement of 345 servers, client and enterprise software, travel and training. The project was completed four weeks early and \$1.9 million under budget.

The introduction of a standard workstation platform and remote systems maintenance is reducing system operational costs. This is allowing system administrators abroad to expand their user support role, as they have to spend less time on network and server maintenance.

SIGNET 2000+ has increased service availability from 91.8% to 99.5%, which has reduced lost client time by an estimated \$2.7 million annually.

Total productivity increases of \$94 million, mainly from new application functionality, are anticipated over the five-year life of the project. In addition, the productivity deterioration expected if the existing platform was retained for a further five years was even greater than this.

Critical success factors

The success of SIGNET 2000+ was largely attributable to close attention paid to the following factors:

- The imminence of the Year 2000 required careful scope planning, analysis and resolution to meet the stringent schedule and avoid “scope creep”, yet deliver cost-beneficial user functionality.
- Detailed project planning, management and monitoring that included comprehensive and timely procurement, logistics and communications planning and execution.
- Adequate resources of funding, appropriately skilled technical and client staff and facilities identified in the project schedule, requiring considerable attention to resource acquisition and planning early in the project life; where contractors were used, technology transfer from contractors to in-house staff was built in as required.
- Effective quality assurance and control of deliverables, documentation and a formal change management process at all stages of the project to avoid delays or costly retrofits overseas.
- Close consultation with client groups and representatives; and unrelenting communications with the user community to prepare them for change.
- Effective and appropriately timed education for clients and technical training for field technical and support staff including “distance education” for reduced costs and greater flexibility.

Potential risks and risk management

The major risks facing the project were those of schedule: *i.e.* not completing the project before Year 2000. These risks were compounded by procurement risks in the form of three trade tribunal challenges, and the risk of procurement delays which are common in government.

The premium on resources (contractors and hardware) associated with the Year 2000 “crisis” heightened the risk of cost overruns, as did the conflicting demands for resources to continue maintaining the unique but arthritic legacy environment that was no longer supported by the vendor.

There were situational risks such as the intrusion of local and international events into the implementation schedule (for example, UN Security Council activities, Team Canada visits, and the Kosovo crisis), and the risk of losing technical expertise at a time of intense demand for such resources.

There were also technical risks of not being able to solve compatibility and software integration problems, or migrate the myriad of existing applications in use in missions around the world.

To counter these risks, a risk management process was established and rigorously followed, including two independent risk assessments of the project. The component build schedule and QA reports on the build integration tests helped measure earned value, and contingency plans, including “off-ramps”, were prepared.

Project management plan

The management of the project was based on two main sources: Microsoft Solutions Framework, and the Treasury Board Secretariat Enhanced Management Framework (EMF).

From Microsoft the team adopted three main guidelines:

- The project should be a team of peers; project management should stress shared responsibility for the project, with individual accountability for components.
- There must be a strong commitment to good quality management practices.
- The project must employ good internal and external communications.

From the EMF the management team adopted the following:

- Top-down and bottom-up schedule and cost estimation, based on a detailed work breakdown structure.
- Project Charter and integrated project planning system including a basic mechanism for earned value tracking.
- Formal deliverable, schedule and cost tracking and reporting.

The adoption of these guidelines led to a project management team with equal managers for: product and communications; user education; implementation; development and infrastructure; the project office; and quality assurance. They reported to a Project Director, who in turn reported to a Board of IMT Directors chaired by the Department's CIO. The Project Champion was the ADM for corporate services.

Twice weekly "war room" exercises were scheduled, in which any team member could raise any issue they felt was critical. Because senior management always attended the war room meetings, team members had the means of getting quick action on these issues. This increased people's involvement in and commitment to the project.

2.4. *Government of Canada Year 2000 Project*

Objective

The Canadian Government has been investing heavily in building computerised systems to support program and service delivery since the early sixties. Because most systems developed prior to the mid-1990s were designed to use two digits only to identify the year, there was a danger of some government systems failing in the new millennium if they were not corrected or replaced. In addition to fixing the systems problems, many government departments required new contingency plans, testing facilities, and training.

Dimensions

Estimated Year 2000 expenditures in the Canadian Government, as of April 2000, were \$1.9 billion. This consisted of:

- \$1.5 billion for Year 2000 remediation and testing of IT systems.
- \$300 million for contingency planning.
- \$100 million for other specifically funded initiatives. These included monitoring the private sector and other governments, setting up and running the central project office, establishing resource centres for embedded and building systems, contingency planning on a national scale, and communications with the Canadian public.

The scope of the Year 2000 project included:

- Forty-three Government-Wide Mission-Critical (GWMC) functions, delivered by 23 departments.
- Over 10 000 people dedicated to fixing the problem.
- One hundred million lines of code, with more than 1 000 external IT interfaces.
- An estimated 100 000 embedded systems.
- Six thousand buildings across the country.
- Contingency plans in 147 institutions.

Results

The government protected its service delivery capability through the transition period. Departments and agencies ended up with better information about their systems than they had ever had previously, and IT infrastructures were strengthened. Many organisations prepared comprehensive contingency plans for the first time. The partnerships that developed between the central agencies and departments were very effective.

Timeframe

Although some departments had started Year 2000 activities, up until the end of 1997 the Canadian Government had taken only very limited steps to tackle the threat to its IT investments. However during 1998 decisive action was taken to set up a management environment to deal with the issues in a co-ordinated manner. Almost all Government-Wide Mission-Critical systems were remediated and tested by the end of July 1999, and all departmental mission-critical systems well before December 1999, leading to a successful transition into Year 2000. Most departments closed down their Year 2000 projects by March 2000. TBS has maintained a small Post-Year 2000 Office to provide information on the Year 2000 experience and to assess lessons learned for current government IT projects.

Organisation

The Prime Minister of Canada designated four departments to take the lead in preparing for Year 2000. These were National Defence, Foreign Affairs, Industry, and Treasury Board Secretariat. Senior committees at the ministerial and deputy ministerial levels were set up to direct the effort nationally.

The TBS established a Year 2000 Project Office to monitor and report on departmental progress, and to co-ordinate the resolution of horizontal issues affecting all departments. This included the early identification of GWMC functions (those essential to the health, safety, security and economic well-being of Canadians).

Departments were responsible for maintaining their own programs, including the GWMC functions they delivered. They defined their budgets, made the critical business decisions, acquired the resources, managed their projects, and delivered the results. Departments established formal Year 2000 Project Management Offices (PMOs) with clear, department-wide roles, responsibilities and authorities.

Project management

The Year 2000 challenge provided an opportunity for government departments to reinforce, and in some cases to re-establish, a project planning function integrating IT planning into departmental program planning. These PMOs had responsibility for all aspects of Year 2000 remediation and preparation, including contingency planning. In most cases separate budgets were established. In some departments the Year 2000 project office was part of the systems organisation, but in a significant number of cases it was independent, reporting directly at a high level, and emphasizing that this was a business issue, not solely a systems matter.

PMOs had the difficult task of cutting across organisational and regional boundaries to obtain the necessary action. Only the strong support of senior management, and the fixed Year 2000 deadline, allowed them to do this successfully.

As resources and time were both limited, departments adopted a risk management approach, paying attention first to their mission-critical systems, and most vulnerable technologies. For the 23 departments delivering GWMC functions, these were the top priority, followed by department-wide mission-critical (DWMC) systems.

Departments that did not have the organisational capacity to perform the work brought in the specialised skills. All departments made some use of contract staff. They were able to utilise fast-track procurement mechanisms put in place by government purchasing authorities to expedite the work.

A focus on business continuity required Year 2000 project teams to extend their views beyond IT and address the broader issues of logistical support for program delivery, including supply chains, utility supplies, building and other embedded systems, and contingency planning. Some departments developed comprehensive contingency plans for the first time during the run-up to Year 2000.

Central Year 2000 project reporting was orchestrated by the Treasury Board Secretariat Year 2000 Project Office; this ensured timely monitoring and reporting of results. Departments were also encouraged to conduct independent reviews of their Year 2000 programs, and all the GWMC departments carried out at least one independent review or audit. Furthermore, most departments put in place ongoing review programs that continued until the Year 2000 project was completed.

To prepare for the transition, most departments instituted a freeze on all except essential system changes during the latter part of 1999. After the transition, all departments went through a formal project close-down phase, which often included an assessment of lessons learned.

Critical Success Factors

Factors that were seen as critical to the success of the Year 2000 initiative were:

- The declaration of Year 2000 as a government imperative established it as a clear priority for government departments.
- Establishing Deputy Minister accountability ensured management commitment at the most senior levels, and provided the context and requirements for the creation of a governance structure (*e.g.* committees and working groups) with roles and responsibilities that would deliver the results.
- The adoption of a risk focus reinforced the first two items and provided a mechanism for determining mission-critical business functions, a context for decision making and issues management, and the framework for the development of a robust set of business continuity plans.
- The results of these three items enabled the initiative to proceed and provided for the funding, disciplined use of project management, the creation of partnerships, and many other support elements.
- Performance management, through very visible reporting mechanisms and monitoring at senior levels within departments and across government, was an essential tool for ensuring progress and establishing credibility for government-wide initiatives.
- The control loop in this chain of events was provided by the public visibility that was accorded to Year 2000 through extensive communications and formalised monitoring and reporting.

- The influence and efforts of individual people over the life of the project significantly influenced the direction and outcome of the initiative.
- The establishment of PMOffices provided effective oversight and management.

3. LESSONS LEARNED

This section describes lessons learned from the cases featured in this report and is presented in two categories: government-wide lessons learned, and lessons learned at the level of the individual organisation or project.

3.1. *Lessons Learned at Government Level*

Government-wide projects should:

- fit within a clearly expressed strategic plan for government investment in technology.
- be joint-venture partnerships between the central agencies and the departments and not the exclusive domain of one or the other.
- be driven by a clear risk and opportunity assessment supported by the program and service delivery community within government.
- be sustained by the highest executive and political management.
- be adequately funded.
- be monitored and measured by precise, pre-defined and negotiated reporting requirements.

Business alignment

- Business should be engaged right from the start of large IT projects. The project needs to be aligned with, and support, the business directions and priorities.
- Planning for information technology investment must be fully integrated with the business/program objectives and planning processes of an organisation.

Governance

- Establishing the initiative as a government priority is fundamental to success.
- Establishing Deputy Ministers' (DM) Accountability as a subsequent step ensures management commitment and decision-making at the most senior levels. It provides governance structures (*e.g.* increased role of the TIMS sub-committee of DMs, other special committees and working groups) across the government, and the hierarchical set of roles and responsibilities that delivers results.
- Clear accountabilities and decision-making authority should be defined at all levels for all stakeholders. Appropriate frameworks should be established to ensure that if problems cannot be resolved promptly, they are referred to the appropriate higher level of resolution.

Role of central agency (Treasury Board Secretariat)

- Large, complex multi-organisational government initiatives are most effectively managed through a collaborative effort that focuses responsibility for end results on departments; the central agency provides facilitation, co-ordination and monitoring.
- Strategic interventions (“swat” type actions) provide valuable opportunities to resolve issues.
- Accountabilities and responsibilities between central agencies and groups should be clearly communicated to departments.
- Policy direction must be more flexible and accompanied by appropriate supportive guidelines and mechanisms.
- Further efforts should be made to entrench and institutionalise the EMF in all departments and agencies.

Risk management

- A continued focus on risk in planning and carrying out the initiative provides a critical context for identifying and managing concerns and potential issues.
- Risk management initiatives for government-wide use in major initiatives needs to be timely and directed to meeting the needs of departments with varied levels of experience in risk management.
- Risk management methodologies and techniques should be adapted to the initiatives. The adaptation of the risk management methodology to the Year 2000 project, which was made available as part of the EMF set of guidelines, was useful. However, the ease of implementation varied across departments and in some cases was dependent upon the availability and skilled resources.

Performance management

- A very visible reporting and central agency monitoring is an essential tool in ensuring that progress is achieved and maintained, and credibility for the whole endeavour established.
- Reporting processes need to be simple and timely.

Communications

- Creation of a formal communication strategy and plan is essential.
- Effective communications are more complex to establish and more difficult to maintain than expected.
- All opportunities and possible vehicles for communicating must be utilised.

Procurement

- Government-wide Standing Offers continue to provide an appropriate and expedient vehicle for obtaining professional services.
- Standing Offers need to be in place as early as possible in order to be effective and need to be more flexible in order to cope with changing situations.

- Departments need to be fully cognisant of the contract selection process and contract content in order to maximise their utilisation of these vehicles.

3.2. *Lessons Learned at Organisation/Project Level*

They are presented roughly in chronological order as they apply during the life of an IT project.

Business alignment

- The alignment of the objectives of a project with business goals should be expressed in the form of a business case, which supports the investment decision. The business case puts the investment decision in a strategic context, providing an analysis of all the costs, benefits and risks associated with a proposed investment, and reasonable alternatives.

Senior management commitment and involvement

- Involvement and commitment of senior program/business management to a large IT initiative at an early stage is essential.
- A “project sponsor” should be identified, preferably a senior official responsible for the business function the project will support. An effective project sponsor ensures that the organisation understands the value and importance of the project, and is ultimately responsible for realising the expected benefits of the project.
- Solid senior management support is demonstrated through the provision of adequate financial and human resources, and active participation in project governance.

Project governance

- Project governance should reflect the complexity of the challenge, and change as the project commences. Typically it will start with a senior management committee. From then on governance should shift structure and focus to meet the program’s evolving needs, from consultation, inclusiveness and dialogue, to the practicalities of implementation.

Project Management Office (PMO)

- The creation and use of a Project Management Office (PMO) significantly improves chances of success in the project endeavour. The PMO’s role is to facilitate, co-ordinate and monitor ongoing activities.
- A central PMO in an organisation can manage portfolios of projects, provide effective project oversight, and act as a source of expertise and support to individual projects.

Project planning

- A Project Charter should be the first step in project planning, once the business case has been developed and the investment decision taken. The Project Charter is an agreement between the technical groups providing the product or service, and the business organisation requesting and receiving the project deliverable.

- The Project Charter is a tool to obtain commitment from all affected groups and individuals within a specific project, and also a communication vehicle that can be referenced throughout the project. It acts as a quick reference and overview of what the project is about, why it is being conducted, who is involved and in what capacity, and the general approach and timeframe that exists for the project.
- Project planning should include top-down and bottom-up schedule and cost estimation, based on a detailed work breakdown structure. Detailed project planning will provide clear definition and documentation of the project. It will encompass management structures, monitoring mechanisms, comprehensive and timely procurement plans, logistics and communications planning.
- Careful scope planning, analysis and resolution are necessary to meet project schedules and deliver cost-beneficial user functionality while avoiding “scope creep”.

Project resources

- The responsibility for day-to-day management of a project can effectively be shared between in-house and contracted resources. Core project management responsibilities and functions should not be outsourced. An internal manager provides essential knowledge about the organisation, its key players and management processes, program functions and requirements, while outside consultants offer technical and functional expertise in developing and implementing systems.
- To be successful a project requires adequate resources of funding, trained staff and facilities. This requires considerable attention to resource identification, acquisition and planning early in the project life.
- The right mix of resources will involve program and information systems staff. The team should ideally include experienced and knowledgeable departmental staff from both the program and systems disciplines. If outside technical resources are needed, they should be used strategically to supplement staff skills. A requirement for technology transfer from contractors to in-house staff should be agreed from the start.
- Including systems management, design and architecture staff very early in the analysis of business processes and development of user requirements gives them a better understanding of business needs.
- Risk management approach
- A risk-based process has been found very effective for determining departmental priorities and identifying mission-critical functions.
- The chances of project success are measurably improved if risk management techniques are performed on a continuous basis. Formal risk assessments at key points during the development life cycle can identify potential problem areas and suggest preventive action.
- Risk management for a project can start at the business case stage, with a review of the options for achieving the required business objective, and an assessment of their risks.
- A risk assessment performed early in the development process can identify exposures against which contingency plans can be prepared, including “off-ramps” and alternative delivery strategies.

Phased approach

- The recommended approach to the implementation of long-term information technology strategies is through small, manageable components, each of which provides an improved capability (efficiency and/or effectiveness) to the organisation. Such an approach provides certain key benefits:
 - it is easier to define requirements more clearly for a smaller component.

- requirements are less likely to be affected by changes in business environment.
- more complete and accurate estimates of costs and schedules can be developed.
- it is easier to obtain project resources with appropriate levels of experience.
- Systems development should be done in well-scoped phases. The use of Function Point Analysis can eliminate guesswork in managing the scope of work that can reasonably be completed within the established timeframe.
- Careful selection of achievable objectives for each phase, with diligent adherence to these objectives, keeps the development package stable; scope creep can be minimised.

Co-location

- Wherever possible, all project staff should be co-located to ensure rapid and accurate communication and information exchange. This includes program and information systems staff, in-house and consultant resources.

Involvement of users

- Project management and communications should involve functional and end-users from as early as possible. Close consultation with client groups and representatives helps build ownership and commitment. Extensive user participation in systems development and testing is essential for a viable end product.

Performance measurement and reporting

- Achievement of project deliverables and schedules should be measured by a precise, pre-defined, and regular monitoring and reporting process. This should be established at the earliest possible stage in project start-up.
- Open and visible tabling of project status information at senior management committees on a regular basis focuses everyone's attention, and ensures continued management support.

Scope management

- A formal change management process, together with effective quality assurance and control of deliverables and documentation at all stages of a project can help avoid scope creep.
- Involvement of business and user staff, leading to a thorough understanding of the links between project quality, schedule and cost, can also reduce pressures to expand the scope of a project. Careful selection of achievable objectives for each phase, agreed to by all parties, with diligent adherence to these objectives, enables a stable development environment to be maintained.

Communications and training

- Establish appropriate logs to document and communicate decisions, changes, issues and problems etc. to all project team members.

- IT initiatives must recognise their potential impact on people and their jobs. A comprehensive strategy for managing change should be part of project planning. This will include targeted communications, training and user support plans.
- All opportunities and possible vehicles for communicating, both internally and externally, must be utilised in order to prepare the user community and other stakeholders for change. Ideally the project team should include one or more communications specialists.
- Project planning should reflect the need for effective and appropriately timed education and training for users, and technical training for technical and support staff. All means of training should be investigated as appropriate, including computer-based or internet “distance education” where staff are geographically dispersed, for reduced costs and greater flexibility.

Independent reviews

The use of independent reviews at key stages of a project’s life cycle can provide an extremely valuable snapshot of the “health” of the initiative. Experienced but independent observers with no stake in the project can identify issues that need to be addressed, but which might not be visible to project staff in the heat of the action.

4. REFERENCES

Enhanced Management Framework for IM/IT

http://www.cio-dpi.gc.ca/emf/EMFIndex_e.html

Creating and Using a Business Case for Information Technology Projects

http://www.cio-dpi.gc.ca/emf/Publications/Publication2/businesscase_e.html

Benefits Driven Procurement

http://www.cio-dpi.gc.ca/emf/Solutions/Procurement/Procurement_e.html

Treasury Board Project Approval Process

http://www.cio-dpi.gc.ca/emf/handbook/tbProjects/tb_ov.html

IM/IT Investment Evaluation Guide

http://www.cio-dpi.gc.ca/emf/solutions/InvEvalGuide/Invest_Eval_Splash_e.html

Risk Management

http://www.cio-dpi.gc.ca/emf/solutions/riskmgmt/RiskManagement_e.html

Project Charter Guide

http://www.cio-dpi.gc.ca/emf/solutions/ProjectCharterGuide/CharterGuide_e.html

Assessment Tools and Methodologies

http://www.cio-dpi.gc.ca/emf/solutions/MethodologiesTools/AssessMethodSplash_e.html

Improving Key Best Practices

<http://www.cio-dpi.gc.ca/emf/solutions/KeyProjectPractices/KeyPracticesSplash.html>

IT Project Managers Handbook

http://www.cio-dpi.gc.ca/emf/handbook/handbook_e.html

PUMA/SBO/RD(2001)1

Software and Project Management Tools

http://www.cio-dpi.gc.ca/emf/solutions/softools/toolsreport_e.html

Project Management Training and Development

http://www.cio-dpi.gc.ca/emf/solutions/PMTrainDev/TrainingDevelopment_e.html

Project Planning, Tracking and Oversight

http://www.cio-dpi.gc.ca/emf/Documents/ppto-gtpss/pptolinks-liensgtpss_e.html

AUDITOR GENERAL REPORTS

<http://www.oag-bvg.gc.ca/domino/reports.nsf/html/9932ce.html#0.2.2Z141Z1.AX4M0M.WAO5LF.II>

<http://www.oag-bvg.gc.ca/domino/reports.nsf/html/mp9723e.html>

<http://www.oag-bvg.gc.ca/domino/reports.nsf/html/9828ce.html#0.2.2Z141Z1.U7BWII.YSCO2F.PD>

<http://www.oag-bvg.gc.ca/domino/reports.nsf/html/9624ce.html>

DENMARK

1. GENERAL INSTITUTIONAL FRAMEWORK

1.1. POLICY

The Danish Government Administration consists of 20 ministries. The ministries are in many respects autonomous units headed by a minister responsible only to the Parliament. Most ministries have a small department serving the minister and a number of agencies responsible for specific tasks. The Budget is allocated by the Ministry of Finance.

There is no national policy for management of large projects. Until 1992 the Ministry of Finance played a regulatory role. All projects with a budget of over 5 million DKK (0.7 million USD) had to be approved.

From 1992 the responsibility was decentralised to the ministries and agencies. Today IT is a management responsibility in line with management responsibilities in other areas.

1.2. *National IT Policy*

Since 1995 the Government has issued a national IT Plan of Action. This plan defines the government objectives on use of IT, and describes a wide range of IT-related activities both in the public and private sectors.

The objectives for the public sector institutions are efficiency, and new and better services to companies and citizens.

The plans have initiated a few cross-government activities: use of e-mail, homepage with access to public sector information and self service.

In many areas Denmark developed e-Government before e-Government was invented:

- Common identifier for the citizens used in all public sector systems.
- An almost fully automated tax system, where more than 80 per cent of the citizens receive a tax-return statement with most information collected and filled in on behalf of the citizen.
- 98 per cent of all payments from the public sector are paid electronically to the receiver's bank account.
- Shared accounting system, budget system and payroll system used in all government institutions. Operated by the Ministry of Finance.
- Network and PC-workstations in all government institutions.

1.3. Funding

In 1986 Denmark introduced a budget reform covering all government institutions. Within the allocated budget the management in the single institution was given several degrees of freedom: surplus (savings) on the budget in one year can be transferred to the following year; savings on one budget account can be spent for other purposes.

Minor IT projects are often financed through savings and reallocation inside the allocated budget.

Major IT projects have their own budget line, either allocated as part of new legislation or through the normal budget procedure. The budget for major IT projects (over 10 million DKK/1.4 million USD) needs specific approval in the Parliament's Budgetary Committee.

Extra budget for a major IT project also needs approval in the Parliament's Budgetary Committee.

1.4. Decisions and assessment

It is a management responsibility in the single organisation to prepare and decide on IT projects. Major projects are often prepared and evaluated in co-operation with the management in the departments of the ministry.

The normal life cycle of a project involves these elements:

- A feasibility study is prepared in a small project group, often assisted by external consultants. This study documents possible solutions, benefits, estimated costs and project plans. There is only limited focus on risks at this stage of the project.
- Management decision on project and appointment of project manager and project organisation. Budget is allocated.
- The project reports to a steering group chaired by the management.
- Preparation of documentation for procurement including functional requirements. External private consultants are normally involved in these activities.
- Procurement following the EU rules.
- Contract is agreed with one vendor. A "government" standard contract was developed 10 years ago, stating the responsibilities of the supplier and of the customer and the project organisation. The basic principle is that the vendor has full responsibility for most of the project activities. The contract normally specifies a fixed price and schedules for delivery. Risks are not normally an element in the contract.
- The contract specifies co-operation and co-ordination between the customer project manager and the vendor project manager.
- The project management reports to a steering group with representation from customer and vendor management.

There is no agency or other public authority involved in assessing the IT projects. In 1992 it was decided that IT projects are a decentralised responsibility. It was also decided that private sector consultants could provide the necessary specialist knowledge.

There are no formal requirements or tradition on measuring promised benefits or financial auditing of IT projects.

This type of follow-up is considered part of the management responsibility in the single organisation.

1.5. Management models

Since 1992 there has been no central agency responsible for government IT procurement.

Because of problems with several large IT projects, and a common recognition of the lack of cross-government exchange of experiences on IT projects, the Government IT Council was established in June 2000. All ministries are represented at management level in the Council. The Director of IT and Telecom in the Ministry of Research and IT chairs the Council.

The Council shall focus on issues related to IT in government including both management issues and organisational and technical issues. A permanent workgroup of IT managers -- the Government IT Forum - shall work on technical issues and issues related to procurement and project management.

2. Cases

The National Auditors have a survey of major IT projects in the Government Administration.

124 projects, each with a budget over 2 million DKK (0,3 million USD), were included. The total budget of these 124 projects was 4 500 million DKK (700 million USD) giving an average of 37 million DKK (5 million USD) per project.

The survey documents that only 18 projects were conducted according to budget and plans for delivery. Another 18 projects are expected to be finalised according to defined plans. These 36 projects represent about 30 per cent of the projects and 40 per cent of the involved budget.

Eighty-eight projects had delays and required extra budget. The delay was on average 9 months or 50 per cent of the planned time for delivery. The requirement for extra budget was on average 33 per cent of the planned budget.

3. Lessons Learned

The report from the National Auditors gives these recommendations:

1. Management attention and involvement is needed.
2. Clearer definition of responsibilities and competencies is required.
3. The feasibility study must be more detailed and cover more subjects.
4. Large projects should be avoided. Divide into separate phases.
5. Evaluate the vendors more thoroughly before concluding a contract.
6. Evaluate the needs for organisational changes as a consequence of the project.
7. The contract must be clear and unambiguous.
8. Quality assurance should be an integrated part of the project.
9. Greater attention to and critical evaluation of new requirements introduced during the project.
10. Critical evaluation of the project experiences during the project. Dissemination of experiences.

In addition to these recommendations the following observations from the general debate can be mentioned:

- There is a lack of “Project culture” in many private and public organisations. Project culture involves teamwork, management support, project managers combining experience of running a project and knowledge of the organisation, and a reward structure which relates to obtained results. Both public and private organisations have a critical view of the vendors. They are very focused on winning a contract, but they focus less on delays and bad quality. Too often, they leave their customers with serious errors and problems in new systems.
- The EU rules on public procurement are difficult to apply to IT projects. They do not allow consultations with vendors in the preparation phase. Nor can one evaluate and make changes in the proposed solution from the vendor. The procurement process is time and resource consuming. It is difficult to procure a project divided into phases. There is a risk that the technology involved becomes obsolete because of the lack of flexibility in the rules.
- Private consultants are often very involved in a project. Do they have the necessary experience and knowledge?
- The Government administration does not utilise the experience from similar projects.

4. Literature, WWW and studies

Most information is only available in Danish. The most relevant publication is: *Beretning om gennemførelse af statslige edb-projekter. Published by the Parliament (www.folketinget.dk).*

FINLAND

1. GENERAL INSTITUTIONAL FRAMEWORK

1.1. Policy

National policy for management of large IT projects

There is no formal policy at the moment. Government decree on information management from 1988 states that large projects must be presented to the Ministry of Finance, as well as all projects that affect other ministries and agencies. The decree has been considered out-of-date due to changes in general steering systems and formal consultations have not been conducted for several years.

Most of the large projects involve partners from other agencies who have data interchange needs with the function under development. The normal procedure to involve partners is direct consultation. Hearings and information days are also used. And it is common to invite partners to participate in the project management committee.

The Ministry of Finance has published contract terms for public sector ICT procurement. These terms and the associated procurement guidance is to help agencies maintain life-long control over the projects.

National IT policy

In May 1994 Council of State decided on a strategy for information management in government. This called for electronic transactions within agencies as well as between agencies and customers.

The Finnish Government prepared the national information society strategy in 1994–95. In 1998 a national strategy was published by the Sitra Foundation for developing the Finnish information society, called “Quality of life, knowledge and competitiveness” (see <http://www.sitra.fi/tietoyhteiskunta/>). Both of these strategies include sections on improving public services with ICT.

The Ministry of Education has a development plan for education and research. The strategy includes eight different project plans: information society skills for all; training for teaching staff; training for IT industry; for digital information professionals; the virtual university; the virtual school; learning environments on the information network; and content production.

The Government Programme

The focus in the information society is evolving towards the development and production of content-based applications and services. The programme of the present Finnish Government encourages, for example, the further development of electronic services and of cultural and informational content that is easy to use, safe and available to everyone. The Information Society Advisory Board which is co-ordinated in the Public Management Department of the Ministry of Finance, follows the progress of the information society and reports to the Government. The first report will be available shortly on the Ministry of Finance website (<http://www.vn.fi/vm>).

The government strategic project portfolio has three information society projects. One of them is e-Government. In May 2000 Council of State made a decision-in-principle on the use of funds from the sale of state-owned companies. One of the seven parts of the decision is improving public services using ICT. Social and medical services get 10 million Euro, content production 7 million Euro, and transport telematics 10 million Euro. Joint network services, information security, development of electronic procurement and improvement of access to public sector information get 7 million Euro extra funding in 2001–03.

Government decisions on information management

The previous Government has put into effect (5 February 1998) a decision on electronic transactions, development of services and reduction of data-gathering (<http://www.vn.fi/vm/kehittaminen/tietoturvaluus/hst/hsteng.htm>).

The decision states, among other things, that “The Population Register Centre shall be nominated as the certification authority responsible for issuing and maintaining the citizen ID card. Other necessary Public Key Infrastructure services will be created. Ministries and agencies will see to it that information on the central services provided for citizens, companies and communities as well as the forms requested by them are available on the Internet and will ensure that a significant proportion of application forms and requests can be instituted electronically by the year 2001.” The costs of data-gathering must be reduced.

According to the decision-in-principle of 5 February 1998, the following infrastructure elements have been implemented:

- Certification authority and certification services (Population Register Centre).
- Citizen identity card has been available since December 1999.
- The Act on electronic transactions with administration was accepted at the beginning of this year.
- The X.500/LDAP directory on electronic addresses in government has been available for one year (<http://www.julha.fi>).

On 2 March 2000 Council of State made a decision-in-principle on information management. The decision puts special emphasis on development of interoperability, joint services and co-operation between agencies on IM. The decision is available at http://www.vn.fi/vm/english/public_management/it.htm.

On 11 November 1999 Government made a decision-in-principle on information security. See: <http://www.vn.fi/vm/kehittaminen/tietoturvaluus/vahti/vahti.htm> (Finnish and Swedish only).

1.2. Funding

Ministries and agencies with the exception of net-budgeted agencies fund their IT investments from the allocation they get for operating expenses. Net-budgeted agencies have more flexibility as they can use part of their profit for investment.

It is possible to get a temporary rise in an agency’s budget for operational costs in the case of a large IT investment. The number of such cases per year is limited, less than 10. These requests are evaluated case by case and generally the better argued and more important projects have received extra funding. A typical case is the introduction of Euro which forces some agencies (Customs, Tax, and Statistics) to make big changes in practically all systems in use.

There is no possibility of an agency borrowing money for IT investments. In some cases lack of funding has led agencies to lease equipment in order to implement their new system.

Generally agencies try to keep their IT budget constant, making investments gradually and avoiding big variations in the level of investment.

1.3. *Decisions and assessment*

The management of the agency or ministry, according to their internal procedures, makes procurement decisions. There is an "IT Steering" body for consultation on IT/IM strategy and projects, but the decisions are always made by management. Procurement decisions are made according to rules of public procurement. Risk analysis *ex ante* is one part of project specifications and tender evaluations.

There is no special agency for evaluations. External auditing is done by State Auditing Office. SAO has been under the Ministry of Finance, but from 2001 will be under the Parliament. SAO has some auditors who specialise in IM. Internally projects are evaluated systematically in some but not all agencies. Some large agencies (*e.g.* tax administration) employ professionals who evaluate and audit IT systems development.

1.4. *Management models*

In Finland agencies are relatively independent. Every year the ministry makes results agreements with its agencies. The key targets are presented in budget proposal. In results agreements targets are usually somewhat more precise and operational. The ministry normally reviews progress with the agency twice a year.

The steering model puts emphasis on results and leaves the means to be decided by the agency. Key IT projects are on the agenda in result negotiations because extra funding is often needed. Outside these discussions ministries do not usually become involved in projects.

Large IT projects are the responsibility of the units who own the substance to be developed. The unit is responsible for systems analysis, application development, and finally, user training. The internal IT unit acts as an internal consultant to the substance unit and is responsible for technology.

Large projects normally have a steering committee and a number of task-specific working groups. These usually consist of the agency's personnel at various levels (substance, IT, end-users) but in cases where the system has many links to the outside, people from these stakeholders are invited to the steering committee. In this type of project stakeholders are also consulted before and during the project.

Political involvement in projects is rare. In some cases changes in legislation are needed and then the project is discussed at some level in Parliament.

Modularisation of projects is becoming more common as technology better supports it. The other reason for trying to avoid huge projects is the financing model that supports gradual upgrades with even expenditure rather than yearly fluctuations.

Systems development (planning, implementation and maintenance) is mainly outsourced. The following chart shows the division of systems development costs in 1999. In-house work is mainly devoted to systems design, testing and training. Only one major agency (environment) does most of its systems development in-house.

2. LESSONS LEARNED

Success factors

- Project management competence of the agency is clearly the most critical. Most other factors are directly linked to this.
- Management involvement.
- IM and ICT competence of the agency is crucial as it must make architectural decisions and technological choices.
- End-user involvement in systems planning.
- Well-planned and organised implementation and end-user training.

Factors for failure:

- Relying too heavily on suppliers due to weak internal resources seems to lead to extra costs and delays.
- Certain technology (e.g. two-tier client-server) has caused nasty surprises, as the need for bandwidth and PC capacity has been much higher than estimated. In some cases there have been delays in implementation, as the agency had not had funds for upgrades. Today 3-tier architecture is more widely used and most agencies prefer to build clients on web-browser.
- Use of unproven technology has led to problems in some cases. It is clear that agencies try to build new systems on modern technology, but suppliers have a tendency to sell too much in advance and agencies do not always have the skills to evaluate proposals adequately.
- Lack of involvement by management leads to problems in funding and implementation.
- End-user training is sometimes neglected, creating problems in customer service when the new system is implemented.

3. LITERATURE, WWW AND STUDIES

Information is available only in Finnish.

The Ministry of Finance report on use of Information Technology in Government gives an overview at: <http://www.vn.fi/vm/kehittaminen/tietohallinto/1999/index.htm>.

The Information Society Advisory Board has produced a report on Finland as an information society (http://www.vn.fi/vm/english/public_management/index.html). Chapter 7 includes information on some large public sector projects.

The Ministry of Finance published a report in March 2000 on service development projects. This is available in Finnish at http://www.vn.fi/vm/kehittaminen/julkisten_palvelujen_kehittaminen/hko23.htm.

FRANCE

INTRODUCTION

This report describes a number of practices followed and lessons learned by the French administration in the management, follow-up and monitoring of large public sector information technology (IT) projects. The format of the paper, prepared for an OECD expert seminar, conforms to the approach outlined for this international meeting.

Monitoring and follow-up practices implemented by institutional structures other than the administration paying for the project are dealt with in section 1 of the report, which covers the institutional context and appear in the chronological order of their involvement in a project. This review starts by looking at the factors influencing major government thinking on IT matters and closes with monitoring after the event by the *Cour des Comptes* (Government Audit Office).

In-house practices in project implementation are illustrated by two case studies of projects currently underway at the Ministry of Justice, which are further examined in the section on lessons learned, together with a number of reflections on criteria for evaluating information systems and the factors making for success in large IT projects.

The final section refers the reader to a number of public information documents on IT matters and the Internet sites from which information on IT work in progress in the French administration can be obtained.

In conclusion, the Annex contains a number of information sheets on the institutional bodies involved in the follow-up and monitoring of large IT projects.

1. THE INSTITUTIONAL CONTEXT

Management and follow-up of large public sector IT projects follows a well-defined institutional path made up of four main sections, two associated with determining the main lines of action and two concerned with monitoring. The lines of action initially concern functional and organisational aspects and then move on to technical implementation. Monitoring, some in the ex-ante phases and some in the ex-post phases, is budgetary and legal in nature. Co-ordination of the work of the various participants in these operations and consistency in decision making are essential to the success of public sector projects, but are not always a foregone conclusion in practice.

Although government policy determines the overall framework governing the development and modernisation of information systems in the administrative services, the ministries continue to be the driving force in the workings of the French administration.

1.1. *The main lines of government policy*

Major government initiatives generally originate from the office of the Prime Minister, who orchestrates formation of French government policy, the Ministry of the Civil Service and Administrative Reform, whose responsibilities by their nature cut across those of the other ministries, and the Secretariat of State for the Budget (Ministry of Economic Affairs, Finance and Industry), which deals with aspects relating to scrutiny of expenditure.

Members of the government may order general strategic studies, as for example on developments related to new information technologies. To this end they have the option of setting up a (parliamentary) task force or referring the matter to administrative authorities or independent bodies with known expertise in the area. The General Council on Information Technologies (*Conseil Général des Technologies de l'Information - CGTI*: see Information Sheet No.1) is involved here by providing specialists in the NTIC (Nouvelles technologies de l'information et de la communication) to give in-house expert and strategic advice to an administration.

The introduction of large IT projects within the state sector increasingly goes hand in hand not only with administrative reform but also with the building of an information society at both national and international level.

A new political boost was given to information technologies in early 1998 by the Government Plan of Action to bring France into the Information Society (*Plan d'Action Gouvernementale pour l'entrée de la France dans la Société de l'Information - PAGSI*). The Plan identifies six national priority areas of action. The one covered in its section 3 focuses specifically on modernisation of public sector services. Two other sections also target the state sector services by means of recommendations relating to the school system and cultural matters.

The provisional subsidiary measures and associated budgetary action entailed by the Plan of Action are approved by special interministerial committees that meet at regular intervals:

- The Interministerial Committee on Administrative Reform (*Comité Interministériel pour la Réforme de l'Etat - CIRE*) dealing with PAGSI section 3 (on 13 July 1999 and on 12 October 2000, fifth edition)
- The Interministerial Committee for the Information Society (*Comité Interministériel pour la Société de l'Information - CISI*) dealing with the other PAGSI sections (on 19 January 1999 and 10 July 2000, third edition).

The major policy thrusts and the impetus given to NTICs follow the same line of thinking as the European e-Europe Plan of Action, to the preparation of which France was a major contributor.

Prior identification and simplification of current administrative pathways and procedures are essential to the introduction of information technology. The Administrative Simplification Commission (*Commission de Simplification Administrative - COSA*) set up in December 1998 to replace Cosiform responds to that need and reflects the French Government's determination to improve the quality and efficiency of the public service and simplify its relations with its users through the introduction of teleprocedures.

Finally, a Committee on Information Technology Strategy (*Comité Stratégique des Technologies de l'Information - CSTI*) reporting to the Prime Minister and composed of leading figures in business and research is in the process of being set up with the task of providing the government with recommendations on innovation, research and development.

1.2. Ministerial involvement

A government decree of December 1986 in conjunction with three prime ministerial circulars (October 1987, February 1994 and September 1996) established the current framework for bringing IT into the administrative services. Ministers are responsible for the introduction of information technology in their ministries and are free to decide the pathway this should take. They are, however, expected to prepare an

information technology development plan (*schéma directeur informatique* - SDI) covering a three- to five-year period for submission to an interministerial government committee that will report its findings to the Prime Minister. The only areas of administration exempt from this procedure are those governed by state secrecy measures.

Information technology development plans

The plan must be in two sections, one devoted to strategy and the other to operational matters. Ministries are provided with a specimen plan, which is nevertheless in flexible enough format to be adaptable to the special needs of the various administrations.

The circular letter of September 1996 represented a major step forward in attitudes to IT as it specifically extended the area to be covered by information technology development plans from data processing to information systems. The circular took note of the thrust of the policies CIRE had issued on 29 May 1996 and directly linked the introduction of information technology to the process of structural and procedural reform underway in each administration. It also pinpointed the requirements for IT policy management.

Modernisation programmes covering a period of several years (programme pluriannuel de modernisation - PPM)

The Prime Minister's circular letter of 3 June 1998 made it incumbent on ministries, in conjunction with the Minister for the Civil Service and Administrative Reform and the Secretary of State for the Budget, to draw up modernisation programmes for implementation periods of three to five years. The programmes were to be drawn up in five sections, one dealing with the introduction of NTICs as part of administrative modernisation. In this context, the circular set a number of priorities including digitalisation, making public sector information available on-line and elimination of paper-based procedures.

Ministerial Plans of Action for the Information Society (Plan d'Action Ministériel pour la Société de l'Information - PAMSI)

The Government Plan of Action (PAGSI) prepared in early 1998 provided that each ministry should have a version applicable to its sector for general publication, which was expected to demonstrate the contribution information and communication technologies would make to modernising the ministry concerned and improving its relations with its users, both individuals and businesses.

The Interministerial Delegation for Administrative Reform (*Délégation interministérielle à la réforme de l'Etat* - DIRE: see Information Sheet No.6) is the administrative body responsible for these plans. A larger group forming a technical validation committee includes the Budget Directorate (see Information sheet No.7), the Central Tender Commission (see Information Sheet No.4) and the Secretariat of State for Industry (Digitip for technical validation). DIRE is also responsible for preparing summaries of ministerial policies and of work done by the ministries.

Work on modernising the various ministries is co-ordinated by working groups and think-tanks set up under DIRE auspices deal with the functional and organisational aspects of modernisation. In particular, DIRE arranges periodic meeting of Senior Officials for Modernisation, who are representatives appointed by each ministerial department.

The requirement for strategic plans spanning a period of several years should give administrations the opportunity to step back for a long look at the changes their duties and services call for. Although this task

represents a heavy burden for administrative departments, as major players in the process of change it is essential that they play an active part and refrain from entrusting the task to outside groups far removed from the day-to-day realities of the service, which would inevitably give the plans a purely intellectual and theoretical aspect unsuited to bringing about change. Continuing efforts must be made to co-ordinate strategic planning exercises if the administrative system is to meet its goals.

In addition to these functional issues, much work is required to create awareness among those responsible for information systems of the need to make such system secure and so ensure that strategic development meets administrative confidentiality requirements.

1.3. Budgetary discussions relating to information technology

The State Budget is adopted by vote of the legislature (National Assembly and Senate). It is prepared by the Secretariat of State for the Budget, which includes the Budget Directorate.

In the run-up to the Finance Act, administrations whose annual IT expenditure exceeds FRF 25 million are called to a technical and budget meeting with the Budget Directorate (see Information Sheet No.7). The latter will earlier have sent to administration specimen IT technical and budget documentation that will form the basis for discussion and an exhaustive review of IT expenditure, focusing on ascertaining the size of various items (number of workstations, number of IT sites, number of different tasks). The discussion at the meeting may also cover equipment and service costs, upkeep and maintenance practices or project implementation.

Follow-up of various allocations provides a framework for discussion of IT budgeting and helps to pinpoint budget options and ministries' margins for manoeuvre. However, this should by no means be the principal aim of technical and budget meetings.

IT budget allocations are reviewed under two headings:

- type of expenditure (equipment, networks, services, etc.)
- magnitude of the expenditure and the urgency of the need to ensure smooth running of administrative departments: annual overheads (upkeep, network costs, maintenance, training, etc.), expenditure on equipment and software replacement where the replacement interval may be adjusted, and expenditure on new or ongoing projects, which may be deferred or staggered in the event of budget cuts.

New or ongoing projects are submitted individually with their justification and a breakdown of expenditure for the years covered. Allocations for new projects in the Finance Act cannot, however, be treated as separate from the priorities opted for by ministries within their total budget envelopes. Structuring expenditure by type and magnitude is for information only and has no effect on the way the total allocation is spent.

An ongoing and growing task is to establish, in co-operation with ministry staff, long-lasting indicators of the type and purpose of expenditure. This is an important precondition for ensuring optimum use of budgetary resources and effective implementation of policies. It is thus a precursor to exhaustive scrutiny of management procedures in administrations.

Consolidation of the project records pertaining to IT budget meetings is accorded high priority by the Budget Directorate. This task must be carried out in step with the cycle of in-house procedures for

reviewing IT expenditure in various administrative structures and use a predetermined common and co-ordinated framework for review of progress.

1.4. IT start-up funds

A number of start-up funds have been established to finance modernisation and NTIC initiatives in the public sector. The two principal interministerial funds for modernisation of and introduction of IT to administrative services are the Fund for Administrative Reform (*Fonds à la réforme de l'Etat* - FRE) and the Interministerial Modernisation Fund (*Fonds Interministériel de Modernisation* - FIM). Support funds for regional and local endeavours also exist and are described in the section dealing with regional activities. In the same way, a number of the larger ministries such as the Ministry of Economic Affairs, Finance and Industry have their own (NTIC) support fund to pay for modernisation efforts in a year when start-up funding has not been provided.

FRE funds are allocated by DIRE (see Information sheet No. 6) following consultation with a selection committee, which includes the Budget Directorate. The selection criteria are essentially functional and organisational and in no way restrict the technical options. Applications now increasingly relate to the IT field.

Allocation of funds from FIM is the joint task of MTIC (see Information sheet No.8) and the Budget Directorate, although DIRE and Digitip are also involved. This Fund focuses on innovative technical initiatives that may lead to expertise and experience that can be shared with others but nevertheless keeps watch on the budgetary aspects of such projects.

The two funds are co-ordinated, which is often useful in preventing the double funding of a project that reduces cost effectiveness.

Start-up funds permit encouragement of interesting initiatives and the redress of imbalances resulting from a plethora of budget negotiations, many of which are over-generous. Some projects receive special attention, which may lead to their being upgraded at interministerial level. The funds also draw attention to ministries acting as trail-blazers or precursors for some operations that could be called upon to show the way to other ministries.

1.5. Technical aspects, references and standards

The introduction of IT projects confronts all administrations with similar technical issues. Guidance is needed to maintain consistency amongst ministries in their technical policies and expertise.

MTIC (see Information Sheet No.8) plays a major part in guidance on technical topics for which it employs a variety of the latest communication tools, including:

- Creating awareness by means of regular information e-mailings
- Holding seminars open to attendance by all administrations and serviced by persons with recognised expertise in the field (INRIA, etc.)
- Harmonising technical standards by placing joint reference systems on-line on their Internet sites
- Establishing interministerial working groups for specific projects (such as introduction of teleprocedures in administrations)

- Guidance of technical expertise promotion groups.

The purpose of this work is not to pass judgement on commercial tenders already on the table but to establish the groundwork to ensure that the options selected individually will be compatible across all ministries.

The new groupware techniques are a core element in such technical guidance and ensure permanent and up-to-date access to the information, support and reference material provided by MTIC.

1.6. Scrutiny of legal issues relating to the protection of personal data

The introduction of IT projects in administrative departments is governed by the Act relating to the protection of personal data dated 6 January 1978, which established the National Commission on Information Technology and Individual Freedoms (*Commission nationale de l'informatique et libertés* - CNIL).

The Act, which governs the introduction of automated processing of personal data, is due for review in the context of the European Directive of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Any project for the automated processing of personal data that is introduced by an administration or a public sector agency, or carried out for public sector purposes must, in the present state of the law, receive prior authorisation from CNIL (see Information Sheet No.2), unless provided for by an Act or the subject of a decree of the Council of State in the event of an adverse CNIL opinion (the latter procedure has never been used).

CNIL is an independent administrative authority that acts as a watchdog - although the justice system may also be invoked - to ensure that information systems are introduced in conformity with the 1978 Act and in particular that the use of information technology does not adversely affect "human identity, human rights, personal privacy or individual or public freedoms".

The period during which documentation relating to a request for a opinion is being prepared is used for technical negotiations with the applicant body; a favourable opinion of the project by the Commission may be conditional on compliance with technical adjustments.

The fundamental principles of legislation relating to information technology and individual freedoms, on which CNIL bases its opinions, may be summed up as follows: data processing may only be introduced for lawful and authorised purposes notified in advance to CNIL; the relevant details - categories of data processed, length of retention, recipients - must be appropriate, suitable and not excessive for the purposes notified and authorised; the data processed must be collected and used in a fair and lawful manner; they must be subject to proper security measures to maintain confidentiality and prevent abuse; persons named in a data processing exercise are entitled to be informed and to exercise the individual rights accorded them by law (right of access, rectification and objection); a strengthened authorisation procedure is provided for categories of information considered to be particularly sensitive (political opinions, convictions, health matters, etc.).

Special treatment is given to NIRs (or social security numbers) because of the potential they offer for cross-referencing data bases, despite their current effective use in the management of sensitive health data. NIRs have also been the main reason for adoption of the Act of 6 January 1978. The Act does not prohibit

cross-referencing of data bases on principle but requires any such project to be subject to preliminary scrutiny.

Lastly, CNIL is not only responsible for prior monitoring of computer processing projects but also has a monitoring capability after the event that allows it to perform verification tasks.

1.7. *Compliance with the regulations relating to public sector tenders*

Operations whose forecast costs exceed a financial threshold currently set at FRF 300 000 are required to be put out to tender. The terms governing this procedure are set by the Code for Public Sector Tenders and are intended to guarantee:

- respect for the principles of fair competition (equal treatment for all tenders)
- clear description of their requirements by administrations
- properly defined conditions for mutual agreement between contracting parties and their responsibilities
- clearly defined length of the tender period and conditions for price review.

The Code for Public Sector Tenders makes a distinction between tenders to state administrations and tenders to public sector establishments other than those with an industrial or commercial role, and tenders to local authorities and attached public sector establishments. It sets out a number of separate procedures for concluding contracts with the options of tying tenders to performance or negotiated contracts.

The orderliness of the procedure for inviting tenders and its conformity with the Code for Public Sector Tenders are scrutinised by a Special Tender Commission (*Commission Spéciale des Marchés* - CSM: see Information sheet No.4), which has sections covering various areas of expertise. CSM-I (Information technology) and M-TM-TCSM-T (Telecommunications) deal with the IT sector.

The monitoring procedures employed by the CSMs begin with a technical secretariat that has the task of picking out suspect cases for submission to the Commission. Each case is then reviewed by a member of the administration.

Unfavourable opinions issued by the Commission may be overridden by the minister concerned, but the decision must be justified to the Chairman of the Commission.

The work of CSM-I is intended to ensure the efficient operation of administrative departments and should help to improve control of expenditure on information technology by the administration. During the period the invitations to tender are in preparation, constructive exchanges between the ministry concerned and the Legal Affairs Directorate take on an increasing importance. This advisory function coupled with its inspection duties should promote the gradual spread of good financial and contractual practices to all administrative departments.

Making information on decided cases available to the general public also promotes transparency and consistency in the work of the state services, which should help to improve control of public expenditure.

1.8. Additional measures and intermediate action

As implementation progresses, a project may be subjected to a number of additional measures such as periodic monitoring and provision of advice from institutional bodies.

The yearly national budget cycle determines the timetable for periodic review of ongoing IT projects. Priority is accorded to projects threatened with budgetary overruns or likely to fail deadlines. The requirement for a balanced budget places a constraint on budget issues at the present time and places some restraints on decision making.

However, it is important to be able to review projects covering a period of years, launched solely on the expectation of funds becoming available and embarked on without consultation with the audit bodies. Such projects could have a considerable effect on budget discussions in subsequent years.

Where there is a risk of major slippage, a budgetary and technical audit procedure may be initiated with the support of institutional players (CGTI: see Information Sheet No.1) or private players (audit and consultancy offices). Corrective measures when a project is in progress are difficult to apply by force, however, and co-operation and consultation are the preferred approaches.

The technical guidance provided by expertise promotion groups (MTIC) are another more acceptable and more flexible means of giving support to administrations with projects in progress.

Lastly, the circular letter of September 1996 relating to the preparation of IT development plans stipulated submission of an annual progress report. These will provide an opportunity for exchanges of views between the ministries and DIRE and could result in recasting the functional and organisational aspects of projects.

1.9. Budgetary and technical assessment

Evaluation of the work done by administrative departments is a difficult and complex task. The gradual introduction of management reviews in such departments and the provision of performance indicators should ensure greater openness and improve oversight of the work of ministries.

The documentation for the technical IT meetings (Budget Directorate: see Information sheet No.7) gives budgeted IT expenditure for the past year as part of an overall review that allows comparisons between administrations. The review, which consolidates at interministerial level the various aspects of information systems management control appropriate to each ministry, enables budgetary standards and trends to be highlighted (network costs, in-house provision or outsourcing of services, etc.)

In addition, a summary sheet and a list of benefits is required for each project completed.

The quality and openness of progress reports encourage an atmosphere of trust between ministries and the Budget Directorate that is beneficial for all parties.

The documents before the information systems budget meetings give information on the size of ministries' information systems as part of a joint review (information equipment stocks; networks and servers; etc.). The elimination of paper-based procedures for the dispatch of official documents (which will probably require the use of electronic signatures) will enable automation of the procedures for consolidating IT indicators. Development plans give a more complete and accurate assessment of the IT work being done by a ministry but are not designed as a tool for interministerial consolidation. Their routine use for purposes of comparison and consolidation is therefore difficult.

The watch on indicators of progress in implementing the main thrusts of government policy on functional and organisational matters (introduction of teleprocedures, establishment of Internet sites, etc.) is entrusted to DIRE. One exhaustive study on the performance of Internet sites has been conducted by DIRE and is available on its own Internet site.

1.10. Monitoring following project completion

Monitoring following project completion is carried out by the *Cour des Comptes* (see Information sheet No.3), which is the senior audit body (*institut supérieur de contrôle* - ISC) of the French administration. It has the authority to oversee bodies making use of public sector funds or calling on public sector generosity. Overview of local authorities in the regional context is carried out by regional audit offices (*chambres régionales des comptes* - CRC). Audit is all-embracing and in general initiated by the *Cour des Comptes* (or the CRC). It is currently conducted at three- to seven-year intervals (four in the case of the CRC).

Because members of the *Cour des Comptes* are not specialised in the field, the approach adopted in the IT sector has long been restricted to a general review of compliance with the regulations in force and adherence to budget schedules and project implementation deadlines. The growing importance of information technology in provision of the data required for audit operations, as in the operation of the departments under scrutiny as a whole, has led the *Cour des Comptes* to extend its audit techniques in this area, in line with the practices adopted by ISCs in other European countries.

In this context, review reference systems that allow monographs to be prepared on the information systems of the departments under scrutiny and on the progress of their projects have gradually been developed and made available to the magistrate preparing the inspection procedure by a cross-sectional task-force on tools and methods. A gradual separation has been achieved between general and technical inspection by recruiting more technically qualified staff or by seeking technical assistance from outside as required.

Furthermore, the importance of being able to call on reliable and relevant indicators of the performance of management information systems in its audit operations has led the *Cour des Comptes* to become another potential user when major new management control projects are in view. This means that when functional specifications are being drawn up for future applications, attention needs to be given to conserving the independence of audit work.

1.11. Opening up decentralised public sector services

Under the leadership of the *préfectures* and with the assistance of the central services of DIRE and MTIC, the networking of decentralised state services is being pursued in the *départements*. Local Information Systems (SIT- *Systèmes d'Information Territoriaux*) include an Intranet shared by all services in the *département* and a single Internet gateway giving access to the State services.

Consideration is being given to providing gradual interconnection of SITs at regional level and, in the context of the work on regional development in progress at DATAR (see Information sheet No.5), gradual inclusion of local public sector players such as local authorities or hospitals.

The recent decision to establish a post of ITexperts in the regional secretariats (which report to the Prime Minister's office) is further proof of the emphasis now being given to the introduction of IT at regional and decentralised levels.

Other specific areas are also likely targets for integration and co-ordination of State services. Ports and airports are centres of innovation where spontaneous action by local players has demonstrated the potential offered by networking State services.

2. CASE STUDIES

Two Ministry of Justice projects are described. The first relates to prison administration and concerns computerised management of prisoner information (Gide software application) and the second concerns the computerisation of district courts (X-TI software). These two projects were launched in 1994 after thorough review by the Ministry of the management of the project. The experience gained during the period the development plan was in operation (1988-1992) has shown that the development of information system applications:

- can only be achieved where contacts with users are close and dependable
- must be based on an organisational set up giving a clear demarcation of the respective responsibilities of the project management team and the contracting authority
- requires that the expertise and numbers of in-house staff be matched to what the project is expected to do
- calls for a strategy tailored to the cultural and political context of the target services.

The two projects described below have followed this approach and were implemented using two very different strategies. The first (computerised management of prison inmate data (*GIDE - gestion informatisée des détenus en établissement*)) took the conventional major project approach, whereas the second (X-TI civil proceedings kit) employed a modular approach.

2.1. The GIDE software application

Purpose

GIDE meets the strategic goals of the Ministry of Justice through the establishment of an information system in the prison administration to rationalise management of the various aspects of the everyday life of prison inmates, improve the working conditions of prison staff by providing dependable and relevant data, and provide a joint prisoner data base for the various departments of the Ministry. In its start-up phase, the project involved installing equipment at nearly 190 prisons throughout France.

The project was developed in the context of a previously existing prisoner management application used in 28 of 183 prisons but operating on a restricted basis and serving only a few of the administrative services of a single prison with the addition of a few local software applications. In some prisons the introduction of GIDE was accompanied by installation of their first microcomputers.

Economics

The total cost of the project was determined at the end of 1994, following a preliminary study, as:

Development	FRF 50 million (including preliminary studies)
Implementation	FRF 163 million
Cabling	FRF 99 million

An intermediate review in 1999, taking account of changing prices and requests from sites, led to a re-estimate of FRF 256.3 million for implementation and cabling, a figure very close to initial forecasts.

In terms of economic implications, GIDE is an application whose development costs in terms of the prison population (theoretical prison capacity) are below FRF 1 000 per inmate. Equipment installation and infrastructure costs came to FRF 4 129 per inmate on average. Operating costs, exclusive of the staff of the prison administration, is assessed at FRF 73 000 per prison on average.

Functionality - results

GIDE is an application giving functional coverage of virtually all aspects of custody, prisoner record-keeping and registry. A number of additional features meeting further needs have been brought into use since introduction of the first version (visiting rooms, rehabilitation, transfers between prisons), without upsetting the overall running of the project. These new operational features increase the life span of the application by improving its response to prison needs.

At the end of the first year of operation the results have been quite encouraging. The deployment goals for 1999 have been met in excess of 90%; a third of the prison population is now being managed by GIDE and over a quarter of prison staff have seen a change in their working practices, notably through the introduction of IT into everyday prison guard duties.

Overall, the users have found GIDE meets most of their expectations. After one year in service, even though most sites have not yet had sufficient time to pass judgement, it is still possible to pick out a number of functional gains:

- Elimination of paperwork and registries (1 to 6 registries were kept by the larger prisons)
- Better management of conditions of custody (elimination of errors in summoning prisoners, improved programming of cell searches)
- Enhancement of the role of prison guards who now have direct access to prisoner information through GIDE. This can be useful in the preparation of correspondence, for instance, and cuts down delays
- Time savings in the work of other administrative departments such as accounts units (as a result of the benefits mentioned above)
- Improved knowledge of the prison population through access to reliable statistical tools (the introduction of a national information centre should help to improve on this performance).

The deployment of GIDE will not by itself give a prison all the expected and observed benefits. Acceptance of new ways of thinking by each prison management and voluntary acceptance of changes in work practices are also needed to ensure the successful reorganisation of prison operation that GIDE offers.

Timetable

The original plan drawn up in 1994 was as follows:

93/94	Preliminary study	prototype
95/96	Phase 1 implementation	installation at 3 pilot sites
97	Phase 2 implementation	full-scale installation
98/2001	Deployment	

Deployment began in January 1999 at a rate of 40 to 50 prisons a year following the decision in 1998 to bring the system into general use. Slippage of a year has been observed to date. This can be attributed partly to the decision (Go/NoGo) to move to general use following pilot site trials and partly to difficulties in getting some prisons to complete the preliminary work leading up to deployment. It was not due to the deployment process itself.

Organisation

In view of the size of the project, it was given an organisational structure based on a contracting body aspect (MOA - *maîtrise d'ouvrage*) and a project management aspect (MOE - *maîtrise d'œuvre*). This form of organisation was designed to promote co-operation and speed up decision making by bringing computer scientists, experts and users together. The project was headed by the Assistant Sub-Director of Administrative Matters of the Prison Administration on 50% secondment for the purpose.

The Team project

The contracting body

The contracting body team, which was responsible *inter alia* for determining requirements and approving the application, consisted of a project leader, who was a user with experience of prison work, and experts in prison accounting, custody and registry. In addition, the contracting body was responsible for training and studies relating to organisation of IT sites.

Project management

Project management was entrusted to the Information Systems Sub-Directorate of DAGE (*Direction d'administration générale du ministère de la justice* - General Administration Directorate of the Ministry of Justice), to which the contracting body project leader belonged. It directed the work of two computer analysts, one of whom was responsible for the technical layout and the other was a data manager responsible for drawing up general specifications. The project management team is responsible *inter alia* for the follow-up and supervision of all technical studies, installation and follow-up at the pilot sites and conversion of the methods adopted to large-scale use in preparation for deployment.

User participation in the project

Apart from the contracting body component of the project team, various aspects of the work required the presence of selected users for their experience and their knowledge of prison practices. Considerable use was made of their services during the specification stages (interactive modelling) and validation (checks on the flexibility of the product in use, its functional capacities and suitability), while they were largely responsible for the planning of tests and trials. These dedicated staff were called on in 1996 and 1997 to ensure the software met all their expectations.

Similarly, the current structure of the project continues to encourage feedback of information and notification of new requirements from users at local and regional level.

Outsourcing

Sub-contracting has been resorted to on a flat-rate basis on the decision of the contracting body (DAGE/SDI):

- A fixed fee for implementation covering detailed specifications, implementation, installation of the application on the equipment, performance tests, establishment of pilot sites and follow-up of their operation for a three-months period.
- A fixed fee to ensure technical returns from the new product and to provide for the operational returns with the contracting body and user groups.

Project management

Independently of the follow-up ensured by the providers, in-house decision-making bodies were established at the highest level.

Strategy committee

Chaired by the Director of Prison Administration, this committee includes the chairman of the Information Technology Committee of the Ministry, the Director of DAGE, the relevant Deputy Directors and the Project Director.

It decides project strategy (lines of action, budgets, organisational matters, application perimeters). It is kept informed of current planning, basic technical options and choice of providers. It meets on a half-yearly basis.

An operations steering committee

Chaired by the Project Director, this body includes a representative of the Ministry's Information Technology Committee, the sub-directors and office heads concerned, the Directors of the pilot sites and the MOA and MOE Project Directors.

The committee decides operational matters relating to the project (preparation of decisions for the strategy committee, follow-up of the planning process, operational decisions, resource management, etc.). It meets on a monthly basis.

An administrative and technical follow-up group

Chaired by the Project Director, this group includes the project leaders, including those of the providers and technical and operational experts.

It follows up progress, prepares the meetings of the operations committee, co-ordinates work, takes technical decisions and validates functional matters. It meets on a weekly basis.

Final results and lessons learned from the project

Deadlines and budgets were generally met throughout the project. The provision in the overall plan for a status report on phase 1 by the end of the last quarter of 1997 was respected within a two-month margin, which was very satisfactory in view of the size of the project.

The initial content of the project was adhered to and the major functionalities planned were all installed with version 1.2 of the software.

The advance planning given the project enabled two fundamental principles, that are usually ignored, to be met:

- development of trial packages in conjunction with the preparation of detailed specifications
- allocation of a sizeable budget (FRF 6.6 million) for the validation phase.

The benefits expected were evidenced by the paucity of bugs in versions 1.0 and 1.2 when GIDE was started up at the pilot prisons.

The following factors also contributed to the success of the project:

- A single location, which allowed for direct contact between all project members, facilitated communication between the various players and between separate operational areas, and ensured a rapid response by the team when any problem appeared
- A team working full-time on the project and thus easier to mobilise in the absence of major external constraints (managing priorities among several projects)
- A small team, made possible by calling on an outside firm for development work
- A favourable mix of those working in prison administration and those working in the IT field, which from the outset ensured the presence of functions experts in each field, thus giving insight into the constraints work requirements and computer requirements imposed on each other;
- An efficient communication arrangement with the outside firm, in particular bringing together aspects relating to observance of deadlines (follow-up of meetings, follow-up of the validation process, etc.)
- Deadlines set to the minimum (by force of necessity?), putting a stop to any work or considerations not directly linked to the project and likely to swallow up resources and nibble away at deadlines.

With regard to the details of the progress of the project, provision for the time taken to finalise contracts could be improved by a number of means:

- clear delineation of the system of consultation to apply within the project as it progresses

- assignment of responsibility for this process to a single individual, given the task of liaising with the decision makers in-house and with the competing firms outside
- measuring the impact of various delays on the overall progress of the project and finding alternative approaches (re-sequencing phases, greater use of parallel action, etc.)
- reporting the impact of delays (on deadlines and budget) to the committee wherever possible.

The work done on determining ways to improve the tendering process could be extended, as was done during the GIDE project, to other areas of project implementation:

- assembling data
- training
- validation
- technical consistency of solutions found.

2.2. *The X-TI civil proceedings kit*

Introduction

The district court (*tribunal d'instance*) is the court at the base of the French justice system. It is the court closest to the general public with some 530 offices throughout the country.

The district court operates principally in the field of civil law: family law, third-party liability, nationality, guardianship, etc. Some district courts have jurisdiction over a few of these fields only and in addition separate court registries and access offices may be attached to a court.

These are minor courts with a few units of some dozen staff.

Objectives

Beginning in the late 1980s, the computerisation of district courts involved providing office hardware with a limited range of software to deal with certain court activities. This software was produced by local services or by outside firms. Their main features were:

- high user satisfaction
- great disparities in technical and functional factors, which limited the ability to follow the work of the courts at national level
- great sensitivity to staff changes within the justice system or to the financial health of the servicing firms.

Installation strategy was based on module-by-module persuasion of the user services or by offering financial incentives to the management services.

Starting in 1995, a range of software called X-TI, adapted to the needs of the district courts, was designed and gradually introduced. It is therefore in the process of replacing manual procedures or existing local software.

This project is a response to the need to cut down gradually the various types of specialised software produced locally and to standardise work practices and electronic procedures.

Functionality - results

The X-TI software package has the following advantages:

- Multifunctional workstations, enabling a single official to undertake a variety of tasks
- Storage of the applications on the same server
- Remote administration of workstations and servers.

The system is based on a server using an Intel processor and a Netware operating system with software operating on SQL Windows using the SQL Base data base and Windows workstations.

Timetable

The IT development plan of the Ministry of Justice has set targets for equipping district courts with all the applications in the X-TI package.

By early 2000, the 400 largest district courts had been fully or partially provided with the x-TI package:

Function	Target	Status of the X-TI package	District courts equipped
Civil proceedings	400 sites by end 99	In general use	400 (85%)
Orders to pay	200 sites by end 99, 400 by end 2001	In general use	380 (81%)
Guardianship of persons of full age	130 sites by end 99, 473 by end 2002	Version 2 at a pilot site	380 (100% of courts with this function)
Guardianship of minors	0 site by end 99, 369 by end 2002	Version 2 under development	240 (100% of courts with this function)
Attachment of earnings	200 sites by end 99, 400 by end 2001	Being brought into general use	130 (27% of courts with this function)
Management	200 sites by end 99, 400 by end 2001	Being brought into general use	0
Nationality	200 sites by end 99	Final stage of being brought into general use	190 (84% of courts with this function)
Police court	370 sites by end 99, 454 sites by end 2000	In general use	400 (95% of courts with this function)

Overview of the X-TI package

The goals of the IT development plan have been met and even exceeded in the case of three applications with only a slight delay in another application.

The management software was developed from a different standpoint, namely to enable various types of court to use it. As a result, installation of the attachment of earnings software interfaced with it has been delayed.

Organisation

Work on developing a new module or application is taken by a Civil Procedures Follow-up Committee consisting of the contracting bodies (Court and Statistical Services), project management (Information Systems Sub-Directorate - SDI) and representative of the national school for registrars. The Committee, which meets approximately once a month, receives a progress report on the project at each meeting and has the authority to make any decisions that will aid its completion. Its decisions are based on the Ministry's information systems development plan.

Each project involves preparation of specifications that must be approved by the Follow-Up Committee. SDI invites tenders for the development work, which is always carried out under the guidance of the Ministry Project Leader responsible for the application.

The programme for installation of the software package is implemented on a yearly basis by the Directorate of Court Services as requested by the appeal courts. The programme is adjusted to take account of budget constraints and the capabilities of SDI regional services, which may have to work on other programmes. The programme is then validated by the Civil Procedures Follow-Up Committee and the various persons concerned are notified.

Project management

The software package was prepared according to specifications determined in conjunction with the central contracting bodies and the users belonging to the courts. There are three stages to the validation process:

- technical validation concerned with the structure of the software and its operation
- functional validation to verify compliance with the specifications
- a pilot-site trial to test the ergonomics and effectiveness of the installation under full-scale operating conditions.

Functional changes made during pilot-site trials are built into the package before installation at other sites.

Following technical validation and pilot-site validation, the application is approved for deployment; it is added to the installation kit for the X-TI package and it can begin to be brought on-line.

As soon as the first site comes into operation, it is taken over by the support (users and operators) and maintenance services. The first level of support is provided by the training staff of the Courts Directorate. Maintenance is the second level and is provided as part of the maintenance and support services of BSI, which consists of SDI officials and service providers.

Maintenance and support staff work in close collaboration with the contracting bodies and the application development teams with a view to ensuring complete control of the application and its evolution in relation to Ministry staff.

Before installation of the IT site at a district court, a preparatory visit is made by CPR and Appeal Court technicians to decide the placement of the server and the interfacing and communication equipment. The cabling layout and the dimensions of the placement bays for workstations are determined during the visit. The "civil proceedings kit" forms the core of the local information system, which involves installation of a server of an appropriate size for the workload expected and the applications to be installed, remote administration equipment and as many workstations as the work demanded of the software version requires. As new applications are installed and the workload of the "civil proceedings kit" increases, the court could be assigned additional workstations.

Final results and lessons learned

The outcome of the project to date has generally been excellent.

Modular installation made it possible to stagger the introduction of new applications and to avoid too abrupt a change for courts or overloading with training teams. The Ministry remained in control of the applications and the courts had access to up-to-date applications that were both technically and ergonomically of a high order.

The support provided to users and to operation of the system made a significant contribution to staff acceptance of the tools provided.

The versatility of the applications package was clearly demonstrated when PACS management was installed. This new task, comparable to management of a new civil status, was added to the civil proceedings kit as an extra module; the data base was the only item specific to it because of the time span for retaining information.

3. LESSONS LEARNED

Criteria for judging the success of a project

Assessing the success or failure of an IT project is, above all, a very subjective exercise that may have different outcomes depending on the persons involved and their role in the follow-up to projects. Although budget compliance or overruns and adherence to deadlines are useful indicators of project performance, one should not lose sight of the empirical basis of the preparatory work or the underlying political implications.

An administration's potential to attract funds and its position in the political chequerboard has a major impact on budgets and planning. Some leading ministries have every incentive to guard against the unexpected by seeking large budget allocations although they can be induced to accept tightly scheduled plans. Others have to make careful estimates of the project funding required in order to have any hope of a budget allocation. If it is imperative for budgetary and management reasons to keep within initial budget ceilings, the fact that such ceilings are respected does not necessarily mean that under such conditions the money will be well spent or the project successful, and the same consideration will apply to deadlines.

The success of a project must thus be determined from several points of view, which sometimes manage to converge:

Technical and functional appropriateness : User satisfaction and the fact that use is made of the project bear witness to this. Failure may be reflected in a falling off of interest in the product, low motivation and difficulties in making the tool an integral part of the work of the service. This could have adverse repercussions on future or associated IT projects.

Furthermore, the expected increases in productivity may not be achieved; quite the reverse. Although the area of use of new products does not exactly overlap that of previous ones, their deployment could well make procedures more cumbersome and time-wasting, thus effectively cutting down productivity.

Cost-effectiveness : User satisfaction does not guarantee cost-effectiveness since it frequently reflects only the end result of a project and not its implementation. Cost-effectiveness depends on achieving a proper balance between the ultimate cost of the product and the minimum amount of technical and functional complexity needed to deliver it. Too many blind alleys, backtracking and question marks undermine cost-effectiveness. Straight-line progress and output environments that do not fluctuate are essential preconditions for good project performance. IT projects and IT design and development also raise the question, from the standpoint of budget efficiency, of the mental productivity of officials and outside suppliers. A pooling of expertise and new developments, often dependent on the quality of the functional and technical framework, are now crucial budget concerns.

Keeping to schedule: Keeping to schedule can be an important contributor to satisfactory progress, notably when the project has to contend with political factors that place severe constraints on an administration, or in the context of a highly competitive private sector.

Investment life span : The length of life of functional procedures and technical options gives another measure of the value given by the money spent. Use of common standards and attention to compatibility issues facilitate adaptation of products to meet changing needs.

It is incumbent on administrations to take account of these four aspects and to find compromises that will allow an effective information system to be put together to serve as a springboard for modernisation.

Some factors leading to successful project implementation

Project environment

The term information system nowadays implies technical and functional consistency in the IT tools used by an administration. Technical advances lead to increased expectations from users, namely political authorities and officials, which means that comprehensive account must be taken of tasks and services across the board.

In line with efforts to bring administrations up to date, new management tools support changes in management methods; the need for exchange of views among departments is increasing as administrations become more open; furthermore, higher productivity within administrations is dependent on reducing the volume of data entries and improving data management. However, the inertia inherent in administrative structures mean that changes need to be introduced gently. Too abrupt a changeover often leads to rejection by staff.

This indicates that inflated ambitions as to the functions to be performed by a project should be treated with wariness. Long-term strategic objectives can be ambitious, but they should be approached by dividing projects into units of more human dimensions with a clearly defined content and workload tailored to the capabilities of administrative departments. The Ministry of Justice's X-TI project for the computerisation

of district courts is a good example of a compromise between determination to achieve a comprehensive consistent in-house information system in the long term and a step-by-step approach to implementing change.

A detailed review of existing organisational structure and technical infrastructures is recommended in order to improve the likelihood of successful integration of the end product in the working environment. This implies:

Involving users

User expectations need to be taken into account at the design stage of projects when modernisation strategies and policies are being introduced.

Establishment of a user group is now a standard practice that gives excellent results. Motivation of users unaccustomed to this approach is essential if their expectations are to be recognised and taken into account. User contribution is important in the following phases:

- Determining functions
- Identifying ergonomic issues and human/machine interfaces
- Evaluating the application in the validation and integration phases.

Study of the impact on organisational issues

Changes in an information system can facilitate a change in practices but cannot of itself achieve it. Deployment of new computer tools gives an opportunity to recast departmental tasks but, however good the product, it will not guarantee a successful changeover. Officials should not have to adapt to a tool but should be able to use tools offered to them to implement the specific structural changes targeted when the product was introduced. Taking user expectations into consideration is in this context frequently a decisive factor in making changes successfully.

Integration into pre-existing technical facilities

The life span of an applications project in an integrated information system depends on how the rest of the system is affected by change. Clear definition of the technical content of the project and the way it interfaces with the rest of the information system is a precondition for success. Changes in programming languages (target language) and system structures are evidence of a search for free-standing modules and techniques that will ensure transparency in the changeover process.

Project implementation

An IT project may be described as a search for the best compromise between functional and organisational aspects on the one hand, and technical and budgetary constraints on the other.

To achieve this ideal, it is important to arrive at a balance between the two aspects. In this endeavour, making a distinction between the contracting body in charge of functional specifications and the project management team responsible for technical implementation is the conventional approach to project implementation.

Too great an overlap between the separate phases of development of a project is a risk factor to be studiously avoided. Completion of the functional specifications, for which the contracting body is responsible, is a phase that should precede the technical review and development phases, which come under project management. Too early a selection of technical options or software development in tandem with consideration of functional issues has in many cases been found to create barriers to the progress of a project.

A functions portfolio immune to change is a decisive factor when part of the work is outsourced. Regular contacts between the contracting body and project management should enable the functions required to be clearly described and priorities to be ascertained when technical constraints are encountered. It is vital, however, for project management to be able to rely on a functions portfolio with a long life span as their motivation is often dependent upon it.

Impressions gained from project implementation point to the importance of the following factors:

- clear and open plans
- clear-cut division of labour
- clearly articulated responsibilities
- introduction of a policy of pinpointing and dealing with risks and constraints.

Provision for unforeseen events or changes on the functional (policy changes) or technical (no feasible technical means of achieving the functionality required) front must involve a comprehensive impact review of the project as a whole and be part of a well-defined decision-making process.

Continuation of the project after completion of a major phase or before a necessary change in operational or technical procedures must be conditional on renewal of the Project Director's commitment in the context of a Go/No Go strategy.

Technical consistency and allowance for staff expertise

Consistency in technical decisions within a project and across the entire information system is also an important factor in ensuring success. This also involves consideration of the need for special expertise that administrations often find it hard to come by. Introduction of expert technical groups covering several projects and providing support and technical expertise to the various project teams is a new approach worth exploring and one that not only improves integration of the technical aspects of new products but makes better use of individual expertise.

The quality of those in charge of project implementation or in deciding major operational and technical issues also needs to be recognised as a factor in all instances. Continuing availability of such staff also ensures longer-lasting choices and methods, and is needed to keep staff motivated. The qualities required of supervisory staff are an ability to listen, to be objective and to identify and sum up different concerns (functional, technical, etc.).

Communication

Lessons learned from past experience underline the importance of communication at the various stages of project implementation:

- Preparation of written specifications: clarity must be the rule, with standard diagrams and concise, practical language
- Reporting: information emanating from different decision-making levels is vital to ensure effective project follow-up. Here too, however, accounts should be brief and focus on priorities
- Exchange of views between in-house teams (contracting body, project management): location of staff in the same place and their availability are also advantageous
- The use of the latest communications tools (groupware) and notably the use of Extranet especially set up for the project are tools for motivating all teams attached to a project.

Outsourcing

Although outsourcing is an attractive option for many administrations, there are traps associated with it.

To start with, it is a mistake to believe that any change can be carried through solely from the outside. In-house teams need to be set up and failure to involve such staff is a frequent, major cause of failure.

The contractual aspects of relations with outside providers need care and attention. For example:

- The outcome of the tendering process needs to be set out clearly
- The mutual commitments and responsibilities of the co-contractors need to be clearly identified
- Project priorities need to be clearly set out in contracts

Follow-up of providers and in-house control of technical issues are essential. The appropriateness of this internal follow-up is often the factor that gets the best out of outside teams. In-house teams that are too small to tackle this task effectively implies a loss of control by the initiator of the project, which opens the door to slippage.

Assignment of a member of the administration with responsibility for ensuring that the terms of contracts are met and with sole authority to deal with the outside provider may help to reduce risks. This has been the option chosen by the Ministry of Justice.

Training

Training determines the level of acceptance and ultimate usage of the product. It is essential to match the technical training provided to the changing operational practices required of officials. The latter must not only be introduced to the product and its potential but must also grasp the use they are expected to make of it in their work. An approach tailored to the individual is also essential at this stage.

Well-designed backup and help for users will also encourage acceptance of the product in all its aspects.

4. DOCUMENTATION ON PAPER AND ON THE INTERNET

PAGSI is the main source of information on French government action in the IT field: *Préparer l'entrée de la France dans la société de l'information - Programme d'action gouvernemental* was issued as a official publication in France in 1998.

On the Internet the above information and the major indicators are available at the following sites:

www.internet.gouv.fr (the PAGSI site)

www.service-public.fr (gateway to the French administration).

The Web sites for the various bodies involved in monitoring and follow-up of the major public sector IT projects may be accessed through the French public service gateway (www.service-public.fr).

ANNEX

INFORMATION SHEETS on the institutional bodies involved in the follow-up and monitoring of major public sector IT projects:

- Information Sheet No.1 : CGTI
- Information Sheet No.2 : CNIL
- Information Sheet No.3 : the *Cour des Comptes*
- Information Sheet No.4 : CSM-I
- Information Sheet No.5 : DATAR
- Information Sheet No.6 : DIRE
- Information Sheet No.7 : the Budget Directorate
- Information Sheet No.8 : MTIC

Information Sheet No.1 : CGTI

Name	The General Council on Information Technologies - <i>Conseil Général des Technologies de l'Information (CGTI)</i>
Status	Established body set up in 1996
Administrative affiliation and organisational details	Ministry of Economic Affairs, Finance and Industry Attached to the Secretariat of State for Industry An inspection committee A legal and economic section A scientific and technical section An innovation and business section shared with the General Mining Council (<i>conseil général des mines</i>) Staff: 25.
Duties	Expert assessment and advice on information technology Supervision of the telecommunications schools group Management of the interministerial group of telecommunications engineers General Secretariat of the Committee on Information Technology Strategy (CSTI) established by CISI at its meeting on 10 July 2000
Principal activities and procedures	Studies in the areas of telecommunications, postal services, information systems and audiovisual techniques for relevant ministers or for the Prime Minister. The resultant reports may be circulated and published. Scrutiny of the proper operation, including accounts and management, of bodies in the post and telecommunications sector. Functions as the general secretariat of CSTI, which is attached to the Prime Minister's office, includes leading figures from business and research, and is responsible for submitting to the Government policy recommendations relating to innovation, research and development in information technologies. May conduct surveys in France or abroad as part of studies or information gathering, monitoring or evaluation tasks assigned to it.
Type of activity	Audit and advice.
Current and future areas of work	Consideration of methods of evaluating good practices or user satisfaction Follow-up of the experience gained by the European Commission in circulating lists of selection criteria in advance to ensure greater transparency in making the Commission's decisions known. Renewed efforts on evaluation and monitoring.
Communications	CGTI's public reports are made available on-line on its Internet site.

Information Sheet No.2 : CNIL

Name	National Commission on Information Technology and Individual Freedoms - <i>Commission nationale de l'informatique et des libertés (CNIL).</i>
Status	Established independent body
Administrative affiliation and organisational details	Independent administrative authority Staff: about 80. Subdivisions for each area of activity, some of which are in the international sphere.
Functions	Compliance with legislation on protection of personal data. The current Act on protection of personal data dates from 1978. A new bill incorporating the 1995 European Directive is being drafted.
Principal activities and procedures	Public sector : Favourable Commission opinion mandatory with regard to processing-related projects. Legal and technical scrutiny of cases Negotiation of adjustments where required. Submission of cases to the Commission for consideration and an opinion. The opinion may be favourable or unfavourable and be accompanied by reservations and/or comments. The project must be modified to take account of the CNIL opinion, unless the opinion is overridden by a government bill or a decree of the <i>Conseil d'Etat</i> . Private sector : notification mandatory. Legal and technical scrutiny of notification documentation Preparation of a note of receipt of notification In the event of any clear breach of the legislation, the only option available to the Commission is to withhold the note of receipt until proper adjustments have been made.
Type of activity	The scrutiny performed by the Commission is generally carried out in advance. Its opinions have force of law for administrations in the absence of a bill or decree of the <i>Conseil d'Etat</i> . CNIL may carry out inspections after the event. It may take action on complaints and initiate an out-of-court non-contentious procedure. The Commission rarely takes such action on its own initiative. As a last resort it may lay a complaint before the prosecuting authorities.
Current and future areas of work	Two fundamental principles guide the Commission's opinions: Security: access to records containing personal data must be made secure and monitored. Justification: the use to be made of data files must be made plain, be warranted and be in conformity with the 1978 Act and other legislation relating to the status of data (fiscal confidentiality, statistical confidentiality, professional confidentiality). The European directive places less emphasis on prior inspection than current national law. This could affect CNIL procedure in future by increasing the number of inspections after the event, which are however more difficult .
Communications	The Commission is active on the Internet and is making every effort to create awareness and communicate. A young people's version of the CNIL site has been set up.

Information Sheet No.3 : the *Cour des Comptes*

Name	The <i>Cour des comptes</i>
Status	Established body set up in 1807
Administrative affiliation and organisational details	Independent jurisdiction Members: some 300 magistrates.
Duties	Scrutiny of implementation of the Finance Act Scrutiny of the management practices of those authorising expenditure in all services subject to public accounting rules (state centralised and decentralised services) as well as the social security services, bodies receiving state or European subsidies and private bodies seeking public support. Certification of the accounts of bodies distributing European funds Legal scrutiny of public accountants
Principal activities and procedures	May on its own initiative or at the request of parliamentary commissions undertake special inquiries into the management practices of the bodies under its inspection The magistrate investigating the case directs the procedure Following preparation of the case, the Court rules as a body Once an inspection procedure has been completed the Court must: Ensure the government is informed Report its findings and comments to the Finance Committee of both parliamentary assemblies Inform the Budget and Finance Disciplinary Court (<i>cour de discipline budgétaire et financière</i> - CDBF) of any unmistakable errors in the management practices of those authorising expenditure Hand over the case to the justice system in the event of offences liable to criminal sanctions.
Type of activity	Inspection after the event, principally on the court's own initiative
Current and future areas of work	Widening the recruitment base to give a more technical turn to some inspection operations Establishment of a cross-body "tools and methods" assignment to assist the Court's magistrates and administrators in the information systems field by means of appropriate reference systems and training Presence in the early stages of major management projects in order to be in a position to defend the needs of the potential users of public sector information services for supervisory purposes. Care needs, however, to be given to maintaining the independence of future potential inspection
Communications	Publication of an annual report (notably on the Internet) and special reports on specific sensitive topics.

Information Sheet No.4 : CSM-I

Name	Special Tender Commission on Information Technologies - <i>Commission spécialisée des marchés informatiques (CSM-I)</i>
Status	Established body
Administrative affiliation and organisational details	Ministry of Economic Affairs, finance and Industry (Minefi) Legal Affairs Directorate (DAJ) Sub-Directorate of Public Sector Ordering Five specialised tendering commissions Staff: a technical secretariat of 2 or 3 per CSM. Commissions have a membership of between 7 and 9: 4 to 5 of whom sit on all the Commissions and 3 to 4 members are specific to a given Commission.
Duties	Verification that public tender procedures are in conformity with the Code for Public Tenders.
Principal activities and procedures	The technical secretariat identify suspect tender cases for submission to the Commission. The cases identified are subjected to detailed individual examination by an independent official. The Commission, which meets every two weeks, considers the cases and makes its rulings. The Commission's ruling may be Favourable and accompanied by comments. reservations expected to be lifted. Unfavourable.
Type of activity	The Commission's rulings have regulatory force for ministries. In the case of an unfavourable ruling, a ministry may: - cancel the procedure and begin again with a new project; - override the CSM-I ruling by means of an official document signed by the minister responsible for the project.
Current and future areas of work	An effort is being made to co-ordinate the work of the five specialised Commissions so as to work out a common and consistent method for handling cases Special attention is being given to the following: Clarity and accuracy in describing the purpose of the tender. Respect for fair competition and equal treatment for bidders in the tender procedure. Compliance with the provisions of the Code for Public Tenders when drawing up contracts. Fair pricing : where fair competition is ensured, the market will decide price rates.
Communications	Communications from CSMs and their advisory work in the area of tenders is handled by the Legal Affairs Directorate. Access to the Commission's previous rulings is still inadequate.

Information Sheet No.5 : DATAR

Name	Regional Development Directorate - <i>Direction de l'aménagement du territoire et de l'action régionale (DATAR)</i>
Status	Established body set up in 1960
Administrative affiliation and organisational details	Attached to the Prime Minister's office and made available to the Ministry of the Environment and Regional Development Staff: 230.
Duties	Co-ordinating implementation of government regional policy Assessing future trends with regard to regional development Secretariat of the national committee to be established in early 2001 to follow up and assess state activity in the regions
Principal activities and procedures	Studies of future trends. Preparation of tripartite schemes for local services: assessments of government areas of activity of all kinds (domestic, schools, businesses, public services, coal authorities), plan of action for the period 1997-2003 and future prospects for the next 10 years. Management of funds partially intended for new information and communication technologies through which the state joins the regions and local authorities in financing projects and which are used for modernisation and regional development (contracts under the state-regions plan, National Regional Development Fund, invitations for projects) Co-ordination of the work of various institutional bodies involved in regional development: General Directorate for Industry, Information Technologies and the Postal Services (<i>Direction générale de l'industrie, des technologies de l'information et des postes (DiGiTiP)</i>), the National Agency to Enhance the Value of Research (<i>Agence nationale pour la valorisation de la recherche - ANVAR</i>), the General Plan Commissioner's Office, the Interministerial Task-Force for Technical Support to the Development of Information and Communication Technologies in Public Administration (<i>mission interministérielle de soutien technique pour le développement des technologies de l'information et de la communication dans l'administration - MTIC</i>)
Type of activity	Promotional work and acting as a government intermediary at local level
Current and future areas of work	Ensuring equity in development matters among the regions. Use new technologies and geographical information systems in particular to improve awareness and knowledge of regional development issues.
Communications	The Internet site gives information on DATAR activities and on specific issues (CISI facilities, data base on service innovations, sharing of regional facilities). Publication of the local services scheme

Information Sheet No.6 : DIRE

Name	Interministerial Delegation for Administrative Reform - Délégation Interministérielle à la Réforme de l'Etat (DIRE) : Task-Force on the Use of New Information and Communication Technologies in Public Administration - <i>Mission Utilisation des nouvelles technologies de l'information et de la communication par l'administration (UTIC).</i>
Status	Established state body
Administrative affiliation and organisational details	Ministry for the Civil Service and Administrative Reform One of the five DIRE task-forces Staff: approximately 10
Duties	To co-ordinate the use made of information technologies by administrations from the operational, organisational and training standpoint. To follow up PAGSI section N°3 (modernisation of public services)
Principal activities and procedures	To prepare jointly with the Office of the Minister for the Civil Service documentation on the Interministerial Committee on Administrative Reform (CIRE) and follow up implementation of measures. To allocate from the Administrative Reform fund (FRE) To advise on allocation of the Interministerial Modernisation Fund (FIM). To run working groups on operational and organisational matters (meeting of senior officials responsible for modernisation, regional information systems (SIT) steering committee, etc.). To establish think-tanks on specific topics and commission studies (Impact of NTICs on the organisation of administrations) Even though DIRE has no direct connection with decentralisation, it contributes to the development of regional information systems (SIT) by running information days and reviewing local applications for joint use and networking.
Type of activity	Promotion and encouragement. Guidance on operational, organisational and training issues
Current and future areas of work	Improvement of relations with users Improvements within administrations: introduction of electronic signatures, training, security, sharing data and data compatibility.
Communications and indicators	As part of the e-Europe project, the Task-Force gives the lead in developing indicators for inter-country comparison Introduction of a control panel to follow up implementation of PAGSI (available on the civil service site) which includes the evaluation indicators from the present to end 2000

Information Sheet No.7 : Budget Directorate

Name	Office of Administrative Modernisation (<i>Bureau de la modernisation de l'administration</i>) of the Budget Directorate (1B)
Status	Established body
Administrative affiliation and organisational details	Ministry of Economic Affairs, Finance and Industry <i>Secretariat of State for the Budget</i> Budget Directorate Staff responsible for information systems follow-up: 2
Duties	To follow up the information systems budget of administrations To guide budgetary policy in the IT area
Principal activities and procedures	Technical information systems meetings: to review with each administration the budgetary and staff resources allocated to information systems and to discuss the budget allocations needed for operation of the existing information system, for advancement of current projects or new modernisation projects. To prepare specimen documentation for information systems meetings: technical information systems meetings centre on the consideration of technical documentation consisting of a report and technical files, the format of which is decided by the Budget Directorate. To follow up grants for IT purposes from public authority budgets. Macro-budgetary review of public sector investment in IT. Share in allocation of the Interministerial Modernisation Fund (FIM)
Type of activity	To provide expert assessment and mediate between the Budget Directorate and the ministries. To help in determining annual budget grants for information systems.
Current and future areas of work	To improve administrations' grasp of the operational, technical and budgetary aspects of information systems by consolidating the documentation for technical information systems meetings and reviewing expenditure on information systems by administrations in terms of total costs. To encourage sharing of expertise and experiences within administrations. To help in the spread of good practices to achieve cost-effectiveness To participate in discussion on identifying, strengthening and training in-house IT skills and provide information on in-house development and outsourcing on IT issues.
Communications	Annual document providing comparative figures of the total annual cost of information services in the administrations: the data reviewed include in-house staff assigned to such work as well as operating costs.

Information Sheet No.8 : MTIC

Name	Interministerial Task-Force for Technical Support to the Development of Information and Communication Technologies in Public Administration - mission interministérielle de soutien technique pour le développement des technologies de l'information et de la communication dans l'administration (MTIC)
Status	Body set up in August 1998 for a period of three years
Administrative affiliation and organisational details	General Services section of the Prime Minister's Office Staff: approximately 15.
Duties	Implement interministerial projects Provide technical support to various administrations Harmonise technical standards and prepare shared technical reference material Identify shared needs in the public service for equipment and material Participate in work relating to international co-operation in the field of information technologies and communication
Principal activities and procedures	Share in allocating the resources of the Interministerial Modernisation Fund (FIM) Act as contracting body for interministerial projects Where required, follow up and evaluate the use made of information and communication technology in specific sectors Run working groups and skill circles Organise technical seminars
Type of activity	Provision of technical backup, support and encouragement
Current and future areas of work	Establish an interministerial Intranet and include ministries' electronic directories Dematerialise the process of drafting and implementing laws and regulations Promote sharing of skills on data networks Promote sharing of skills in the area of dematerialising procedures Promote the use of freeware within administrations Help to make administrations aware of security issues in relation to information systems
Communications	The work of MTIC is based on a policy of extensive communication centred on the Internet and operating at three levels: Intranet, Extranet for projects and the Internet itself. Distribution of electronic information circulars is also a part of communication efforts

IRELAND

1. GENERAL INSTITUTIONAL FRAMEWORK

1.1. Policy

A number of initiatives are in place to ensure there is a proper framework within which large projects are run.

The first and most important is regulatory and this applies to how IT is developed. In 1997 new "Delegation arrangements for IT Related Expenditure" (Circular 16/97) was issued. While this covers a number of areas which ensure that monies spent on IT must be aligned with business and strategic objectives, there is a requirement stated that all IT projects must be run in a controlled fashion, and yearly returns must provide details and mechanisms on how projects are controlled.

The project management methodology PRINCE is used to manage and control projects. Methodologies were adopted in 1990 throughout the Irish Civil Service and these are used as appropriate in each project. Methodologies are used as a means to an end and not as an end in itself. A project management training programme identified by civil service staff has been developed and is now run by a commercial company (following a market exercise).

To assist departments and offices in their projects, various advice notes and publications have been issued since 1993 on issues around projects, *e.g.* providing assistance on how best to manage consultants.

In general we have a policy of using non-propriety software platforms with a number of suggested open platforms for consideration. All business solutions must be run as part of a tendering process and must be flexible and cost-effective.

1.2. Funding

1.2.1. IT Vote Control

Funding is provided for in the estimates process. Delegated sanction is given for yearly expenditure following this, and each year there is a review on achievements as per Circular 16/97. Expenditure must follow from an IT Strategy against the backdrop of business plans as part of the overall strategic objectives.

1.2.2. Decisions and Assessment

IT Vote Control approval is required either as part of the delegated sanction process or on the foot of an RFT and market exercise following procurement rules and regulations.

Expenditure in the estimates is related to business objectives and strategic objectives. Expenditure must be planned for on a yearly basis.

Successful tenders are accepted on the basis of weighted award criteria in the proposal. These typically include the quality of the proposal; content; experience of the people proposed to complete the job; CVs of the personnel; time-scale and cost.

Each project is proposed on expected results; benefits; outcomes proposed and value for money (VFM).

IT Vote Control liaise with the division in the Department of Finance responsible for overall expenditure. All assessments are on the basis of VFM, inclusion in the estimates process, and ensuring outcomes and outputs are in line with government spending and policy.

Progress is monitored by Steering Groups, Project Boards and Status Groups, with high membership from the business side of the projects.

Benefits are not always measured on cost. On many occasions they are measured on administrative necessity, or are required as a result of policy as outlined in the government's budget, or as a result of broader EU requirements, or sometimes as a result of a ministerial decision.

Projects are audited by the Comptroller and Auditor General as part of a VFM examination or, indeed, as a comparison of the realisation of benefits versus proposals.

1.3. Management Models

Projects are usually commenced as part of discussions. Partnerships are formed; project Boards are set up; and the first formal documentation is usually the Project Initiation Document (PID). This defines the scope; ownership; organisational and control frameworks; and responsibilities, etc. As a result, ownership is clear, formal project management is in place, a steering committee is established to oversee the project, and risks are stated, monitored and managed.

There is a clear QA strategy. All project planning includes resources, activities, technical details, controls and end stage assessments. Change management, if required, is also included and there are clear project closures. Most importantly, there is clarity on project structures and matching resources where the need arises.

2. LESSONS LEARNED

Systems which are successful have the required structures in place. In many cases failures have the same structures, but the difference is in how they are managed. Successful projects are driven forward. Tasks and people are focused towards the goal, *i.e.* the end product. Failures arise because tasks and people are simply monitored. Project management is not about monitoring, but about achieving.

Some examples of why projects fail are:

- using consultants without managing them;
- not seeing potential problems and acting on them before they became real problems;
- not having the right expertise in place;
- ownership not clear or not accepted;
- no project sponsor;

- people not working together towards the one goal;
- risks not assessed nor continually monitored and updated;
- tasks being monitored - not being driven forward;
- advice being sought and given but not acted upon;
- scope changing;
- not putting resources in place;
- roles changing;
- lack of trust in parties.

A successful project outcome would seem to depend on the following factors:

- quality assurance and audit processes in place;
- resources in place before commencement;
- adapting to changing needs;
- legal advice on contract before commencement.

Other:

- ownership must be clear with defined responsibilities;
- risks should be assessed and modified as time passes;
- independent legal advice should be taken;
- project management guidelines available;
- compliance process to assess success;
- benefits achieved in place;
- QA and audit in place;
- in-house resources in place;
- legal advice focused on risk;
- penalty clauses (or liquidated damages) included if necessary.

3. REFERENCES

Planning Extreme Programming, Kent Beck and Martin Fowler, Addison-Wesley at <http://www.awl.com/cseng/titles>.

<http://www.irlgov.ie/finance>

<http://ringd@cmof.finance.irlgov.ie>

NORWAY

1. INTRODUCTION

This report has been prepared by Statskonsult, the Directorate of Public Management, Norway in response to OECD's invitation of 7 July 2000 to interested member countries to participate in a project on management of large IT projects in the public sector.

The invitation to participate was accompanied by a set of working definitions and a template for the country reports. These have been adhered to as strictly as possible in order to increase the comparability of the different country reports.

In preparing this report Statskonsult has addressed all Norwegian ministries to obtain their views on questions about decision processes, reporting and cases. Seven ministries provided us with answers about IT projects within their areas of responsibility. In addition, the Ministry of Finance and the Ministry of Labour and Government Administration have been asked to contribute information on topics connected to their specific responsibilities. In the more judgmental parts of the text, we also rely on the experiences of the authors as advisors to ministries and agencies on IT management issues. The content of the report is, of course, the sole responsibility of Statskonsult. Whenever possible we have referred to English translations of government documents. We have also provided the references with appropriate URLs to better enable the readers to become acquainted with the documents in question.

Within Statskonsult this report has been prepared by Senior Adviser Mari Vestre and Assistant Director General Pål Sjørgaard, both from the Department of IT Co-ordination and Planning.

1.1. General institutional framework

Norway has a population of 4.3 million. It is a unitary state with 19 counties and 434 municipalities. The country is a kingdom run by a parliamentary system. The ministers in the government are individually accountable to the Storting (Norwegian parliament). There are 16 ministries plus the Prime Minister's office. There are two ministers in two of the ministries. Including the Prime Minister, there are 19 ministers in the government.

As a result of Nordic co-operation, one of the authors of this report worked two months in the Ministry of Finance in Helsinki preparing a report on IT co-ordination and public management reform in Finland and Norway 0. That report contains a more detailed description of the Norwegian co-ordination mechanisms pertaining to IT than this report.

1.2. Policy

The national IT policy is expressed in the action plan *eNorway 1.0 0*. While published by the Ministry of Trade and Industry, the action plan also addresses IT in the public sector. The plan addresses use of IT in customer services, internal administrative reform and better health services. It does not address the problems in managing large IT projects. Another central policy document is the action plan on Electronic Government 0 published by the Ministry of Labour and Government Administration. This action plan defines eight areas for cross-sectoral IT development. These are year 2000 security, infrastructure, IT security, information services on the Internet, electronic administrative procedures, electronic data interchange, electronic commerce for public procurement, and IT management and organisation.

Regarding management of IT there are several central principles and documents:

- The principle of responsibility in the line organisation. This principle, formally adopted around 1980, states that IT is mainly an internal responsibility of each agency. The logic behind this is obvious: in order to be responsible for the way an agency works, management in each agency must also be responsible for the agency's use of IT.
- As from 1 January 2000 a special procedure for risk evaluation must be applied to all investment projects (i.e., not only IT) where the total investment exceeds NOK 500 million. This procedure is further described below.
- As mentioned, the action plan on Electronic Government 0 (section 5.8) addresses IT management and organisation. The plan addresses issues like manageability, predictability and professionalism in IT work. The plan states that good implementation capacity for IT is a prerequisite for the political manageability of government administration.
- Statskonsult, the Directorate of Public Management, has made a series of standard IT contracts. There are contracts for acquisitions (hardware or software), maintenance and program development (mainly for projects which follow the waterfall model). Use of the contracts is not mandatory, but recommended. They are widely adopted by government agencies as well as by other organisations inside and outside the public sector. The standard contracts are templates that must be adapted to the case in question, preferably without modifying the juridical contents. Two of the contracts, the purchase agreement 0 and the maintenance agreement 0 are available also in English translation.
- As a result of a major IT failure in a large agency in 1996 (see the Tress-90 case below) Statskonsult undertook an investigation of the state of IT project management in several ministries and agencies (project FASIT: Pitfalls and criteria for success in major central government IT projects). This work resulted in a report on experience 0, a guide for better project management 0, and the standard contract for program development 0 mentioned above. In the report on experience Statskonsult identified 12 sources of project failure, see table 1. In the guide on project management Statskonsult makes a distinction between three distinct roles that need to be identified in IT projects. These are the role of the customer, strategic manager and supplier. These roles are often mixed in IT projects.

1 Project not anchored in plan of operations or IT strategy	7 Plans and estimates made on an insufficient basis
2 Unrealistic goals, overly ambitious, lack of focus on ability to run the project	8 One-sided focus on technology, lack of emphasis on development of organisation and skills
3 Unclear relations of organisation and responsibility	9 Choice of technology has too often become a choice between either being in the very front or lagging behind
4 Too large, too all-embracing systems – deliverables not split according to functions and deadlines	10 Lack of skills – especially on the management level
5 Insufficient project management and follow-up, lack of readiness for change management	11 Negligence of changed requirements and new conditions for the project
6 Contracts left in a drawer instead of using them as a tool for managing the project	12 Inadequate attention to division of work between internal development and commercial suppliers. Lack of care when trying to commercialise the systems.

1.3. Funding

The main, and actually only, principle concerning the funding of IT projects is that they are funded using the same mechanisms as those used for funding other projects and investments. The budget system is based on gross budgeting, annual budgeting and budgeting using budget limits.

Gross budgeting means that income and expenses are kept separate. This applies even for agencies with large revenues. Also, agencies are not allowed to use credits to fund investments. There are exceptions to this rule. There are, e.g., some net budgeted agencies. There are also some state enterprises, and they have considerable freedom in financing their investments.

Annual budgeting means that normally funds are allocated and spent on an annual basis. Unspent funds can be carried forward to the next fiscal year up to a limit of 5% of the annual budget. For special purposes, typically for large investments, special accounts (the so-called “post 45”) can be used, within which large amounts more freely can be carried forward from one fiscal year to another. Such accounts are normally limited to a period of three years.

Budget limits mean that there are relatively fixed amounts allocated to each ministry. Within these limits the ministries enjoy considerable flexibility. A ministry can finance a large investment in one of its agencies with little interference from the Ministry of Finance provided there is room for the investment within the ordinary limits of the ministry. Similarly, there are normally stable funds for each agency. As an example, Statskonsult has an annual budget of around NOK 80 million (EUR 19 million), and the ministry does not split this amount into funds for salaries, investments or other expenses. As a result, Statskonsult can launch small IT projects without ever informing the ministry. Larger agencies, like the revenue authority, can in practice fund very large IT projects within their ordinary budgets.

There are mechanisms to fund projects and initiatives outside the principle of budget limits. Such projects must be accepted in the budget process. There is considerable competition between “good” initiatives, and the Ministry of Finance will have to turn down several worthy projects. The budget process is, of course, highly political. The Ministry of Finance experiences artificial inflation of the needs of the other ministries, while the other ministries experience unjustified rejections from the Ministry of Finance. Since a project in practice needs to have a certain size in order to achieve funding outside ordinary budget limits, there is an incentive to increase the ambition level (and risk) of a project in order to obtain funding.

The special procedure for risk evaluation of large investments applies to all projects above the threshold amount, irrespective of whether the project is funded within the budget limit or receives separate funding.

1.4. Decisions and assessment

In the discussion below, it will be stated several times that there are no fixed rules or special procedures for large IT projects. This makes the text somewhat abstract. In addition to the general answers to the item in the report template, we have therefore chosen to add text from one specific (and very large) example, the SIAMO project in the Labour Market Agency (SIAMO stands for “Service og Informasjon for et Arbeidsmarked i Omstilling” which means “Service and Information to a Changing Labour Market”). This project first got special funding on the state budget in 1998 and is planned to complete by the end of 2002. The total budget is NOK 675 million (price level of 1998) (EUR 83 million). Further details about this project are provided in the section on cases.

Who makes the procurement decision

It follows from the above discussion of funding that there is no fixed rule on who makes the procurement decision in relation to a large IT project. This may range from the Director General of a large agency to the Storting. Most large IT projects will in practice be accepted by at least a Director General (“ekspedisjonssjef”) in the ministry in question. Several ongoing projects have been accepted by the Storting.

Example: As regards the SIAMO project, the decision to start the project was made by the Storting as a part of the annual budget decisions.

On what information basis is the decision taken

Normally an agency will run a pilot project, feasibility study or something similar before making large investment decisions on its own or proposing to the ministry that an investment should be made. Again, there are no fixed rules as to how risks are evaluated, but a ministry may request an independent evaluation of an investment proposal.

Example: The government’s proposal to adopt the SIAMO project was based on detailed plans from the Labour Market Agency. The ministry had hired independent specialists to undertake quality assurance of the plans and assessments from the agency.

Relation to project characteristics

The answers to the questions above depend on several factors. As previously explained, a large agency or a ministry with a large general budget limit may accommodate larger projects without passing the decision upwards in the system than what can be done by smaller agencies and ministries with tighter limits. Politically important projects may receive more attention at the ministerial and Parliament level than do projects that only deal with internal administrative affairs. And, as explained below, there are special procedures for investments above 500 million NOK.

Ex ante and ex post assessments

There is, per se, no agency, institution or authority responsible for ex ante or ex post assessment of projects, but there is a special procedure for risk evaluation of large investments and Riksrevisjonen (Office of the Auditor General of Norway, a body reporting to the Storting) performs some evaluations. We will describe this in more detail.

The Office of the Auditor General continually audits all ministries and agencies, and thus also audits large IT projects. Since the Office of the Auditor General essentially is a control body *external* to the government administration, it will only report on findings that are severe enough to warrant special reports to the Storting. This is clearly a very powerful mechanism. It can only be used in severe cases, however, and it does not form part of a systematic process of ex post evaluations from which the government administration can continually learn to improve its handling of large projects.

In 1997 the Ministry of Finance started a project on risk evaluation of large investments. The project was inspired by a series of projects with significant overspending (bridges, IT, large buildings, military investments) and subsequent harsh criticism from the Office of the Auditor General. The existing procedures were analysed, and found to be of insufficient relevance to the kind of investment projects undertaken. A new regime for ex ante evaluations was proposed and put in operation in the year 2000.

Content and nature of assessments

In the new regime for ex ante evaluations all investments above NOK 500 million (EUR 62 million) must undergo independent risk evaluation after the planning stage (pilot study). These evaluations are performed by independent companies, which have entered into a framework contract with the Ministry of Finance. The Ministry of Finance and the responsible ministry acquire the evaluations in partnership in order to obtain full insight into the result of the evaluation. The evaluations address project delimitation, project charters and management models, contract strategies, factors of success and failure, and a comprehensive analysis of risks based on investigations of estimate uncertainties and event uncertainties. Different techniques are in use in order to produce a total indication of risk.

The projects must present prioritised lists of uncertainty-reducing measures. When many good measures are available, the project can be funded with a limited budgetary reserve. If few measures are available, a larger budgetary reserve is needed. As the total project budget (including reserves) must be allocated within the responsible ministry's total allocation (possibly delaying other initiatives), the ministries will have strong incentives to undertake uncertainty-reducing measures.

Since this is a new regime it is too early to present an evaluation of its effects. It has so far been used in 6 projects, and only one of these is an IT project.

Example: The SIAMO project started before the new procedures for ex ante risk evaluations were in place. As mentioned, an external risk evaluation has been undertaken. During the project period external risk evaluations will be repeated independently of the risk management in the project. When new sub-projects (they may be large!) are started, they will be evaluated with respect to risks such as complexity, IT maturity, technology and organisation. Risk factors should be divided into external factors that cannot be influenced and internal factors that can be reduced through actions undertaken by the project. The risk factors are followed up during the whole project period.

Progress monitoring and reporting

There are no specific practices on progress monitoring and reporting, as this depends on who has responsibility for the project. When a project is an internal matter in an agency, it will be up to management in that agency to deal with monitoring and reporting. For larger projects it is common, but not mandatory, to set up specific steering groups to follow up the projects. Sometimes these steering groups receive assistance from independent quality assurance personnel. When the ministry is involved in the decision about the project, the ordinary reporting chain between agency and ministry will also deal with the project. This kind of reporting is not very frequent. For very large projects a ministry may choose to set up special and more frequent reporting procedures.

Example: In the SIAMO project the agency reports monthly to the ministry. The reports address issues like general status, financial information, deviations from plan (and actions taken), change management, risk evaluation per sub-project and in total, and need for decisions by the ministry.

Measuring attainment of benefits

There are really no common practices for this. When the promised benefits are in terms of increased efficiency or reduced workforce, the benefits will be attained in terms of reduced budgets in the future. In some cases, however, very clear goals have been set while there is no effective way to measure the benefits. In some agencies, there has been a concerted effort to ensure that reduced efforts in some areas have resulted in more time spent on new work areas of high priority. Whether this yields better results in the new work areas may be very hard to measure.

In several cases, an IT project is undertaken to facilitate a new way of operation, e.g. a new set of rules for computing taxes, a new benefit for families with small children, etc. In these cases attainment is the simple result that the new way of operation actually works.

Example: In the SIAMO project there is a stated efficiency benefit which will be attained through reduced budgets for administrative purposes in the future. Moreover, there is a separate subproject working on current work practices and resource consumption, future organisation and work practices in case handling, increased visibility of possible benefits, and organisational consequences.

Financial auditing ex post

Again, this will depend on who has responsibility for the project, and also on the funding of the project. The responsible level will perform auditing as appropriate. If the project has been given separate funding by the Storting, the project will be visible in the government's annual reports.

The Office of the Auditor General will also conduct a financial audit. This audit, however, mainly addresses the legality of the way money has been spent. The Office of the Auditor General may also choose to audit specific projects in more detail.

Example: In the SIAMO project, which has separate funding, the ministry will report to the Storting in the annual budget on how the budget will be spent next year and how it was spent last year.

1.5. Management models

Relationship between agencies and ministries

In the Norwegian public administration, the directorate model is fairly well implemented. This means that the ministries are relatively small (around 250 employees in average) and in principle should work as secretariats for the ministers, preparing material for processes in government and the Storting (e.g., the annual budget), and implementing policies on behalf of the ministers. The latter includes management and follow-up of the ministries' subordinate agencies. Directorates, i.e. agencies governed by a responsible director general, deal with other tasks. It is considered good public management to delegate the practical implementation of policies to the agencies, and thus to keep only political and strategic issues in the ministry.

In general the agencies enjoy considerable independence (arms length agencies). As mentioned above, agencies may (and are expected to) initiate and fund IT projects within their annual allocations. In large agencies projects of substantial size may be run this way. Therefore, as some ministries report, the ministries do not have an overview of the IT projects in their subordinate agencies.

In Norway, each minister is individually accountable to Storting (like Denmark and Finland, but unlike Sweden). The minister is in principle responsible for all activity in the ministry's subordinate agencies. As a result, directorates are normally governed directly by the ministry. Boards of directors are uncommon, and if used they often have limited responsibilities. There may in many cases be a discussion on where the limit goes between adequate overall governing of agencies and a practice that satisfies the needs arising from the responsibility of the minister.

Management models for large IT-projects

There are no commonly adopted management models for large IT projects except what can be derived from the line principle (see section on policy) and what is otherwise stated above.

As to recommendations and guidelines, Statskonsult has published a booklet on guidelines for the management of large IT projects 0. In the booklet, three roles are identified. These are the roles of strategic management, customer and supplier. In other terms, this is a distinction between those who make the decisions, those who have a need and those who provide the solution. The general recommendation is that care should be taken in the identification and fulfilment of these roles, as severe problems may arise if this is not clear.

In a practical situation, there are several groups of actors that have a relation to these three roles:

- The responsible ministry
- The agency's senior management
- The "owners" of the future system, often the managers in the relevant part of the agency
- The end users¹
- The agency's IT department
- The project group
- External commercial suppliers (if any)

In the guidelines there is a general warning against unclear roles. A common problem has been that the agencies' IT departments have ended up with a mix of roles, sometimes indeed with all three roles. The guidelines also contain some advice on what type of assistance can be bought from external suppliers. These range from a fully responsible supplier of a ready to use system, via consultants used within the project organisation of an agency to independent, external quality assurance.

2. CASES

The first two cases are described on the basis of published material, the rest are based on material collected especially for this report.

Case 1: Tress-90

National Insurance Administration, Ministry of Health and Social Security

This project was the first publicly known and by far the biggest IT scandal in Norway. The project was stopped after several years of development and at a considerable economic loss. It was followed by inquiries by Riksrevisjonen (Office of the Auditor General) and official hearing in the Storting in February 1996 0.

1. End users were not included in the guidelines for the management of large IT-projects, but for the sake of completion, they are mentioned here.

Purpose

The purpose of the project was to develop a common electronic case handling system for all the Local Social Security Offices (approximately 460, one in each municipality, the largest cities has up to 20). The National Insurance Administration is responsible for these offices and took the initiative to develop the system. When the project started, the Local Social Security Offices used two different case handling systems and they were to be replaced by a totally new system. The project also included extensive investments in a new technological infrastructure in all the Local Social Security Offices.

Economy

Tress-90 was a fixed price project that included computers, systems development and education. Total cost was NOK 1.2 billion (EUR 150 million). The cost of the software development part of the project amounted to about NOK 26 million (EUR 3.4 million).

Functionality

The system was to cover all the tasks performed at the Local Social Security Offices. It contained administrative procedures in connection with calculations of different kinds of social security payments and various administrative tasks. The two existing systems had to be maintained and kept running in parallel with developing the new system.

Time frame

The decision to start the project was taken in 1989. The project started with deciding system architecture and acquiring technical infrastructure. The part of the project that included designing the new system started 1 April 1992, with 1 March 1993 as completion date. It was a fixed price project. However, the requirements were not fixed and already half a year later, the supplier wanted to renegotiate the agreement because of numerous changes and additions to the requirements. There were many revisions in the plans and finally came the decision to stop the project from 12 March 1993. The main reason for this decision was that the project was far behind schedule.

Organisation

The National Insurance Administration was responsible for the total project management and the co-ordination between the subprojects. The Ministry of Health and Social Affairs did not play any active part in the project. It did not participate in the project organisation. Progress and budget reports were made as part of the ordinary reporting between Ministry and Agency.

Project management

Project management was handled within the National Insurance Administration. Many of the sub-project managers were inexperienced and lack of professional project management was pointed out as a main reason for the problems the project ran into. A large amount of money was paid for modules that were not finished.

Case 2: FLID

Directorate of Taxes, Ministry of Finance and Customs. 0

Purpose

The purpose of the project was to introduce IT-based tools in the Local Tax and Registration Offices (about 4300 users in 435 different locations, one in each municipality). In addition to the acquisition and roll out of the technical infrastructure, the project included development of an electronic case handling system and a central national register. These systems replaced manual routines. The project also included implementation of organisational changes, training and considerable investments in technical infrastructure.

Economy

Total expenses in the pilot period came to NOK 197.1 million (EUR 24.4 million). The amount included development, testing, and implementation of organisational changes at the Local Tax and Registration Offices. The hardware acquisitions, software, training and establishment cost for the user support organisation was estimated at approximately NOK 445 million (EUR 55.5 million).

Functionality

The administrative system performs control of tax forms and calculations of income tax. The system also contains administrative routines and systems administration. The central national register is a database containing information about Norwegian citizens.

Time frame

Planning started in 1986. In 1987 the directorate of Taxes started running pilots at 9 Local Tax and Registration Offices. The number of pilot offices was gradually extended. When the system development was completed, the total system ran through a pilot period. Rolling out of the finished system took place in three distinct groups from 1992 to 1994.

Organisation

The system was developed internally with some hired consultants. The acquisition and roll out of technical infrastructure were organised as a separate project that started after the system had been tested and run in pilot installations.

Project management

The project management organisation was led by the project director. There were separate projects for developing the administrative system and the National Central Register.

Case 3: TOPP

Norwegian Public Service Pension Fund, Ministry of Labour and Government Administration.

Purpose

The project started as a result of an external analysis. The Ministry commissioned both this analysis and the IT project. The purpose of the project was:

- To develop an IT system that could handle frequent changes in regulations pertaining to the calculations of pensions.
- To reconstruct the organisation according to the new work processes introduced by the new IT system.

Economy

Total cost of the project: NOK 86.1 million (EUR 10 million), NOK 68.1 million, (EUR 8 million) special funding from the state budget, NOK 17.7 million (EUR 2 million) cost of own labour resources. There is an additional need of about NOK 200 million (EUR 25 million) to improve the data quality in connection with the changeover from old to new system. This was not included in the initial estimates.

Functionality

The system is an electronic case handling system that includes calculations of pensions. It is flexible and allows for frequent changes in the regulations.

Time frame

The Norwegian Public Service Pension Fund ran a pilot project that included a cost/benefit analysis before deciding to run the project. The main project started in 1995 and finished in February 2000. In 1997 it was enlarged due to an extension of the project itself, combined with cost overruns. The completion date was postponed 1 year due to problems with access to key personnel and greater complexity than expected in advance. Statskonsult is conducting an evaluation of the project and the evaluation report is due early in 2001.

Organisation

The managing director of the Norwegian Public Service Pension Fund has been the “owner” of the TOPP project. A steering committee with representatives of the Norwegian Public Service Pension Fund and hired experts from the consultant company have been leading the project. Representatives of the Ministry were originally members of the steering committee, but withdrew in order to avoid mixing roles. There was continuous reporting on deviations from plan and/or budget. In addition the cost/benefit analysis was adjusted after each stage. The project has also been a topic of the ordinary steering meetings three times a year between the ministry and the agency.

Project management

The project was divided into 5 stages. The main contract is with a large consultant company (Andersen Consulting). This main contract has been followed by sub-contracts for each stage.

Each stage contained analysis, design, construction, tests and roll out. The contract was signed after the design phase of each stage. According to the contract, the project could have been stopped at any stage.

Case 4. SIAMO

Directorate of Labour, Ministry of Labour and Government Administration 0, 0

Purpose

To develop a new overall system for the local labour offices (approximately 3700 users).

Economy

Total cost NOK 675 million (price level of 1998) (EUR 83 million). The last two years the allocations over the central government budget have been reduced compared with the initial plans, and this has led to displacements in the original phases of the project even though the total frame of the project has not been changed. However, it has not given rise to serious problems for the project.

Functionality

The system covers most of the needs of the Local Labour Offices. The project is divided into four:

1. New case handling system.
2. New financial management and personnel system finalised in 1999.
3. External user services for job-seekers and employers. First version finalised in June 1998.
4. New technical infrastructure finalised in 1999.

Time frame

The planning of the system started in 1995 and the project started in the summer 1997, financed by the Directorates ordinary budget. From 1998 the project got special funding on the state budget. In spring 1998 there were serious problems in the development of the new case handling system. The problems were due to the chosen developing-tool, not satisfactory plans, organisation and managing of the project. The project was reorganised and the contract with one of the suppliers was terminated. It was decided to acquire a case handling system instead of self-developing it. The problems have not affected the planned date of completion. The other parts of the project have been delivered according to schedule.

Organisation

The project is now organised in 4 sub-projects and there are steering committees both for the project as a whole and for each of the sub-projects. The Director General is member of the steering committee for the main project. The project organisation also includes a project counsel with employee representatives from all levels of the organisation and from the trade unions.

The Director General and the project management were heavily criticised in an internal audit report because of the problems mentioned above. As a result, the Project Director was replaced. The use of external consultants for planning, follow up and quality assurance was exceeded and the Ministry established tight reporting routines and followed the project closely. These reporting routines are used as example in the previous sections of this report.

Project management

In spring 1998 criticism was directed at the project management because of the problems mentioned above. The Director General of the Directorate of Labour admitted that the project management responsibilities were not undertaken in a professional way. Major alterations were made as mentioned above. Before the problems in 1998 the project tried out both reporting true the hierarchy/line and direct from the project manager to the Director General.

The project manager now reports directly to the Director General. The project is using a contract for incremental systems development that is quite new to the public sector.

Case 5. Hydra II

The Norwegian Water Resources and Energy Directorate, Ministry of Petroleum and Energy

Purpose

The project relates to the development of hydrological databases in order to establish a national hydrological archive.

Funding

The project was financed through the ordinary budget. Up to now about 20 person-years have been spent. System maintenance requires about 2 person-years. Hardware investments were also handled within ordinary budgets.

Functionality

The system replaced an earlier system that did not satisfy the requirements regarding flexibility, data capacity and support of new technology in front end systems. Management wanted to be up front technologically with efficient use of computer-based tools. The system handles long time data series with variable resolutions in space and time. It can also handle other environmental data.

Time frame

The planning of the system started in 1991. Development started one year later and in 1994 the first version was put into operation. The system is being continuously maintained and new modules are added.

Organisation

The system was developed using internal resources. It was followed up through ordinary reporting in the Directorate according to line principles and half-year/year reports.

Project management

Project management was weak and unprofessional when the project started. There was much focus on being up front technologically and on system design, and little focus on risk analysis. However due to close contact with the users and good skills in analysis and design, the system now functions according to expectations. It has a good structure, is well documented and easy to maintain.

Case 6: Diskos/PetroBank®

Norwegian Petroleum Directorate, Ministry of Petroleum and Energy

Purpose

The project is the result of collaboration between the Norwegian Petroleum Directorate and petroleum companies in Norway. The purpose of the system is to establish a common petroleum technical database. Petro Data AS, which was founded in 1993 as a joint venture between the companies IBM, PGS and TNN, has been assigned the operational responsibility for the database according to contract with the Diskos group (the Norwegian Petroleum Directorate and 16 petroleum companies, figures by October 1999).

Economy

The development of the system was financed through collaboration between the Norwegian Petroleum Directorate, three Norwegian oil companies (which formed the original Diskos group) and IBM (later taken over by a seismic company called PGS (Petroleum Geo-Services). All the current members of the Diskos group contribute with yearly funding for the maintenance of the system. Development costs are distributed according to an algorithm decided by the management committee. In addition, all the companies pay for access to the database.

Functionality

DISKOS 0 is a common national data repository for exploration and production related data. The DISKOS/PetroBank® software has been developed to handle digital seismic, data on wells and production data. It handles complicated ownership of data with frequent changes. Petro Data AS has established an operation centre where large amounts of data are stored in a secure way. Access to the data is secured through special security solutions.

Time frame

The project was started in 1993 and the first version of the database was put into operation in 1995. The system is being maintained continuously.

Organisation

The Norwegian Petroleum Directorate is operator for the database and leads the Management committee and the Steering Group. All members of the project have to sign an accession document that describes the decision process and the budgeting process. A group of 5 members participate in the Steering Group. There are work groups that define data types. These work groups keep close contact with system developers and the project management. The objective of these work groups is to ensure that the user requirements are handled satisfactorily. All principal decisions are treated in the Diskos Management Committee.

Project Management

The Norwegian Petroleum Directorate is responsible for project management. This includes the project manager position, the secretary and legal assistance. The Norwegian Petroleum Directorate is also responsible for the book keeping.

3. LESSONS LEARNED

Previous large failures have created a certain fear of new failures. Awareness about the problems with large IT projects has therefore increased in later years.

There is, however, a lack of tradition in dealing with IT-related issues in management and in governing agencies in the government administration. IT has to a large extent been seen as a purely technical matter, in isolation of other issues. A special problem is how a ministry can deal appropriately with IT in its subordinate agencies while at the same time not interfering unnecessarily with internal matters of the agencies. Sometimes ministries govern IT in their agencies close to unknowingly, for example in terms of working with bylaws, which need to be implemented in IT systems to have an effect, but not bringing the IT related considerations into the work with the bylaws. Statskonsult has documented that top level managers in the government administration have little IT competence⁰. This may partially be explained as a matter of seniority, but part of the explanation may also lie in the lack of IT issues in the typical educational backgrounds of senior government employees. There appears to be a difference in the IT content in the typical educational backgrounds of business and government managers.

Norway has a very tight labour market. While this is a blessing in terms of a relatively low rate of unemployment, it means that the shortage of new IT related occupational groups is a real problem. Government struggles to be competitive in terms of compensation and in terms of offering interesting tasks. As a result, government may lack the capacity and competence needed to fulfil its intentions with regard to the use of IT.

IT investments are different from other investments in their relatively high level of risk and uncertainty. While in traditional investments uncertainty is normally eliminated in early pilot studies, this is often not the case with IT. The design activity is proportionately larger for IT projects than for other construction projects. It may make sense, and is technically feasible to delay selected decisions to a very late stage of the project. Government has in general had problems in dealing with risks, as reflected in the motivation for the new regime on risk evaluation of large investments. This new regime clearly is a step forward, but

its threshold may be too high for IT investments. Moreover, it is not evident how the procedures can be used cost effectively for smaller IT projects.

In systems development, it is a matter of fact that requirements do sometimes change, although professional practices should try to eliminate as many uncertainties as early as possible in the projects. The need for change management results in challenges in budgeting and contracting. Often, these challenges are not met, resulting in projects deviating considerably from the contracts, rendering the contract useless as a means of managing the relationship to the supplier. Statskonsult's IT contracts do not handle incremental systems development sufficiently well. Statskonsult has co-operated with research and industry in developing a more open-ended contract, called PS 2000. Experience from use of this contract has not yet been collected, but it has been used in the SIAMO project.

Within a relatively hierarchical organisation such as the Norwegian government administration, project work traditions are not very strong. This may pose challenges in many areas, but is clearly felt in the area of IT. Managing projects is never easy. As described in the section on management models, there is a need to work with the different roles of various actors with respect to an IT project. Specifically, there are difficulties with steering groups. There is considerable variation in how the notion of steering group is understood. Sometimes they are used as mere discussion groups. There is no common understanding as to whether a ministry can or should participate in a steering group for large IT projects within one of its agencies.

There are examples of projects which are highly successful in isolation, but which appear to struggle with issues of co-operation with other parties. Co-operation between agencies to reduce the burden on businesses through better co-ordination of data collection is hard to achieve. In addition, exchange of data between agencies is subject to problems. The problems are not technical, but more in terms of achieving the appropriate alignment of practices in the agencies. As a result, data may be transferred successfully, while severe problems related to "data quality" persist.

The recommendation from the FASIT project 0 on pitfalls and criteria for success addressed a series of issues related to the project. However, connections between project internal successes and actual implementation of the project results in the user organisations are still lacking. We may now see a development where more professional project managers are hired in, to the benefit of the project itself, but sometimes detrimental to the relationship between the project and the line organisation.

As mentioned in the section on funding, it appears that there are some incentives in the budget process that may indeed encourage larger, more sophisticated and more risky project initiatives than what would be formulated based on internally defined needs. A careful proposal, neatly designed in small modules, may end up as too small to be worthy of attention in the larger budget process.

Although not really touched upon in this report, we have experienced large differences between different agencies in terms of how IT is managed and funded within the agency. In some agencies there is a strong, central control over IT development and investments. In these agencies there is little variation between the branch offices in how they use IT. In other agencies there is a tendency to deal with IT locally in the regional or branch offices, and the central directorate thus has much less power over IT investments and the use of IT in the organisation.

4. REFERENCES

In this list of references we have included the documents referred to in this report. Whenever possible we have included URLs to documents available online. For ordinary publications from Statskonsult we have dropped the URL. Most reports from Statskonsult can be found at <http://www.statskonsult.no/publik>

We have also included some references to classical literature on IT failures, e.g. Ackoff 0, Boehm 0, Oz 0, and Willcocks 0.

Russel L. Ackoff. Management Misinformation Systems. *Management Science*, 14(4):B-147–B-156, December 1967.

Aftenposten Interaktiv Netthinnen 21. October 1998. Datafiasko til 675 mill. i Arbeidsdirektoratet (IT failure for 675 mill. in the Directorate of Labour) See <http://www.aftenposten.no/nyheter/nett/d56624.htm>

Aftenposten Interaktiv Netthinnen 22. October 1998. (Løwer: Hanish har ansvaret) (Løwer: Hanish is responsible (Løwer was the Minister of Labour and Government Administration at the time and Hanish was the Director General of the Directorate of Labour) See <http://www.aftenposten.no/nyheter/nett/d56719.htm>

Barry W. Boehm, Software Risk Management. *2nd European Software Engineering Conference*, pages 1–19, University of Warwick, Coventry, UK, September 1989. Published as Lecture Notes in Computer Science, 387, Springer Verlag.

DISKOS, The Norwegian data repository for petroleum data. See <http://www.npd.no/engelsk/projects/diskos/diskosfr.htm>

Electronic Government: Cross-sectoral development of information technology in central government administration. Action Plan, Ministry of Labour and Government Administration, Oslo, 13 January 1999. <http://www.odin.dep.no/aad/engelsk/publ/rapporter/002001-990156/index-dok000-b-n-a.html>

eNorway 1.0. Action Plan, Ministry of Trade and Industry, Oslo, 29 June 2000. <http://www.dep.no/nhd/norsk/p10001865/p10001876/024031-990036/index-dok000-b-n-a.html> See also <http://enorge.dep.no/>

Erfaringer fra store statlige IT-prosjekter (Experiences from large government IT projects). Report 1998:6, Statskonsult, Directorate of Public Management, Oslo.

Innst.S.nr.190 (1995/96) Innstilling fra kontroll- og konstitusjonskomiteen om Riksrevisjonens konstitusjonelle antegnelser til statsregnskapet for 1994, Tress-90. Sluttoppgjør mellom Rikstrygdeverket og Norsk Informasjonsteknologi (Recommendation from the Control and Constitution Committee on the remarks from the Office of the Auditor General to the National Account 1994, Tress-90 Final agreement between the National Insurance Administration and the supplier: Norsk Informasjonsteknologi AS)

Intervjuer om IT og IT-kompetanse: Hvordan IT-medarbeidere og ledere mener at statlige IT-virksomheter skal få dekket sitt behov de neste 5–7 årene (Interviews on IT and IT-competence: how the IT-workforce and managers think government agencies can meet their needs in the next 5–7 years). Note 1999:6, Statskonsult, Directorate of Public Management, Oslo.

IT i staten 1999. (Government's use of IT, 1999.) Report 2000:08, Statskonsult, Directorate of Public Management, Oslo.

IT-kompetanse hos toppledere i staten: en kartlegging (IT competence among top managers in government: a survey). Note 2000:1, Statskonsult, Directorate of Public Management, Oslo.

IT-personell, behov og tilgang: Hvordan skal statlige virksomheter kunne dekke sitt behov de neste 5–7 årene? (IT-personnel, need and supply). Report 1999:11, Statskonsult, Directorate of Public Management, Oslo.

The Maintenance Agreement. Report 1998:11, Statskonsult, Directorate of Public Management, Oslo. See <http://www.statskonsult.no/publik/publikasjoner/avtaler/index.htm>

NOSIP 3, datakommunikasjonsstandarder for offentlig forvaltning. (Norwegian OSI Profile 3, data communications standards for public administration). Statskonsult, Directorate of Public Management, Oslo, 2000.

Tron Øgrim. Staten og nerdene: Hvordan kan statens behov for IT-arbeidskraft dekkes de neste 5–7 årene? (The government and the nerds: how can the government's need for IT workforce be met in the next 5–7 years?). Note 1999:5, Statskonsult, Directorate of Public Management, Oslo.

Effy Oz, When Professional Standards are Lax: The CONFIRM Failure and its Lessons. *Communications of the ACM*, 37(10):29–36, October 1994.

Programutviklingsavtalen (Standard agreement for program development). Standard agreement, Statskonsult, Directorate of Public Management, Oslo, 1999.

The Purchase Agreement. Report 1998:10, Statskonsult, Directorate of Public Management, Oslo. See <http://www.statskonsult.no/publik/publikasjoner/avtaler/index.htm>

Pål Sørgaard, IT Co-Ordination and Public Management Reform: A comparison of Finland and Norway. Research report 4/2000, Ministry of Finance, Public Management Department, Helsinki, 2000. See <http://www.vn.fi/vm/julkaisut/tutkimukset/jaselvitykset/pdf/rr42000.pdf>

Store statlige IT-prosjekter: Styring, organisering og ansvarsfordeling (Large government IT projects: management, organisation and division of responsibilities). Guidelines, Statskonsult, Directorate of Public Management, Oslo, 1997.

St. prp. nr. 88 (1990/91) EDB og omstilling i skatteetaten (Electronic Data Handling and reorganisation in the tax administration)

Leslie Willcocks, Informatization in public administration and services in the United Kingdom: toward a management era? *Informatization and the Public Sector*, 1(3):189–211, 1991.

NEW ZEALND

INTRODUCTION

The New Zealand public sector, as defined by the OECD “working definitions”, has around nine major IT projects in progress in any given year. Currently five of the major IT projects are classified as high risk and subject to close monitoring by the State Services Commission (SSC) and The Treasury.

History has created the impression that public sector IT projects have performed poorly due to a number of high profile failures. However recent research clearly shows this not to be so, compared to the private sector and internationally.

This research, commissioned by the Department of the Prime Minister and Cabinet (DPMC) in November 1999, was to determine:²

- The successes and problems in New Zealand public sector IT projects.
- The key contributors to success and deliverables.
- How public sector projects compare with those in the private sector.
- How New Zealand IT project performance compares internationally.
- What opportunities exist for improving IT projects deliverables.

The key findings of this research were that IT project performance was slightly better in the public sector than the private sector; there was little difference between New Zealand and international performance; and there is significant room for improvement.

There have been a number of initiatives by Cabinet over the last 12 months to improve the IT project monitoring and approval processes. Although some changes occurred prior to the research report, it was too early for their impact to flow through into the report’s findings.

More detail from the DPMC research is included below in the Case Study Section (2).

1. GENERAL INSTITUTIONAL FRAMEWORK

1.1. Policy

There is an accepted governance structure to support major IT projects in the New Zealand public sector. Within this structure the monitoring agencies (SSC and The Treasury) develop their approach to each IT project following consultation with each other and agreement from the Chief Executive (CE) of the agency planning the project.

2. ‘Information Technology Projects: Performance of the New Zealand public sector in perspective’, SIMPL Group and NZ Institute of Economic Research (Inc).

There is an agreed budget process and monitoring regime based on the imperative that the CEs are accountable for the project business case, budget, project implementation, and deliverables.

There are also a number of guidelines, pointers to the best practice for agencies to follow and approaches to monitoring of major IT projects by the SSC and The Treasury.

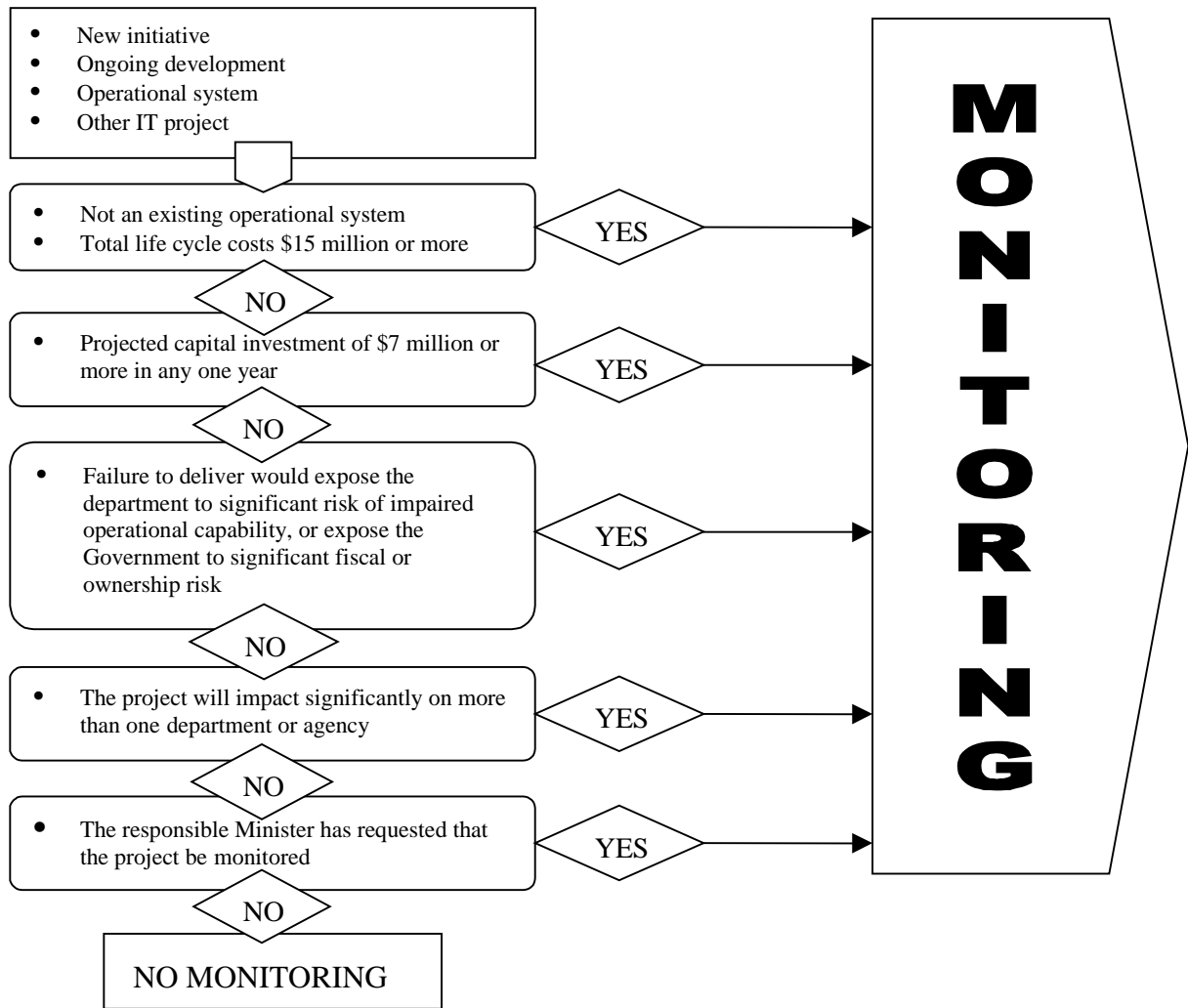
1.2. What constitutes a major project?

A major IT project is a new initiative, an ongoing development or acquisition project, an operational system, or other type of IT project (including studies against existing contracts) that meets any one or more of the following criteria:³

- The project is not an existing operational system and its projected life cycle costs are NZ\$15 million or more (gst inclusive). Costs include all equipment, software, contractor services, supplies, staff compensation and related staff costs, and inter/intra agency payments.
- The project includes a projected IT capital investment equal to or exceeding NZ\$7 million (gst inclusive) in any one year.
- Failure to deliver the project in line with the projected functionality requirements, costs and timeframes would expose the department to risk of impaired operational capability, or expose the government to fiscal or ownership risk.
- The project will impact significantly on more than one department or agency.
- The responsible minister has requested that the project be monitored.

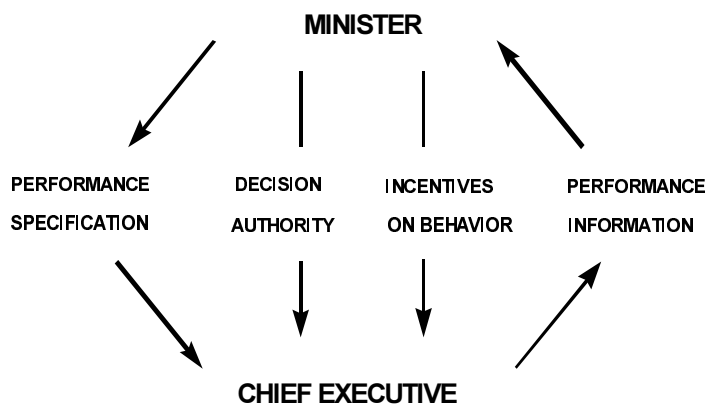
The following diagram depicts the process of deciding whether or not a proposed project is to be monitored.

3. Cabinet decisions in 1999 and 2000.



1.3. Accountability

The public service CE accountability framework consists of a series of relationships underpinned by legislation and documents. This framework is shown below.⁴



Under this model, the responsible minister:

- Specifies certain standards of performance for the CE to meet.
- Delegates decision-making authority (including the allocation of resources) to the CE.
- Establishes appropriate performance incentives for the CE.
- Requires the CE to certify actual performance, through independently verified reporting.

The following table shows the key elements of an IT project and how they fit into the accountability framework.

Accountability Element	Key Documents/Project Elements	Responsibility for Element
1. Performance specification	IT strategic plan Individual project business cases Relevant milestones in CE performance agreement	Department prepares Department prepares, monitoring agencies advise, Cabinet approves Department prepares, SSC implements and monitors
2. Decision authority	Ministerial approval	Responsible Minister (within legislative and Cabinet authority)
3. Incentives/sanctions	Annual performance review against performance agreement	State Services Commissioner
4. Performance information	Project reporting and independent QA (if required under monitoring regime) Departmental quarterly reporting (unaudited) Departmental annual reporting (audited)	Department for original preparation Monitoring agencies and independent QA for external monitoring

4. The Chief Executive Accountability Framework and Budget Process as they Relate to Information Technology Projects. The Treasury and SSC report to Government, April 2000.

The specification of performance and the delegation of authority take place during the budget process for approval of IT projects. The requirements for performance information and operation of incentives/sanctions form part of the monitoring regime for IT projects. The CE's financial accountability includes:

- Full control of the level of working capital held by the department.
- The right to sell or dispose of surplus fixed assets without Cabinet approval.
- The right to use the department's working capital to purchase new assets without prior ministerial or Cabinet approval within certain delegated limits,⁵ and provided the total value of the department's assets is not increased.
- The responsibility for capital budgeting, asset maintenance decisions and risk management.

Therefore, if the cost of an IT project is within the delegated limits and can be funded from the department's balance sheet, Cabinet approval is not required. However, if the project requires partial or full new funding, or exceeds the responsible minister's delegation limits, Cabinet must approve its funding.

1.4. Budget and approval process

Any request for new funding for a major IT project must be approved by Cabinet, as the Executive arm of government. In certain circumstances, departments seeking to invest existing capital in an IT project must also seek Cabinet approval. The Cabinet approval process is commenced when the responsible minister puts forward a department's proposal and business case to Cabinet. In certain cases the project may be considered by a Cabinet sub-committee in the first instance, but the final decision will be taken by Cabinet. This decision is then considered for ratification by Parliament as part of one of the two annual Appropriation Acts.

The table below sets out the recommended budget process for delegating authority to the responsible minister and CE. This approach may not be the most appropriate for low-risk, small or low-cost IT projects, but should be followed unless otherwise agreed between monitoring agencies, the department and the minister.

5. The current limits are that CEs have authority to spend up to \$7 million on capital expenditure without ministerial approval. The responsible minister's authorisation is required where the total cost of capital expenditure projects is between \$7 million and \$15 million. Cabinet approval is required for capital expenditure greater than \$15 million. Prior to 1999, the delegation limits for capital expenditure were lower, with any project over \$5 million requiring responsible minister approval, and any project over \$10 million requiring Cabinet approval.

Step	Stage in process	Supporting document	Owner	Approver	Timing
1	Strategic planning	Strategic business plan IT strategic plan	Department	Responsible Minister	Any time during year
2	Initial approval for scoping for each module	Business case (focusing on strategic fit with indicative costs)	Department	Cabinet	Budget round (to allow trade-offs with other projects)
3	Approval of capital injection for each module	Revised business case (with detailed costings, benefits, deliverables and project management)	Department	Cabinet	Following completion of submission
4	Completion of each module	Report with independent QA	Department (independent QA if required)	Joint Ministers	Following completion of each module
5	Annual CE performance review	Report of achievement against business case	Department	State Services Commissioner	End of each year

Following approval of a major IT project, a quantitative risk analysis approach is used as the basis for appropriations, access to contingency funding and cash draw-downs.⁶

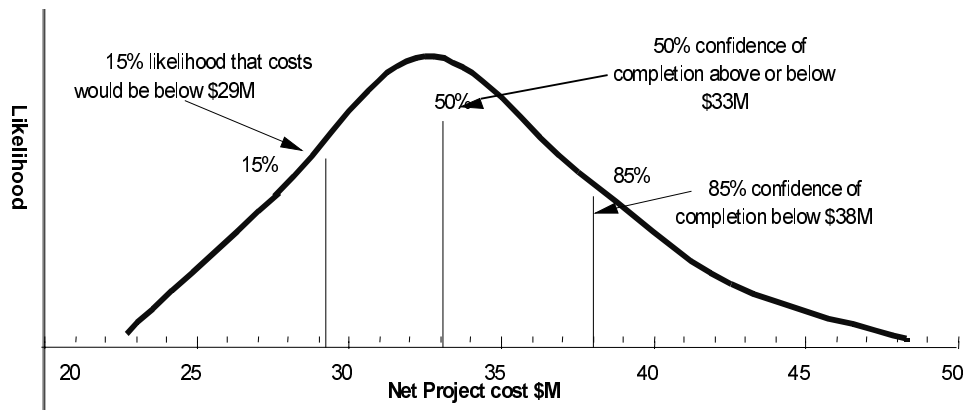
Quantitative risk analysis techniques and risk-based funding, where cost-effective, incorporate the relative risk of the project into the funding decision, and make risks explicit to ministers considering the business case.

Quantitative risk analysis involves assessing each risk (impact and probability) and modelling the project outcome on simulations of these risks. This will produce an estimated probability distribution of total costs. The final probability distribution describes the range of outcomes and their relative likelihood. The potential impact of both project-specific and other risks on costs, benefits and timeframes are then considered explicitly by the department, monitoring agencies and ministers as part of the project analysis. Examining the distribution enables high risk proposals to be identified and deferred. Because such projects have a very wide range of likely total cost outcomes, their deferral may allow the department to identify or implement strategies to reduce risks.

Using this approach, the approved baseline amount would be based on the most likely cost (the 50th percentile on the distribution), but the department would initially receive cash to less than the 50th percentile. If project risks materialise, the department could seek Joint Ministerial approval for cash disbursement up to the approved baseline. For example, the funding structure for one current IT project means the department receives cash up to the 15th percentile on the probability distribution, with the facility to request Joint Ministerial approval to disburse cash between the 15th and 50th percentile. If costs appear likely to exceed the 50th percentile appropriation, further Cabinet approval must be sought to continue the project.

This is illustrated below.

6. The Chief Executive Accountability Framework and Budget Process as they Relate to Information Technology Projects. The Treasury and SSC report to Government April 2000.



While this risk-based approach to funding may not on its own prevent cost over-runs, using a funding distribution enables the fiscal impact of the project’s risks to be made explicit to ministers in their consideration of the business case. At the same time, it provides some flexibility for departments to manage their projects within defined parameters. However, as the use of quantitative risk analysis techniques is resource intensive for departments, it may only be cost-effective for major IT projects.

Although both the contingency and quantitative risk analysis approaches may be appropriate in certain circumstances for “major” IT projects, quantitative risk analysis appears to be the most appropriate means of incorporating risk into the project decision and funding.

1.5. Monitoring Regime

In July 1997 Cabinet set up a monitoring function for major IT projects in the public service following ministerial concern over the management of the risks of IT projects, in particular the National Library’s NDIS and the Police INCIS projects.

Since 1997 a number of refinements have been made to the CE’s accountability as it applies to IT project management, and the budget process in relation to the estimation of costs for IT projects.

The current monitoring regime is as follows:

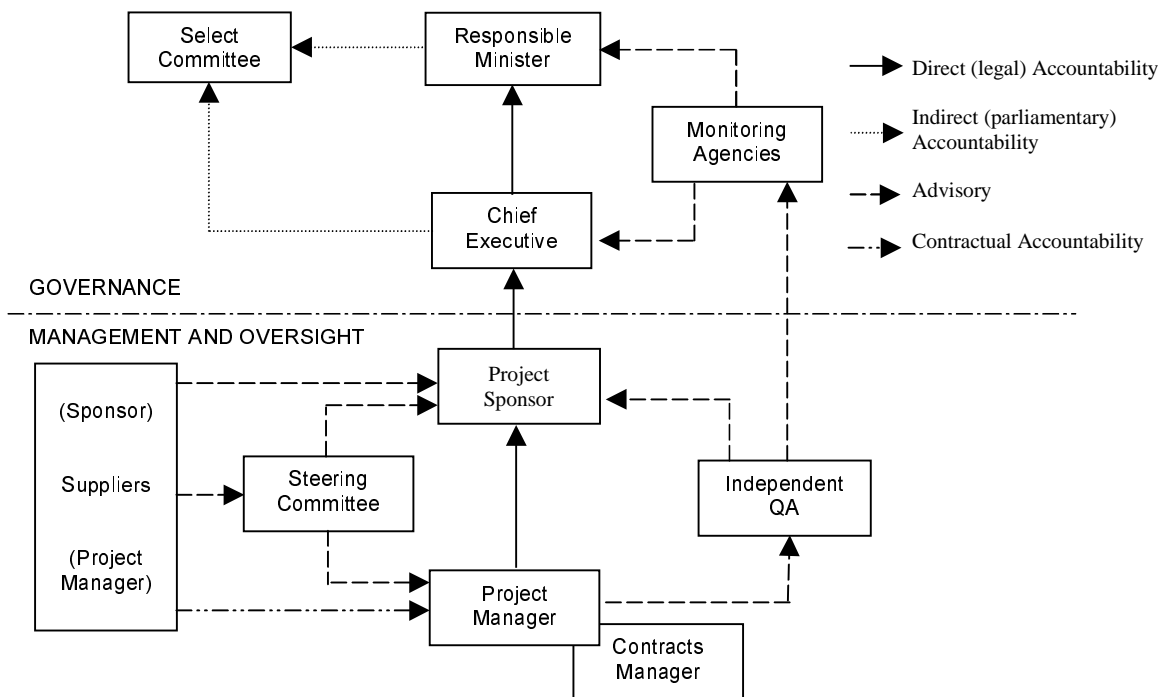
- For IT projects, the CE of the initiating department is accountable for:
 - a) Ensuring that the business case is sound and the department’s risk management, project management, and monitoring structures follow “best practice”.
 - b) Delivery of the module and associated benefits, as outlined in the business case.
 - c) Processes put in place to manage off-track projects, if this becomes necessary.
- On all major IT projects, departments ARE required to provide regular independent quality assurance (QA) reports to the project sponsor and CE on key issues and risks arising from the project.
- Departments are required to forward an unedited version of the independent QA reports to the State Services Commission (SSC) and The Treasury.
- The SSC and The Treasury will make provision for external QA of off-track projects, reporting to the monitoring team but charged to the department.

- The Ministers of State Services and Information Technology receive regular reports on the risks associated with IT projects across the public service.
- The SSC and The Treasury, with an interdepartmental group, produce “good practice” guidelines on principles, processes and practices for developing and managing projects with a major IT component.
- The agreed guidelines are used by The Treasury and the SSC when assessing departmental performance and capital funding bids.

1.6. Governance of Major IT Projects

In the central government context, it is important to distinguish between “governance” and “management” roles. Governance and oversight are undertaken by those with the authority to approve projects and the use of resources for those projects; management is about the actual delivery of projects. Overall, CEs, ministers and parliamentarians have a governance role; project sponsors and project managers a management role.

The following diagram summarises the relationships between the roles.⁷



7. Governance and Oversight of Large IT Projects. Office of the Controller and Auditor-General.

1.6.1. Roles

Project Sponsor

The Project Sponsor is accountable for promoting the interests of the project, monitoring its progress, ensuring that it is appropriately resourced, mediating its interests with any competing interests of other business units, and, in general, facilitating achievement of the CE's interests in the project.

Project Manager

A project manager becomes accountable for a project after agreement with the CE (delegated to the Project Sponsor) that he or she will deliver the specified deliverables within the framework of the management strategies, and taking account of the project risks.

There are reciprocal responsibilities between the Project Manager and the CE.

From the CE's perspective, the Project Manager is responsible for ensuring the project deliverables within time and budget unless variations are approved by the Project Sponsor. The CE relies on the professional expertise of the Project Manager to achieve these deliverables.

From the Project Manager's perspective, this assumes that the CE, through the Project Sponsor and his or her staff, has confidence that the specification of the new system and contracts with suppliers will deliver what the Department wants, and that the CE will provide the framework and resources to enable this.

Contracts Manager

This is an emerging, usually part-time role, which is likely to require a commercial or legal background, and might be sourced either externally or internally.

The Contracts Manager is accountable for monitoring and reporting on the compliance of each party's formal and informal obligations, on behalf of the customer.

Establishing and monitoring reporting requirements is a key part of this role.

The Contracts Manager advises the CE of the impacts any proposed change may have on the contract, especially liabilities and warranties.

Chief Executive

The CE is responsible for the resourcing and appointment of key personnel for the project. These are amongst the most critical decisions to the project's success. The CE needs to be fully satisfied that the Sponsor and the Project Manager have the requisite skills and experience.

The CE is also accountable for the use of funds allocated to the project, ensuring:

- that the business case is sound, and:
 - a) is linked to the strategic plan.

- b) is able to deliver the business benefits.
 - c) identifies the proposed technology for delivering these.
 - d) specifies the method of implementation, for example, usually to free the infrastructure from applications and provide for the delivery of business benefits in modules.
 - e) assesses any uncertainties in the financial estimates.
 - outlines the main risks and the proposed risk management process.
 - outlines the project governance and management structure.
- that the project team is actually delivering the specified system to the schedule.
 - that the organisation is preparing itself to use the new system and its business processes to meet the department's business objectives.
 - that the risks arising from the project are manageable and reported to Government.

Monitoring Agencies

The Treasury and SSC officials are accountable to their ministers to provide correct, complete and timely advice on the viability of the business case, on monitoring project progress against benchmarks, on the risks arising, and to alert ministers in advance of any difficulties. There should be no surprises.

Responsible minister

The responsible minister is accountable to Parliament for the performance of the department, including its management of the project. Government periodically modifies its political direction. Where this changes the business objectives of a department with a project in progress, the minister needs to consider the impact on the project deliverables, time scale and budget in the following ways:

- Is there any conflict between the objectives and deliverables of the existing project and the new policy or legislation?
- If there is, should the project proceed?
 - If so, what changes are needed to ensure it delivers the new political direction? What allowance should be made for the new time and cost to deliver to the modified policies?
 - If not, the minister should withdraw funds and cancel the project.

Select Committee of Parliament

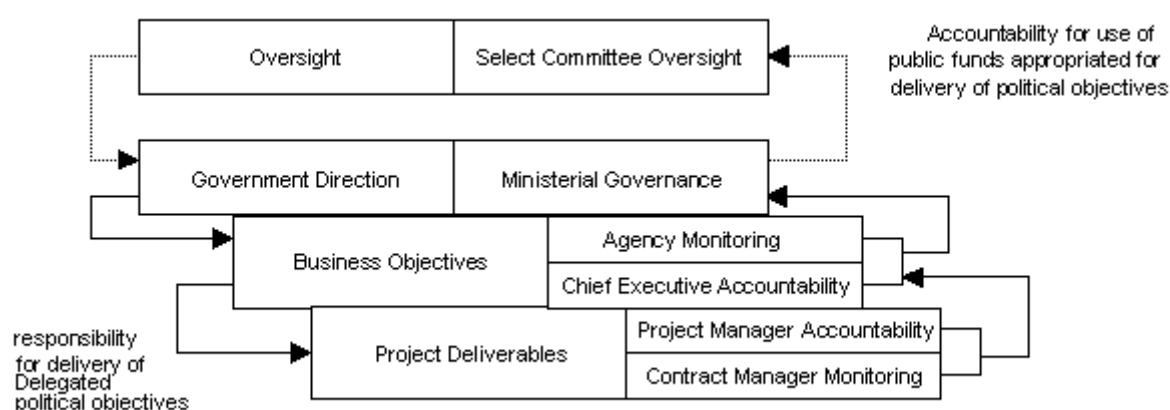
The functions of the Select Committee are to:

- review the capital components (if any) of the Estimates for each department, during examination of the Estimates; and

- review the department’s performance and current operations – and its capability (including IT capability) during the annual financial review.

Select committees can also undertake special inquiries into any aspect of departmental activities, including IT projects.

This means that, unless a project requires a significant capital injection, or is a very significant part of a department’s activities, the Committee is unlikely to be proactively informed of its status and health by the department.



Independent Quality Assurance

Independent Quality Assurance (QA) has an established role in the project. As a general rule, QA reports should be made directly to the highest level of project management - such as the CE, Project Sponsor and Project Steering Committee. QA reports are most effective when they are distributed unfiltered to the Steering Committee. They should not be subject to any undue influence from the Project Manager. They should also be made available directly to monitoring agencies.

Major IT projects should ensure that QA consultants are very senior, experienced and independent, thus able to provide objective opinions. Extra cost incurred for this expertise is low relative to its benefits.

2. CASES

2.1. Case Study 1: Risk-based Funding Rules for Complex Projects

Overview

Land Information New Zealand (LINZ) and The Treasury have improved management and ministerial decision-making by adopting quantitative risk analysis techniques to estimate costs and completion time for a major complex IT project – “Landonline.”

Endorsement of this approach by Cabinet and the Auditor-General is a major development in the evolution of public sector IT project planning and implementation. The quantitative risk analysis approach has also been adopted by a number of public and private sector organisations.

About LINZ

LINZ holds more than 30 million land records and provides annually 1.5 million title searches, processes 900 000 land transactions, and approves 18 000 survey plans. LINZ started the Landonline project in 1997 to automate processes for title registration and survey approvals.

At the time, public sector approvals for business case expenditure were based on collating single-point estimates for the likely least cost and duration of each project component, with no formal contingency funding.

Due to the limitations of this funding approach for projects such as Landonline, LINZ and The Treasury developed a quantitative risk analysis and associated funding methodology. This methodology has now been endorsed by Cabinet and the Auditor-General and adopted by other public and private sector users as a basis for deciding on investment in high-risk projects and controlling ongoing project funding.

Conception

LINZ used the old approach in 1997 to estimate and secure funding for Landonline but its limitations became apparent when market quotes exceeded initial cost and time estimates. Unquantified risks that materialised in 1999 compounded the situation.

LINZ and The Treasury decided to develop a better way to assess possible cost, timeframe, and benefit deliverables for IT projects, based on the likelihood and impact of identified risks materialising. The type of quantitative risk analysis used to simulate risk impacts on oil exploration project costs and timeframes was seen to have potential.

Implementation and Evolution

Undertaking quantitative risk assessment involved:

- Risk identification to create a risk register and assign owners for each risk.
- Risk impact workshops to assess their effects.
- Detailed assessment of project dependencies and the inter-relationships between individual components.
- Using quantitative risk analysis software to build a model of the impact of risks on *Landonline*, generating a probability distribution curve. Rules were developed to control access to funds based on agreed reporting arrangements and project governance. The risk analysis and associated rules were used to support Cabinet submissions seeking funding and support.

Purpose

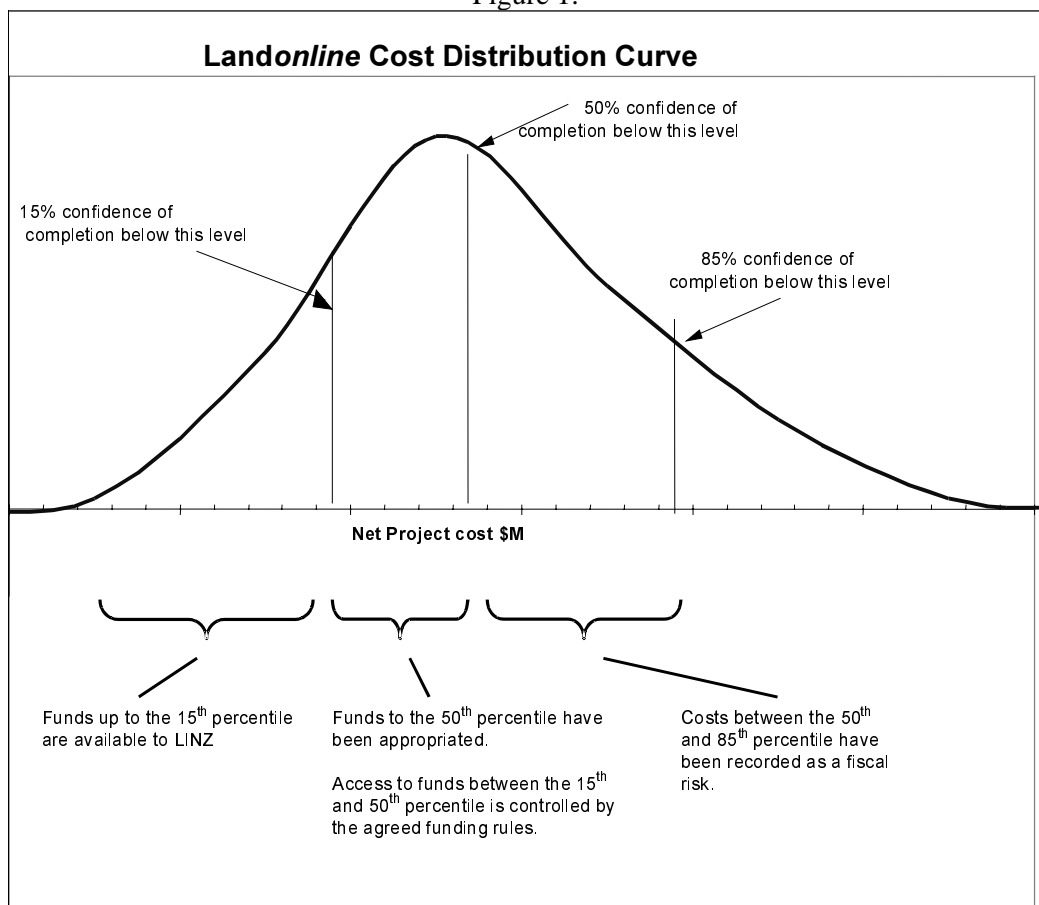
LINZ and The Treasury adopted quantitative risk analysis and developed the associated funding methodology to:

- Create a tool capable of identifying benchmarks to monitor progress and performance of the entire *Landonline* project.
- Monitor individual components of the project over the course of each financial year and over the project's life.
- Provide LINZ management, The Treasury and the Minister with a better understanding of the cost and time risks associated with *Landonline*.
- Provide LINZ and the Minister with a clear understanding of accountabilities for the financial management of the *Landonline* project.

Nature and Scope

Outputs of the risk analysis provide decision-makers with representations of possible outcomes. The level of uncertainty (as a result of risks that may materialise) can be presented graphically as a spread of the distribution of likely outcomes (see Figure 1).

Figure 1.



The distribution curve makes it easy to see that a range of possible project outcomes exists. This enables ministers and public sector officials to understand and accept that project costs are not fixed but are expected to fall within an identified range, depending on the likelihood of risks materialising.

Funding Methodology

Because the range of project funding costs is linked to the likelihood of risks materialising, LINZ and The Treasury were able to develop a clear set of funding rules to govern access to appropriations. Cabinet has accepted these rules.

Using the new methodology, LINZ has been appropriated funds for Landonline to the 50th percentile of likely completion cost but may incur expenditure only up to the 15th percentile.

Access to funds above the 15th percentile requires ministerial approval and is subject to LINZ demonstrating that additional expenditure is justified because an identified risk has materialised. Only Cabinet can approve expenditure that results in the total cost of Landonline exceeding the 50th percentile.

Controls

Deriving distribution curves for individual project components enables management control, management reporting, and creation of incentive frameworks to control activities and monitor progress throughout the project's life.

The work required to quantify risks within discrete components of the overall project enables early identification of risks materialising, and early implementation of mitigating strategies.

Specific Innovations

Specific innovations related to the introduction of this methodology include:

- Introduction of an explicit risk management approach to public sector project management.
- Introduction of funding rules that recognise the uncertainty in cost and timeframes, and that allow for expenditure variations on individual project components and variations in expenditure between financial years.
- Incentives for project managers to identify and disclose risks.
- Recognition of the likelihood and impact of risks, making them more visible and measurable.

Improved Communications

Other innovations include the clarity with which projects can be explained and communicated to interested parties. Graphical representation of likely and possible project outcomes simplifies explanation of the parameters of key project variables.

Better Budget Management

The methodology supports integrated control frameworks for measuring, reporting and monitoring progress against estimates of cost, quality, time and other identified risks.

Project component budgets are now managed within approved ranges rather than as discrete budgets based on single-point estimates. An incentive framework that fosters desired outcomes can be applied to each project component.

Better Project Management

Management control and financial performance is reinforced because funding rules give flexibility to transfer under-expenditure or over-expenditure between financial years and between project components, without resubmitting the business case. This rolling risk-adjusted funding increases management control and the ability to enforce accountability by:

- Risk ownership and early development of mitigation strategies.
- Providing incentives for managers to manage risks for which they are accountable.
- Easily and rapidly modelling the effect of changes to business case assumptions.
- Providing timely information on the effect of a change in any component on the likely outcome of the entire project.
- Involving monitoring agencies, vendors, operational staff and users in identifying and quantifying risks.

Multiple Benefits

Quantitative risk analysis in the public sector budgeting and appropriations process benefits many stakeholders, including:

- Taxpayers – benefit from improved assessment of the viability of complex projects and from better management of public sector risks.
- Ministers – benefit from improved assessment of the viability of complex projects, better disclosure and communication of project risks, and a clear set of rules governing accountability for project budgets.
- Monitoring agencies – benefit from improved assessment of the viability of complex projects and from the existence of benchmarks against which to measure progress.
- Public sector – benefits from an approved methodology to construct business cases for approval, and from the fact that effective project monitoring limits media and public perceptions of poor management.
- Project managers – benefit from improved understanding and management of risks through better identification, assessment and modelling of their impact and likelihood.

- Professional bodies – benefit from a wider understanding, acceptance and use of quantitative risk analysis techniques.

Benefits for LINZ

As a result of developing this methodology:

- LINZ managers are more aware of risks, their impacts and mitigation options.
- Quantitative risk analysis is now a standard technique in LINZ.
- Control and monitoring is more robust, and processes for adjusting estimates are seen to have a sound, objective basis.
- LINZ's relationships with monitoring agencies have improved because of their involvement in risk identification and an agreed framework for monitoring and adjustment.

Confidence in Outcomes

Integration of the quantitative risk analysis methodology into government budget, appropriation and public sector control processes, replacing single-point estimates, is a measure of its success. This is illustrated by the following:

- Cabinet has endorsed the methodology and made it a requirement for all major public sector IT project business cases.
- The Auditor-General has sanctioned the methodology.
- Ministers, ministerial sub-committees and advisory boards have greater certainty and confidence in the outcome of *Landonline* due to the rigour applied to identifying cost and time risks and the clarity of communicating their impact.
- *Landonline* is progressing on target and operating within the new business case parameters.
- The LINZ CEO spends less time dealing with media inquiries about budget issues.

Cabinet Endorses for Wider Use

The initiative is easily replicable, and benefits projects with risks on account of long timeframes, or where a large initial investment is required before benefits are realised. Evidence of replication is seen in Auditor-General and Cabinet endorsement throughout the public sector and adoption by other organisations. The cost of replicating this innovation is minimal compared to the scale of potential savings and the gains in better management and financial control.

Adopted in the Private Sector

One of LINZ's private sector IT vendors has adopted the methodology and is applying it to the internal risk analysis and project tendering processes.

LINZ is applying the methodology to non-IT projects, such as the Continental Shelf Delimitation programme and Crown property litigation cases.

2.2. *Case Study 2: Customs Department CusMod Project*

From 1992 to 1997, the NZ Customs Service underwent an extensive and successful programme of change called CusMod⁸ (Customs Modernisation) in order to improve its organisation.

The management team began by preparing an intensive strategic plan, with the purpose, as the CE put it, of getting “everyone pointing to the same compass point”.

The team started to work with other senior managers to understand better the wider environment in which Customs operated. In particular, they had a series of meetings with key stakeholder groups to identify the ways in which Customs could become more effective. These meetings showed that there was not only a need for a change in work processes, but also for some major “attitudinal” change. Customs was widely perceived as a “policing, law enforcement agency” with little regard for customer service or client responsiveness.

It became clear that the old system of random checks would no longer work. Customs needed to become more sophisticated, to capture high-quality intelligence in order to target its interventions. This new philosophy was based on striving for minimum intervention by stopping only “high-risk” goods and passengers.

Once this vision was in place, and senior executives supporting it, CusMod had a clear mandate to proceed. With key stakeholder expectations under close management, the CusMod programme could begin transforming the organisation. Customs soon discovered that this would require substantial outside support, both in sheer resources to do the work, and in knowledge and expertise (especially in change management) which were not available in-house.

Customs decided that it wanted a “business partner” who would work with them in understanding the business, work out the goals, architect a solution, and then help in selecting and building the component parts of the solution. Above all, they were looking for a partner who would share responsibility for implementation – thus reducing risk to Customs.

Following a tendering process which produced a shortlist of three candidates (from 55), Customs appointed Andersen Consulting as its partner. This firm had recently completed a high-profile IT project with the New Zealand Inland Revenue Department. Although it did not have a track record in the customs business, its proposal showed a “genuine willingness to share responsibility throughout the programme.”

By establishing new work processes, systems, technology, and modes of behaviour, New Zealand Customs has developed a robust and responsive infrastructure and become one of the most innovative customs organisations in the world. The successes of the CusMod programme have been dramatic:

- The average time to clear goods through Customs has been reduced from 1.5 days to 40 minutes or less, for 90% of imports.

8. Building the Intelligence-Based Organisation: The New Zealand Customs Service. June 1999, Derek LeDayn and David Keane.

- Over 50% of goods are now cleared in transit. Goods can be collected directly from ships and aircraft without being stored on the wharf or in warehouses, thus reducing importers' costs.
- All communication for the importation of goods into New Zealand is now fully electronic.
- Passengers can now be “cleared in the air”. High-quality intelligence targets and checks high-risk individuals as they leave their aircraft, so that less than 2% of passengers are stopped (down from 10%).
- Client satisfaction across a range of services has been significantly improved.

The main reasons for CusMod's success were:

- The philosophy of “striving for minimum intervention by stopping only high risk goods and passengers” had real meaning to management and staff.
- Staff and management participated in the development and achievement of the strategic plan.
- Changes to the business processes were clear to all stakeholders and most staff did not feel threatened by the change.

In other words, staff knew what needed to be done, were in agreement with it, and focused on its achievement.

2.3. *Case Study 3: Performance of IT Projects in the New Zealand Public Sector*

The following are edited extracts from the report commissioned by DPMC summarising the results of the five areas commissioned for research. They provide a good overview of current New Zealand public sector IT projects performance.

The research approach and criteria were similar to that used by The Standish Group.⁹

The rate of successes and problems

Two sets of project performance criteria were adopted:

Tight (*project management*) – “Was the project on time, within budget, and to scope?” (These were the criteria used by Standish, and were adopted for this project in order to achieve comparability with the US results.)

Broader (*project product*) – “Did the project achieve organisational goals, in an acceptable timeframe and at an acceptable cost?” (This was adopted as a pragmatic basis for assessment of projects in the New Zealand private and public sectors, and to indicate the sensitivity of results to the definition of success adopted.)

New Zealand public sector results were:

9. The Chaos Chronicles. The Standish Group (1999).

	Tight – all projects	Broad – all projects
Success rate	38%	88%
Problem project rate	59%	9%
Failure/cancellation rate	3%	3%

The key contributors to success and deliverables

The respondents from core government identified the following top six factors as contributing to project success, problems and failures. The weightings reflect the aggregate importance placed on the factors by all core government respondents.

Top six Success Factors	Weighting
Professional project management and planning	20%
Clear statement of requirements	16%
Executive management support and ownership	14%
Clear vision and objectives	11%
Competent, hard-working, focussed staff	9%
Realistic expectations/expectation management	6%

Top six Problem Factors	Weighting
Changing or escalating requirements	13%
Incomplete requirements	13%
Lack of project management/ownership	11%
Lack of resources/insufficiently skilled resources	9%
Lack of executive support	8%
Unclear objectives	6%

Top six Failure/Cancel Factors	Weighting
Lack of project ownership/management	15%
Incomplete requirements	14%
Lack of executive support	13%
Changing and/or escalating requirements	10%
Unclear objectives	6%
Unrealistic timeframes	6%

Comparing the New Zealand public sector with the private sector

The same approach was used to analyse the results of the private sector IT projects reviewed. The comparative results were:

Success Rate	Tight – all projects	Broad - all projects
Government	38%	88%
Non-core public sector	38%	83%
Private sector	31%	82%

How New Zealand IT project performance compares internationally

	Revised US (Standish) findings	New Zealand study (development projects only)

Success rate – all projects	36%	32%
Problem project rate – all projects	64%	66%
Success rate – government projects	25%	30%

Using the “tight” criteria, New Zealand organisations as a whole recorded success rates broadly similar to those reported by Standish for the United States.

Opportunities to Improve Outcomes

The main lessons arising from the research were:

- Project risk increases with project size and duration, so special attention needs to be paid to major projects.
- Project management skills are essential to the conduct of complex IT projects.
- Risk of failure increases with the extent of development activity.
- In almost all cases it is good strategy to avoid using leading-edge but untried technology.

3. LESSONS LEARNED

There have been a number of documented project successes and failures in New Zealand over recent years from which to draw lessons and recommendations. This section summarises the more comprehensive list provided in Appendix B.

As most of the lessons have general application, they are grouped into categories familiar to IT project management, and listed below to provide context to their circumstances. The index characters (*e.g.* B.4) represent the relevant section in Appendix B.

Technology and Architecture (B.1)

Key issues impacting on technology and architecture were:

- Use of emerging technology, and that unproven in the planned environment.
- The application development was not broken down into a number of discrete business deliverables. Unable to measure project progress and baselines continually changed.
- No sound process to verify the proposed technical solution was deliverable and would meet the business requirements. Caused significant delays whilst a deliverable solution was sought.
- The proposed technical infrastructure met the requirements of the new application but within a very short period of time did not meet the requirements of the wider organisation. The resulting changes caused significant project delays and costs.
- Significant technology advancements took place in the industry during the project placing significant pressure on the project to change its technical direction.

- No business and technical blueprint at the beginning of the project led to change management and systems integration problems.

Governance and Management (B.2)

Governance and management has been the greatest contributor to project failure. Some of the issues to arise were:

- Lack of sound governance and management structures led to a loss of support from a large section of the business, significant risks were not quickly addressed, the project manager felt isolated and the monitoring agencies were not receiving balanced reporting.
- The chief executive didn't have strong links with the project. This caused continual resourcing issues, poor risk management processes and lack of support from the business.
- An inexperienced project manager appointed to run a large complex project. Too many problems arose from this project to list here, suffice to say there were significant cost overruns and most business deliverables were not met. The cost of a good project manager is insignificant compared with the losses incurred from a failed project.
- Expert advice is sought for a number of reasons. There were occasions where the expert's terms of reference were poorly drafted causing key areas for review to be omitted from their report. Also the reports were either presented or interpreted too positively. This led to poor decision making and major risks were not addressed adequately.

Risk Management Process (B.3)

The key findings with relevance to risk management were:

- Typically, the risks in a major IT project are very high both because of its complexity and also because the context of rapidly developing technology leads to a high degree of uncertainty. Without a pervasive and thorough quality management and risk management policies at all levels, there is a high likelihood of under-performance if not outright failure.
- It is imperative that a business case addresses all relevant issues to enable a sound business decision to be made. Business forecasts and financial estimates are worthless unless they are based on sound and well understood technical and operational plans.
- One of the major functions of a contract is to specify and manage risk. It specifies how risks are distributed between the parties. It follows that if this role is not well understood, and if the nature of the risks is not clear, then there will be trouble, particularly if the risks are later perceived to be unfairly distributed.
- A number of lessons arise from viewing the failure of a project to fully achieve its objectives from the point of view of risk indicators. The main lesson is that indicators of potential trouble and increased risk are there to be seen well before difficulties arise. Priority must be given to looking for such indicators, and if they are found, then prompt action must be taken.

Change Control (B.4)

Change control is normally a well understood process. An unusual problem arose in one project where the issue was due to the level of inscope change. The project had difficulty holding to a plan primarily because a business process re-engineering (BPR) sub project was generating a large number of 'minor' inscope changes for the application developers.

Project Formation (B.5)

Care needs to be taken in the strategic formation of a large IT project. This includes the initial research, business case, RFI/RFP process, identifying the key risks, methodology to test the business proposal and supporting technology, governance structures and appointment of key personnel.

One approach to address technology concerns is to carryout a 'proof of concept' exercise. A proof of concept should be completed prior to any technology commitment, in an environment capable of saying 'No Go' without loss of face or credibility.

The Contract (B.7)

For large IT projects provision should be made for a Contracts Manager to regularly verify both parties are conforming to the contract. The Contracts Manager should be a legal expert reporting to the sponsor, not necessarily a full time role.

Some recent lessons:

1. The contract should be used to define where risks will fall – purchaser verses supplier. For example, a fixed or capped priced contract places most of the risk on the supplier. However if the price has been seriously underestimated there is a real likelihood the supplier will make a commercial decision to walk away from the project.
2. Many provisions in a contract maybe designed to provide flexibility, however unless there is a common understanding between the supplier and purchaser over the life of the project significant problems can arise. As an example, a contract provided for technology substitution to future proof the project delivery. With a change of key personnel, the provision was used for a range of reasons other than future proofing leading to significant change control problems, delays and cost overruns.
3. Changes to the project deliverables should always be checked against the contract to ensure they do not impact warranties and end to end guarantees. Technology changed from that defined in the contract may relieve the supplier from warranties and performance guarantees.

Project Implementation (B.8)

Some lessons within this phase of the project were:

- There is interaction between the business changes and technology associated with a major IT project. The business changes should drive the technology and not vice versa. If business process re-engineering is not carried out till after the technical solution has become fixed (normally at the latest at the time of the signing of the contract), there is an increased risk that technology will drive

the business changes. There can then be an underground function creep that is hard for management to detect.

- For a major IT project to be successful it must be adequately resourced, particularly in terms of skilled and experienced personnel, and governance and management at all levels.
- Many major IT projects are likely to be subjected to pressure from many sources. Governance and management should be aware of and guard against negative aspects of pressure.

4. FUTURE PLANS

We are now seeing benefits arising from the approaches the monitoring agencies are taking *e.g.* recognising and taking corrective action where risks have risen to a prohibitive level, and better understanding and communication of risk to Government. However the approaches tend to fall into the reactive category. There is significant potential benefit to be gained (improving the 38% success rate) by augmenting current monitoring practices with more pro-active initiatives.

A key imperative to be taken into account when addressing pro-active initiatives, is to ensure CEs continue to be fully accountable for the successful completion of major IT projects. The initiatives should strengthen the agency's ability to attain a successful outcome, not take over their responsibilities. Potential avenues to achieve this are to:

- Establish and publish standards that should apply to major IT projects *e.g.* risk management, project management methodology and selection criteria;
- Improve the knowledge of those participating in projects. The 'Governance and Oversight of Major Information Technology Projects' report by the Controller and Auditor-General is a good example of this approach;
- Provide the means to communicate best practice; and
- Provide advisory services where appropriate.

There are examples where other countries have made significant progress down these paths including the provision of online support facilities. New Zealand does not wish to 'recreate the wheel' and plans to take on board the experiences of these overseas initiatives.

As many of the issues arising from IT projects are common to the public and private sectors, there is potential to improve the management of projects through the co-operation of both sectors. An initiative to explore ways for this to happen should be considered.

5. LITERATURE, WWW, AND STUDIES

The logical framework method for defining project success. Project Management Journal, (1999). Baccarini, D.

Software Runaways: Lessons Learned from Massive Software Project. Glass, Robert L (1998)

Failures, Prentice Hall, Inc., USA, which relies heavily on data from a comprehensive study about software "runaways" conducted by KPMG in the UK in 1989 and again in 1995.

PUMA/SBO/RD(2001)1

A Guide to the Project Management Body of Knowledge. Project Management Institute. www.pmi.org

The importance of the utilisation of a framework for senior executives to measure risk in IT projects. Royal, P (1995) Massey University

Information Technology Projects: Performance of the New Zealand public sector in perspective. The SIMPL Group and NZ Institute of Economic Research (Inc). www.ssc.govt.nz

The Chaos Chronicles. The Standish Group (1999)

The Chief Executive Accountability Framework and Budget Process as they Relate to Information Technology Projects. The Treasury and SSC report to Government April 2000.

Governance and Oversight of Large IT Projects. Office of the Controller and Auditor-General. www.oag.govt.nz

Building the Intelligence-Based Organisation: The New Zealand Customs Service. June 1999, Derek LeDayn and David Keane

High Level Analysis of the Government's Y2K Programme: A Future Perspective. State Services Commission.

CoBit. www.cobit.org.

**APPENDIX A
BUSINESS CASE CHECK LIST**

Overview Questions	Comments
Does the sound business case comply with Cabinet criteria (refer to Annex 3 to CO(98)17)?	
Are there technical issues that need to be resolved prior to consideration by Cabinet Committees and/or Budget Ministers?	
How ready would the proposal be to proceed if approved, and would alternative timings be viable or preferable? What impact would timing changes have on investment and baseline implications?	
Will the project assist the department in achieving its strategic goals?	
Do these strategic goals contribute to Government policy or the Key Government goals?	
Have possible alternatives been identified, and how do these compare?	
Is the investment in the department appropriate to the likely projected outputs to be purchased? Is the level and mix of assets appropriate?	
Are other votes/departments affected by the project?	
How is the collective interest affected? <i>e.g.</i> Where there are multiple users of a facility and one withdraws, the costs to those remaining may increase.	
Is the capital expenditure greater than \$7 million? Have Cabinet delegation procedures been followed in accordance with CO(99) 7?	

Questions on the estimation of costs and benefits	Comments
How strong is the business case (<i>e.g.</i> are there net benefits to proceeding, how robust are these, what is the financial return to the Crown)?	
How have the project costs been estimated? Can the department substantiate the robustness of the cost estimates and assumptions supporting them?	
Have people actually involved in the management of the project been involved in the estimation of the costs?	
Does the business case set out the total cost of the project, including non-cash items such as depreciation?	
Does it detail the assumptions made in discounting future cash flows (<i>e.g.</i> real or nominal cash flows and discount rate)?	
Does the project result in any social costs or benefits outside the department?	
If the estimated costs and/or benefits do affect other votes/departments, have they signed up to the costs/benefits?	
<p>Where internal staff costs are involved:</p> <ul style="list-style-type: none"> · Do the project costs include additional costs for internal personnel above normal operating costs? How many staff are required? · Are these reasonable? What comparisons or benchmarks are available to support these? · What happens to staff surplus to requirements following the implementation of the project? · Have redundancy costs, if applicable, been included? Does the timing align with the project milestones? 	
<p>Where consultant costs are involved:</p> <ul style="list-style-type: none"> · What comprises these costs? Are these costs likely to change during the course of the project? · Is it more cost-effective to utilise the department's own staff? Do internal staff have the appropriate skills? <p>Does the report justify the use of consultants and identify the risks of using consultants or internal staff?</p>	
Will the project lead to the avoidance of any costs? (These costs should be quantified and included in the analysis as benefits.)	
Will the project lead to increased or decreased business compliance costs, in terms of the requirements of the department acting in its own right and acting as agents for other Government departments? Has the department established appropriate mechanisms to meet these requirements?	
How have the benefits been estimated? Has the department broken the estimates into separate categories of benefit, <i>e.g.</i> operating efficiencies, decreases in corporate overhead, etc.?	
Are salvage values for assets at the end of the project accounted for?	
What is the impact on the price of outputs? For example, is there a trade-off between quantity and quality; price and quantity (increased prices may lead to lower demand)?	
Is the change in the price of outputs directly related to the project? (Are there extraneous variables?)	
Are the assumptions made in the benefit estimation realistic?	
Does the project result in any intangible benefits? Have these been detailed in the business case?	
Are NPV calculations included in the proposal?	
Could the timing of the costs and benefits change? Have different timing options for receipts and payments been explored?	

Projects that have positive *ex ante* NPVs sometimes fail because the actual costs are much greater than estimated, or the benefits or savings are not realised, or both. In many cases, the difference between *ex ante* estimates and the *ex post* realisation can be attributed to poor project management and implementation.

Questions on the control of the costs and the realisation of benefits:	Comments
Does the department have a formal project management structure for the project? Is there a Project Sponsor; Steering committee; Project managers? Are the roles and responsibilities of each of these clearly established?	
Does the department have the requisite expertise to oversee the successful implementation of the project?	
To what extent have relevant risks (either of proceeding or not proceeding with the proposal) been adequately identified?	
How will changes to the scope and scale of the project be approved?	
How will the actual project costs and benefits be tracked? Have appropriate milestones been developed? Will individual managers be held responsible for controlling costs and realising benefits?	
How frequently will reporting be? What will be covered in the reports? Who will receive the reports? Are these included in the recommendations to OCEC? Note that for IT projects, reporting requirements are set out in CAB(99)M24/6B - have these been followed?	
Is there an independent post-implementation review?	

Questions on the financing of the project	Comments
Is the department seeking an additional capital contribution from the Crown?	
<p>Are there alternative financing options that would avoid the need to draw on constrained Government capital funding <i>e.g.</i> financing from within baseline or from reprioritising the department's existing capital programme? Does the business case consider the pros and cons of alternatives for funding <i>part</i> of the project from within the current baseline?</p> <p>Note that additional capital from the Crown as owner should be the last resort for capital expenditure or working capital injections. The entity needs to show that other financing options such as accumulated depreciation and cash and asset sales are not available.</p>	

APPENDIX B

LESSONS LEARNED AND RECOMMENDATIONS

This list is not exhaustive, but includes issues experienced throughout the life of a number of large IT projects in New Zealand.

- B.1. Technology and Architecture
- B.2. Governance and Management
- B.3. Risk Management Process
- B.4. Change Control
- B.5. Project Formation
- B.6. Project Approval
- B.7. The Contract
- B.8. Project Implementation
- B.9. Approval and Monitoring Regimes

B.1. Technology and Architecture

Proposed Solution

Lesson	Recommendation
The project sought to achieve its objectives by implementing technology and architecture unproven in terms of size, complexity and geographical distribution.	Normally it is desirable to use proven technology. Where it is necessary to depart from this, a New Technology Testing programme (<i>e.g.</i> proof of concept) should be completed prior to contract and the CE and monitoring agencies should be satisfied that the technologies will deliver the business benefits.
Major IT projects will normally change the technical infrastructure and applications. The two are separate, though complementary, and should be dealt with as such. The bundling of applications and IT infrastructure into a single contract for a major IT project will significantly increase the project's complexity which will, in turn, increase the risk of serious problems.	For major IT projects, the IT infrastructure should preferably be "unbundled" from the applications and, where possible, the applications should be modularised into discrete business deliverables.

Core Architecture

The extensive changes to core architecture, whilst a major application development is in progress, will adversely affect the project.	Core architecture should not be changed unless absolutely necessary. Any changes should be in strict compliance with change control, be referenced to the business case and be reported by the Project Manager and to the Monitoring agencies. Where possible, changes should be delayed until after the application development has been completed.
The rate of change of technology over the life of the project can create significant pressures on project governance.	The life of the project should normally be limited to no more than one year. Any project of greater length needs to be broken down into a number of modules and predefined points where decisions can be made to modify technology to meet the new requirements.

New Technology Testing

<p>A contract requirement for emerging or unproven technology brings high risk. The normal approach would be to complete a New Technology Testing programme <i>e.g.</i> proof of concept. In the absence of New Technology Testing, the risk is usually prohibitive.</p>	<p>Emerging or unproven technologies should be subject to New Technology Testing, and used only after careful assessment of risk.</p>
--	---

Blueprint

<p>Without a blueprint at an early stage, a major IT project will lack the essential and integrating focus required for guiding the detailed design, development and change process.</p>	<p>Any major IT project should develop an effective blueprint prior to application design.</p>
--	--

Technology Substitution

<p>A technology substitution regime should not be used in place of a sound technical solution at the outset.</p> <p>A technology substitution provision in a contract is in principle an appropriate approach, as it is a means of giving some of the technical flexibility necessary for a major IT project. There are other ways of providing flexibility, however, such as in the form of the contract itself. A danger inherent in a technology substitution provision is that it is open to misuse. It cannot be used as a means of making up for shortcomings in the contract, such as the lack of a clear technical specification, and its use as a mechanism for changing major technical components of the solution will lead to increased delay and risk.</p>	<p>Major IT projects should have sound technical solutions at the time of contract and any technology substitution should be limited to substitution of items or components within the existing technical solution. Technology substitution provisions should not be used as a primary means of managing a contract.</p>
---	--

Role of Systems Integration

<p>Systems Integration for major IT projects is a skilled operation, normally requiring specialist advice.</p>	<p>Major IT project should normally engage a systems integration specialist.</p>
--	--

B.2. Governance and Management

Governance and Management of the Project

<p>Good governance and management structures, and experienced and skilled personnel are essential for the success of a major IT project, at the commencement and throughout the project.</p>	<p>Government and government agencies should ensure that major IT projects have sound organisation structure, adequate resources, and experienced and skilled personnel for project governance and management.</p>
--	--

Chief Executive

<p>Projects are likely to suffer without CE attention to governance and management.</p>	<p>The Chief Executive should oversee the governance and management of a major IT project by:</p> <ul style="list-style-type: none"> Ensuring acceptance and continued commitment by the whole of the organisation to the project. Ensuring the project and business case support the overall strategy of the organisation. Ensuring adequate resourcing. Appointing a qualified Project Sponsor. Being fully briefed, at least monthly, on progress, major risks and resourcing issues. Receiving and acting on relevant reports and information. Ensuring achievement of objectives. <p>The CE should be aware of and resolve any serious dispute between senior project personnel that impacts adversely on the project.</p>
---	--

Project Sponsor

<p>The primary responsibility for the appointment of the Project Manager rests with the Sponsor. The appointment by the Sponsor of a Project Manager lacking the appropriate skills and experience carries high risk.</p> <p>The Project Manager should report to the Sponsor and departure from this carries increased risk.</p> <p>Failure by the Sponsor to ensure good relationships amongst senior personnel can be detrimental to the project.</p> <p>Lack of commitment of all personnel in the business can be detrimental to the success of the project.</p>	<p>The Sponsor should be either the CE or a senior executive manager.</p> <p>Sponsors should appoint a Project Manager who has the necessary project management skills and experience.</p> <p>The Project Manager should report to the Sponsor.</p> <p>The Sponsor should address and resolve any unsatisfactory relationship between senior personnel immediately.</p> <p>The Sponsor should continually reinforce commitment to the project by the entire staff.</p>
---	--

Project Managers and CIO

The success of a major IT project is critically dependent on the skills and experience of the Project Manager. For a large complex project it is more important to get good IT project management skills than to appoint an unskilled Project Manager from within the organisation.	The person appointed as Project Manager should have the appropriate skills and experience in management of major IT projects.
Difficulties can arise in a major IT project if there is an inappropriate reporting structure. There are likely to be problems where Project Managers are not reporting directly to the Project Sponsor, for example, reporting to a line manager.	The Project Manager should report directly to the Sponsor.
There are serious risks to a project if proper procedures are not followed in the appointment of key personnel.	Governance and management should follow proper procedures, <i>i.e.</i> a “from the top down” process, in relation to the appointment of key personnel.
Serious disagreements between or within governance or management of a project can be detrimental to its success.	Governance and management should be aware of the potential for conflict in human relationships, and take action to avoid this. Where a serious dispute arises, governance or management need to address and resolve the dispute promptly.
Poor or inadequate reporting inhibits proper governance and management and is prejudicial to the efficient operation of the project.	In order to perform their functions, government and management must enforce timely, full and frank reporting at all levels and in particular by the PM, independent QA and audit. Any departure from that should be heeded by governance, management and monitoring agencies.

Steering Committee

The lack of an effective Steering Committee as part of the project governance and management structure is detrimental to a project.	It is essential that all major IT Projects have an effective Steering Committee. The membership should include senior line management. Monitoring agencies should insist on a Steering Committee, and attend, or receive minutes of, meetings.
---	--

Baselines and Milestones

Proper baselines and milestones need to be established to enable effective management and monitoring.	Cabinet ministers and monitoring agencies should require that proper baselines and milestones are indicated in the business case, and that material changes be referenced to the business case and reported to the monitoring agencies. Reports on project progress should reference the original business case baselines.
---	--

Project Managers' Reports

The lack of timely and comprehensive PM reports is detrimental to the project and to monitoring.	PM reports need to be at least monthly, address key risks, and be concise, focused and properly reflect the current project status.
--	---

Culture

<p>The culture of an organisation can have a detrimental impact on the ability of a major IT project to perform and deliver its objectives.</p>	<p>Governance and management needs to be aware of the adverse impacts culture may have on major IT projects.</p> <p>Monitoring agencies should also be aware of the problems that might arise if a major IT project is being managed within a culture likely to impact adversely on the project deliverables.</p>
---	---

Experts' Reports

<p>There are many occasions when outside experts must be asked to review and report on aspects of a major IT project. However, the effectiveness of the process can be reduced for a number of reasons.</p> <ul style="list-style-type: none"> • Difficulties can arise if the terms of reference are not clearly defined. • The report may be deficient in some way and not deal adequately with the issues it addresses. • At times, reservations and negative comments in the body of the report are missing from or downplayed in the report's executive summary. • Selective quotation from an expert's report can give a very wrong impression of its findings. <p>A report can be used as a substitute for action. Reservations and negative findings in a report by outside experts often appear to be ignored or downplayed.</p>	<p>Agencies, when considering an expert's report, should:</p> <ul style="list-style-type: none"> • Check the terms of reference of the report; • Assure themselves of the adequacy of the report, use a peer review if needed; and • Consider the whole of the report, particularly any reservations and negative comments. <p>Management needs to be sure that an expert's report is adequate, accurate and balanced, and should look out for any indicators to the contrary.</p>
---	---

Approved Quality Management and Warnings not Heeded

<p>Major problems in a major IT project do not arise suddenly. There are always warnings of trouble and indicators that all is not well. If these are sought, seen and dealt with promptly, the risks to a project can be reduced and problems averted. On the other hand, not heeding warnings and hoping optimistically that all will be well is a sure path to disaster.</p>	<p>Throughout major Government IT projects, policies and practices should be adopted that encourage an awareness of the need to notice and, where appropriate, take immediate action on warnings and indicators of trouble.</p> <p>Monitoring agencies should be alert to any departure from this requirement and should pay particular attention to how, and how promptly, issues are resolved.</p>
---	--

B.3. Risk Management Process

General

<p>Typically, the risks in a major IT project are very high, both because of its complexity and because the context of rapidly developing technology leads to a high degree of uncertainty. Without pervasive and thorough quality management and risk management policies at all levels, there is a high likelihood of underperformance, if not outright failure.</p>	<p>Major IT projects should have comprehensive formal quality management and risk management processes that are fully integrated into all aspects of project management. All personnel should be aware of risk, and of the risk consequences of all their decisions and actions. Monitoring agencies should monitor the observance of and adherence to the formal risk management process.</p>
--	--

System Complexity

<p>Highly complex processes are difficult to manage successfully. They require special systems-related skills. The unexpected and often unpredictable interactions within complex systems leads to counterintuitive consequences and to high uncertainty and risk .</p>	<p>Major and complex IT projects should ensure that they have special systems skills available to their management.</p>
---	---

Risk Manager

<p>It is difficult to manage the risk within a major IT project and to adhere to a formal risk management process without a Risk Manager, whose role should be to ensure the presence and continuing health of the risk management process.</p>	<p>Major IT projects should have a Risk Manager.</p>
---	--

Governance

<p>Major IT projects are particularly vulnerable to increases in complexity and uncertainty arising from lack of a clear and central integration and focus. Too frequent changes of technology and direction will also increase the risk.</p>	<p>Major IT projects must have tight management and control.</p>
---	--

Reporting

<p>A major IT project requires full and frank reporting of both positive and negative information and assessment. Where problems and issues are known but information about them is not distributed either within governance and management, or to monitoring bodies, serious trouble can be expected.</p>	<p>The reporting mechanisms, communication channels and culture in major IT projects must both allow and encourage full dissemination of all relevant information, no matter how unpalatable it may be.</p>
--	---

Business Case

<p>It is imperative that business cases address all relevant issues to enable a sound business decision to be made. Business forecasts and financial estimates are worthless unless they are based on sound and well-understood technical and operational plans.</p>	<p>Cabinet should prescribe a comprehensive specification for all the aspects to be addressed in a business case. These should include assurance of and evidence for the soundness of the technical and operational solutions underlying the business forecasts and financial estimates. The forecasts and financial estimates should address risk by including estimates of uncertainty. Government and monitoring agencies should ensure that these aspects are covered effectively.</p>
--	--

Contract

<p>One of the major functions of a contract is to specify and manage risk. It specifies how risks are distributed between the parties. It follows that if this role is not well understood, and if the nature of the risks is not clear, then there will be difficulties, particularly if the risks are later perceived to be unfairly distributed.</p>	<p>In a major IT project, risk and risk management matters should be specifically addressed before a contract is signed.</p> <p>Flexible forms of contract should be used for major IT projects.</p> <p>If there is material change in risk from those identified in the business case, the change should be referenced to the business case and be reported, including a report to the Monitoring agencies.</p> <p>Government agencies contracting out major IT projects should monitor risk control mechanisms within the contract.</p> <p>Government agencies should not sign a contract for a major IT project without first being assured that the risks inherent in the project are:</p> <ul style="list-style-type: none"> · Well understood. · At an acceptable level. · Capable of management in accordance with the risks identified in a business case. · Fairly distributed between the parties.
---	--

Communication

<p>Good communication is essential in a complex project. Good communication is clear, complete, balanced and accurate. Furthermore, it is a two-way process.</p>	<p>The governance and management of a large and complex project should ensure that good communication is in place.</p> <p>Reports must also be written in clear language and be delivered on time.</p>
--	--

Role of Advisers

<p>Independent expert advice is particularly important in projects with a high degree of complexity and with a major technological component. Two things follow: that the advice is certified to be sound, and that it is acted upon appropriately.</p>	<p>The management of large and complex IT projects, and monitoring agencies involved with the approval and oversight of them, should seek independent expert advice where appropriate.</p> <p>A peer review or second opinion on expert advice should normally be sought where there is doubt, or where the issues are critical.</p> <p>Project management must deal promptly and thoroughly with issues raised by independent advisers.</p> <p>Expert advisers must make every effort to ensure the advice contained in their reports is sound, and that their reporting of it is clear and balanced.</p>
---	--

Risk Indicators

<p>A number of lessons arise from viewing the failure of projects to achieve its objectives fully from the point of view of risk indicators. The main lesson is that indicators of potential trouble and increased risk are there to be seen well before difficulties arise. Priority must be given to looking for such indicators, and if they are found, prompt action must be taken. More detailed lessons are:</p> <ul style="list-style-type: none"> • Pressure on a project to succeed can arise from a number of quarters. A high degree of pressure can lead to increased risk. • New technology can bring high risk to a project. • Management inexperience leads to increased risk. • Major organisational change brings high risk. • Human relationship difficulties in a complex project lead to increased risk. • The complexity inherent in major IT projects leads to increased risk. • Inexperience and inappropriate technical skills in a major IT project bring with them increased risks. 	<p>Priority must be given to looking for risk indicators. If they are found, management must take prompt action.</p> <p>Management must be aware of the danger that pressure on and within a project can lead to increased risk. It must therefore watch for symptoms of high pressure and take steps to deal with its sources, which can be many. Where this is not possible, care must be taken with other aspects of the management of risk.</p> <p>New or emerging technology should be avoided wherever possible. Where it is adopted, the high risk it brings must be managed. Wherever possible, proven technology and off-the-shelf packages should be used for major IT projects.</p> <p>High priority must be given to the risk management of major organisational change.</p> <p>Because complex projects bring high risk, complexity should be reduced wherever possible.</p> <p>Human relationship difficulties in a complex project must be dealt with promptly.</p> <p>Because risk management and quality management are closely related, where there is high risk there must be thorough quality management.</p> <p>Large and complex IT projects must have management with particular skills for dealing with complex systems.</p> <p>The increased risks brought to a major IT project by inexperience and inappropriate technical skills must be appropriately managed by bringing in external reviews and other means.</p>
--	---

Project Manager

<p>A PM's reports to the project sponsor, independent QA, auditors and oversight bodies provide a major means by which the health of the project can be assessed. It follows that where there are deficiencies in the reports, particularly with regard to project risk, the consequences can be serious. However, it is generally the case that deficiencies in the reporting process are indirectly signalled for all to see by, for instance, a lack of timeliness or a failure to report on risks.</p>	<p>It is essential that a PM give full and timely reports, particularly with regard to project risk.</p> <p>Monitoring agencies and others overseeing major projects should ensure there is comprehensive reporting of risk by the PM.</p>
--	--

B.4. Change Control

Change Control

<p>An effective change control process is essential for a large complex project. The process should reflect changes to the project budget and impacts on the business case.</p> <p>The process should record both change out of scope as well as change within scope.</p>	<p>The governance and management of major IT projects should put in place and enforce a proper change control process. Monitoring agencies, as part of their duties, should confirm that a proper change control process is in place and being observed.</p> <p>The impact of changes should also be reflected in the project budget and on the business case.</p>
---	--

B.5. Project Formation

Project Development (RFI, RFT and RFP)¹⁰

<p>Unless care is taken in the strategic formation of a major IT project, risks can be increased and this was apparent in the project by the adoption of a fixed or capped price contract for the whole of the project including infrastructure and application development.</p>	<p>The CE should ensure that there are adequate resources for the consideration of strategic formation and that decisions in accordance with generally accepted practice are made on relevant issues including the nature and type of the contracts for infrastructure and applications. A fixed or capped price contract for the whole of a major IT Project should normally be avoided.</p>
<p>The RFT and RFP should not have had such an emphasis on the technical solution and in particular on unproven technology and architecture.</p>	<p>In major IT projects the tender documents should normally specify the business objectives, state a preference for proven technology, state any conditions regarding already installed technology, and require the tenderer to specify the technical solution.</p> <p>Today the inquiry would recommend obtaining the maximum flexibility through an open system. A major IT project should have a blueprint and a proof of concept.</p>

Role of Advisers

<p>The lack of a peer review just prior to contract meant increased risk to the project. This was particularly so given the complexity of the project and the unproven technology proposed.</p>	<p>Normally the CE and the monitoring agencies should require an independent peer review of the project and the proposed contract before proceeding to contract.</p>
---	--

Proof of Concept

<p>The lack of a proof of concept results in increased risks and this is particularly so where unproven technology or architecture are proposed.</p>	<p>Major IT projects should perform a proof of concept before contract, particularly where unproven technology is proposed or when the credentials of the supplier are in doubt.</p>
--	--

10. Request for Information, Request for Tender and Request for Proposal.

Business Process Re-engineering (BPR)

BPR should be completed or substantially completed prior to contract or application development, as the information from BPR is necessary to define the scope of the contract. If this is not done, subsequent variations to the contract are inevitable.	A failure to complete or substantially complete BPR prior to contract is usually detrimental to the Pproject and carries a risk that the BPR will result in an increase in scope not provided for in the contract.
---	--

B.6. Project Approval

General and Business Case

Operational and financial risk attending a proposed project must be included in an application for project funding and approval, and the technical and functional soundness of the proposal should also be established. Otherwise, a project should not be approved.	Cabinet should specify the components required for a sound business case so that operational, technical and financial information supporting this is disclosed. The CE is responsible for the preparation of the business case and should approve and sign it to acknowledge that responsibility. Cabinet should be assured by the monitoring agencies that a proposed project is technically, functionally and financially sound.
--	--

Role of Advisers

The terms of reference of an expert adviser need to be carefully defined and carefully considered by any person relying on advice. This person should: <ul style="list-style-type: none"> • Check that the advice is timely and accurate. • Study the whole of the advice and not just an executive summary. 	The terms of reference of experts, the timeliness and applicability of advice, and the advice of an expert included in an application for approval should be critically reviewed in full by monitoring agencies, and any uncertainties or contradictions resolved.
--	--

The Role of Monitoring Agencies

Unless the actions of the monitoring agencies are effective, Cabinet may be requested to approve a major IT project without having reliable information.	The monitoring agencies should be sufficiently resourced, skilled and experienced to advise Cabinet effectively on major IT Projects.
--	---

Financial Return

The focus on financial return and government participation can cause a distortion to the application to Cabinet for approval for the project	Government should specify that non-financial matters can properly be put forward in support of an application and give them due weight. Government should require an explicit assessment of the uncertainty underlying financial estimates put forward in applications for funding.
--	--

Application as a Whole

Any application for funding is likely to be couched in the most favourable terms possible. It will therefore contain a certain degree of bias and distortion. Care needs to be taken to detect any unduly favourable presentation.	Monitoring agencies should be aware of any tendency to present an application in an overly favourable way, and should adopt a critical appraisal.
--	---

B.7. The Contract

Form of Contract

<p>A fixed price contract for the whole of a major IT project has a high level of risk; a more flexible form should be used, requiring delivery in stages.</p>	<p>A flexible form of contract or contracts should be used for major IT projects, normally with separate contracts for infrastructure and applications, with delivery in modules of business benefits and infrastructure, and in time for delivery of applications.</p>
--	---

Off-Ramp and Lay-By

<p>Off-ramp and lay-by provisions are important means of risk control. When in a contract, they must not be overlooked and instead be kept under proper assessment.</p>	<p>Governance, management and monitoring agencies should require that procedures are in place to ensure that critical issues such as the contract off-ramp are properly assessed.</p>
---	---

Time Not of Essence

<p>In a major IT project where time of delivery is always critical and delays are costly, time should be of the essence.</p>	<p>The CE should not agree to a contract in which time is not of the essence unless the time issue is specifically addressed and there are compelling reasons for taking such a course</p>
--	--

Warranties

<p>The warranties and end-to-end guarantees in a contract are an important means of risk control. Therefore any decision that affects warranties or guarantees needs to be carefully assessed in relation to the risks of the project.</p>	<p>In major IT projects any decision that affects warranties or guarantees should be carefully assessed by the Project Sponsor, Project Manager and Contract Manager in relation to risks of the project.</p>
--	---

Technology Substitution

<p>A provision for technology substitution in a contract can be worthwhile. However, it is not a surrogate for having a sound technology solution in place.</p> <p>There are risks if the effect of a technology substitution clause is perceived to be wider than a correct interpretation of the clause.</p>	<p>Care needs to be taken in interpreting and assessing the effect of a technology substitution clause. It should not be used beyond its scope nor as a surrogate for a sound technology solution.</p> <p>Significant technology substitution should be avoided whilst the application is being developed.</p>
--	--

B.8. Project Implementation

Business Process Re-engineering (BPR)

<p>There is an interaction between the business changes and technology associated with a major IT project. The business changes should drive the technology and not vice versa. If BPR is not carried out until after the technical solution has become fixed (normally, at the latest, at the time of signing the contract), there is an increased risk that technology will drive the business changes. There can then be an underground function “creep” that is hard for management to detect.</p>	<p>In major Government IT projects BPR should be completed or substantially completed prior to contract in order to stabilise the level of change impacting on application design and development.</p> <p>Furthermore, during the course of a BPR, every effort should be made to ensure thorough acceptance and buy-in throughout the organisation of the whole project, including both organisational and technical changes.</p>
--	--

Project Charter

A project charter is the project's management and governance "glue". Without a charter, or where the contents are spread over a number of documents and not maintained throughout the life of the project to reflect change (especially when the project lasts longer than one year), there is a high risk of the governance and management of the project becoming unstuck.	A project charter should be completed and agreed to by all the major stakeholders, including the monitoring agencies, immediately following project initiation. The charter should be maintained throughout the life of the project. The charter should be readily accessible to all interested parties.
--	--

Personnel and Resource Issues

For a major IT project to be successful it must be adequately resourced, particularly in terms of skilled and experienced personnel, and governance and management at all levels.	In large and complex government IT projects, there should be appropriate resourcing of skilled and experienced personnel at governance and management levels, and monitoring agencies should monitor the proposed and actual resourcing throughout the life of the project.
---	---

Pressure

Many major IT projects are likely to be subjected to pressure from many sources.	Governance and management should be aware of and guard against negative aspects of pressure.
--	--

B.9. Approval and Monitoring Regimes

General

Annual accounts and reports to Parliament will not, under GAAP, disclose contingent liabilities in respect of contracts for major IT projects unless special risks are identified.	Government agencies and their auditors should ensure that there is inquiry and investigation of the issue of special risks in relation to major IT projects and that any special risk is reported in the annual accounts and reports.
--	---

Approval and Monitoring Regimes

The approval and monitoring regimes (until a late stage) in the project did not provide sufficient information on which Cabinet and ministers could base decisions.	The approval and monitoring regimes should be made more robust by: Cabinet and ministers specifying the requirements for an application and attaching directions to any approval. The monitoring agencies having sufficient resources to participate effectively in the approval and monitoring regimes.
---	--

Use of Experts

In the approval and monitoring regimes, care needs to be taken in the instruction and use of experts and the assessment of their reports. Failure to do so can lead to adverse consequences for government and the project.	Monitoring agencies should develop skills in instructing and using experts and the assessment of their reports.
---	---

Improvements to Monitoring

<p>Defects in the business case and lack of proper baselines, milestones and measurements inhibit or preclude effective monitoring. Likewise, the lack of an effective change control process can result in material changes or de-functioning not being properly recorded or reported, to the detriment of effective monitoring.</p>	<p>Cabinet, ministers and the monitoring agencies should require a proper business case, baselines and milestones that provide a base from which effective monitoring can be performed. Monitoring agencies should identify specific measurements and reporting they require from the project and independent QA. Likewise, there should be a direction that in the event of an effective change control process be implemented, and that any material change or de-functioning be referenced to the business case and be reported to the Monitoring agencies.</p>
---	--

POLAND

1. GENERAL INSTITUTIONAL FRAMEWORK

1.1. Policy

There is no national policy in Poland for the management of large public IT projects. Even worse, such undertakings are not properly co-ordinated at the government level.

For example, Polish citizens and firms use several different identifiers (PESEL, REGON, NIP, NUSP). Our nation-wide registers constantly agree among themselves on data concerning the same subjects, but lack of uniform standards, *e.g.* concerning the spelling of names (places, streets), makes that task difficult. The existence of differing rules generates problems. For example, in the census system, in the case of incorporating place *A* to place *B*, for persons born in *A* the place of birth is changed to *B*, but in the tax system the old name *A* remains.

Legal regulations fundamental for the realisation of large IT projects are often incoherent. For example, the definition of the place of employment in tax rules has little in common with the definition of the employer in the act on social insurance.

1.2. Funding

In the case of the Ministry of Finance, IT projects are funded from budget and foreign subsidiary funds.

Decisions and assessment (on the basis of the Ministry of Finance POLTAX^{system})

The POLTAX System Programme Council makes the decision on starting the large project. The Vice-Minister of Finance is the Chairman of the Council and the MF General Director orders realisation of smaller projects.

The *Project Definition* is the basis for the decision. It is prepared according to strictly determined standards and covers the elements specified below:

1. Motivation for starting the project
2. Aims of the project
3. Scope of the project and realisation environment
4. Methods of project implementation
5. Products and approval criteria
6. Realisation threats
7. The project organisation
8. Financial analysis
9. Quality control plan
10. The project implementation scenario, time frameworks and control points
11. Monitoring the work progress

12. Servicing problems and control of changes
13. Contingency plans
14. References.

Point 6 contains the first version of the risk register known in the phase of preparing the project. Usually it is an evaluation of threats for efficient project realisation, supplemented by subjects to be considered in the future. A possibly versatile identification of external conditions of the undertaking are recommended. One should document all factors that may influence the course of the project such as its scope, way of implementation or other additional requirements that can appear during the tenure of the project.

- Financial analysis (Point 8 of the *Project Definition*) contains the comparison of the project cost and financial benefits to be gained on its completion. One has also to present the financial consequences in the case of renouncing the project.
- The Steering Committee and the Project Management Team evaluate large projects of the POLTAX system.
- The first phase in project planning includes identification and justification of the need to carry out the project, presentation of advantages resulting from it, and outlining the costs of its conception and implementation. These enable a decision on whether or not to start the project and create the foundations for the control of changes in initial assumptions.
- The *Project Definition* enumerates and defines, in a measurable way, what the project is to bring. Settlements with the orderor cover efficient ways of checking the degree of achieving the assumed goals. The list of material products (*e.g.* documentation, software) that should be created as a result of project realisation and criteria of quality evaluation of those products agreed upon with the orderor are being presented.
- Monitoring the work progress is settled already in the introduction of the *Project Definition*. It defines the frequency of examinations by the project management. They are planned for significant moments in the project – control points that most often are connected with the creation of particular effects or products. Examinations constitute the basis for approving the performed works, releasing financial means and assigning resources for the next phase.
- Determining the organisation of current monitoring (consisting *e.g.* of the report format, its assignment and frequency) is a significant element.
- The admissible tolerance of deviations from the project's original assumptions (scope of work, delays, budget) are also being determined and detailed procedures of change control are presented.
- Financial control of projects is carried out currently by the orderor (most often it is the MF General Director). The project manager presents the report on the progress and financial results every month.
- Most projects are subject to the *ex post* control of the Chief Board of Supervision.

1.3. *Management models*

The present POLTAX System Programme Council was set up with the decision No 2/DI/99 of the Minister of Finance dated 16 June 1999. The Vice-Minister of Finance is its Chairman and the Council is [variably] composed of: the MF General Director, directors of some MF departments and tax chambers, as well as chosen representatives of tax chambers and tax offices.

The Council's tasks are as follows:

- stating opinions on decision drafts on the POLTAX system for the MF top management;
- shaping strategy of the development, implementation and maintenance of the POLTAX system;
- monitoring progress of the work on the POLTAX system.

The Management of the IT Department periodically updates the document entitled "The concept of development of use of the information technology in the Ministry of Finance units" determining the strategy for the next five years. This document is presented to the management of the Ministry of Finance.

The international teams of consultants verify those plans.

More important project tasks are supervised by Steering Committees. They are composed of four to six people (directors of the MF departments; representatives of the orderor, "owner" of products and directors of tax chambers as well as heads of tax offices; representatives of end users of the POLTAX system).

The *Project Definition* names the persons composing the Project Management Team: Head of the Project, Head of the Steering Committee (if necessary), Auditor-Head of Quality Assurance and heads of teams. The scopes of responsibilities for each of those roles are determined.

The most important threads and stages of project realisation, as well as its time frameworks are being described. The decomposition of the project into sub-projects and basic phases of their implementation should be presented. Milestones are specified in order to clarify the project progress. It is also necessary to identify critical time dependencies on other projects being realised in parallel.

In general, alternative solutions are being presented (in the case of anticipating potential difficulties) and contingency plans are being prepared (in the case of failure to reach the project goals).

The project schedule is presented in the form of the Gantt diagram. It is being detailed similarly as the scenario. The schedule is updated and possibly modified during the project implementation in response to the changing circumstances, influence of external factors, and so on.

The Ministry of Finance outsources some work. We only exclude planning, quality control, contract management and the security policy. Our department has very positive experiences with "internal" outsourcing, by which we understand employing IT teams from tax chambers.

2. CASE: INFORMATION TECHNOLOGY IN THE POLISH TAX ADMINISTRATION (POLTAX)

The POLTAX computer system supports at present three basic areas of tax office activities:

- Within the sub-system *Registration* 28.8 million tax identification numbers (TINs) have been assigned to taxpayers. Generally, registration (including the *Central Taxpayers Register*) covers the taxpayers and withholders register, associations between parties, and information on tax due reckoned by a tax office. Central verification of the data of taxpayers that claim for TINs assignment has been recently made available assuring assignment of a unique TIN to each taxpayer.
- The sub-system *Assessment* facilitates the control of correctness and term tax payments, and verifies or defines amounts of certain tax dues that constitute the budgetary dues. Tax offices assessment divisions process the data from all the tax forms (PIT, CIT, VAT, and excise) – about 78 million declarations in 1999. Some of the changes have been recently introduced enabling transfer of taxpayer's data and annual declarations through digital media. In the first place, data from pension institutions that deal with over 10 million pensioners are being served by these tools.
- Implementation of the sub-system *Accounting* has been carried out according to the schedule started on 1 January 2000. Tax accounting deals with tax due payments and overpayments, refunds registers, verifies correctness of paid tax due payments according to the decisions made by tax assessment divisions, distributes budgetary funds according to tax offices qualification, and defines tax dues to be executed. From 1 November 2000 the accounting sub-system is expected to be fully operating in all the tax offices.

Development of the POLTAX system to provide full IT support for all tax office activities is getting to its final stage:

- The sub-system *EGAPOLTAX*, dedicated to the tax dues execution that is being performed by the tax administration, has been testing in chosen pilot tax offices for several months. Full implementation in all the tax offices is scheduled for January 2001.
- The conceptual works on the sub-system *Tax Control* commenced in 1998. The sub-system is designed to support the analysis of inconsistencies that may occur in tax dues fulfilment and cases of avoiding payment, based on the data available in a certain tax office. The implementation of the sub-system is planned to start in 2001.
- Works on the sub-system *Management Reports* have benefited from replacement of the CIT reports, that used to be prepared individually by tax offices, with the tax data analysis environment (tools called the Management Information and Decision Making Support Systems based on the data warehouses technology) being now created in the Ministry of Finance and accessed to the objective departments. The new module has recently been added to the POLTAX system, allowing definition, verification and transfer of the extracts of annual PIT declarations to be used in statistic reports for 1999 directly to the Ministry of Finance in electronic form. For the first time there will be no paper declarations processed at the central level.
- In 1999 the *Wide Area Network* connecting the Ministry of Finance with the tax chambers has been built up. Works on the network are being continued to cover all the rest of the Ministry of Finance units.

- At present, the *Electronic Data Interchange* (EDI) project is being tested in three pilot tax offices. The project's scope envisages the use of the Internet by the tax administration for gathering information from external entities (withholders and taxpayers) as well as for the dissemination of information from the tax administration to external entities.

Centralisation of the POLTAX system is mandatory in order to raise its effectiveness:

- Presently distributed architecture of the POLTAX system is very expensive to operate. Each tax office has to be equipped with individual server (or several servers) and employ at least two to three highly qualified IT specialists.
- The database of the POLTAX system consists at present of 356 databases located in individual tax offices. There are tax parties (taxpayers and withholders) registered in several offices with different tax liabilities. According to the present law, neither of the tax offices can be sure that their data are up-to-date.
- Establishment of the *Data Processing Centre* running the Central Taxpayers Register and incorporated *Documents Database* would be the best solution in this situation. Existence of the Central TIN Register would enable the tax administration units (Customs and other registers like the Social Insurance and Central Statistics) access to the single and unique set of information on certain parties together with the information on taxes and individual liabilities. The Documents Database would constitute a source of original tax data that could support the management systems of information and decision-making.

The Centre, together with the *Central Linkage Office*, would also allow performance of other additional tasks associated with the future EU membership of Poland, including:

- setting up the central register of the VAT payers accessible to the EU parties;
- setting up and continuous update of the database of transactions made between Polish and EU parties;
- integration and data exchange between the POLTAX system and the EU systems like VIES, SEED, FISCAL SCENT and INFRASAT.

The key role in all of the above activities is preparation and maintenance of the proper equipment-system platform. The scale in which the MF IT Department operates is best shown in numbers concerning the equipment used and purchased in order to ensure proper efficiency of system operation.

In 1999 tenders were carried out for the purchase and delivery of 258 IBM servers, 7 000 PC computers, 1 200 matrix printers and 1 040 laser printers, and several thousand licences for software (SCO, ORACLE, MICROSOFT).

Service and maintenance of the equipment presently being used in the tax administration covers:

Servers	800
PC computers (of different class)	19 000
Character terminals	8 000
Laser printers	3 000
Matrix printers	6 500
Ink printers	2 100

Modification of cabling and active elements of local computer networks in tax chambers and offices is currently being carried out. Training of the tax chamber and office staff, training personnel, administrators, and end users (about 30 000 persons in total) is ongoing.

The degree of work advancement on the POLTAX system is the result of a series of factors appearing in the period of its realisation:

- variability of the tax system (it is evaluated that in the years 1995-1999, Acts directly or indirectly influencing the functioning of the POLTAX system were changed 123 times and executive deeds changed 50 times);
- irregular inflow of financial means;
- instability of IT staff in the tax administration (a problem for the whole Polish public administration);
- the necessity of fulfilling strict requirements in the field of protection and safety of data (protection of tax and personal data confidentiality).

3. LESSONS LEARNED

Important factors favouring the success of the project were:

- applying standards and procedures;
- well-defined competencies and responsibility of contractors;
- early co-operation of the orderor, the project team and end-users;
- stability of external conditions (legal, financial and political).

Serious threats to projects are as follows:

- over-optimism in planning, and yielding to the pressure of superiors for “success”;
- changes in expectations and requirements of the orderor and/or customers during project implementation;
- legal regulations coming into force too promptly after they are passed, without sufficient time to make adequate changes in the IT system.

SWEDEN

The report seeks to describe the requirements of successful management of major IT projects in Sweden at central-government level. The structure of the report is partly influenced by the report 'Managing large information technology (IT) projects in the public sector - Template for country reports' (<http://www.oecd.org/puma/Risk/template>).

1. General institutional framework

1.1. *Growing use and escalating costs of IT*

Sweden's public administration has implemented a series of modernisation programmes, and there are more to come. Today it is, in fact, difficult to envisage developing new organisations, processes, and services that do not involve using applied information technology (IT) or, to be more exact, information and communication technology (ICT), on a large scale.

Public funds provided by taxpayers must be used efficiently and effectively. The use of IT is no exception, but is a 'mystery' in the sense that public agencies' IT investments are escalating in the absence of traditional productivity gains. This is no less true of the private sector. One major difference, however, is that public investments are openly scrutinised. In the public sector, the universal problems encountered in the management of large IT projects therefore become highly visible.

Growing, and increasingly sophisticated, use of IT has been a precondition for the Government's modernisation process. When the modernising process began, a broad platform of mainframe systems covered most of the large service functions, backed up by large databases and registers. These systems, often of the 'stovepipe' type, yielded gains from mechanisation but also required significant groups of clerical employees to feed in information and perform other manual support functions.

The level of technical integration between central-government agencies and their external partners has gradually increased, first in the form of internal networks with links to other organisations for high-volume data exchange, and more recently with the gradual opening of Internet portals. This has been accompanied by means of aligning and standardising information content (identifiers, terminology, message structure) to improve inter-institutional collaboration. New information resources are being established in the form of databases, registers or other repositories, many of which are accessible to other public institutions as part of transaction or other routines.

A number of the databases linked to the major systems have also come to serve all sectors and segments of society with basic information about people, addresses, companies, property, etc. Exchange and joint use of information are facilitated by Sweden's Freedom of the Press Act.

By 1995, 83% of state employees were already using computers in their daily work, mostly through terminals or PCs. By May 1998, the ratio of PCs or workstations to employees had passed 1:1.

By May 2000, 70 per cent of the Swedish population aged from nine to 79 had Internet access either at home (57%), at work or at school. The percentage is steadily rising. As a result, the 'digital divide' or 'broadband backwater' is not seen by public agencies as a serious obstacle to the implementation of online self-services (also known as 'Government Online', 'eGov' and '24/7 services').

1.2. The Government's 'light touch' management model

The 'light touch' is, to a high degree, a corollary of the overall picture of public administration. At national level, Sweden's 8.9 million inhabitants have at their disposal some 280 highly independent agencies (employing 225,000 people) and 11 small ministries (employing 3,000). Additional factors are that all Cabinet decisions are made collectively, and that there is a culture of compromise and consensus derived from decades of minority or coalition governments.

In terms of managing large public IT projects, the 'light touch' approach is underscored by absence of IT as an item in the multi-year budget framework of the 27 expenditure areas (managed by the 11 ministers).

How the budgetary process works

Based partly on the agencies' annual reports, the multi-year budget framework is updated and critically reviewed in meetings between the Minister of Finance and the other ministries concerned. In the collective decision-making at the Cabinet's budget meeting, funding is then allocated to the 27 spending areas and, on 20 September, the Budget Bill is submitted to Parliament. By the end of December, Parliament has approved the final budget, voting on each of the 27 spending areas separately. The ministers thereafter act as their own 'portfolio finance ministers' and allocate funding from the respective spending areas for individual appropriations, in accordance with the parliamentary resolution. Finally, the Minister of Finance and the Cabinet collectively review the end results.

In this process, IT-related appropriations are rarely specified. In its Budget Bill, the Government requests parliamentary approval for the maximum amount that the Government may borrow on the capital market. The details are not known, but much of this borrowing is intended to fund the agencies' planned IT investments. The volume of these loans rose sharply between 1993, when the system was introduced, and 1996. The expected borrowing limit for 2001 is SEK 21 billion.

1.3. Flexibility in the agencies' IT expenditure

Extensive delegation of autonomy and administrative discretion by the Government enables the agencies to decide on their own selection of premises, facilities and IT investments. Agencies are given global (framework) appropriations that they may then use for staff, premises or spending as they see fit. Even in projects involving more than one ministry, each agency must fund its own participation.

Part of the framework budget (up to three per cent) may be carried over to the following year. It is also possible for an agency to 'borrow' from the following year's framework appropriation. The frameworks are laid down for three-year periods. Agencies may also take out regular (five-year) loans to finance equipment. For each agency, the Government specifies the upper limit for such loans. Interest payments and amortisation must be financed within this framework.

The de facto 'meta-management' system employed by the Swedish Government and Parliament means that every government agency is responsible for its own activities, and also bears responsibility for monitoring and reviewing its own IT projects. There is, moreover, no overall reporting on the relevance of IT development to the efficiency of public administration. This is a neglected issue, and only a few agencies have principles and systems for dealing with it. The neglect may be seen as a result of an adherence to the historical traditions of Swedish public administration.

Several features distinguish Sweden's government and public administration from those of other countries. Back in the early 17th century, a principle of autonomous agencies was introduced, and the monarch's power was separated from that of the civil service. This 17th-century principle of central management is still being applied in the modern 'cyber era'.

In contrast to the 'executive agencies' that have been created of late in many countries, Swedish central-government agencies' autonomy is protected by the Constitution. Autonomous agencies do not preclude Government control, but it must be general and based on:

- legislative provisions and appropriations approved by Parliament
- the Government's interpretations of the law in its instructions, and specifications in its official appropriation documents
- appointments — nowadays confined to Director-Generals, board members and judges
- discussions with agency representatives concerning matters not relating to application of law or the exercise of authority.

To the trained eye, the agencies' freedom and independence with regard to development of large public IT systems are apparent in the use of *should* and *allow* rather than 'shall' and 'enforce' in the following excerpt from the Government's latest Budget Bill:

'The development of IT systems, including system components, makes up an appreciable share of expenditure under the government budget. Besides the above statements concerning the separate spending areas, the Government particularly wishes to emphasise the importance of efficient planning and management of IT development in these areas. Project planning *should* be designed so as to *allow* monitoring to check that systems meet the schedule and content requirements laid down in the budget. All procurement and development of IT systems must yield clearly defined benefits to public administration and its customers, and must be cost-effective for the state. This means that consultation between agencies *should* take place in connection with system procurement and development so as to *allow* co-ordination benefits...'

Swedish Budget Bill, 2000 (author's italics)

1.4. Enforced quality assurance

In the event that the Government is not fully convinced of an agency's IT development thrust, the Swedish National Audit Office and the Swedish Agency for Public Management can be commissioned by individual ministries to carry out reviews or audit projects of particular importance. The Swedish Agency for Public Management has recently received several such commissions. These are not project reviews proper, but rather an aspect of enforced quality assurance (a second-opinion approach which is not always appreciated by the first-opinion agency).

The overall lesson is that major IT projects frequently miss their targets, are difficult to manage, and entail substantial unforeseen costs. This can be established through traditional post facto project reviews. The second-opinion approach is an attempt to get to grips with the problems before they become insoluble.

Three cases exemplify the meaning and results of enforced quality assurance, as carried out by the Swedish Agency for Public Management.

2. Cases

2.1. *The National Social Insurance Board*

In 1999 the costs of social insurance for the whole population amounted to 16.6 per cent of Sweden's GNP. The National Social Insurance Board administers the system in co-operation with the 21 semi-autonomous regional social insurance offices (and some 300 field offices). Altogether, there are some 50 different benefit categories.

Managing all this is not an easy task, and for some years there have been complaints and criticisms in audit reports concerning efficiency, costs, and the legal rights of benefit recipients.

Time and again, attempts have been made to 'tighten up' the systems, especially with regard to the use of IT. There is a widely recognised need for general modernisation, including effective and efficient IT support.

For the past couple of years, such a modernisation thrust has been under way. Known as the Development Programme, its aim is an IT-supported process of re-engineering along business lines. This is, in fact, the largest single IT project in the Swedish civil state sector.

The ministry to which the National Social Insurance Board is subordinate is, naturally, on its guard and has not issued a *carte blanche* for the Development Programme. As a precaution, the government has asked the Agency for Public Management to provide a running second opinion on the progress of the Programme.

The Agency's feedback to the Development Programme and the Government has confirmed the impressions expressed by the ministry in charge. Among the problems highlighted are the two sides of the coin: over-ambitious aims and inadequate management. More importantly, the documentation on which the Development Programme was based lacked the stringency and quality needed for the Government to make appropriation decisions concerning the huge investments that were planned.

In accordance with the suggestions put forward by the Agency for Public Management, the Development Programme in April 2000 started a restructuring process. This included the setting-up of brief, manageable projects and step-by-step implementation of results. Of the utmost importance is the fact that resources will be allowed to be channelled to the Development Programme only when the Government is convinced that this does not interfere with the more basic task of implementing and running the new old-age pension system.

The Agency for Public Management was given the task of continuing to provide second opinions, thereby helping to ensure that the revised Development Programme works smoothly. This further work has led the National Insurance Board to concentrate on the setting up of pilot implementations, and of a new IT strategy unit.

2.2. *The 'premium pension' system*

Domiciled Swedish residents are covered by the system of 'guaranteed pension', which provides basic cover for people who have earned little or no lifetime income. The 'income pension' system is based on individuals' lifetime income.

Each month, an amount equivalent to 18.5 per cent of the individual's pensionable income is charged in the form of a pension contribution. Of this contribution, 16.0 per cent goes towards paying for pensions for

present-day pensioners. In return, taxpayers' pensions are eventually disbursed in the form of PAYE pension from the day they retire. The remaining 2.5 per cent is deposited in personal 'premium pension' accounts that can be managed by the account-holders (i.e. future pensioners) individually, if they so wish.

Some 65 per cent of all domiciled residents of Sweden are covered by the Premium Pension system. From July 2001, individual account-holders will be able to change their portfolio composition (holding up to five of the 456 funds available) online, using their self-service PIN code.

To guide account-holders, each fund is described in terms of risk category (fsee the diagram below) and the performance, value, manager and annual management charge of the fund concerned.



The brand-new premium-pension system is a grand design, operated by the brand-new Premium Pension Authority (PPM). The initial phase of introducing the premium-pension system was completed in the autumn of 2000.

PPM's very extensive IT system, as envisaged, was not only very large and sophisticated. It also had to be created from scratch within a very short period of time. At the same time, PPM itself and the legal premium-pension framework had to be established.

Development of the first IT system never came to fruition. One reason was the underdeveloped system design specifications. Another was that the whole of PPM was in flux, and this affected the contracted system designer to some extent. As a result, the development work was cancelled.

Two years were lost and concerns were raised with regard to citizens' lost opportunity of managing their own premium-pension accounts. In this situation, the Agency for Public Management suggested that an interim system should be implemented, this being the early prototype developed jointly with PPM.

Since the prototype held up well during the roll-out of premium-pension accounts, the decision has been taken to upgrade the former 'IT prototype' to a fully-fledged business system for PPM. The Agency for Public Management has been commissioned to monitor the work until its completion at year-end 2003, and report quarterly to the Government.

2.3. *Civil Rescue and Emergency Planning*

The Swedish Rescue Services Agency (SRV in Swedish) is the central supervisory government authority for the rescue services. This agency promotes practice that improves accident prevention and response, and limits injury and damage in the event of accidents. It also develops methods and equipment for use by the rescue services, and is responsible for the training of all personnel in the municipal rescue service brigades.

The Swedish Agency for Civil Emergency Planning (ÖCB in Swedish) is the central authority responsible for overall co-ordination of activities aimed at strengthening society's capacity to cope with emergencies. One of ÖCB's main tasks is to guide and support civil-defence agencies in developing and implementing various civil emergency-planning measures. Civil defence in Sweden consists of planning and preparations by a number of agencies representing sectors considered essential for the continued functioning of society in times of war or in severe peacetime emergencies. An effective management and command system is obviously crucial to ÖCB.

The above two agencies report to the Ministry of Defence. However, owing to the Swedish Government's 'light touch', very little co-ordination had taken place in the development of the IT-based management and command tools critical to their respective operations. It was gradually realised that the money spent on the two separate agency systems could be used more efficiently. One trigger was that SEK 100 million had already been spent on the two years' development work for the ÖCB management and command system, and that another SEK 140m was needed.

The Agency for Public Management was therefore asked to examine the possible overlap in work carried out by ÖCB and SRV. It was found that the systems do, indeed, have some look-alike features and modules. The systems will, however, be used for different purposes (and have different target groups) and could well be developed separately, without any major detriment. Thus co-ordination is not essential in this case.

More important is the implementation of the two systems, and especially of ÖCB's more far-reaching system. A fair number of public authorities will be users of, and integrated into, the ÖCB and SRV systems. In this connection, there was a deeply-felt need for co-ordination between the primary agency users and the many secondary system users (other state agencies, regional governments, municipalities, hospitals, police stations, etc). The Agency for Public Management's recommendation was that the development work at ÖCB should be put on hold pending successful pilot implementation at one of the 21 regional government authorities.

3. Lessons learned

3.1. *Government dissatisfaction with roll-out of major IT projects*

Reviewing some 215 large IT projects in the Swedish central government in 1998–99, the National Audit Office found that:

- Of the projects that had been in progress for at least seven months, 75% had overrun their time schedule and/or budget.
- Of the projects that had been obliged to change their time schedule and/or budget, 75% still had problems. Projects that had previously encountered problems continued to experience difficulties of some kind.
- Projects in the area of IT infrastructure had fewer problems than projects relating to business support.
- Very large projects that had undergone external audit or review also had fewer problems, or not so many problems with severe consequences.

The total cost of the projects reviewed was SEK 4.6 billion, and the average cost per project was SEK 22.4 million. Nonetheless, nearly 20 per cent of the projects involved no organised quality reviews. These projects had more time-schedule and budget problems than the others. Systems based on software purchased on the open market also had more severe problems than others.

How does the performance of the Swedish public sector compare with that of other countries and sectors? The literature tells us that we are in good (that is, bad) company. For example, The Standish Group (<http://standishgroup.com/visitor/chaos.htm>) has, year after year, concluded (roughly speaking) that, irrespective of the soundness of project goals, international statistics for major public IT projects show that:

- 25% are not too far off target (in terms of time, budget, features and functions)
- 45% are severely crippled (in terms of time, budget, features and functions)
- 30% are complete failures (i.e. terminated, never delivered, never completed).

3.2. *Are we learning from failure?*

History does, indeed, tell us that we make the same mistakes over and over again. The findings from the National Audit Office and the Agency for Public Management also tells us that the risks would be reduced by such approaches as:

- short, manageable projects
- implementing results step by step
- basing development on a sound vision, not on troubleshooting
- avoiding automatic, knee-jerk responses
- purchasing turn-key systems
- refraining from extensive customisation of systems purchased
- a ‘slow trigger, fast bullet’ approach
- rejecting spurious or makeshift quality assurance.

At the IT project management level of Swedish central government, nodes would most likely be the response to the following table of success criteria condensed by the Standish Group from the comments of North American IT project managers (see the above website reference). The table lists the criteria in order of importance, with their respective success points.

SUCCESS CRITERIA	POINTS
1 User involvement	19
2 Executive management support	16
3 Clear statement of requirements	15
4 Proper planning	11
5 Realistic expectations	10
6 Smaller project milestones	9
7 Competent staff	8
8 Ownership	6
9 Clear vision & objectives	3
10 Hard-working, focused staff	3
TOTAL	100

3.3. *The way ahead*

The overall task of making all the central-government agencies' IT systems Y2K-compliant was seen as a matter of urgency. The Government therefore temporarily dropped its 'light touch' and established fairly firm and coherent Y2K process control at the agency level. The outcome was encouraging.

The outcomes of the enforced quality assurance reported in section 2, i.e. the second-opinion reviews of major IT projects that were commissioned by wary or apprehensive ministries, have been appreciated by the Government (but less so by the 'health-checked' agencies). The lingering vibrations and subdued signals may be read as showing that the Government leans more towards the establishment of more regimented and professional management procedures.

If the Government decides to retain its 'light touch', the tool of enforced quality assurance needs to be elaborated, refined and institutionalised. The issues requiring to be dealt with include the following:

- *IT* is not synonymous with *results*, but it is increasingly used to obtain *results*. What, then, is the crucial difference between managing business development and managing IT-based systems development?
- Is it an anachronism to budget for the *efficacy* of business development, while demanding interim reports on the *efficiency* of IT-systems development?
- What are the respective strengths and weaknesses of *auditing*, *enforced quality assurance* and *coaching*.

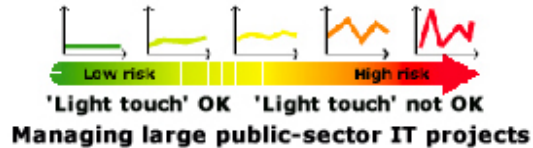
In the name of 24/7 services, a system of nationally networked agencies and cross-agency services is envisaged and encouraged by the Government. There is, obviously, a limit to how far this encouragement can go in a 'light touch' environment.

In 1994, in the early years of eGovernment, the Ministry of Finance initiated the Top Managers Forum to bring about more coherent development. The initiative was, however, weakened when in 1998 the Minister of Finance stepped down from chairing this group of agency heads. But the need for joint and enforced policy work is keenly felt by the agencies. So, in June 2000, a bottom-up approach resulted in the formation of the 'State Agency E-Forum', in which agency managers identify and discuss strategic issues.

Rapid and widespread development of networked eGovernment services is unattainable unless the extensive delegation of autonomy and administrative discretion is matched by firm central management.

One particularly troublesome fact is that the Government has yet to devise a model for the financing of multi-agency development work.

Moore's and Metcalfe's laws regarding ever accelerating hardware performance and network usability, respectively, underscore the untenable situation of building new systems and at the same time altering development platforms and infrastructure. Moving and at the same time aiming at an independently moving target is not an easy task. Project complexity is growing, as is the vulnerability of built systems. This is clearly a risk scenario of substantial magnitude, and a scenario of Government IT management in which the 'light touch' model may have to be retired.



UNITED KINGDOM

1. GENERAL INSTITUTIONAL CONTEXT

1.1. Policy

Is there a national policy for management of large IT projects; and what are its characteristics?

The recent review of major IT projects in government (*Successful IT: Modernising Government in Action*, published May 2000) has made extensive recommendations for improved management of large IT projects. These are based on evidence from extensive research undertaken in the UK public and private sectors and abroad, which shows that there are many reasons why failures occur. The aim of the study was to make prescriptive recommendations that will raise the standards of all projects to the level of the best, and provide mechanisms to underpin the process of improvement.

The Review Team was based in the Central IT Unit (CITU), Cabinet Office. This Unit has now merged with the Office of the e-Envoy (OeE), Cabinet Office, and any reference to CITU in the *Successful IT: Modernising Government in Action* report now refers to OeE.

The recommendations from this review are currently being developed as policy for the management of all large IT projects in government. In summary, the recommendations for improved performance are:

- improving the focus on business change across government. Recommendations include methods for achieving and maintaining this and structures to support their use.
- encouraging good leadership and clear responsibility for IT-enabled change programmes and projects. Recommendations include the requirement of a Senior Responsible Owner, and give a description of that person's role.
- improving project management across government. Recommendations include the establishment of systems for matching project managers to projects, and increasing skills and awareness.
- improving the management of risk. Recommendations include measures to ensure the skills and mechanisms needed are in place.
- addressing modular and incremental approaches to implementing IT-enabled change. Recommendations include introducing a presumption in favour of such approaches and supporting guidance.
- improving the measurement and realisation of benefits. Recommendations include reinforcing systems for monitoring benefits, and greater sharing of experience.
- establishing improved interactions between government and its suppliers. Recommendations include a more strategic approach to suppliers, addressing problems with current guidance and setting out actions suppliers need to take.

- ensuring that all of the report’s recommendations are applied appropriately to cross-cutting initiatives.
- providing the skills needed to deliver improvements in the handling of IT-enabled change. Recommendations include developing, implementing and monitoring a framework for the skills needed and making links to other work on Civil Service reform.
- establishing means of learning from lessons and sharing experience. Recommendations include a system of peer review and requirements and mechanisms for obtaining and sharing good practice.

Ownership of the report is vested in the e-Envoy who will hold overall responsibility for its implementation. He will report to the e-Government minister on progress.

The full list of recommendations is provided in Annex A.

Is there a national IT policy and does this policy include prescriptions for the use of IT in government?

The ability for public sector organisations to work together and share information is an essential factor for the successful achievement of ‘joined-up’ government. The **e-Government strategy** fulfils the commitment in the *Modernising Government* White Paper to publish a strategy for Information-Age Government. It sets out a commitment to using IT to deliver services in new ways focusing on the needs of the citizen rather than those of government departments.

The **e-Government strategy** has ten framework policies that must be adopted by all government departments and agencies:

Websites

The framework policy focuses largely on electronic publishing and the creation of a sound organisational basis within departments for managing their on-line presence, on good content and on technical standards that provide for consistency and the widest possible access to public sector sites.

Call centres

The call-centre guidelines set out an approach to implementing call centres in the public sector, ensuring they are viewed as part of an overall business change process. The guidelines provide a set of standards for ensuring public sector call centres are accessible, efficient and helpful and provide a consistent and accurate interface with government services.

Smart cards

The smart card framework policy provides a set of standards and guidelines to facilitate interoperability. It also provides advice on acquisition issues for public authorities, to ensure that accessibility is an integral part of any card scheme and to provide guidance on data protection issues.

Authentication

Effective government services will require a widely accepted means for citizens and businesses to authenticate themselves for the purposes of those transactions. The authentication framework policy and guidelines establish a common approach to authentication for government departments, agencies and the wider public sector.

Digital TV

Although digital TV is still very new and will continue to develop over the next few years, this early guidance is considered essential to ensure that public sector organisations are suitably informed about the strategic opportunities and practical implications of deploying digital TV-based services.

Security

Information-Age government services, from simple information-giving websites to large, complex transactional services, are reliant upon the application of appropriate IT security measures. The security policy represents a call for a general alignment with best e-Commerce practice. This applies across the public sector, and extends to all service delivery channels and all bodies which deliver public services. Supplementary guidance on specific security topics will also be published including Trust Services, Confidentiality and Privacy, Business Services Security and Network Defence Security Requirements.

Privacy

The Modernising Government White Paper committed government to “address concerns about privacy” and to “provide a proper and lawful basis for data sharing where this is desirable, for example in the interest of improved service or fraud reduction”. This paper outlines the key topics of privacy relating to Information-Age government. Data sharing is at the heart of the Modernising Government agenda. The Performance and Innovation Unit (PIU) in the Cabinet Office has begun a study on the issues surrounding Privacy and Data Sharing. It will be based on analysis of consumer attitudes, of existing government efforts in data sharing, of current benefits of data sharing and projected benefits from further data sharing, of existing institutional barriers, of the domestic and EU legal boundaries, and of developments in IT to safeguard information. The project team will also evaluate efforts in other countries, both within the EU and overseas.

Electronic records management

The framework on electronic records management provides guidelines to support greater commonality and inter-departmental working in electronic document and records management, and in the sharing and exchange of electronic records across the GSI.

Metadata

This paper sets out a work programme to deliver a metadata policy for Information-Age government.

Interoperability

The interoperability framework policy sets out the policy and standards for achieving interoperability across all government departments and the wider public sector.

These framework policies are underpinned by implementation guidelines on developing e-Business strategies and ensuring that the required skills for Information-Age government are in place. This is supported by a centrepiece of the e-Government drive: the new Performance and Innovation Unit report, *e.gov: Electronic Government Services for the 21st Century*. This report recommends putting in place new financial incentives, levers and structures to make sure the transformation of services takes place across the public sector. It also recommends opening up the electronic delivery of government services to the private and voluntary sectors to encourage the improvement in service quality.

1.2. Funding

What are the processes for funding large public IT projects - e.g. net budgeting, possibilities for using credits to fund investments, mechanisms in the budget process, etc.?

The UK Government spends large sums on IT each year. Overall expenditure in the public sector in 1998-99 on IT hardware and software, maintenance and other services was in the region of £7 billion. (*Source: the UK Parliament's Public Accounts Committee First Report.*)

The role of HM Treasury

HM Treasury's Expenditure Divisions control public expenditure.

The UK Government carries out an annual Spending Review of central government expenditure. This now includes a cross-cutting review on the knowledge economy, which will consider funding for electronic government. Departments and agencies carry out annual Spending Reviews internally and produce high-level plans, budget allocations and performance measures. These are used as the basis of formal agreements with HM Treasury, which are Public Service Agreements (PSAs) for a rolling period of three years. The PSAs contain performance targets and a budget allocated for an agreed portfolio of projects; they are published via the HM Treasury website.

The **Invest to Save Budget** makes capital funding available (in addition to the PSA allocation) where major opportunities for improvement have been identified. The **Modernisation Fund** is part of this budget, with funding specifically for IT projects; it is managed under the direction of the **e-Envoy**, who owns the e-Government strategy on behalf of ministers.

Sourcing options

Most IT in government is outsourced. The main approaches are as follows:

- **PFI:** From 1992 the Private Finance Initiative has promoted the procurement of major projects as packages in which the private sector designs, builds, finances and operates the project, possibly for many years. This is in contrast to traditional procurement in which the public sector provides all the finance and, typically, takes much of the development risk. A number of deals have involved the implementation of IT provision, including the new National Insurance Recording System.

- **PPP:** An organisation is likely to seek business partners and/or a Public/Private Partnership (PPP) consortium for services where the business aspects are the primary concern, with IS/IT as a supporting component. Typically, there would be an advertisement in the supplement to the Official Journal of the European Community (OJEC) inviting expressions of interest from a wider range of major players such as financial institutions rather than a framework catalogue's narrower, specialised range of IS/IT providers.
- **Framework catalogues:** A recent development has been the development of framework deals, in which departments work closely with suppliers. Contracts are phased and let out on a modular basis so that competition can apply at subsequent stages, and other suppliers can be brought in as appropriate. The Department of Social Security's ACCORD programme, announced in 1998, is an example where the Department have established a close, long-running relationship with a single preferred service provider to design, develop, implement and operate their IT strategy. At the same time, they announced that they intend to work with three service providers for the provision of a wide range of IT services in the future.
- **Channel services:** These are intended to provide citizens with the best possible range of access paths or "channels" to government through electronic service delivery, which could be provided by a number of public and private sector organisations working in collaboration. In some cases service delivery will be paid for entirely by the private sector where the incentive exists. This approach is new and experience so far is limited. An example of a channel service project underway is the Department for Education and Employment (DfEE) Connexions Card project. A number of private sector providers will contribute to service delivery, which will use smart card technology to play an important part in ensuring that every young person stays on in learning post 16 and achieves a worthwhile qualification by the age of 19.

Internal approvals mechanisms: the business case

Where a business need for IT-enabled change has been identified and agreed in PSAs, the organisation produces a business case for management approval. The business case is also a management tool for planning and managing the progress of a project. A key recommendation in *Successful IT: Modernising Government in Action* is that the public sector produces business cases that address the whole business change, not just the IT component. Currently most departments and agencies develop their business cases in two stages: an Outline Business Case setting out initial assumptions about potential options, costs, benefits and risks; and a Full Business Case that validates and updates these assumptions through the procurement process. In future they will start the business case development with a Strategic Outline Case, which will identify a preferred procedure at a high level. Experience in the NHS and to some extent in central government has shown that the main advantages of adding this preliminary stage are:

- senior management and key stakeholder commitment from the early stages of the project;
- concentration on the strategic aspects of the project early on, before committing to detailed options appraisal;
- more rapid and focused development of the business case.

1.3. *Decisions and assessment*

Who makes the procurement decisions in relation to large public IT projects?

Departments' programme/project boards make procurement decisions on the advice of their procurement teams, reporting ultimately to their Principal Finance Officer.

In the past, some change programmes and projects have suffered from a lack of active ownership at senior management level. *Successful IT: Modernising Government in Action* makes the recommendation that overall responsibility for delivering the business objectives and benefits of any programme or project must be vested in a single, responsible and visible individual, the **Senior Responsible Owner (SRO)**. The seniority of the SRO will be dependent on the size, complexity and associated risk of the project/programme.

Successful IT: Modernising Government in Action emphasises that effective business change programmes and projects require clear, active and visible leadership from the top. Top management needs to send out a clear signal that effective delivery of projects is crucial to meeting the organisation's overall objectives.

It is vital to raise awareness among ministers and senior officials of the way that their leadership and decision making affect the environment for project delivery, and the roles they play in individual projects and programmes. This includes their part in encouraging a culture of openness so that potential difficulties are highlighted early and lessons learnt.

The UK Government recommends that professional development events for ministers and senior civil servants should be organised by the Centre for Management and Policy Studies (CMPS) informing them of their role in, and responsibility for, major IT projects and programmes. These events include joint seminars. CMPS will also explore the scope for running joint events with the IT industry.

On what information basis is the decision taken?

The key deciding factors are:

- value for money;
- affordability;
- achievability (can the organisation realistically cope with the proposed level of change?).

The decision is based on a thorough investigation of the available options to meet the business requirements, which includes cost/benefit, risk and sensitivity analysis as well as appraisals of the provider's capabilities and the likelihood of cultural fit between customer organisation and provider. (The analysis is based on HM Treasury guidelines for investment appraisal, the *Green Book*.) The findings are documented in the **business case** (described earlier under *Funding*).

Successful IT: Modernising Government in Action recommends that the programme/project board's decisions are informed by independent review. **Peer reviews** provide independent assurance to the Senior Responsible Owner (SRO) that decisions taken at key points in the project are based on sound information. Peer reviews take place at four key points in the life cycle of IT-enabled projects:

- at project initiation after the initial business case has been prepared, to confirm business need;

- after the procurement strategy has been defined but before issuing an advertisement in the Official Journal of the European Community (OJEC), to confirm the procurement method and sources of supply;
- before contract award, to confirm the investment decision;
- before implementation of an operational service, to confirm “readiness for service” of both customer organisation and provider.

Peer reviews give the project team the benefit of advice and guidance from fellow project practitioners and provide assurance that the project can progress safely to the next stage of development or implementation. They seek assurance that:

- the project can demonstrate that **quality** is addressed from the perspectives of delivering to the business case, delivering to the customers’ and users’ requirements, and delivering to appropriate technical, technology or specialist standards;
- **changes** that are required to any aspect of the project (including the business case, the deliverables, budgets) have been properly planned and controlled so that the project’s continuing ability to deliver the required outcome can be managed;
- appropriate **training** is being given to staff taking on project management roles so that the required responsibilities are matched to the available skills and competencies;
- the **processes, products, decision points**, stages and overall approach taken to manage the project are based on best practice and adapted to suit the context and the environment in which the project will operate;
- the project demonstrates that **the business case** is driving the project activities and that it continues to be viable;
- major decision points are built into the project plans to ensure that the continued **viability** of the project can be reviewed and confirmed by the Project Executive and the Senior Responsible Owner.

In addition, **gate reviews** will be required for major projects identified as high risk (see the next section on risk for selection criteria). Gate reviews will be conducted by peers from other departments or by HM Treasury’s Office of Government Commerce (OGC - described below). Work is underway on developing policy on gate reviews for IT-enabled projects; they have proved to be a successful mechanism for controlling risk in construction projects.

How are risks evaluated ex ante?

Currently the quality of risk management varies widely across government. New ways of working will require much more robust approaches to risk management. The Modernising Government agenda requires government to be innovative in seeking better ways to deliver services to the public. It calls for a new approach to the management of risk, moving away from a risk averse attitude to one which embraces and actively identifies, assesses, monitors, manages and communicates risk in the interests of securing major improvements.

Successful IT: Modernising Government in Action sets out the key recommendations that public sector organisations must adopt to avoid failure with IT-related business change. It recommends that more effective risk management will enable departments and agencies to undertake the increasingly complex and cross-cutting projects that are demanded by the Modernising Government agenda. All management activity is conducted in an environment of risk and uncertainty, and therefore management of risk must be supported at the highest level by awareness of its importance.

The National Audit Office's study *Managing Business Risk in Government* aims to encourage "innovation through well thought through risk taking". Business risk management should be "an attitude of mind whereby all staff are fully aware that events or circumstances which can affect the achievement of their outcomes need careful management". Departments and agencies must have in place the right skills, management structures, procedures, processes and organisation.

HM Treasury's draft guidance *Management of Risk - A Strategic Overview* (the *Orange Book*) addresses critical factors for successful management of risk. These include:

- processes in place to monitor risks;
- access to reliable, up-to-date information on risks;
- control mechanisms in place to deal with those risks;
- decision-making processes supported by a framework of risk analysis and evaluation.

There must be a "risk owner" at senior level, such as the SRO, supported by risk managers. There must also be effective processes for upward referral of major problems.

Risk management frameworks. From September 2000 all departments will be required to establish a risk management framework. The minimum requirements are:

- the organisation's risk policy;
- main stakeholders;
- approaches for identifying, assessing and reporting risks, and action to deal with them;
- responsibilities for managing risk and reporting to senior management, especially risks which cut across core business activities and organisational boundaries;
- quality assurance (QA) arrangements to ensure that risk management reflects current good practice.

All projects must use a **Risk Register** (also referred to as a Risk Log) as part of the risk management activities on the project (as described in CCTA's Programme Management and PRINCE 2 methodologies below). The Risk Register must be reviewed and updated regularly. Project level risk management must be integrated with the programme level activities where the project is part of a programme.

The two main questions for any public sector project which must be addressed are:

- Can the public sector organisation meet business objectives and achieve value for money?
- What are the risks of not achieving the desired outcomes?

Value for money is addressed through the business case process, as described earlier, using well-established techniques for investment appraisal such as those in HM Treasury's *Green Book*.

Formal approaches to risk assessment are being developed to help departments gauge the level of risk for their projects at specific points in the project life cycle. A Project Profile Model (used as a guide) provides a standard set of high-level criteria against which SRO can assess the intrinsic characteristics and degree of difficulty of a proposed project, in order to establish the appropriate:

- control structures (including peer review);
- risk profile and corresponding risk strategy;
- design approach (for example, modular or incremental approaches rather than “big bang” - described in a later section).

These criteria are used to assess business impact, technical impact and client/supplier arrangements. A detailed table of the criteria is provided in Annex B.

Other factors that need to be taken into account for evaluating risk include:

- ratio of business benefit to cost (high ratio may merit more risk than low);
- client-side skills in business process modelling, project management, etc.;
- capacity of organisation to embrace/implement the change;
- degree of technical complexity.

Additional factors for consideration during the assessment of risk include:

- the effect of government priorities on the allocation of resources to the project;
- externally imposed time delays, such as waiting for requirements from other departments;
- capability of the supplier in terms of technology, expertise, skills, etc.;
- inexperience of government departments in projects of particular size or complexity;
- inadequate reliable estimates, feasibility studies, user-trial programmes, or other similar data upon which to base a risk assessment.

Is there a special agency, institution or authority responsible for assessing projects ex ante and/or ex post? If so, what are the characteristics of this entity in regard to staff, legal basis, rights and responsibilities and institutional affiliation?

The **Office of Government Commerce (OGC)** is an office of HM Treasury, set up on 1 April 2000. It has been created to enable and facilitate reform of commercial activities across government; administratively and legally it remains part of HM Treasury. OGC brings together Treasury procurement policy, the practice development units and the Private Finance Policy team with three former Cabinet Office executive agencies:

- Central Computer and Telecommunications Agency (CCTA);
- Property Advisors to the Civil Estate (PACE);
- The Buying Agency (TBA).

OGC's interests span the whole process of acquisition from third parties, including goods, services and construction projects, from the initial concept right through to the end of a services contract or the useful life of an asset.

Its activities are guided by a Supervisory Board, chaired by the Chief Secretary to the Treasury. Membership of this Board is made up of Permanent Secretaries, the Head of the National Audit Office (NAO) and two senior external representatives. This provides OGC with continuing top-level support and strategic direction, as well as helping to ensure a coherent cross-departmental approach.

OGC will monitor progress on peer reviews where it is involved in providing resource or expertise, and take the lead in building a knowledge network to support the peer review process.

OGC will own the processes and criteria described to:

- assess the effectiveness of knowledge transfer between projects;
- amend and update the scoring mechanism for categorising projects;
- identify resource constraints and future requirements;
- ensure that processes are effective and of benefit to projects, individuals and departments involved;
- confirm that lessons learnt are applied across government so that better performance is achieved overall.

Individual departments are responsible for ensuring that reviews, such as peer reviews, are carried out.

The role of the NAO is to report to Parliament on the spending of central government money. They conduct financial audits of all government departments and agencies and many other public bodies, and report to Parliament on the value for money spent. They therefore have a role *ex post*.

What is the content or nature of these assessments?

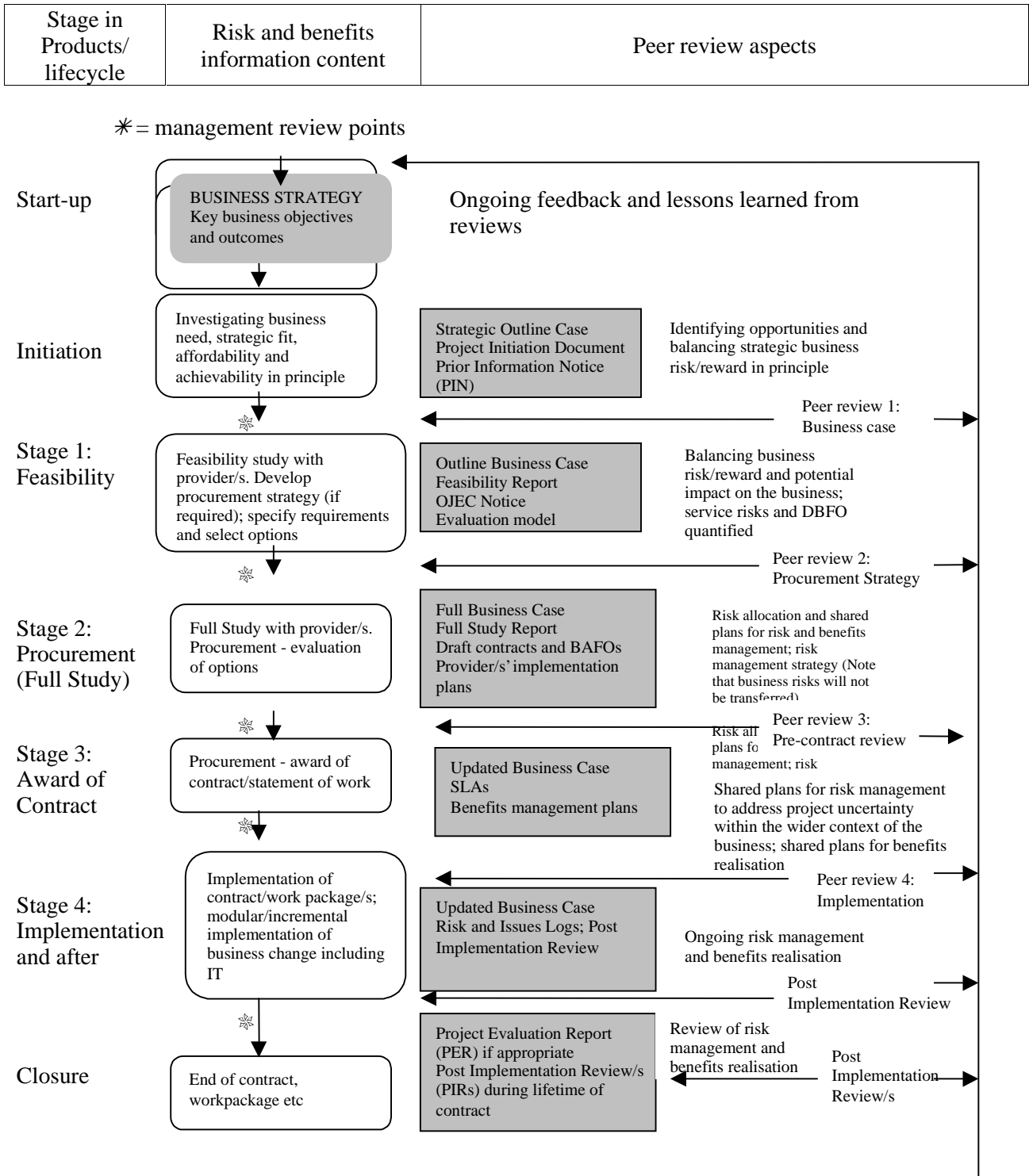
Best practice recommends that quality, performance and risk are monitored throughout a project, and services, supplier/customer relationships and contracts are continually managed to an agreed standard in order for the benefits of a project to be realised.

Project board, peer and gate reviews are outlined in the previous section on decisions and assessment.

How is progress monitoring and reporting undertaken? How often, to whom, and reporting on what?

Figure 1. Acquisition life cycle

The key stages below assume a procurement project. However, the principles can be adapted to any type of project where a full business case process is required, including cross-cutting projects.



The SRO is responsible for monitoring the impact of the project on the organisation and, conversely, identifying external impacts on the project.

Recent experience has shown that there is often a missing link between effective risk analysis and management and raising the awareness of business risks to the organisation - mechanisms for appropriate reporting and escalation of problems. Such mechanisms could ensure that action is taken when necessary without inundating senior management with detail. It is vital that difficulties with a project are raised to the appropriate level as soon as possible. Existing approaches described in PRINCE 2 (project management methodology <http://www.ccta.gov.uk/prince>) address this problem:

- they suggest the use of a project assurance function responsible for monitoring all aspects of a project's performance and products independent of the project manager;
- they set tolerance levels for cost, time and functionality at the start of the project outside of which the project manager must seek approval before proceeding. There are also software tools available.

A recommended simple mechanism to increase visibility of risks is a graphical summary risk profile. The Project Manager or Risk Manager would update this graph in line with the risk register on a regular basis and provide this to the SRO.

How is the attainment of promised (particularly less tangible) benefits measured ex post? Benefits realisation is a central component of the government's formal approach to programme management which is widely adopted, with a Business Change Manager appointed specifically to take responsibility for benefits realisation. The benefits achieved are measured against the expected benefits set out in the business case that justified the investment.

Post-Implementation Reviews, sometimes known as Post Project Reviews, are used widely as the mechanism to report formally on outcomes against the business objectives and business case.

Contractually, performance targets are set and agreed in contracts with service providers; service managers monitor progress against those targets. Some contractual arrangements, especially PFI, feature payment mechanisms that are tied to benefit realisation - if the provider achieves the benefit they receive the agreed payment; if they exceed the targets they may be entitled to a share of the additional benefits. Treasury Taskforce guidance provides advice on benefits realisation and payment mechanisms.

However, the *Successful IT: Modernising Government in Action* review has identified that too few projects or programmes have been subject to the necessary review or reporting of the actual benefits. Even if they are delivered on time and to budget, it has not been clear that they have delivered the expected returns. The report recommends that mechanisms for benefits measurement and realisation should be improved; the recommendations include reinforcing systems for monitoring benefits and greater sharing of experience.

Currently no central reporting or recording is undertaken. In future benefits realised from specific projects and programmes will be collected and the information maintained in order to share it across government. Without this information, the government as a whole would be unable to ensure that future projects and programmes learn from such cases and take account of these when embarking on new initiatives.

How are projects audited financially ex post?

It is the responsibility of individual departments and agencies to audit their projects. Internal auditors must report their findings to their Management Board or Finance Officer. External financial audits carried out by the NAO take place annually. External project audits have to be specifically requested or referred for audit.

1.4. Management Models

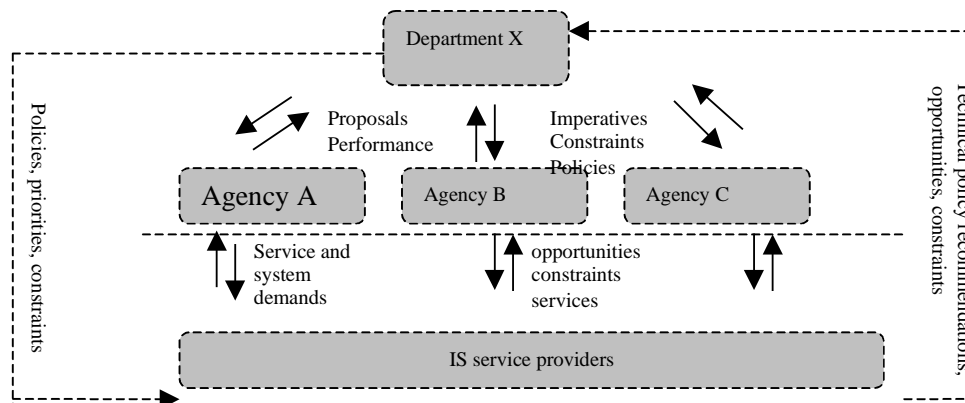
How can relationships between agencies and ministries/departments be characterised, and what consequences does this have for the management of large public IT projects in these agencies?

Department-Agency relationship

Departments are policy-making bodies and their executive agencies work closely with them to implement policy on their behalf. Their size and structure varies widely. Some departments are very large, with a number of executive agencies working autonomously; others are small single units.

Figure 2 shows typical relationships between a parent department, its executive agencies and its IT service providers.

Figure 2.



Cross-cutting initiatives

Departments and agencies may work together in cross-cutting initiatives:

- a cross-cutting project or programme is one with objectives that require contributions from more than one department or agency;
- increasingly, public sector organisations are contributing to the delivery of cross-cutting projects with partners in both the public and private sectors;
- to be successful, cross-cutting projects and programmes need to apply the same disciplines as those being developed within one organisation.

An example of a cross-cutting initiative is SureStart, which aims to ensure that all children under five years old have the best possible start in life. Departments collaborating on this initiative include the Department of Health, Department for Education and Employment and local government's social services divisions.

There are some examples of departments approaching other departments on an *ad hoc* basis to learn from their IT procurement experience, thus developing a pool of experience and knowledge across government.

The Performance and Innovation Unit report *e.gov: Electronic Government Services in the 21st Century* recommends that the Office of the e-Envoy should have dual key responsibility for the release of electronic service delivery funding. It will be responsible for approving e-Business plans, and for recommending that the Chief Secretary release funding to support them. Release of funding should be conditional on satisfaction that plans put forward support the government's wider objectives for e-Government and that departments have robust plans for realising efficiency gains. This includes the programme design being fit for purpose, compatible with the single portal and with cross-cutting delivery.

Can management models for large IT-projects be described? The description could include the use of steering groups, political involvement, the use of modularisation of projects, allocation of responsibility for outcome and the use of in-house development versus development contracted out.

Most government departments and agencies follow the PRINCE 2 methodology for managing large IT-enabled projects. The SRO role recommended in *Successful IT: Modernising Government in Action* is consistent with this approach, as shown in Figure 3. Figures 3 and 4 show the role of steering groups, SROs and how contractors are involved.

Although some departments and agencies still retain significant in-house technical capabilities, responsibility for much of government's technology has been transferred to the private sector. Most IT projects and requirements for IT service provision are outsourced. CCTA's guidance on the "Intelligent Customer" outlines the core capabilities that need to be retained to ensure effective control of third party services. More recently, CCTA has produced guidance on the Informed Partner, which focuses more on management of the relationship with the service provider. The Office of the e-Envoy/e-Government skills framework outlines the customer and service provider capabilities required. This is currently being used to assess the extent to which departments have access to the necessary skills for e-Government and for managing successful IT projects.

Political involvement

Professional development events for ministers and senior civil servants have been organised by the Centre for Management and Policy Studies (CMPS) to inform them of their role in, and responsibility for, major IT projects and programmes. These events include joint seminars. CMPS will also explore the scope for running joint events with the IT industry.

Figure 3. The Role of the SRO in the PRINCE 2 Project Management Structure

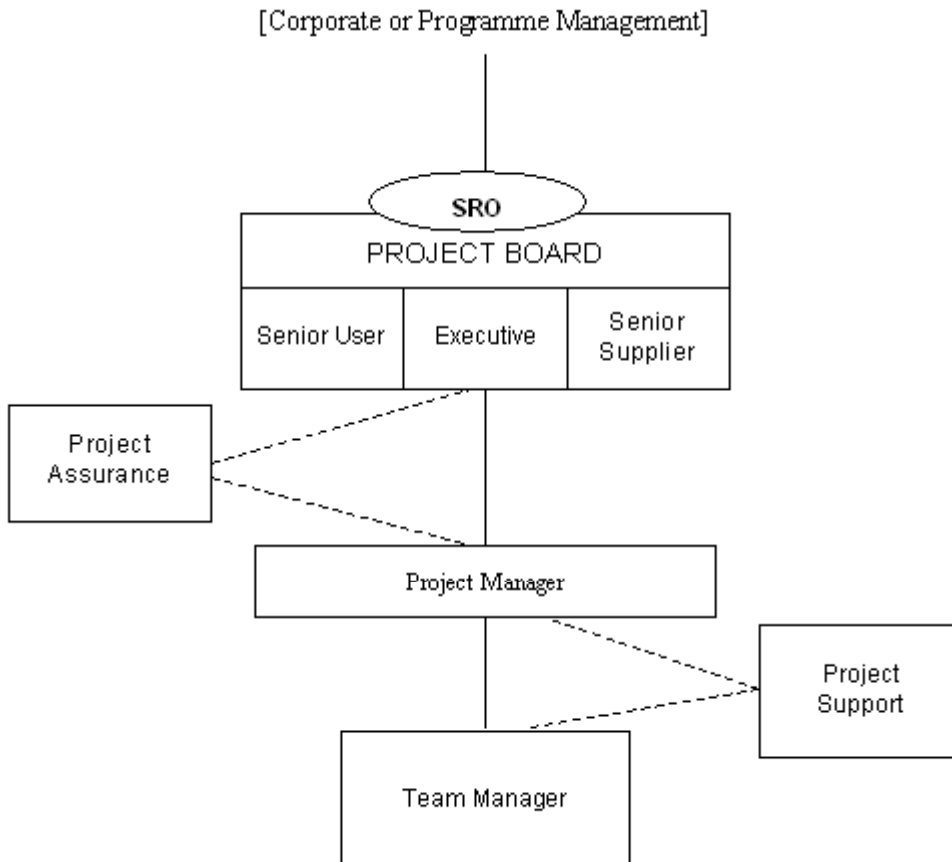
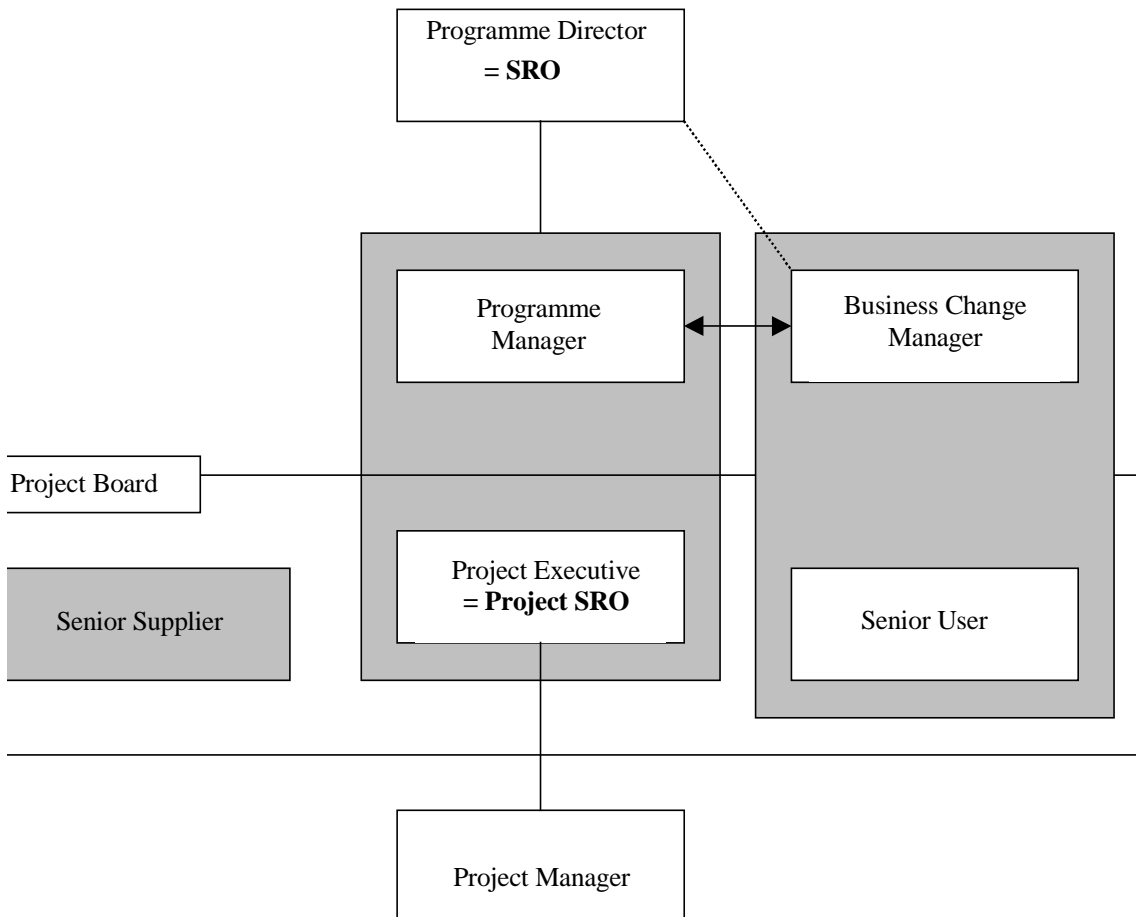


Figure 4 illustrates how SROs fit with the current Central Computer and Telecommunications Agency (CCTA) Programme Management Guidance, which complements PRINCE 2. Individual projects within a programme would have individual SROs. Although individual Business Change Managers may not all report in line management terms to the SRO, they are accountable for realising elements of the business benefit in their business areas, a process for which the SRO is ultimately responsible.

Figure 4.



Programme Organisation Adapted from Managing Successful Projects with PRINCE 2 (HMSO 1999), Figure 5.

Modular and incremental development

CCTA's Programme Management methodology provides a formal approach for managing interdependent portfolios of projects and for breaking down projects into realistic components. However, experience has shown that this advice is not always followed. *Successful IT: Modernising Government in Action* gives the following guidance:

- large, ambitious projects carry a high risk of failure to meet some, or all, of their goals;
- government and the private sector have recognised that an effective way to bring about a large reduction in this risk is to break these large projects into smaller, more manageable components;
- departments and agencies must consider the subject explicitly, and must document their chosen approach before initiating large projects.

The Modular Approach

A module is a distinct part of an overall programme of work that offers some value to the organisation, even if the other parts of the programme are not complete. In a modular approach, the overall business requirement will be delivered by providing IT support in modules, each able to underpin a limited set of business processes.

When faced with a large project, it is best to look at the overall range of business support functions required. High priority functions that can be identified should be separated out from the project to be delivered as modules and will thus have a higher probability of success. It is critical that the boundaries of modules are accurately identified at the outset to enable either parallel or sequential delivery of modules. Progress will be determined by:

- financial limitations;
- the ability of the organisation's staff to adjust to multiple simultaneous changes;
- the organisation's ability to manage multiple projects effectively;
- other activities such as existing operations, that make unavoidable demands on resources.

The Incremental Approach

The incremental approach allows evolutionary development of the overall system by beginning with and subsequently building on a component to increase its value to the organisation. The approach is based upon the timely delivery of a baseline requirement followed by planned upgrades to increase capability incrementally through manageable steps. This allows for continuous cost versus benefit evaluation, risk reduction and responsiveness to technology maturation and operational feedback. Incremental acquisition should be adopted for fast-moving or rapidly evolving technologies.

Where the level of IT support can be phased in, this allows an incremental development approach, which will deliver increasing levels of support in a series of smaller, more manageable projects. This approach is particularly valuable where some of the requirements are likely to change due to environmental factors such as legislative or policy change, or improvements in technology.

In an incremental acquisition project, it is vital that the perceptions of both the end-user and the supplier are properly managed. The initial standard of equipment to meet the baseline requirement is not in any sense a prototype; it must be robust, supportable and operable.

Combining modular and incremental approaches

It is perfectly feasible, and advisable, to combine modular and incremental approaches, thus limiting the risks and delivering support to a wider range of business functions.

CCTA, in collaboration with the Office of the e-Envoy and corporate OGC, is producing new outline guidance for departments on modular and incremental approaches.

1.5. *Suppliers*

Procurers of successful projects, IT suppliers, management consultancies and academics all cite effective communication between client and supplier as a major factor in achieving success in the delivery of complex projects. Recommendations in the *Successful IT: Modernising Government in Action* acknowledge this by stating that:

- departments must ensure that they put in place processes that will actively encourage co-operation and open dialogue between supplier and client;
- before contracts are signed, suppliers must have produced a realistic plan, including time scales, resources and technology, for how they will deliver the desired outcomes;
- the OGC continues to gather and share information about the top 10 suppliers of IT to government (by volume and value of business).

2. CASES

The following case examples have been drawn from *Successful IT: Modernising Government in Action*.

Business change

A government agency developed a new system using leading-edge technology but failed to implement it within the context of its existing IT. So many changes were made to the existing system during the development of the new one that the two proved difficult to integrate.¹¹

Time scale

A large, updated business system was delivered late. This was due, in part, to a high-level decision to implement the system on an extremely tight time scale in an attempt to meet a deadline in proposed legislation.¹²

Success

In implementing a resource accounting and budgeting system in the public sector, the senior official with responsibility for finance took an active hands-on approach, established a board for stakeholders and regularly briefed senior managers. Key decisions on implementation were referred to the departmental management board for approval. The project was delivered to time and within budget.¹³

11. NATS, NERC Project.

12. CAPITAL project, Ministry of Defence.

13. Department of Social Security.

Project management

A project to deliver an application to a large number of users was developed by the IT supplier with negligible representation from the users. As the application was rolled-out, user hostility was such that the hoped for benefits of the application did not materialise. The system did not meet the needs of its users. Effective adoption of a project management methodology would force a project to consider key stakeholders (such as staff) and their needs (such as training) in the project.¹⁴

Risk

A government project adopted a formal risk management approach but with little visibility or appreciation of the risks to the organisation outside the project. However, learning from past experience, this project has now introduced a series of risk reporting channels running from the project manager to the board and an executive sub-committee tasked with reviewing progress. A channel also exists between an independent consultant and the board, resulting in an increased visibility of risk.¹⁵

Incremental/modular approach

A public sector project successfully used both modular and incremental approaches to implement a resource accounting system. The functionality was split into “initial” (basic resource accounting) and “additional”, ensuring early implementation of a working system while allowing more time to get the additional functionality right. Eight Early Implementation (EI) sites were identified and proved useful in clarifying the implementation process and system sizing.¹⁶

Benefits realisation

A media company conducted a project for handling copyright that technically performed as expected but did not deliver the claimed benefits. The company has since focused on monitoring projects against the planned benefits at each stage before committing further resources.¹⁷

Roles and responsibilities

A large, business-critical system was procured using PFI. Failure at the outset by the purchaser and the supplier to agree on roles and responsibilities, or a mutually acceptable management structure, hampered the progress of the project and caused serious diversion of management effort, with damaging consequences.¹⁸

14. Immigration and Nationality Directorate, Home Office.
15. Private Sector.
16. Private Sector.
17. Private Sector.
18. QUANTUM, Prison Service, Home Office.

Peer reviews

A government department has an established and successful programme of peer reviews. They intend to significantly expand their in-house capability, accelerate the process of skills transfer and reduce their reliance on consultants.¹⁹

3. LESSONS LEARNED

Some of the major lessons learned have been:

- There has been a lack of clarity about UK Government procurement policy and how it supports departments, agencies and IT suppliers. There is concern that in negotiations with IT suppliers, particularly under PFI, current policy and guidance places too much emphasis on the financial aspects at the expense of business considerations around the quality of new and existing services. Important questions, for example on contingency planning, supplier capability and recent performance, and integration of technology with business processes, have at times been overlooked in the pursuit of a financial deal.
- In the past, some change programmes and projects have suffered from a lack of active ownership. As a result the UK Government has made the recommendation that overall responsibility for delivering the business objectives and benefits of any programme or project must be vested in a single, responsible and visible individual, the SRO. The seniority of the SRO will be dependent on the size, complexity and associated risk of what is being undertaken.
- Some UK Government organisations and private sector firms are much better than others at recognising and addressing this need for projects to have intelligent, active ownership from a single individual. There is also evidence that projects and programmes run into serious problems if they do not have a business owner to perform this role. Of course, having such an owner is not a guarantee of success. However, not having one significantly increases the prospects of failure.
- The quality of risk management varies widely across government. Its application ranges from simple lists (without ownership of risks or actions to mitigate them) to the allocation of full-time risk managers with comprehensive risk registers. Some of the reasons for poor risk management include:
 - Too narrow a focus on inward-looking project risks which are tangible and within the project manager's control, without considering risks to the organisation's business as a whole.
 - Lack of understanding that the ultimate risks of not meeting the business objectives, realising the business benefits, or delivering satisfactory service to the public cannot be transferred to partner or supplier.
 - Failure to understand or define the boundary between the responsibilities of the supplier and the purchasing department or agency.

19. California, USA.

- Too much reliance on the contract or penalty clauses and not enough on action to mitigate risk or devising effective contingency plans.
- Failure to monitor the effectiveness of mitigating action or to refer serious risks to the appropriate level quickly.

For successful IT management, key lessons learned show that you must be able to:

- treat IS and IT as a business issues, not as something to delegate to technical staff;
- think innovatively but pragmatically about the opportunities to transform the business;
- demonstrate leadership in bringing about IT-related business change;
- be realistic in assessing your organisation's ability to cope with change;
- Understand the implications of providers' proposals for change;
- commit realistic resources to supporting staff to work in new ways and set achievable time scales for implementation;
- demonstrate robust management of risk, especially business risk;
- have access to effective project management skills;
- manage business change as an ongoing programme, not as an event that concludes with implementation of new services and systems;
- manage effective working relationships with providers.

Project failures occur due to:

- lack of adequate contingency planning;
- lack of senior level management commitment;
- incomplete/changing requirements and specifications;
- overstatement of the requirements;
- inadequate supplier appraisals and market research;
- lack of resources provided by the contracting authority/supplier;
- problems with suppliers leading to breach of contract and litigation;
- lack of controlled planning in contracts/projects;
- lack of experience of project teams provided by suppliers;
- organisational politics;

- over-ambitious time scales and underestimated budgets;
- overuse of external consultants;
- lack of business user involvement/too much user involvement.

Recommendations for the future based on these lessons are:

- departments should ensure that they analyse and understand fully the implications of the introduction of new IT systems for their businesses and customers;
- departments must adopt a formal project management methodology such as PRINCE 2;
- departments must consider carefully the scale and complexity of projects to assess whether they are achievable;
- delays in implementing projects place them at risk of being overtaken by technological change;
- the project specification must take into account the business needs of the organisation and the requirements of users;
- senior management has a crucial role to play in championing the successful development of IT systems;
- the development of high-quality project management skills within government is essential;
- it is vital that departments pay attention to the management of risks and have contingency plans in case projects are not implemented as planned;
- relations between the department and the supplier will have a crucial effect on the success of the project;
- contracts between departments and suppliers must be clearly set out;
- departments should seek to review the success of projects as soon as possible so that lessons can be fed back into consideration of later projects;
- sufficient time and resources should be spent on ensuring that staff know how to use the IT system

It is essential that departments learn from past mistakes and consider how they can better co-ordinate their considerable resources to ensure better value for money from IT development. One of the recommendations of *Successful IT: Modernising Government in Action* is for the UK Government to develop a database for gathering, maintaining and sharing information about the progress of projects and programmes. A questionnaire is currently being drafted for circulation to departments.

4. LITERATURE, WWW AND STUDIES

Guidance

New electronic guidance in response to Review of Major IT Projects, *Successful IT: Modernising Government in Action* report – briefings on procurement, business cases and risk

<http://www.ccta.gov.uk/bestpractice/mccartneyreport.htm>

IS Management Handbook <http://www.ccta.gov.uk/bestpractice/handbook/>, 2000

Acquisition (CCTA 1999)

IS Strategy: Process and Products (CCTA 1999)

Managing Change (CCTA 1999)

Managing Performance (CCTA 1999)

Managing Services (CCTA 2000)

Managing Partnerships (CCTA 2000)

Managing Successful Programmes (CCTA 1999)

Managing Successful Projects with PRINCE 2 (CCTA 1998)

PRINCE 2: An Outline (CCTA1997)

Standardisation of PFI Contracts - Information Technology (HM Treasury 2000)

Studies and reports

National Audit Office, Value for money study: *Missed Opportunities - Managing Business Risk in Government*, May 2000

Office of the e-Envoy, Review of Major Government IT Projects, *Successful IT: Modernising Government in Action*, 2000

Cabinet Office, *Modernising Government White Paper*, 1999

Public Accounts Committee, *Improving the Delivery of Government IT Projects*, January 2000

Office of the e-Envoy, e-Government: *A strategic framework for public services in the Information Age*, April 2000

Department of Health: *Maximising Value for Money: Examining the role of Strategic Outline Cases*, July 2000

WWW Links

Cabinet Office

<http://www.cabinet-office.gov.uk/>

Central Computer and Telecommunications Agency (CCTA)

<http://www.ccta.gov.uk/>

e-Envoy, Office of the

<http://www.e-envoy.gov.uk/>

Central IT Unit, Cabinet Office (CITU)

<http://www.citu.gov.uk/>

Government Commerce (OGC), Office of

<http://www.ogc.gov.uk/>

Government Information Service (Open)

<http://www.open.gov.uk/>

Her Majesty's Stationary Office

<http://www.itsofficial.net/>

HM Treasury

<http://www.hm-treasury.gov.uk/>

Information Age Government Champions

<http://www.iagchampions.gov.uk/>

National Audit Office (NAO)

<http://www.nao.gov.uk/>

Annex A: Recommendations from *Successful IT: Modernising Government in Action*

Business Change

Recommendation

Recommendation 1: Business development skills must be included as a key feature in the extended Skills For the Information Age (SFIA) framework to be developed by the Central IT Unit (CITU) supported by the Office of Government Commerce (OGC) and the Centre for Management and Policy Studies (CMPS) – see Recommendation 25.

Recommendation 2: CITU (supported by OGC) will, by building on existing best practice and ensuring flexibility for different departments with different needs, involve departments in the provision of guidance and expertise to strengthen the application of the necessary business development skills across government – see Recommendation 29.

Recommendation 3: Business cases must reflect all of the business change to be delivered. Practical guidance on the contents of such a business case will be provided by OGC using the draft business case model developed by the study team (Annex D). The model, available by August 2000, will be taken into account in the OGC audit of procurement guidance – see Recommendation 19.

Leadership and Responsibility

Recommendation

Recommendation 4: Professional development events for ministers and senior civil servants being organised by the Centre for Management and Policy Studies (CMPS) will include informing them of their role in, and responsibility for, major IT projects and programmes. These events will include joint seminars. CMPS will also explore the scope for running joint events with the IT industry. The first of the development events will take place in May 2000.

Recommendation 5: All IT-supported change projects or programmes must have a single, named Senior Responsible Owner (SRO). This individual is responsible for ensuring that the project or programme meets its overall objectives and delivers its projected benefits.

The seniority of the SRO will depend on the size, complexity and associated risks of the work being undertaken but, in all cases, they must be the business sponsor of the change that is driving the IT development. This applies to individual projects and also groups of projects making up a programme.

Recommendation 6: An interim checklist of the roles and responsibilities of the SRO will be made available to departments and agencies by June 2000. A fuller version will be issued by December 2000. The guidance will be regularly updated and refined in the light of experience, and supplemented by information-sharing processes, including forums and networks. This work will be led by OGC.

Recommendation 7: An individual's responsibilities as an SRO must be explicitly included in their personal objectives. The SRO for a project or programme should remain in place throughout or change only when a distinct phase of benefit delivery has been completed. Departments and the Centre should take the need for continuity and previous experience into account when jobs are advertised and appointments made.

Project Management

Recommendation

Recommendation 8: The SRO of each project must ensure that a formal approach to project management, such as PRINCE 2, is applied.

Recommendation 9: Key staff on major projects must undertake formal project management training appropriate to their role in the project, and mentoring should be made available to all project managers across government through mechanisms put in place by OGC from December 2000.

Recommendation 10: Departments and agencies must assess the difficulty of their projects, using the Project Profile Model, and match this against the abilities of their project management.

Risk Management

Recommendation

Recommendation 11: Taking into account the NAO and HM Treasury initiatives already under way, the OGC will investigate further methods of problem reporting and upward referral. These will be based on the Project Profile Model and incorporate the Summary Risk Profile. OGC will bring forward a flexible method that can be modified according to the complexity of each project. Supported by clear guidelines for project managers and peer review teams, the model will be available by December 2000.

Modular and Incremental Development

Recommendation

Recommendation 12: Departments and agencies must adopt a modular and/or incremental approach to projects, unless there are very strong reasons for not doing so. The approach to be taken must be clearly documented before large projects are initiated and must explicitly consider the capabilities of the organisation and its supplier(s) and the size of each proposed increment.

Recommendation 13: OGC must refine and expand on the preliminary guidance issued by the Major IT Projects Review team (Annex E) to provide more advice to help project planners determine their approach to modular and incremental developments. This guidance should be completed by December 2000.

Benefit Realisation

Recommendation

Recommendation 14: All major projects or programmes must undertake periodic reviews of proposed benefits throughout development and implementation. The SRO is responsible for ensuring that this is done.

Recommendation 15: A post-implementation review must be undertaken of all projects or programmes and benefits realised assessed against projected benefits outlined in the original business case or subsequent amendments. These reports must be endorsed by the SRO and, for projects where their involvement is required, tabled with HM Treasury and the OGC.

Recommendation 16: HM Treasury (HMT) should review the systems departments and agencies have in place for monitoring the realisation of benefits and take these into account when considering proposals for major initiatives and investments. These reviews should be undertaken in parallel with the regular reviews of departmental investment strategies.

Recommendation 17: The OGC should review the results of post-implementation reviews, and ensure that valuable common information, such as trends in areas of successful or difficult realisation, is widely available. The work is to be ongoing, but should start by September 2000.

Recommendation 18: OGC, in consultation with CITU, should examine what additional measures and guidance need to be established to ensure government maximises benefits from its investments in technology. This work to be complete by December 2000.

Procurement and Supplier Relationships

Recommendation

Recommendation 19: OGC should audit existing policy and guidance on procurement and produce a consolidated and unambiguous set of material for IT, making it clear which elements are mandatory. This should be made available on-line and at no cost to government users. The work should be completed by October 2000.

Recommendation 20: Departments and agencies must ensure that they put in place processes that will actively encourage co-operation and an open dialogue between supplier and client. Projects already under way should immediately re-examine their communication mechanisms to ensure appropriate processes are in place.

Recommendation 21:

Before contracts are signed, suppliers must have produced a realistic plan, including time scales, resources and technology, for how they will deliver the outcomes being sought under the relationship. The same applies to evolutionary or modular phases within an existing contract. These supplier plans must be re-examined during the development stages of the project to ensure a close fit between business design, assurance and implementation intentions and the supplier activities concerned with developing the solution.

Part 2: Guidance for departments on how to evaluate such plans should be developed, initially by HM Treasury Task Force and then by OGC.

Recommendation 22: OGC should continue to gather information about the top 10 suppliers of IT to government (by volume and value of business). The first set of intelligence data should be available by December 2000. The information gathered should include, for each supplier:

the range of IT services supplied (as defined in the Project Profile Model);

their recent performance with government; and

in time, their ongoing performance against our recommendations.

Cross-Cutting Initiatives

Recommendation

Recommendation 23: Cross-cutting projects and programmes must have a unified, regularly updated business case. An SRO must be appointed to all such initiatives and they must assure themselves that the recommendations of this study are being applied.

People and Skills

Recommendation 24: Government, through CITU (supported by OGC), must develop the processes and guidance necessary to enable the SFIA or an equivalent technical skills framework to be used by departments and agencies as they develop their responses to the e-government Strategy.

Recommendation 25: CITU (supported by OGC and CMPS) must develop an extension to the SFIA, embracing the core IS skills identified in the SLOAN review. We recommend that:

departments and agencies should use the extended SFIA in developing their responses to the e-government Strategy; and

in order to meet the demanding timetable of the Modernising Government agenda, initial processes and guidance must be made available by August 2000, so that departments and agencies can use them in preparing their responses to the e-government Strategy (due October 2000).

Recommendation 26: The work on Civil Service Reform, being led by Civil Service Corporate Management (CSCM) in the Cabinet Office, should explicitly take into account the findings of this study.

Recommendation 27: The government, through CITU (supported by OGC and CMPS), must develop processes to support the co-ordinated and ongoing assessment of its IS skills base and mechanisms to ensure delivery of improvements. These proposals should be in place by December 2000.

Learning Lessons

Recommendation

Recommendation 28: The draft peer review process developed by this study (see Annex B) should be implemented by OGC by September 2000, in parallel with their gateway approvals process, and departments and agencies should carry out and contribute to project peer reviews at the recommended intervals.

Recommendation 29: Government must establish effective permanent mechanisms for obtaining and disseminating information about managing programmes and projects. This should be carried out by CMPS in co-operation with OGC and CITU. The first outputs, including information on GSI, to be available by September 2000.

Recommendation 30: The government, building on specifications developed by this review, must construct a system for gathering, maintaining and sharing information about the progress of projects and programmes. This system will be developed and maintained by OGC, in consultation with CITU and others, with completion of the system due by December 2000.

Annex B: Project Profile Model - criteria for assessing risk

Criteria	Comments
Total value of the business benefits in £.	Total (as opposed to annual) value, calculated in line with HM Treasury guidance.
Total value of the business costs in £.	Total (as opposed to annual) costs, calculated in line with HM Treasury guidance. Excludes IT costs which are covered later.
Number of individuals affected.	Refers to internal personnel within Government – i.e. includes technical and business staff and users, but excludes citizens, suppliers, etc.
Impact on business processes (includes changed processes).	Refers to the impact that the project will have on the organisation (both during development and after implementation). Allocate a score between 1 and 6.
Impact on Government services at implementation.	Refers to the impact that the project will have outside the organisation, for example on the public and businesses (both during development and after implementation). Allocate a score between 1 and 6.
Impact on other projects and changes.	The degree to which the project is dependent on and connected to other projects and changes. Allocate a score between 1 and 8.

Technical Impact

Criteria	Comments
Total IT costs.	Total (as opposed to annual) IT costs, calculated in line with HM Treasury guidance. For commercial contracts this will be the total charge to department rather than cost to supplier.
Number of IT practitioners (including internal and out-sourced suppliers).	
Degree of innovation.	The extent to which the project involves innovative solutions, and the level of familiarity and experience available. Allocate a score between 1 and 4.
Impact on legacy systems and data.	The degree to which the project will need to develop interfaces to existing systems and data stores. Allocate a score between 1 and 4.
Scope of IT supply. (Note: for this criterion score for each element, <i>i.e.</i> may be cumulative.)	The range of activity that will be undertaken by the IT supplier, and the extent to which these will impact on the business processes of the organisation.

Client/Supplier Arrangements

Criteria	Comments
Client-side organisation.	The complexity of the client-side arrangements. Allocate a score between 1 and 4.
Supply-side organisation.	The complexity of the supply-side arrangements.

UNITED STATES

INTRODUCTION

Despite the best efforts of the federal government, most policy makers are troubled by the high failure rate of large IT projects. It is difficult to understand how many of these projects can go on for years, returning no useful product, finally having to be scrapped. At the same time there are many notable successes, many valuable lessons learned, and much improved policy and direction to help ensure success in new projects. This report summarises the policy framework for managing IT projects in the US Federal Government, as well as experience with specific cases during the last few years. Lessons learned and several emerging IT management issues are also discussed.

1. GENERAL INSTITUTIONAL FRAMEWORK

1.1. Policies

Background

During the last forty years, the federal government has been working to increase the effectiveness of its management of information and technology. The first major policy direction was provided by the 1965 Brooks Act, which established central oversight of federal information technology acquisitions by the General Services Administration (GSA).²⁰ This law was aimed primarily at the effective purchase and use of the large and expensive mainframe computers of the time.

In 1980, the Paperwork Reduction Act (PRA) addressed the management of information, reducing the burden of the collection of information, and emphasizing life cycle management principles. It also created senior information resource management officials across government to manage IT activities, focusing attention on the importance of this in effective operation. Responsibilities were spelled out for planning, budgeting, controlling and reviewing all information management activities including major IT projects. The Act also created the Office of Information and Regulatory Affairs in the Office of Management and Budget (OMB),²¹ which oversees federal regulations and information requirements, and develops policies to improve government statistics and information management. A major responsibility of this office is to direct, manage and review IT policies and activities across the government. The law also includes the following goals for federal agency use of information technology:

20. GSA provides policy leadership and managed space, supplies, services, and solutions for the US Government. GSA also provides workspace, security, furniture, equipment, supplies, tools, computers, and telephones, as well as travel and transportation services, and develops, advocates, and evaluates government-wide policy.

21. OMB's predominant mission is to assist the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies. In helping to formulate the President's spending plans, OMB evaluates the effectiveness of agency programs, policies, and procedures, assesses competing funding demands among agencies, and sets funding priorities. OMB ensures that agency reports, rules, testimony, and proposed legislation are consistent with the President's budget and with administration policies. In addition, OMB oversees and co-ordinates the Administration's procurement, financial management, information, and regulatory policies. In each of these areas, OMB's role is to help improve administrative management, to develop better performance measures and coordinating mechanisms, and to reduce any unnecessary burdens on the population.

- improve service delivery and program management
- increase productivity
- improve decision making,
- reduce waste and fraud, and reduce the information processing burden for the federal government and for the public who provide information to the federal government.

Contemporary Policy

In the early 1990s, additional direction was provided for overall organisation performance, recognising the critical role of IT and information management in the delivery of government functions. The Government Performance and Results Act (GPRA)²² of 1993 required that agencies set strategic goals, measure performance toward the goals, and report on their progress. Effective implementation of GPRA relies critically on agencies' ability to produce the meaningfully integrated information needed to manage performance and measure results.

Further policy and direction was provided with the reauthorisation of the PRA²³ in 1995 which requires that agencies indicate in strategic information resources management plans how they are applying information resources to improve the productivity, efficiency, and effectiveness of government programs, including improvements in the delivery of services to the public. Provisions in this law also require OMB to help agencies acquire and use information technology through the review of agency budget requests, other plans, and analysis that supports information technology projects.

Consolidated IT Management Direction

In 1996, policies for management of large IT projects were consolidated and reformulated in the Clinger-Cohen Act.²⁴ This law describes responsibilities and actions for the Executive Branch of government including:

- The Director of the OMB, and
- Executive Agencies (including Chief Information Officers).

IT policy is provided for:

- capital investment decision processes to ensure good return on investment
- modular development processes to avoid "large scale failures"
- risk assessment processes to ensure sound security practices and high success probability, and
- post implementation review and evaluation processes to ensure continuing results and course corrections where appropriate.

22. Section 5501 of Title 15, Public Law 103-62.

23. Public Law 104-13.

24. Public Law 104-106, previously known as the Information Technology Management Reform Act (ITMRA).

The Clinger-Cohen Act prescribes specific direction for:

- creation of Chief Information Officers in each major agency
- planning and acquiring of IT
- IT multiple award schedule contracting
- incremental procurement of IT, and
- maintaining a directory of information resources.

Provisions of this law are described in more detail below, particularly the direction for the capital investment decision process.

Emerging IT Management Issues

In addition to the above policies formulated and implemented through the 1990s, two major issues have evolved during the past several years that are strongly influencing future IT management across the US Government:

- transformation of government functions to the electronic medium (e-Government), and
- problems with computer or “cyber” security.

E-Government

With the phenomenal growth and impact of the Internet and the World Wide Web over the past five years, there has been a strong recognition of the need for the federal government to interact with the public via this medium. Guidance for converting federal government activities to electronic commerce and general paperless operation is provided in the Government Paperwork Elimination Act (GPEA).²⁵ This Act requires federal government agencies to “offer the option, when practicable, for the maintenance, submission, or disclosure of information by electronic means by October 2003”. The Act specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form, and encourages federal government use of a range of electronic signature alternatives. The implementation of GPEA is rapidly driving many major IT projects to meet these e-Government initiatives in addition to their original objectives. IT policies and guidance are being transformed to accommodate this shift.

Cyber Security

Rampant federal government computer break-ins, denials of service, and general disruption of computer services has been causing increasing concern that these services cannot continue to operate and grow effectively without greater security. In partial answer to public concern about these issues in both the private and public sector, guidance and direction on Computer Security has been provided in the

25. Public Law 105-277.

President's January 2000 National Plan for Information Systems Protection.²⁶ Among general provisions, this plan outlines a number of new, centrally managed entities and projects that have been initiated to assist agencies in strengthening their security programs and improving federal intrusion detection. In addition, on March 3 2000, in response to recent Internet disruptions, the President issued a memorandum to the heads of executive departments and agencies urging them to renew their efforts to safeguard their computer systems against denial-of-service attacks from the Internet. These risk considerations cause particular concern about the interdependence of IT systems, and inject another element of complexity in the application of the above policies governing a particular IT project.

1.2. IT Funding/Decision/Assessment

The US Government spends more than \$38 billion each year on IT, and this figure will continue to grow as virtually all functions of government take advantage of efficiencies provided by IT. Well-selected, controlled, and managed IT projects provide some of the best opportunities for agencies to fulfil their missions with the lowest cost and greatest benefits. The budget of the US Government for FY 2001 includes a priority management objective to strengthen government-wide management of IT by using capital planning and investment control. For a summary of these investments, Table 22.1 of the Analytical Perspectives of the FY 2001 Budget²⁷ provides both a total of all IT investments for the US Government and a selection of IT investments focusing on program and performance benefits.

The following three central management offices play the major role in the IT investment and decision-making process in the federal government:

- Office of Management and Budget (OMB)
- General Accounting Office (GAO),²⁸
- General Services Administration (GSA).

The Office of Management and Budget provides direction on Evaluating Information Technology Investments.²⁹ This direction describes three major phases of the investment and control process for IT projects:

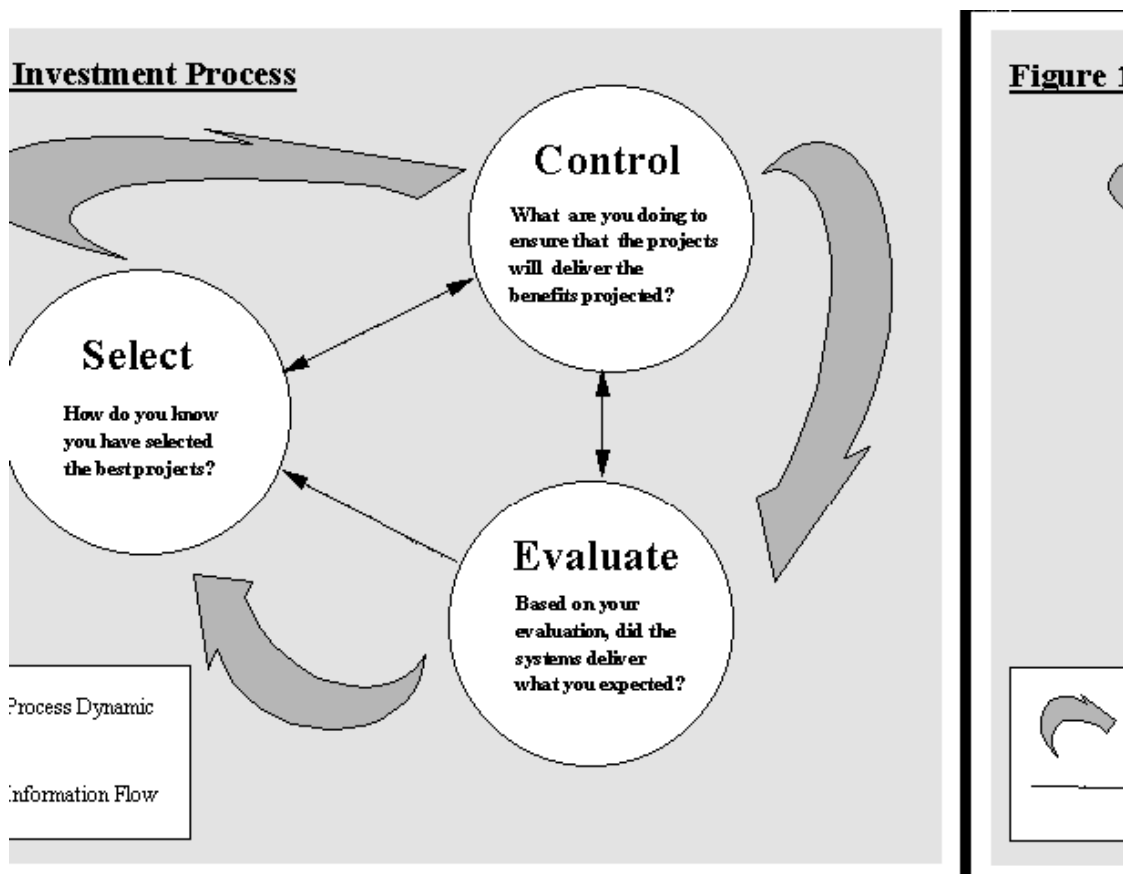
- selecting (screening, evaluating risks and return, and mission mix)
- controlling (monitoring against costs, schedule and performance)
- evaluating (post implementation reviews, adjustments, and lessons).

26. Defending America's Cyberspace: National Plan for Information Systems Protection: An Invitation to a Dialogue, issued by the President on January 7 2000.

27. Budget of the United States Government for FY 2001.

28. The General Accounting Office is the investigative arm of Congress. GAO exists to support the Congress in meeting its Constitutional responsibilities and to improve the performance and accountability of the federal government.

29. Office of Management and Budget Memorandum M-97-02 and additional guidance.



The IT investment process illustrated in Figure 1 is followed in each agency as it proposes IT investments in the annual budget. OMB reviews and decides on all aspects of an IT proposal, including what level of funding will be contained in the President’s budget when it is submitted to Congress. Final funding decisions are made in the Fiscal Year Appropriations process as the Congress of the United States sends each of the 13 Appropriations Laws to the President for signature. Large IT projects are always multi-year, and at any point in the project’s life cycle OMB may conduct a review of progress. At least annually, as part of the budget process, major technology projects must be reviewed.³⁰

Additionally, at any point in the funding and decision process, GAO may be asked to conduct a review of an IT project by any member of the US Congress. These reviews may be at the proposal, funding, implementation, or post-implementation stage. Agencies are generally allowed to comment on, and respond to, the contents of these reviews before they are presented to the requester or made public. There are also occasions where private reports are provided to the requesting member and no public report is made. GAO has described an IT Investment Framework³¹ which describes five maturity stages and the critical processes for each. This framework is used as a standard in reviewing IT investment processes in agencies:

30. As stipulated in OMB Circular A-11, Preparation and Submission of Budget Estimates.

31. Information Technology Assessment Management: An Overview of GAO’s Assessment Framework, May 2000

Stage 1 – Creating investment awareness

Critical Processes

- IT spending without disciplined investment processes
- IT subordinated in mission expenditures

Stage 2 – Building the investment foundation

Critical Processes

- IT investment board operation
- IT project oversight
- IT asset tracking
- Business needs identification for IT projects
- Proposal selection

Stage 3 – Developing a common investment portfolio

Critical processes

- Authority alignment of IT investment boards
- Portfolio selection criteria definition
- Investment analysis
- Portfolio development
- Portfolio performance oversight

Stage 4 – Improving investment process

Critical processes

- Post-implementation reviews and feedback
- Portfolio performance evaluation and improvement
- Systems and technology succession management

Stage 5 – Applying IT for strategic outcomes

Critical processes

- Investment process benchmarking
- IT-driven strategic business change

Agencies expect to be reviewed on these criteria, and have a strong incentive to develop the critical processes described in this framework.

GSA formulates and administers IT investment policy as well, and is the controlling agency for the IT procurement process. This includes the oversight and management process for granting Delegated Procurement Authority (DPA) for large IT projects, which are required to proceed with IT contracts. GSA also has a division for providing specific IT services³² to agencies, allowing them easier access to technical skills and IT management expertise.

1.3. IT Project Management Elements

For large IT projects, within the policy framework above, major management elements are:

- investment management
- information management
- IT architecture
- systems development environment
- management of the paperless environment
- information security.

IT investment management is an integrated view that provides for life-cycle management of the IT project. As described above, there are three phases of the process: selection, control, and evaluation. In the selection phase, the agency or organisation determines priorities and makes decisions about which projects will be funded, based on their technical soundness, contribution to mission needs, performance improvement priorities, and overall IT capital funding levels. The costs, benefits, and risks of all IT projects are assessed and ranked. In the control phase, all projects are compared at similar stages in development. Progress reviews, in which progress is compared against projected cost, schedule, and expected mission benefits, are conducted at key stages in each project's life cycle. The evaluation phase compares actual performance against estimates to identify areas in which future decision making can be improved.³³

32. GSA Federal Technology Service delivers a range of telecommunications, information technology systems, hardware and software, consulting services, information security services and products, and integrated technology solutions.

33. More detail can be found in the GAO Guide "Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making", February 1997.

Information management is the consideration of the collection, use, and dissemination of the information contained in a large IT project. Each system must provide for public access to records where required and appropriate. The system must be designed so that it will collect or create only that information necessary and useful for the proper performance of agency functions. Agencies must ensure that proper records are maintained, and that the public is not unduly burdened by the requirement to provide information mandated by an information system.³⁴

IT architecture is a blueprint - consisting of logical and technical components - to guide the development and evolution of a collection of related systems. The architecture provides a high-level description of an organisation's mission, its business functions, the relationship between functions, the information needed to perform the functions, and the flow of information between them. Technically, the architecture provides the rules and standards needed to ensure that the interrelated IT projects are built to be interoperable and maintainable.

A systems development environment is also defined so that each major IT project can apply the elements of that environment for consistent management and control. Systems development is the most sensitive part of large IT projects, and most failures occur because the development of software never meets expectations, or cannot be made operational. To provide the software needed for a major IT project, the organisation can develop its own, use a contractor, use commercial off-the-shelf software, or a combination. To manage software development and acquisition processes effectively, however, the organisation needs to have well-defined software management processes, including methodologies and standards. Key processes for software development include requirements management, project planning, project tracking and oversight, quality assurance, and configuration management. For software acquisition, additional management is needed for solicitation, contract tracking and oversight, product evaluation, and transition to implementation and support.

Management of the paperless environment is the increasingly important consideration of how the business of the agency is conducted in the electronic medium, including that between agencies, the public, and the commercial sector. Large IT projects must participate in this environment, and special consideration must be given to authenticity, electronic signature, adequate electronic audit trails, and related elements. Consideration must also be given to equal access by participants in a system, where electronic access is required. Paper, or other alternatives may need to be maintained, if some participants cannot gain electronic access.³⁵

Information security policies and practices provide the framework to protect an organisation's computer-supported resources and assets. This protection ensures the integrity, confidentiality, and availability of the data and systems of an organisation. Integrity ensures that data have not been altered or destroyed in an unauthorised manner; confidentiality ensures that information is not made available or disclosed to unauthorised individuals or entities; availability ensures that data will be accessible upon demand by an authorised entity. Key activities for managing information security are risk assessment, awareness, evaluation, and central management. Risk assessments consist of identifying threats and vulnerabilities to information assets and operational capabilities, ranking risk exposures, and identifying cost-effective controls; awareness involves promoting knowledge of security risks and educating users about security policies, procedures and responsibilities; evaluation involves monitoring effectiveness of controls and awareness activities through periodic evaluations. Central management involves co-ordinating security through a centralised group.

34. More detail can be found in OMB Circular A-130, "Management of Federal Information Resources".

35. This is sometimes known as the "digital divide" issue.

2. CASES

We often cite notable failures of major IT projects, but it is also important to recognise when major information systems are working well, making real contributions to the business of government. An example of this type of recognition is the Government Technology Leadership Awards³⁶ program, whose purpose is to highlight IT program contributions and successes. Three recent winners of this program are summarised³⁷ here as a reminder of the kind of results being achieved by major IT projects, in spite of the risks and problems that exist.

Case 1 – National Weather Service “Advanced Interactive Weather System”

On May 3 1999 more than 70 tornadoes ripped through Oklahoma and southern Kansas. The tornadoes left hundreds injured, took almost 50 lives and caused more than \$1 billion in damage. Had the National Weather Service been caught unaware, casualties could have been worse. Thanks to NWS’ new \$540 million Advanced Weather Interactive Processing System (AWIPS), forecasters were able to issue warnings with an average lead time of 32 minutes before the severe weather hit. The Norman, Oklahoma office issued 70 tornado warnings and 46 severe thunderstorm warnings over 10 hours on May 3. NWS attributes part of their successful coverage to the use of multiple AWIPS workstations that enabled NWS forecasters to divide their areas of responsibility geographically.

"We’ve put in place a new line of super computers for atmospheric modelling," says Mary Glackin, AWIPS program manager. "The key element of this is AWIPS. It brings all of these new data sets right to the forecaster on one display and allows for data analysis in a short amount of time." Glackin says speed in forecasting is vital. "Many hazardous weather events happen in a short timeframe, like flash flooding or tornadoes. We can manipulate the data and get a warning out virtually within seconds. . . . With AWIPS we are able to pick up precursors of significant weather events," adds Glackin. "Even a few minutes improvement makes a lot of difference." AWIPS employs an open systems architecture that allows the NWS to continually modify the system. "Our intent is not to let it get obsolete. Ultimately the goal is to keep pace with the sciences of meteorology and hydrology."

Case 2 – US Geological Survey “National Atlas of the United States”

When the first National Atlas of the United States appeared in 1970, it weighed 12 pounds and was limited to a production run of 15 000 copies. Almost 30 years later, in a meeting between US Geological Survey officials and Senator Slade Gorton, of Washington, the senator hefted a copy of the 1970 behemoth and asked, "When are you going to do another one of these?"

In 1997, the USGS received the first \$1 million of \$5 million in Congressional funding for its National Atlas project. However, this National Atlas is very different from its predecessor—it is on the World Wide Web. Users can create their own maps using data from the USGS, Census Bureau, Environmental Protection Agency, and other agencies. "This has been a leadership role for the USGS and as much a co-ordination role as anything else," says Jay Donnelly, the Atlas’s managing editor. "With the World Wide Web as the publishing medium we no longer have to restrict content. We can make the digital representations of maps available to the public regardless of theme." This means users can create maps using a standard Web browser. The maps can combine demographic, environmental, geographic, geologic

36. Sponsored by Government Executive Magazine and a public-private partnership.

37. Government Executive Magazine, December 1999, Vol. 31, Number 12.

and even biological data. For example, users can create a map that displays the nation's streams and watersheds overlaid with data on toxic releases or large scale pollution sites.

USGS has produced hard-copy counterparts for the maps available on the Web, but the days of the 12-pounder are gone. These are separate maps on subjects such as the nation's principal aquifers/groundwater resources, watershed boundaries and the distribution of federal and American Indian-owned land. Most recently the USGS released a shaded relief map of North America, and will issue next a map on the nation's wetlands.

Case 3 – US Department of Transportation “Docket Management System”

When the Transportation Department (DOT) prepares new rules on air bags or hazardous material transport, each new regulation is tracked with a bulging file of petitions, public comments and final decisions called a docket. In 1993 DOT operated nine docket rooms, each with its own staff. Researching a docket thus meant trips between rooms and sometimes long waits. So the agency formed a central docket room in Washington and then moved the whole process on to the Web.

Now, interested public and private sector parties can stay up to date by looking at the Docket Management System (DMS) Web site which provides all the information that was contained in a single paper-based docket -- commentary, adjudications, extensions. DMS lists the top-requested dockets on the system. Last fall, for example, the leader was a Maritime Administration docket on attempts to re-register eight ships designed to carry liquefied natural gas under a foreign flag. It had chalked up more than 12,000 hits. Interested parties include everyone from the petitioning companies and concerned citizens to the sailors on the ships who would be affected by such re-registration. Commentary and official documents can be submitted on paper or via e-mail. Decisions by DOT officials are listed as well, and DOT is now in the process of putting its entire backlog of paper-based dockets online.

Case 4 – The Y2K Problem

Beginning in earnest in the spring of 1997, the course of IT in all sectors was altered significantly with the extraordinary effort on the Y2K problem. By 1999, the US Federal Government had designated “resolving the Y2K problem as our foremost management objective”. IT and related general management policies, practices and processes were all refocused during this period until the Y2K problem was successfully resolved in January 2000. Factors contributing to its success were the values of:

- attention from top-level management
- effective risk analysis in guiding direction
- complete systems inventories
- reviews by independent auditors and contractors
- comprehensive testing methods and procedures, and
- business continuity and contingency planning.

The IT management institutional framework has been strongly influenced by the successful experience with these factors in the Y2K effort, and they are consequently now being incorporated into policies and practices.

Of course, many major IT projects do not work well, and are subject to intense scrutiny in the management and oversight process. Several cases are summarised here to highlight problems, characteristics, and help identify lessons that can be learned from these efforts as well.

Case 5 -- A large-scale federal land and minerals record system – a failure

In a review of this troubled system in 1999, GAO³⁸ described the history as follows:

During the energy boom of the early 1980s, the bureau found that it could not handle the case processing workload associated with a growing number of applications for oil and gas leases. The bureau recognized that to keep up with increased demand, it needed to automate its manual records and case processing activities. Therefore, in the mid-1980s, it began planning to acquire an automated land and mineral case processing system. At that time, the bureau estimated that the life-cycle cost of such a system would be about \$240 million.

In 1988 the bureau expanded the scope of the system to include a land information system (LIS). The expanded system was to provide automated information systems and geographic information systems technology capabilities to support other land management functions, such as land use and resource planning. The bureau combined the LIS with a project to modernize the bureau's computer and telecommunications equipment, and estimated the total life-cycle cost of this combined project to be \$880 million. The project was reduced in scope in 1989 to respond to concern about the high cost. The project consisted of three major components—the Initial Operating Capability (IOC), a geographic coordinate database, and the modernization of the bureau's computer and telecommunications infrastructure and re-host of selected management and administrative systems. Estimated life-cycle costs were \$575 million (later reduced to \$403 million), and the bureau planned to complete the entire project by the end of fiscal year 1996.

The IOC was to be the flagship of the modernization, and was to replace various manual and ad hoc automated systems. The bureau designated the IOC a critical system for (1) automating land and mineral records, (2) supporting case processing activities, including leasing oil and gas reserves and recording valid mining claims, and (3) providing information for land and resource management activities, including timber sales and grazing leases. The system was expected to more efficiently record, maintain, and retrieve land description, ownership, and use information to support the bureau, other federal programs, and interested parties. It was to do this by using the new computer and telecommunications equipment that was deployed throughout the bureau, integrating multiple databases into a single geographically referenced database, shortening the time to complete case processing activities, and automating costly manual records.

Despite the promise of IOC to significantly improve business operations, repeated problems with its development have prevented deployment. For example, during a user evaluation test in May 1996, problems were reported involving unacceptably slow system performance. Subsequent testing in 1996 uncovered 204 high-priority software problems, which delayed project completion by about a year. In testing conducted in November 1997, the bureau encountered workstation failures and slowdowns caused by insufficient workstation memory and by problems discovered in two bureau-developed software applications. Some of these problems had been identified in earlier tests but had not been corrected.

38. GAO Congressional Testimony GAO/T-AIMD-99-102, March 4 1999.

Additional testing uncovered software errors that resulted in missing, incorrect, and incomplete data, and error files that contained accurate data. As a result of these problems, the bureau postponed the Operational Assessment Test and Evaluation (OAT&E) that had been scheduled for December 1997. The OAT&E was to determine whether the IOC was ready to be deployed to the first state office.

In October 1998, the OAT&E was conducted and showed that the IOC was not ready to be deployed because it did not meet requirements. During the test, users reported several problems, including that the IOC (1) did not support the bureau's business activities, (2) was too complex, and (3) significantly impeded worker productivity. For example, one tester reported that entering data for a \$10 sale of a commodity, such as gravel, required an hour of data entry using the IOC, whereas with the existing system, the same transaction would have taken about 10 minutes. Users also reported that system response time problems were severe or catastrophic at all test sites. One user said "It is ridiculous to spend 2 or 3 hours to enter information in this system, when it takes 30 minutes to an hour to process the information into the legacy system." Finally, users reported data converted from legacy databases were not accurate, and that validation of the converted legacy data required inordinate effort and time.

Because these problems are significant, senior bureau officials have decided that the IOC is not currently deployable. According to the bureau, it obligated about \$411 million on the project between fiscal years 1983 and 1998, of which more than \$67 million was spent to develop the IOC software. The \$67 million does not include the IOC costs that are part of other cost categories, such as costs for work performed from fiscal years 1983 through 1988, project management, computer and telecommunications hardware and software, data management, and systems operation and maintenance.

This is not an isolated incident, but it is hard to understand how so many years and so much energy could be expended on a project before deciding to terminate it. In looking for shortcomings leading up to the cancellation of this project, it was concluded that the bureau:

- did not develop a system architecture or formulate a concept of operations before designing and developing the project
- never had a credible project schedule, reliable milestones, or a critical path to manage the development and deployment of the project
- invited serious risks because it planned to stress-test only the IOC component—and not the entire system workload including e-mail, office systems and other production applications
- incurred serious risks because it had not established:
 - a) a robust configuration management program for the project
 - b) a security plan or security architecture for the project
 - c) transition plans to guide the incorporation of IOC into its daily operations
 - d) operations and maintenance plans.

All of these items are covered in policies and direction above, but were not made a critical part of the project management process. A major lesson here is the value of independent project review and evaluation, *i.e.* objectively identifying risks and problems in the direction of the project. In this case, there were reviews and warnings along the way (in the "monitoring and controlling phase"), but these were not taken seriously by bureau management. An additional lesson is the danger created by the momentum of a project that is too ambitious in scope, and takes on a life of its own. This can threaten the reputation of the

organisation to the point that “it cannot fail” leading to defensiveness on the part of management. A modular project formulation (instead of the “grand design”³⁹ approach) with opportunities to adjust to changes in circumstance, technology, and requirements could have avoided the total cancellation resulting from the “all or nothing” nature of this case.

Case 6 – A large agency modernisation – gaining coherence in major systems.

In a review in May 2000 GAO⁴⁰ described this system as follows:

Over a decade ago, the Service began its systems modernization program, then called Tax Systems Modernization (TSM), to establish a virtually paper-free tax processing environment where taxpayer information would be readily available to service employees for updating taxpayer accounts and responding to taxpayer inquiries. In 1995, we identified serious management and technical weaknesses with TSM that jeopardized its successful completion. Accordingly, we made over a dozen recommendations to fix the problems, such as formulating a comprehensive business strategy, establishing information technology (IT) investment management processes, and completing and enforcing an integrated enterprise architecture. In addition, because of the seriousness of the weaknesses, we designated TSM as a high-risk IT initiative, placed the modernization on our list of high-risk federal programs, and have continued to monitor this program.

In 1998, the Congress established an Information Technology Investment Account (ITIA) and limited the Service’s obligation of ITIA funds until the Service submits to the Congress for approval an expenditure plan that meets certain conditions. The conditions are that the plan should (1) implement the modernization blueprint, (2) meet OMB’s IT investment guidelines, (3) be reviewed and approved by the Service’s Investment Review Board, OMB, and the overseeing agency Management Board and be reviewed by GAO, (4) meet the requirements of the Service’s life cycle program, and (5) comply with acquisition rules, requirements, guidelines, and systems acquisitions management practices of the federal government. To date, the Congress has appropriated \$506 million for the account via the Service’s fiscal year 1998 and 1999 appropriations acts.

In May 1999, the Service submitted its first or “initial” expenditure plan, requesting about \$35 million for modernization initiatives and commitments to be delivered by October 31, 1999. As part of this plan, the Service also stated its intention to modernize its systems incrementally and submit incremental expenditure plans for release of ITIA funds. We reviewed the plan and reported in June 1999 that this incremental approach was an industry best practice, and if properly implemented, the plan was an appropriate first step. However, to measure the Service’s modernization performance and accountability on this and future expenditure plans, we recommended that each plan fully disclose the Service’s progress against incremental goals, deliverables, and benefits set forth in earlier plans. Based on our report, the House and Senate Appropriations Subcommittees approved the Service’s \$35 million expenditure plan in June 1999.

At that time, the Service planned to submit a second expenditure plan in October 1999. However, it was unable to do so on time, and in early December 1999, submitted to the House and Senate appropriations subcommittees a “stopgap” funding measure to obligate about \$33 million from ITIA until the next plan was submitted. We reviewed the “stopgap” funding measure and raised concerns about projects that were scheduled to begin detailed design and software development before, among other things, the enterprise

39. The “grand design” approach involves investing in a large, long-term, expensive project based on cost and benefit estimates prepared at the outset and attempting to deliver the entire project years later as a single increment.

40. GAO Report GAO/AIMD-00-175, May 2000.

architecture and the Enterprise Life Cycle (ELC) was defined and implemented. Later that December, the appropriations subcommittees approved the Service's \$33 million "stopgap" funding measure but in discussions and correspondence, directed IRS to (1) expedite completion of the architecture and implementation of the ELC and (2) explain in future expenditure plans how it plans to manage the risk of performing detailed design or development work if the architecture is not completed or the ELC is not implemented.

This is a case where concerns with the co-ordination and control of the "modernisation" of the tax systems were so pervasive, that special funding controls were put in place to help manage the projects. Concerns centred on the need for coherent enterprise life cycle and architecture before detailed systems design and implementation were begun. These concerns were heightened by past problems in delivering IT projects in the Service – there have been many previous cases with poor performance. One of the lessons learned from this case is that the basic policies for management and control of a very large environment are not very different in concept from projects of a far more moderate size. The needs for life cycle funding and management, coherent enterprise architecture, incremental goals, tracking deliverables, and accurately measuring benefits are all directly applicable to the largest of projects.

Case 7 – "ILOVEYOU" virus -- system security in an interconnected world.

In Congressional Testimony on May 10 2000, GAO⁴¹ testified on this system as follows:

ILOVEYOU is both a "virus" and "worm." Worms propagate themselves through networks; viruses destroy files and replicate themselves by manipulating files. The damage resulting from this particular hybrid— which includes overwhelmed e-mail systems and lost files—is limited to users of the Microsoft Windows operating system.

ILOVEYOU typically comes in the form of an e-mail message from someone the recipient knows with an attachment called LOVE-LETTER-FOR-YOU.TXT.VBS. The attachment is a Visual Basic Script (VBS) file. As long as recipients do not run the attached file, their systems will not be affected and they need only to delete the e-mail and its attachment. When opened and allowed to run, however, ILOVEYOU attempts to:

- send copies of itself using Microsoft Outlook (an electronic mail software program) to all entries in all of the recipient's address books,
- infect the Internet Relay Chat (IRC) program so that the next time a user starts "chatting" on the Internet, the worm can spread to everyone who connects to the chat server,
- search for picture, video, and music files and overwrite or replace them with a copy of itself, and
- install a password-stealing program that will become active when the recipient opens Internet Explorer and reboots the computer.

In short, ILOVEYOU looks a lot like Melissa in operation: it comes via e-mail; it attacks Microsoft's Outlook; it's a hybrid between a worm and a virus; and it does some damage—but it mostly excels at using the infected system to e-mail copies of itself to others. The one main difference is that it proliferated much faster than Melissa because it came during the work week, not the weekend. Moreover, ILOVEYOU sent itself to everyone on the recipient's e-mail lists, rather than just the first 50 addressees as Melissa did.

41. GAO Congressional Testimony GAO/T-AIMD-00-171, May 10 2000.

In fact, soon after initial reports of the worm/virus surfaced in Asia on May 4, ILOVEYOU spread rapidly throughout the rest of the world. By 6 pm the same day, Carnegie Mellon's CERT Coordination Center had received over 400 direct reports involving more than 420,000 Internet hosts. And by the next day, ILOVEYOU appeared in new guises, labeled as "Mother's Day," "Joke," "Very Funny," among others. At least 14 different variants of the virus had been identified by the weekend, according to DOD's Joint Task Force-Computer Network Defense. These variations re-triggered disruptions because they allowed the worm/virus to bypass filters set up earlier to block ILOVEYOU. At least one variant—with the subject header "VIRUS ALERT!!!"—was reportedly even more dangerous than the original because it was also able to overwrite system files critical to computing functions.

Reports from various media, government agencies, and computer security experts indicate that the impact of ILOVEYOU was extensive. The virus reportedly hit large corporations such as AT&T, TWA, and Ford Motor Company; media outlets such as the Washington Post and ABC news; international organizations such as the International Monetary Fund, the British Parliament, and Belgium's banking system; state governments; school systems; and credit unions, among many others, forcing them to take their networks off-line for hours.

The virus/worm also reportedly penetrated at least 14 federal agencies—including the Department of Defense (DOD), the Social Security Administration, the Central Intelligence Agency, the Immigration and Naturalization Service, the Department of Energy, the Department of Agriculture, the Department of Education, the National Aeronautics and Space Administration (NASA), along with the House and Senate. We still do not know the full effect of this virus on the agencies that were penetrated. While many were forced to shut down their e-mail networks for some time, many also reported that mission-critical systems and operations were not affected. Of course, if an agency's business depends on e-mail for decision-making and service delivery, then the virus/worm probably had a significant impact on day-to-day operations in terms of lost productivity.

After this incident, GAO highlighted six areas of management and general control problems in computer security:

- Poor security planning and management is the rule rather than the exception. Most agencies do not develop security plans for major systems based on risk, have not formally documented security policies, and have not implemented programs for testing and evaluating the effectiveness of controls they rely on. These are fundamental activities that allow an organisation to manage its information security risks cost-effectively rather than by reacting to individual problems *Ad hoc*.
- Agencies often lack effective access controls to their computer resources (data, equipment, and facilities) and, as a result, are unable to protect these assets against unauthorised modification, loss, and disclosure. These controls would normally include physical protections such as gates and guards and logical controls, which are controls built into software that (1) require users to authenticate themselves through passwords or other identifiers and (2) limit the files and other resources that an authenticated user can access and the actions that he or she can take.
- Application software development and change controls are weak. For example, testing procedures are undisciplined and do not ensure that implemented software operates as intended, and access to software program libraries is inadequately controlled.
- Agencies lack effective policies and procedures governing the segregation of duties. It is commonly found that computer programmers and operators are authorised to perform a wide variety of duties, such as independently writing, testing, and approving program changes. This, in turn, provides them with the ability to modify, circumvent, and disable system security features.

- Reviews frequently identify systems with insufficiently restricted access to the powerful programs and sensitive files associated with the computer system's operation, *e.g.*, operating systems, system utilities, security software, and database management system. Such free access makes it possible for knowledgeable individuals to disable or circumvent controls.
- Service continuity controls are incomplete and often not fully tested to ensure that critical operations can continue when unexpected events (such as a temporary power failure, accidental loss of files, major disaster such as a fire, or malicious disruptions) occur.

This incident is a typical example of the emerging cross-cutting issue of international cyber security. It is not related directly to the formulation, development, and management of a single IT project, but requires the focus of IT management at all levels to address the potential vulnerabilities across the entire world-wide electronic infrastructure. In that sense, it is very similar to the Y2K issue, and will have a large impact on the formulation and management of large IT projects during the next several years, as well as the retrofitting of the existing IT infrastructure. The lesson here is that we now must provide more focus on cyber security risk, vulnerabilities, and architecture in the design of IT projects. If we don't change, we can predict more spectacular failures due to these vulnerabilities in the future. Old IT project designs have new flaws.

3. LESSONS LEARNED

To sum up, the following factors can be listed as contributing to the success and failure of government IT projects:

- IT projects must support business objectives, they are not an end in themselves.
- Modular IT project design, with opportunities to adjust to changes in circumstance, technology, and requirements, have a much higher probability of success than "grand designs".
- When using contractors to develop and implement IT projects, it is critical to recognize incentives for the contractor (not just adhering to contract specifications) to create a healthy business relationship.
- IT projects are increasingly dependent on a global electronic infrastructure (networks, diverse databases, etc.) and their design must recognize both vulnerabilities and opportunities as a result.

4. REFERENCES

Websites containing IT project management direction, policy and related documents:

Office of Management and Budget – www.whitehouse.gov/OMB/index.html

General Accounting Office – www.gao.gov

General Services Administration – www.gsa.gov

Chief Information Officers Council home page – www.cio.gov

General Services Administration listing of IT policy document – www.policyworks.gov/policydocs/policy_list.htm