1-2006

# Review of State-wide Planning and Management of Information Technology — State is at Risk from Fragmented Practices; Enterprise Transformation Underway and Needs Steadfast Support, 2006

Maine State Legislature

Office of Program Evaluation and Government Accountability

Beth Ashcroft
*Maine State Legislature*, beth.ashcroft@legislature.maine.gov

OPEGA
REVIEW

FINAL
REPORT

# Review of State-wide Planning and Management of Information Technology — State is at Risk from Fragmented Practices; Enterprise Transformation Underway and Needs Steadfast Support

Report No. CR-IS-05

a report to the
Government Oversight Committee
from the
Office of Program Evaluation & Government Accountability
of the Maine State Legislature

January
2006

## GOVERNMENT OVERSIGHT COMMITTEE

Sen. Elizabeth H. Mitchell, Chair
Sen. Kevin L. Raye
Sen. Philip L. Bartlett II
Sen. Jonathan T. E. Courtney
Sen. Joseph C. Perry
Sen. Dana L. Dow

Rep. Edward R. DuGay, Chair
Rep. A. David Trahan
Rep. Marilyn E. Canavan
Rep. Ronald F. Collins
Rep. Lillian LaFontaine O'Brien
Rep. Robert H. Crosthwaite

## OFFICE OF PROGRAM EVALUATION & GOVERNMENT ACCOUNTABILITY

Director Beth Ashcroft, CIA

Mailing Address:
82 State House Station
Augusta, ME 04333-0082
Phone: (207) 287-1901
Fax: (207) 287-1906
Web: http://www.maine.gov/legis/opega/
Email: beth.ashcroft@legislature.maine.gov

## ABOUT OPEGA & THE GOVERNMENT OVERSIGHT COMMITTEE

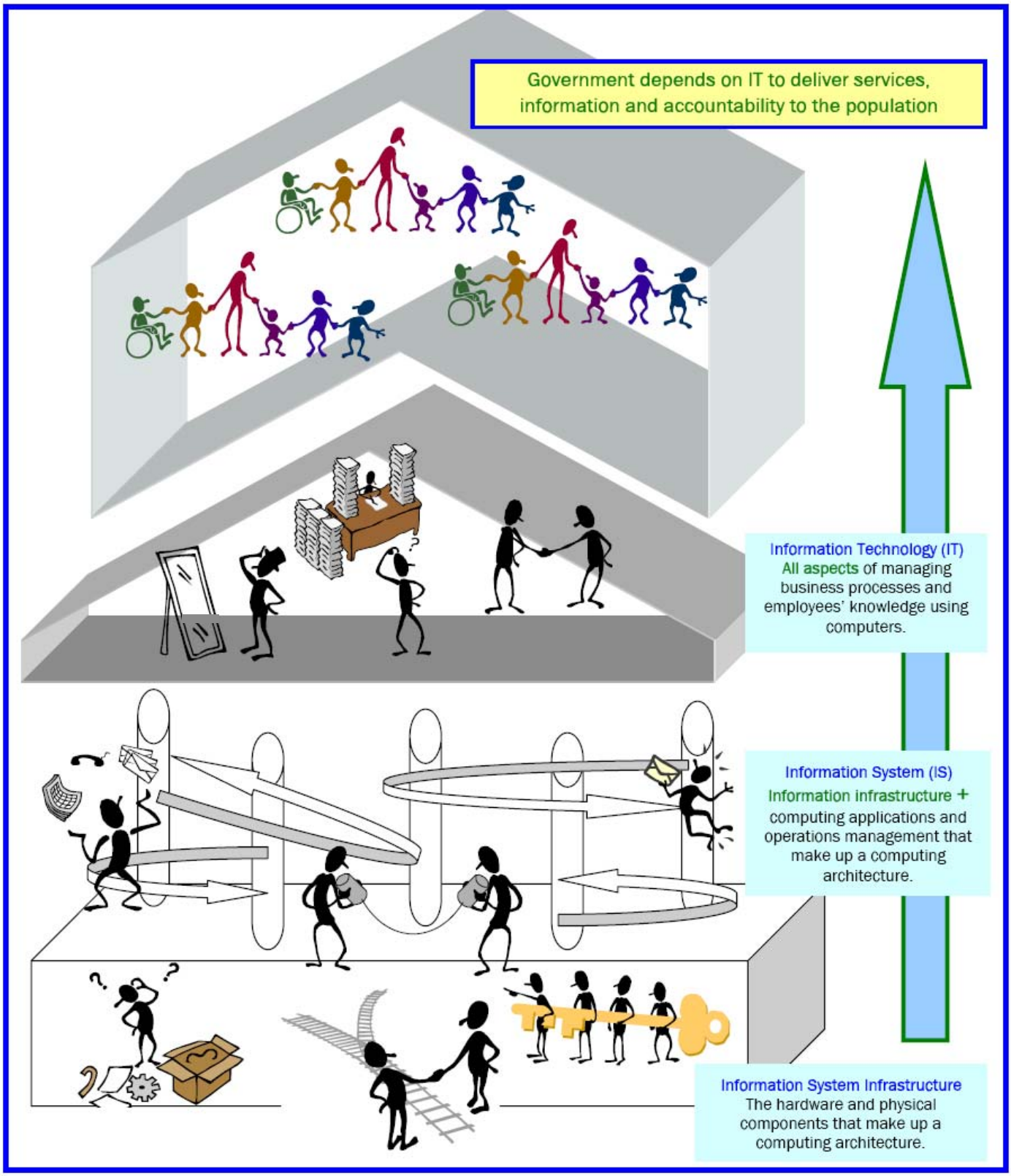
The Office of Program Evaluation and Government Accountability (OPEGA) was created in 2003 to assist the Legislature in its oversight role by providing independent reviews of the agencies and programs of State Government. Oversight is an essential function because legislators need to know if current laws and appropriations are achieving intended results.

Although the Maine Legislature has always conducted budget reviews and legislative studies, until OPEGA, the Legislature had no independent staff unit with sufficient resources and authority to evaluate the efficiency and effectiveness of Maine government. The joint legislative Government Oversight Committee (GOC) was established as a bipartisan committee to oversee OPEGA's activities.

OPEGA's reviews are performed at the direction of the Government Oversight Committee. Legislators, committees, or members of the public should make their requests for reviews to the Chairpersons or any other member of the Committee.

Copies of OPEGA's reports are free.
Reports are available in electronic format at:
http://www.maine.gov/legis/opega/

Hard copies of reports may be obtained by contacting OPEGA at:
(207) 287-1901
Office of Program Evaluation & Government Accountability
82 State House Station • Augusta, ME • 04333-0082




Helpful definitions of terminology used in this report. See reverse for more.

# Terminology Used in this Report

**Asset Management**
The practice of collecting and maintaining a comprehensive list of items an organization owns, such as hardware and software.

**Change Management**
The practice of steering an organization in a new strategic direction and keeping all involved people and projects aligned with the new goals as the organization, jobs, technology and processes are uprooted.

**Data Warehouse**
A database that stores large amounts of historical data.

**Distributed Computing**
Using a number of remote computers to collaboratively process information or work on problems.

**E-Government**
Any government functions or processes that are carried out in digital form over the Internet. Local, state and federal governments essentially set up central Web sites from which the public (both private citizens and businesses) can find public information, download government forms and contact government representatives.

**Enterprise Approach (EA)**
Planning, managing and operating Information Technology (IT) such that investment, business and Information System (IS) management practices integrate organization-wide deliverables of IT elements throughout their lifecycles.

**Enterprise Architecture**
An organizational blueprint that defines -- in business terms and in technology terms -- how an organization operates today, intends to operate in the future, and intends to invest in technology to transition to this future state.

**Information Age**
The period where movement of information became faster than physical movement, more narrowly applying to the 1980s or 1990s onward. It is often used in conjunction with the term post-industrial society.

**Information System (IS)**
The physical infrastructure + computing applications and operations management that make up a computing architecture.

**Information Technology (IT)**
All aspects of managing business processes and employees' knowledge using computers.

**Information System Infrastructure**
The hardware and physical components that make up a computing architecture.

**Integration**
The process of combining separately produced components of a product and altering them so that they can interact.

**Knowledge Age**
The period where more than 50% of the GDP of developed nations is knowledge based.

**Knowledge Management (KM)**
The practice of researching, collecting and organizing an enterprise's employees' knowledge.

**Server**
Either a program that provides services (such as routing or file access) to other programs in the same or other computers, or the computer itself that is used to provide those services to other computers in the network.

**System Development Life Cycle (SDLC)**
The process of developing information systems through investigation, analysis, design, implementation and maintenance. SDLC is also known as *information systems development* or *application development*. SDLC is a systems approach to problem solving and is made up of several phases, each comprised of multiple steps:

- The software concept - identifies and defines a need for the new system
- A requirements analysis - analyzes the information needs of the end users
- The architectural design - creates a blueprint for the design with the necessary specifications for the hardware, software, people and data resources
- Coding and debugging - creates and programs the final system
- System testing - evaluates the system's actual functionality in relation to expected or intended functionality

**World Wide Web (www)**
The graphical interface with which millions of users access Internet files that conform to the hypertext protocol (HTTP). The Web is the most accessible and widely used branch of the Internet.

**Worm**
A program that can replicate and send itself between computer systems. A worm can cause damage by itself or act as a delivery agent for a virus.

# Table of Contents

*EXECUTIVE SUMMARY*

# Review of State-wide Planning and Management of Information Technology — State is at Risk from Fragmented Practices; Enterprise Transformation Underway and Needs Steadfast Support

## Purpose

The Maine State Legislature's Office of Program Evaluation and Government Accountability (OPEGA) has completed a review of State-wide Planning and Management of Information Technology at the direction of the joint legislative Government Oversight Committee.

Despite huge IT expenditures, State remains constrained by information gaps and uncoordinated use of information technology. New system implementation projects have been troubled.

The Executive Branch of the State of Maine plans to spend $118 million dollars on information technology (IT) in state fiscal year 2006, and has spent more than $500 million[1] state-wide since the year 2000. Despite this huge expenditure, efforts across the State to improve services, reduce costs and deliver information for accountability remain constrained by information gaps and uncoordinated use of information technology.

Further, Maine has been experiencing continuing information system (IS) management difficulties. New system implementation projects have frequently been over the established budget, behind schedule and/or result in systems that have serious weaknesses upon implementation.

In July 2005, a new approach to planning and managing IT across the Executive branch began to take shape. The consolidation of Executive branch IT functions into the Office of Information Technology (OIT) under the direction of the State's Chief Information Officer (CIO) is meant to transform planning and management of IT from fragmented, agency-specific operations to integrated enterprise operations.

OPEGA evaluated whether IT is being planned for and managed in a way that maximizes effectiveness and efficiency of State government and keeps risk exposure at an acceptable level.

The purpose of this review was to determine whether IT across the State is being planned for and managed in a way that:

- maximizes the effectiveness and efficiency of State government; and
- keeps exposure from associated risks at an acceptable level.

This review primarily focused on providing an in-depth assessment of IT planning and management functions in the Executive branch, which is where most of the State's IT risk lies.

1 Information technology expenditures that could be identified and captured through the State's financial information system, Maine Financial & Administrative Statewide Information System (MFASIS).

# Conclusions

OPEGA has formed the following conclusions as a result of its work:

State's historical approach to planning and managing IT has not been adequate for some time now; State is currently exposed to an unacceptable level of IT-related risk.

A. For some time now, the State's historical approach to the planning and management of information technology (IT) has not been adequate to maximize the effectiveness and efficiency of State government nor to keep risk at an acceptable level. The State has shown a tendency to lag behind the rest of the country in adopting innovative information system practices or technology in many areas. Instead, an IT culture of operational expediency has been created. Planning, risk management, and sound policies and procedures have been put on the back burner in this culture. As a result, the State is currently exposed to an unacceptable level of IT-related risk.

OIT consolidation poised to significantly improve situation through enterprise approach; strategic plan should include additional elements; "enterprise" does not include all branches of government.

B. The organizational transformation that began in July 2005 with the establishment of the Office of Information Technology is poised to significantly improve the planning and management of information technology as it takes an enterprise approach across the State's Executive branch. OPEGA did note, however, there are some additional elements that need to be incorporated into the CIO's strategic plan and the enterprise within the CIO's jurisdiction does not include the Judicial or Legislative branches.

Success of transformation efforts depends on CIO's capabilities and support from Executive and Legislative branches. Related risks need to be monitored and managed by leaders in both branches; Legislature currently has no real mechanism for doing so.

C. The success of transformation efforts is heavily dependent on the capabilities of the CIO and support from both the Executive and Legislative branches. There are risks related to the transformation itself that need to be monitored and well managed by leaders in both branches. OPEGA noted that currently there is no mechanism through which the Legislature can focus on support and oversight of the long-term, enterprise-wide strategic plan and the transformation required to accomplish it.

Management actions and other OPEGA recommendations related to findings and observations from this review are summarized next. For more detail, see the Full Report.

# Summary Table of Findings, Observations, Management Actions, and OPEGA Recommendations ----------

**Finding** - a situation where actual or potential deficiencies in internal control elements may expose the State to significant potential risks.

**Observation** - a situation where opportunities for improving effectiveness or efficiency exist.

| Findings and Observations | Management Actions and OPEGA Recommendations |
|---|---|
| **Enterprise Architecture Management** | |
| **Finding 1. Enterprise Architecture**<br>OIT has not yet developed a picture or map that describes the "as is" and "to be" environments of the enterprise, as well as specific steps for accomplishing the transition. | **Management Actions**<br>The CIO will assign responsibility for creating descriptions of the "as-is" and "to-be" environments to the new Policy and Strategic Planning Unit.<br>The CIO plans to provide regular updates on enterprise architecture progress to the Executive Steering Committee, CIO Council, Commissioner of DAFS and the Governor. |
| **Finding 2. Policies and Procedures**<br>Written policies and procedures are either non-existent, inadequate or inconsistent across the Executive branch in a number of IT areas. | **Management Actions**<br>The CIO has assigned responsibility for developing standardized policies and procedures to specific individuals, who are currently in the process of determining a reasonable timeframe for completion. OIT will work to see that the policies and procedures are communicated and implemented across the enterprise. |
| **Observation 1. State Government as the Greater Enterprise**<br>The current move to an enterprise approach is focused on the Executive branch and does not include the Judicial or Legislative branches. | **OPEGA Recommendations**<br>The State's Constitutional Officers and representatives from the Judicial and Legislative branches are currently invited to participate on the CIO Council. At a minimum, all of these individuals should be encouraged to actively participate.<br>As OIT matures, Judicial and Legislative branches should explore opportunities to contract with OIT for services (which they may outsource) as an alternative to directly contracting with entities outside of State government.<br>Legislation could be enacted to establish a specific group tasked with developing and managing an enterprise architecture and investment management strategy for all three branches of State government. |

| Findings and Observations | Management Actions and OPEGA Recommendations |
|---|---|
| **Investment Management** | |
| **Finding 3. Finance and Accounting**<br>Current accounting structures and financial practices do not easily allow the Administration or the Legislature a clear view of IT budgets and expenditures across the State as a whole, or by any specific agency, program or statute. | **Management Actions**<br>By July 2006, the CIO will pursue a study to determine the advisability of OPEGA's recommendation to establish IT as a specific "program" within the Executive branch for budgeting, appropriation, expenditure and oversight purposes.<br>The CIO and OIT's Performance Management and Administration Office are currently developing a rate structure and billing process for OIT services to agencies that reflects actual costs of providing specific types of services.<br>**OPEGA Recommendations**<br>Establish IT as a specific "program" within the Executive branch for budgeting, appropriation, expenditure and oversight purposes.<br>For the same purposes as the Executive branch, OPEGA also recommends that the Judicial and Legislative branches explore the possibility of establishing Information Technology as a specific "program" within their respective branches. |
| **Finding 4. Investment Decision-making**<br>Decisions on IT investments to date have not been made from an enterprise perspective or by a centralized State entity. Consequently, there are few mechanisms in place to assure that such investments are the best use of the State's resources or are being made in a way that will lead to increasing effectiveness and efficiency. | **Management Actions**<br>In April 2006, OIT's Policy and Strategic Planning Office will begin developing an enterprise architecture. Once completed, that architecture will be used to guide investments in information systems and allow the enterprise to leverage its resources.<br>Proposed or requested capital investments in IT will be reviewed and approved by OIT as it strives to move the Executive branch from the "as is" to the "to be" environment within the enterprise architecture. OIT has formed a Project Review Committee to evaluate major projects prior to their inception for project risk, strategic alignment and sound business investment criteria. This committee is currently testing its evaluation plan on several project proposals in order to refine the process and develop a formal procedure. |

| Findings and Observations | Management Actions and OPEGA Recommendations |
|---|---|
| **Risk Management** | |
| **Finding 5. Risk Assessment and Audit**<br>Regarding overall exposure to risks assessed by Jefferson Wells International (JWI), Maine's IT exposure level is unacceptably high and requires dedication to reduction and control. JWI summarized the risk-status of Maine's IT environment as followings:<br>• one percent is highly controlled;<br>• eleven percent had a satisfactory (medium) level of control; and<br>• the remaining 88% had an undesirable (low) level of control.<br><br>Specific exposure identified are addressed within the other findings. | **Management Actions**<br>OIT will construct a risk management plan that builds on the JWI assessment, works to mitigate or eliminate priority risks, and measures the effectiveness of the risk management process;<br>OIT plans to develop an on-going internal audit process to measure the effectiveness of established risk management procedures and controls; and<br>OIT will continue to cooperate with OPEGA on its reviews and IT audits to improve its processes and performance.<br>**OPEGA Recommendations**<br>The legislative Government Oversight Committee may direct OPEGA to establish a schedule of independent IT reviews to be included in future OPEGA Annual Work Plans and support OPEGA in obtaining funding to hire IT audit consultants that would likely be needed to accomplish these reviews. |
| **Project Management** | |
| **Finding 6. Enterprise-wide Project Management**<br>The need for strong project managers has often not been recognized as a factor critical to the success of major IT projects. Consequently, there has been little concerted effort to build project management skill sets within agencies or to assure that individuals assigned as project managers have the appropriate knowledge, skills and abilities. | **Management Actions**<br>The new OIT Project Management Office (PMO) will educate staff in best practice project management methods. Agency and PMO staff managing significant IT projects must now successfully complete training (that OIT will provide quarterly) on the adopted Ten-Step protocol. The PMO will begin providing Project Sponsor training sessions, which are a component of the Ten-Step protocol training, in March 2006.<br>OIT is developing enterprise-wide policies and procedures (to be communicated by April 2006) requiring agencies to engage OIT's PMO **prior to formulating a solution** to their system needs or problems.<br>Effective January 2006, OIT has responsibility for contracting with IT vendors for system development projects, and managing the resulting contracts. |
| **Finding 7. System Development Life Cycle (SDLC) Methodology**<br>The State of Maine lacks an effective System Development Life Cycle (SDLC) methodology, putting IT capital projects at significant risk of failure. | **Management Actions**<br>OIT's Policy and Strategic Planning Office will be assigned responsibility for selecting and adopting a SDLC methodology. This will be accomplished during 2007. |

| Findings and Observations | Management Actions and OPEGA Recommendations |
|---|---|
| **Security and Business Continuity** | |
| **Finding 8. Physical Security**<br>The risk assessment performed by JWI identified a number of weaknesses in physical access security controls, particularly in regard to the State's primary data center. | **Management Actions**<br>JWI and OPEGA have shared the details of the identified weaknesses with the CIO. Based on these details, the OIT Security Officer has developed an action plan to address the physical access weaknesses in order of priority as determined by the degree of risk associated with each. This action plan was submitted to OPEGA on January 9, 2006. A number of high priority actions to strengthen physical access security controls have since been taken by OIT. |
| **Finding 9. System Security**<br>The results of the JWI risk assessment suggest that system access controls do not measure up to industry standards. | **Management Actions**<br>OIT is taking, or plans to take, a number of steps to improve system access controls (see details in full report).<br>The OIT Security Officer plans to conduct an independent audit of the firewall rule set. |
| **Finding 10. Business Continuity Planning**<br>Business Continuity Planning (BCP) is inadequate across the Executive branch IT environment. In the event of a natural or man-made disaster, there is not an effective plan in place to guide the recovery of the Executive branch IT systems and services. | **Management Actions**<br>To improve business continuity planning, OIT will: consolidate and standardize data centers to make the technology portion of continuity planning easier and less expensive; assess current Continuity of Operations Plans (COOP) of the individual agencies in the context of the new enterprise approach; conduct a gap analysis to identify and prioritize shortfalls; and recommend actions to remedy inadequacies.<br>**OPEGA Recommendations**<br>Each agency, in all three branches of State government, should also develop their own Business Continuity Plans detailing how operations will be continued if critical information systems and/or the agency's current physical location(s) are unavailable for an extended period of time. |

| Findings and Observations | Management Actions and OPEGA Recommendations |
|---|---|
| **Knowledge Management** | |
| **Observation 2. Performance Management**<br>Inadequate attention has been given to designing information systems that create accountability and are themselves accountable. This is a major root cause of the State's failure to employ performance budgeting practices. | **Management Actions**<br>The CIO will investigate and make recommendations for assimilation of knowledge management practices into the enterprise to improve performance monitoring and increase accountability. This effort will include consideration of the following OPEGA recommendations:<br>• Design new or upgraded systems to collect data and produce information that measures performance of programs, functions or activities. These features should link performance measures to resource allocations. Both management and legislative needs require consideration in this process.<br>• Establish and monitor IS performance metrics with automated tools across the enterprise. OIT should include a function that is responsible for this type of activity.<br>**OPEGA Recommendations**<br>Legislative bodies responsible for oversight of information system implementations should take an interest in whether, and how, the system is being designed to provide accountability, and evaluate impact of enacted legislation. |
| **Observation 3. Enterprise Data Management**<br>The ability to combine data from different systems across the enterprise is very limited. This limitation is due both to differences in the way data is captured and coded in various databases (data compatibility) as well as a lack of electronic capabilities to easily bring the data together for analysis (systems interoperability). Therefore:<br>• it is difficult to convert data into information that can answer questions and inform decisions about particular geographic, demographic, economic or consumer groups; and<br>• the same data is captured in multiple systems, all with different field names, data formats and codes. Such duplication of information across the enterprise makes it difficult to determine which pieces of data are most current or valid. | **Management Actions**<br>OIT is addressing the need for data consolidation, integration and exchange as an important long-term strategic objective.<br>• As part of its enterprise architecture, OIT will develop data standards to begin codifying common data elements, their formats, meanings and sources across multiple information systems.<br>• As opportunities arise, new systems will be evaluated to see if common data elements can be shared or architected as a common resource rather than duplicate data.<br>• OIT is investigating tools to assist in exchanging data between existing "legacy" applications. The goal is to provide documented standard linkages between systems that can be maintained as the cooperating applications change over time. |

| Findings and Observations | Management Actions and OPEGA Recommendations |
|---|---|
| **Knowledge Management (continued)** | |
| **Observation 4. Best Practices and Emergent Technology.**<br>Professional development opportunities have been limited by resource constraints resulting in IT professional staff who may not be receiving enough exposure to emerging or proven concepts, approaches or innovations in information technology and best practices -- exposure critical to helping Maine stay current. | **Management Actions**<br>The Policy and Strategic Planning Office will facilitate a professional development program looking for "to-be" opportunities for the enterprise architecture. The program will ensure that technical staff remains current within their skill sets, and that new and emerging technical trends are appropriately assimilated to support the business. |
| **Observation 5. Staff Knowledge as a Capital Asset.**<br>The IT staff in the Executive branch, particularly at the management level, has many years of knowledge and experience working in the State's IT environment. As they approach retirement, or leave the State for other reasons, the wealth of accumulated knowledge these individuals possess may be lost. | **Management Actions**<br>Knowledge transfer and staff succession planning for senior management was a consideration during the hiring of the initial enterprise management team for OIT. This focus will be extended throughout all disciplines within the enterprise.<br>At the PMO, specific training in knowledge transfer and succession planning is underway starting with the Director. A career ladder is being established for those working directly in the office and tangentially in the agencies. OIT will build upon activities such as Maine Fusion Conferences to develop an ongoing series of professional seminars in IT and management. |
| **Observation 6. Knowledge Management Techniques**<br>The State's IT is not yet being well utilized to help bring together cross-organizational groups, "communities of practice" within or outside of the State, that need to share knowledge around particular topics.<br>Maine is not actively and explicitly using technology to foster better ways of sharing and transferring staff knowledge to improve governmental functioning. | **Management Actions**<br>OIT will make the following efforts to increase the use of technology for information sharing:<br>• investigate the feasibility of appointing a Chief Knowledge Officer to coordinate and manage the State's knowledge-based assets;<br>• advocate that Data Stewards and Product Managers be designated by the business units to provide on-going support, training and product planning for important knowledge assets; and<br>• continue to foster the introduction and use of technology to facilitate knowledge sharing whenever opportunities arise. |

| Findings and Observations | Management Actions and OPEGA Recommendations |
|---|---|
| **Leadership and Oversight** | |
| **Observation 7. Leadership and Succession Planning**<br><br>The reality of the political process is that changes in IT leadership may occur with every new administration. The potential for frequent short-term leadership changes will always present risk in an area like IT that requires more long-term strategic planning. The current CIO may change with administration beginning in January 2007. A potential change in leadership at that particular time does present an elevated level of risk because OIT will only be 1 ½ years into its enterprise transformation. | **Management Actions**<br><br>The CIO has initiated a two pronged approach to mitigate the risk of a change in leadership.<br>• prong one - strengthen the OIT management team, to create leaders who can maintain the current transformation effort if the CIO changes.<br>• Prong two - create a new Strategic Plan which will be widely supported by agency leadership and will provide on-going direction for the efforts of the enterprise technology governance team.<br>In addition, two groups, the Executive Steering Committee (government business) and CIO Council (government technology and management), have been established to work with the CIO in an advisory capacity. These groups should help bring continuity to the transformation effort over time.<br>**OPEGA Recommendations**<br><br>In addition to the CIO's efforts, OPEGA recommends that the Legislature further mitigate this risk through:<br>• actively providing legislative support and oversight from the responsible JS Committees of jurisdiction;<br>• continuing independent OPEGA reviews of IT; and<br>• enacting legislation that requires individuals appointed to the position of Chief Information Officer to have appropriate knowledge, skills and abilities in IT and IT organizational leadership. |
| **Observation 8. Legislative Oversight**<br><br>Legislative oversight activities devoted exclusively to the State's IT are absent. All JS Committees perform some oversight of information systems as they relate to the agencies and/or programs within their jurisdictions. However, there is not one legislative body assigned responsibility for overseeing the planning and management of the IT enterprise. | **OPEGA Recommendations**<br><br>Support any actions taken by the Administration to establish IT as a specific "program" for budgeting, appropriation, expenditure and oversight purposes. As previously discussed in Finding 3, the CIO is exploring the feasibility of taking this approach to finance and accounting for IT.<br><br>Assign responsibility for oversight of this "program" to either the Joint Standing Committee on:<br>• Utilities and Energy – a Committee familiar with the concepts, approaches and risks involved in planning and managing enterprise-wide infrastructure (e.g. Telecommunications and Electricity); or<br>• State and Local Government – a Committee familiar with the State's processes for managing investments in other large capital asset areas. |

*This page intentionally left blank.*

*FULL REPORT*

# Review of State-wide Planning and Management of Information Technology — State is at Risk from Fragmented Practices; Enterprise Transformation Underway and Needs Steadfast Support

## Purpose

More than fifteen years ago, government professionals recognized that:

> "In short, to govern our nation effectively, we must manage our technology effectively."
>
> (GAO 1988)

The Maine State Legislature's Office of Program Evaluation and Government Accountability (OPEGA) has completed a review of State-wide Planning and Management of Information Technology at the direction of the joint legislative Government Oversight Committee. OPEGA conducted the review in accordance with M.R.S.A. Title 3, Chapter 37, §991-997 and the Government Auditing Standards set forth by the United States Government Accountability Office (GAO).

Despite huge IT expenditures, State remains constrained by information gaps and uncoordinated use of information technology.

The Executive Branch of the State of Maine plans to spend $118 million dollars on information technology (IT) in state fiscal year 2006, and has spent more than $500 million[2] state-wide since the year 2000. Despite this huge expenditure, efforts across the State to improve services, reduce costs and deliver information for accountability remain constrained by information gaps and uncoordinated use of information technology.

New system implementation projects have been experiencing budget, schedule and implementation troubles.

Further, Maine has been experiencing continuing information system (IS) management difficulties. New system implementation projects have frequently been over the established budget, behind schedule and/or resulted in systems that have serious weaknesses upon implementation. This is partly due to the fact that approved budgets for projects are often lower than what agencies originally request for funding. The two most recent examples of troubled implementations are the new Medicaid billing system (MECMS), and the Bureau of Motor Vehicles' computer migration, both of which have had widespread public impact. Answers to the question "How could this happen?" are complex and likely rooted in the evolution of the State's IT governance and organization.

2 Information technology expenditures that could be identified and captured through the State's financial information system, Maine Financial & Administrative Statewide Information System (MFASIS).

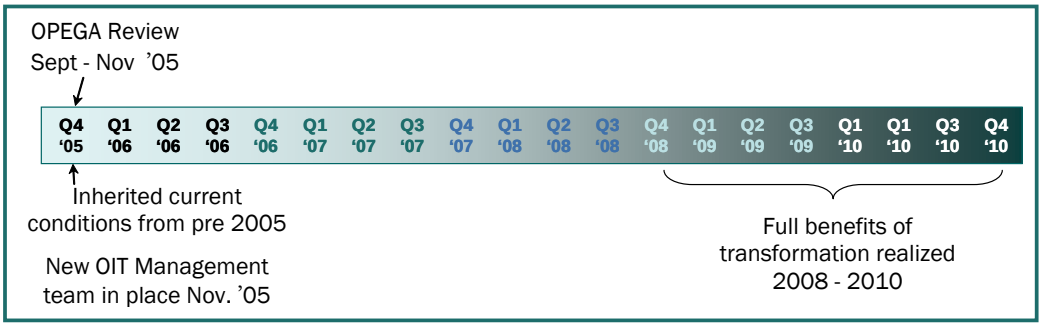
Recent consolidation of Executive branch IT functions into Office of Information Technology is meant to transform State's approach to IT planning and management.

In July 2005, a new approach to planning and managing IT across the Executive branch began to take shape. The consolidation of Executive branch IT functions into the Office of Information Technology (OIT) under the direction of the State's Chief Information Officer (CIO) is meant to transform planning and management of IT from fragmented, agency-specific operations to integrated enterprise operations. The enterprise approach considers the State's IT as a whole, applying standards and practices that create efficiencies, guide major capital investments, leverage IS compatibility, and reduce risk. It is likely to take 3-5 years before benefits of the transformation are fully realized.

**Enterprise Approach**

Planning, managing and operating Information Technology (IT) such that investment, business and Information System (IS) management practices integrate organization-wide deliverables of IT elements throughout their lifecycles.

**Figure 1. Timeline for Realizing Full Benefits of Transformation to Enterprise**




OPEGA's review was performed during initial phases of OIT consolidation.

As depicted in Figure 1, OPEGA's review was performed from September through November 2005 and thus occurred during the initial phases of the OIT consolidation. A significant amount of reorganization, including the appointment of new IT leadership, was occurring at this time. Consequently, this review contains a final assessment of performance under the outgoing organizational structure. It should provide benchmarks to measure any improvements stemming from the new organizational structure and enterprise approach going forward.

OPEGA evaluated whether IT planning and management maximizes effectiveness and efficiency of State government and keeps risk exposure at acceptable level.

The purpose of this review was to determine whether IT across the State is being planned for and managed in a way that:

- maximizes the effectiveness and efficiency of State government; and
- keeps exposure from associated risks at an acceptable level.

This review primarily focused on providing an in-depth assessment of IT planning and management functions in the Executive branch, which is where most of the State's IT risk lies. Related activities or major information systems in the Legislative and Judicial branches were given only limited consideration in certain parts of this review. Therefore, in the context of this report, the term "State-wide" or "State" is most often used to refer to the Executive branch.

# Methods

OPEGA combined high-level "Best Practices" evaluation with IT risk assessment to identify State-specific risks and their root causes.

In reviewing Maine's IT management and planning, OPEGA combined a high-level "Best Practices" evaluation with an IT risk assessment in an effort to identify State-specific risks and their root causes. To accomplish this OPEGA researched:

- the role of IT in government;
- best practice models for planning and managing IT in government;
- Maine State history related to IT; and
- Maine government's current IT organizational structure and plans.

OPEGA then compared current IT organizational structure and plans to best practice models for planning and managing IT in government. OPEGA used best practice models that were consistently identified by: the federal Government Accountability Office (GAO) and Office of Management and Budget (OMB), the National Association of State Chief Information Officers (NASCIO), and the Customer Management Community (CRM)-Forum.

OPEGA partnered with contracted team of specialized IT auditors to perform the IT risk assessment.

OPEGA performed a comprehensive risk assessment by partnering with a contracted team of specialized IT auditors from Jefferson Wells International (JWI). The goals of the risk assessment were as follows.

1. Identify areas where IT risk exposures are at an unacceptable level.
2. Determine root causes for unacceptable risk levels.
3. Identify specific control practices intended to successfully mitigate high risk exposure.
4. Assess whether adequate plans are in place to address these exposures going forward.

Risk assessment methodology was based on industry standard model for IT auditing known as COBIT.

The JWI team conducted the risk assessment using a matrix based on the industry standard model for IT auditing known as "Control Objectives for Information and Related Technologies" (COBIT). The risk assessment matrix is a detailed compilation of standard IT risks and related controls in the following areas (bulleted items are provided as examples of topics reviewed):

**General Administrative Controls:**

- IT organization
- IT management controls
- job descriptions (roles) and segregation of duties
- hardware and software inventory controls
- physical security and environmental controls

**Business Continuity Planning Controls:**

- business impact analysis and management awareness
- alignment of IT and business recovery requirements and capabilities
- recovery time objectives
- independent observation and analysis of disaster recovery tests

**Systems Development Life Cycle (SDLC)/Change Management Controls:**

- project control reviews – both pre- and post-implementation
- compliance with SDLC methodology
- change management approval and testing processes

**End-User Computing Controls:**

- end-user acceptable use policies and procedures
- workstation and document security controls; asset tracking and physical security
- end-user security awareness programs

**Operations Management Controls:**

- system and device maintenance controls
- capacity planning and monitoring
- job scheduling and management reporting

**Information Security Controls:**

- comprehensive security policies, standards and procedures
- authentication and authorization techniques and controls
- accountability, monitoring and follow-up programs

**Operating System, Database, and Application Controls:**

- standardized build and configuration controls
- operating system, database, and application hardening controls
- encryption controls
- system authentication and access controls

**Network Controls:**

- network security controls like firewalls, intrusion detection, log monitoring and alerting, and encryption
- remote access, modem, and wireless security controls
- network authentication and access controls

JWI performed a survey of Maine's IT environment to accomplish the risk assessment. The team evaluated whether sufficient controls were in place by:

- requesting and reviewing large volumes of written documentation (policies, procedures and planning documents);
- conducting interviews with 28 IT managers and technicians from across the State; and
- observing essential processes and conditions during on-site tours of major IT facilities.

OPEGA integrated results from risk assessment and best practice evaluation in developing its conclusions, findings and recommendations.

The risk assessment involved 31 different organizational units within Maine government. While most of these organizational units were within the Executive branch, agencies outside the Executive branch that had information systems with significant public impact, i.e. Secretary of State's Bureau of Motor Vehicles, were also asked to provide information.

OPEGA integrated the risk assessment results with the best practices evaluation to develop conclusions, findings and recommendations for this review. At OPEGA's request, JWI also prepared a recommended three year audit plan prioritized to provide more in-depth reviews of areas where the State's IT risk exposures are highest.

# Background

## *Role of Information Technology in Government*

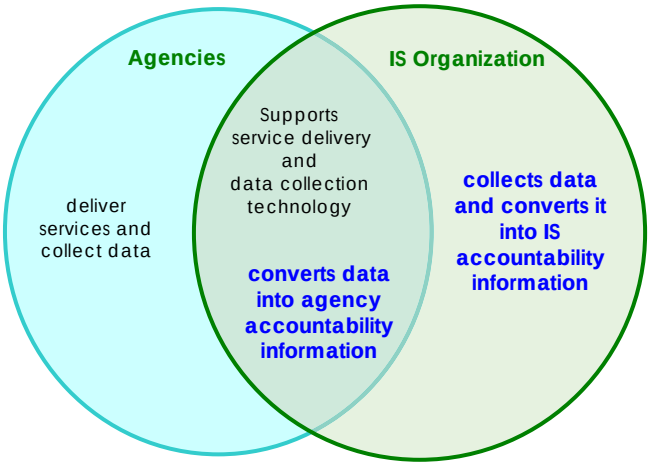
Government has become reliant on IT to provide services; share information; assure compliance; improve decision-making; and measure performance.

The evolution of technology for information management over the past 50 years has been nothing short of radical. As technology has advanced, the opportunities for utilizing electronically managed data and the information it produces have also rapidly expanded. The national economy has transformed from the "Industrial Age" to the "Information and Knowledge Age". As a result, government has joined other organizations in becoming reliant on information technology to:

- support operations and provide services;
- facilitate access to and sharing of information;
- assure compliance with organizational policies and regulations;
- improve decision-making; and
- measure performance.

Information and records generated in the course of government business are critical to accountability. They provide evidence that government is functioning effectively and efficiently. They indicate whether government business is managed and conducted in accordance with laws, statutes, regulations, and other requirements. Government records also document state history, and contain valuable information about citizens and the environments in which we live.

Figure 2. Dual Accountability Role of Information Systems




IT has become a function or "program" that needs to be held accountable to the public.

At the same time, information technology is no longer just a tool to provide accountability information about other activities. It has become a function or "program" in and of itself that needs to be held accountable to the public. IT operations and initiatives need to be monitored as they move through their lifecycles. Figure 2 depicts the dual aspects of IS accountability.

Whereas IT in government once meant using computers as tools to accomplish business (like cars) -- today it has evolved into the work of creating and maintaining information systems -- like the highway systems of roads, bridges and regulation. Information technology is the

IT provides critical infrastructure that must be carefully developed, maintained and managed.

critical infrastructure underlying information, communication, service and safety.

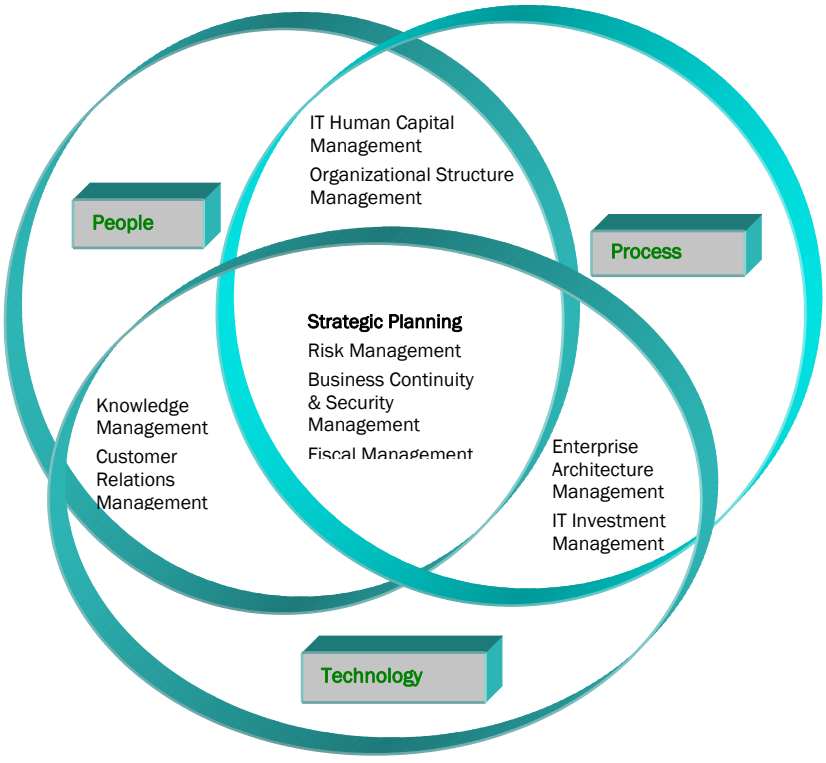
In economic terms, information technologies began as "private goods" – like lamps and heaters -- and government could financially manage them as such; but now they are more akin to "public goods" – like energy. By virtue of their key role in service delivery, knowledge management and accountability, information technology must be carefully developed, maintained and managed.

## *Best Practice Models for IT Planning and Management*

Effective planning and management of IT requires institutional practices that serve as high-level management controls in mitigating IT risks.

The planning and management functions for IT are complex and challenging in any environment, and especially so in government. Effective planning and management involves establishing and coordinating a number of institutional practices that bring together people, processes and technology to achieve goals. They are interdependent as illustrated in Figure 3.

**Figure 3. Relationship among Management Controls, People, Processes, and Technology**
**Modified from US GAO**




These institutional practices serve as high-level management controls designed to mitigate the many risks associated with information technology. Collectively, they provide an organization with a comprehensive understanding both of current business approaches and of

efforts (under way or planned) to change these approaches. Table 1 describes these current best practices and notes Maine's status with respect to them as it relates to IT.

Appendix A provides detailed descriptions of 4 best practice models (*) to lend context and understanding of terminology that may be unfamiliar: Enterprise Architecture Management, IT Investment Management, Knowledge Management, and Risk Management.

Table 1. Institutional Best Practices that Serve as High-Level Management Controls

| Institutional Practice | Definition | IT Current Status |
|---|---|---|
| * Enterprise Architecture Management | developing, maintaining, and using an explicit blueprint for operational and technological change | very early stages |
| * IT Investment Management | selecting and controlling IT spending so as to maximize return on investment and minimize risk | aware but not yet underway |
| * Knowledge Management | capturing, understanding, and using the collective body of information and intellect within an organization to accomplish its mission | unaware |
| * Risk Management | addressing potential events or situations that threaten the successful achievement of organizational objectives | very early stages |
| Strategic Planning | establishing the agency's mission and vision, including core values, goals, and approaches/strategies for achieving the goals | very early stages |
| Organizational Structure Management | aligning operational responsibilities with business and mission goals and objectives, and maintaining an accountability framework | largely underway |
| Business Continuity Planning And Security Management | ensuring the maintenance or recovery of operations, including services to customers, when confronted with adverse events such as natural disasters, technological failures, human error, or terrorism | very early stages |
| Human Capital Management | attracting, retaining, and motivating the people who possess the knowledge, skills, and abilities that enable an organization to accomplish its IT mission | largely underway |
| Fiscal Management | budget formulation and execution, financial control and acquisition that enables an organization to track its use of material resources | very early stages |
| Customer Relations Management | focusing an organization's operations on how to best satisfy customer needs | largely underway |

While many of these practices and controls are well understood and employed in private sector and federal government IT, they are at various stages of maturity as applied to IT in state governments. The National Association of State Chief Information Officers (NASCIO) is a professional organization that provides key knowledge management services to state CIOs from across the country. It is one group that is focused on bringing these institutional practices or controls into state governments.

## *Evolution of IT in Maine State Government*

IT has developed in environment dominated by rapid technology change; drastic changes in government policy and mandates.

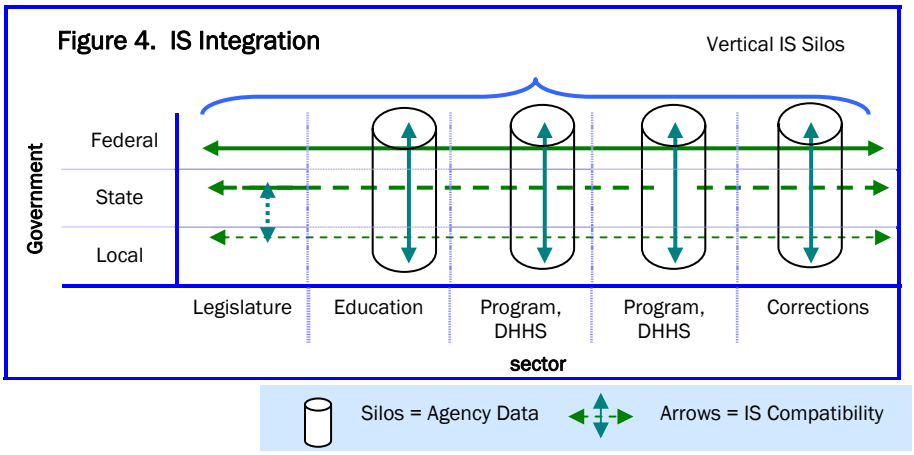
In state governments nation-wide, IS infrastructure and applications have developed in an environment dominated by rapid technology change and drastic changes in state and federal reporting, regulatory and compliance mandates. Appendix B highlights just some of the technological and policy shifts that have impacted IT development in state governments.

The effect of such a rapidly changing environment is seen in the specific challenges that Maine must overcome when developing and implementing large and complex information systems. These include:

- implementing long-term projects under short term administrations that often refocus program priorities;
- responding to state and federal policy changes that affect data, information and technology requirements;
- determining whether to incorporate new technologies that become available during new system implementations;
- addressing security concerns arising from rapid technology changes and the proliferation of telecommunications and personal computers; and
- managing additional exposure to compliance failures as emergent technologies trigger increases in regulatory demands.

Federal government has had fragmenting effect on state IT development through funding of programs.

The federal government has had a fragmenting effect on state IT development through funding. Most tax-payer dollars dedicated to information technology have come directly to state agencies from the federal government to support the administration of specific programs (e.g. Social Security, Medicaid, TANF, etc.).




In Maine, this arrangement promoted vertical integration of national and state service departments while inhibiting horizontal integration of state-level information systems. Consequently, the State's IT has developed in a fragmented, and mostly uncoordinated, manner. The fragmentation of IT is apparent between the three branches of

In Maine, impetus for vertical integration resulted in IT operations being "silo-ed" in each state agency. IT resource decisions have been mainly made at agency level; driven by available federal funding.

government as well as within the Executive branch. Figure 4 depicts an example of vertical and horizontal integration of information systems.

The impetus for vertical integration resulted in separate and distinct IT operations being established and "silo-ed" in each state agency. IT management practices have been focused at the agency level supporting the needs of particular agency components. For the most part, decisions about financial and human resources devoted to IT have also been made at the agency level and are often driven by the degree of federal funding available.

Maine state government has been experiencing the drawbacks of planning and managing IT through this fragmented structure in several ways. First, this approach has curtailed the capacity to perform core state-level governmental functions, for instance:

Fragmented approach to IT across State has curtailed capacity to perform core state-level governmental functions.

- tracking spending and investment on various demographic, economic or geographic segments in the State;
- understanding the actual costs and impact of enacted legislation;
- delivering cross-agency services in an integrated manner (e.g. the same child receiving services from Juvenile Justice, Corrections, Education and Health and Human Services) to reduce costs and improve client services;
- leveraging existing data systems to reduce duplication;
- sharing knowledge and expertise throughout government;
- capitalizing on economies of scale in providing IT security, business continuity, acquisition, maintenance, technical support, and other operations;
- strategically managing IS infrastructure capital assets as investments; and
- keeping the workforce up to date on technological and work process advances.

The Joint Select Committee on the Year 2000 Computer Problem, though not tasked with evaluating state-wide information systems problems, nevertheless observed:

> "Although the Committee was not directly charged with studying how technology is purchased and managed in State government, it became obvious to us during our study there were significant problems in those areas. The Committee has found that the process of planning and buying computers and computer systems within state government suffers from a serious lack of coordination, decentralization of decision making and, on occasion, from simple wastefulness. Some of those communication and coordination problems stem from the historically independent nature of the Executive, Legislative and Judicial branches of government. But even within these branches of government there are serious questions about inter-agency coordination as well as major questions about how state agencies plan for and acquire computer systems and how the Legislature oversees agency spending on technology that need to be addressed. These are critical issues which the Committee feels must be addressed not only in the short term, but in the long term as well."

**~ Maine's Joint Select Committee on the Year 2000 Computer Problem**

State has also experienced real financial consequences from uncontrolled IT expenditures on uncoordinated contracts; lack of investment in IS infrastructure.

Second, the State has experienced real financial consequences from this fragmented arrangement. Maine has attempted to manage IT costs by contracting for services, both in and out of house. Problems with this arrangement are noted in the Maine State Government Annual Reports dating back as far as the 1980s. In retrospect, the result of this fiscal policy has been uncontrolled expenditure on uncoordinated contracts outside of the enterprise, and a lack of synergistic investment in critical IS infrastructure.

Inefficiencies, duplication of efforts, and missed opportunities have come from lack of consolidation, coordination and communication.

Third, the lack of consolidation, coordination and poor inter-agency communication have resulted in inefficiencies, duplication of efforts and potential missed opportunities to save money in the purchasing of information technology. These concerns were noted by Maine's Joint Select Committee on the Year 2000 Computer Problem when the State was preparing its financial information systems for the transition to the Year 2000.

IT culture of "operational expediency" has evolved in Maine state government.

Lastly, the fragmentation, coupled with constant financial resource constraints in an environment of rapid change, has created an IT culture of "operational expediency" in Maine state government. It is not surprising that Maine (as well as many other states) became "caught up" in trying to "keep up" while falling behind all the while. The culture of operational expediency has led to:

- administrators operating without the financial and management information they need to truly improve mission performance;
- no effective strategic, enterprise-wide IT planning;
- lack of enterprise-level project management processes and organization;
- agency administrators constantly reacting to IT crises;
- expensive retrofitting of new systems due to inattention to proper planning and safeguards in the early stages of system design;
- weak checks and balances critical for effective acquisition and contract oversight; and
- employees struggling, under increasing workloads, to do their jobs while hampered by out-dated information systems or problematic new ones.

The culture of operational expediency is premised on:

> "If it does not help me deliver services better, faster, cheaper, **right now**, then I don't have time for it!"

It results in staff working as technical craftsmen & artisans, versus planners and managers.

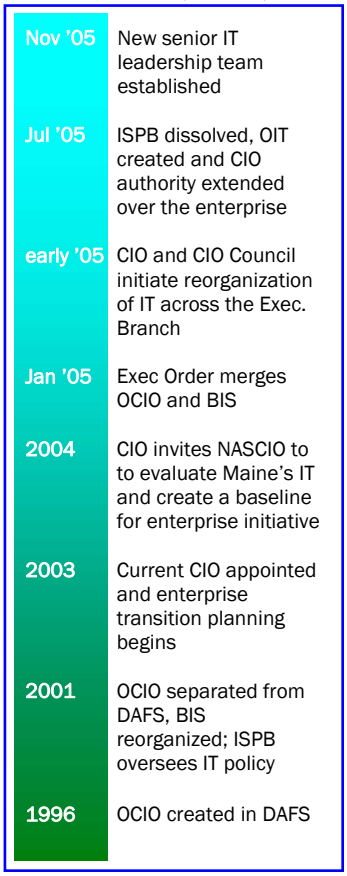
~ Michael Flowers, IT Risk Consultant, Jefferson Wells International

Problems created by fragmentation have become evident over time but Maine has been slow to adopt true enterprise approach.

The problems created by of fragmentation have become increasingly evident over time, but Maine has been slow to adopt a true enterprise approach to planning and managing IT. Reviewing the history of Maine's IT development (see Appendix C) shows a number of initiatives to coordinate or centralize some IT functions within the Executive branch while still supporting agencies' compliance with federal requirements.

These efforts have involved attempts to develop a strategic plan, implement standardized policies and procedures across the Executive branch and provide some centralized services. There have been some successes from these efforts, like a common email system for all in the Executive and Judicial branches as well as Constitutional Offices and e-government capabilities that span all three branches. However, these attempts were not far-reaching enough to help avoid the IT pitfalls or reap the benefits that a true enterprise approach could bring.

In April 1996, the first Office of the Chief Information Officer (OCIO) position was created and established within the Department of Administrative and Financial Services (DAFS). In 2001, the OCIO was separated from the DAFS/Bureau of Information Services (BIS) and accomplished the internal reorganization of the BIS unit. Statewide IT policy was established through an Information Services Policy Board (ISPB).




Planning for major IT enterprise transformation commenced in 2003 with the appointment of the current CIO.

In 2003, the current CIO was appointed and planning commenced for a major IT enterprise transformation. The CIO's Management Plan for 2004 – 2005 articulates specific strategies to transform the culture of operational expediency. Appendix D contains key excerpts from this plan.

A 2004 NASCIO assessment of Maine's enterprise architecture concluded Maine was at earliest stage of development.

In September of 2004, Maine's CIO solicited the National Association of State Chief Information Officers (NASCIO) to evaluate the status of Maine's Information Technology. According to the NASCIO Assessment in September of 2004, Maine was at Stage 1 of the Enterprise Architecture Management Maturity Framework (see Appendix A) -- characterized by architecture efforts that were ad hoc and unstructured and lacking the management foundation necessary for successful architecture development. The evaluation provided a baseline from which the CIO can measure progress of Maine's enterprise architecture and also "next steps" to move forward.

It became evident, however, that the office of the CIO had not been structured to make the plans a reality. As noted in the 2004-2005 management plan,

> "IT governance structure is weak; CIO's responsibilities extend beyond scope of authority."

An Executive Order was published on January 6, 2005. This order merged the OCIO with BIS to create a single enterprise IT organization led by the CIO. A CIO Council was also created.

The CIO worked with the CIO Council early in 2005 to begin a major reorganization of IT across the Executive branch. The reorganization would be the beginning of a transformation to move Maine's legacy of fragmented IT operations to a new enterprise with IT governance structure. The idea was for policy, strategic planning, technical architecture and procedures to span across all of State government.

Real transformation began during 2005 with consolidation of Executive branch IT functions into new Office of Information Technology led by CIO.

**The 2005 IT Executive Order**

The current administration recognized the need for change in this area as evidenced by the Governor's Executive Order of January 6, 2005. This order acknowledges that:

> *"…the taxpayers of the State expect their government to operate efficiently… and to have mechanisms in place to ensure accountability for the monies that fund information technology investments; and*
>
> *Maine's IT for state government should be managed from the perspective of the entire enterprise, thereby ensuring unified vision and meaningful strategic planning, a common technology architecture and infrastructure, effective project management, accountability, and establishment of statewide priorities."*

The order further describes actions that will be taken to move toward this goal, for instance:

- a merger of the Office of the Chief Information Officer (CIO) and the Bureau of Information Services (BIS) into a single office led by the CIO;
- a charge for the CIO to explore opportunities for consolidation of information technology infrastructure and services, and aggregation of resources among departments; and
- a requirement for each agency's information technology lead to report jointly to the Commissioner of the agency and the CIO.

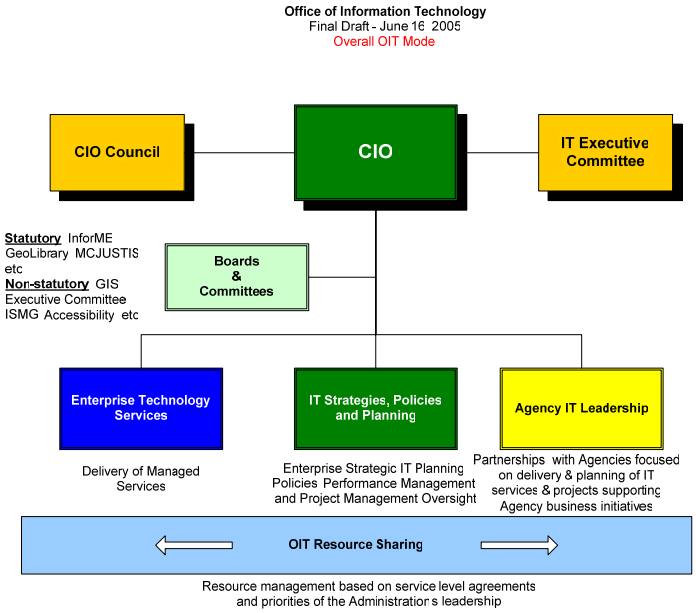
Legislation, effective on July 1, 2005 dissolved the Information Systems Policy Board (ISPB), created the new Office of Information Technology (OIT), and extended the authority of the CIO over the enterprise.

Many organizations, including other states, have consolidated IT operations and have realized benefits from their efforts. After several attempts, the State of Maine is finally experiencing a successful transition to consolidating IT across the Executive Branch. The new organizational structure for the Office of Information Technology (OIT) was established as of July 1, 2005 and the IT community in the Executive branch has been undergoing an organizational transformation ever since. The top level of management for the new enterprise organization was put in place on schedule in November 2005.

New organizational structure supports goals of enterprise philosophy; improved effectiveness and efficiency; and IT budget savings.

This new organizational structure supports the goals of the Administration relating to: enterprise philosophy for delivering services; improved effectiveness and efficiency; and IT budget savings. As shown in the organizational chart in Figure 5, there are three organizational elements.

Figure 5. OIT Organizational Chart




**OIT Line Agency Support** - Under the new structure there are nine Agency IT Directors (AITDs) who provide management and business interfaces to one or more agencies. AITDs are responsible for building a strong partnership between OIT and the agency, and provide IT leadership within the agencies. Core enterprise services will be delivered via the OIT Enterprise (central) Technology Services group, allowing the Agency IT Directors the critically needed time to focus on building a strategic IT plan that maps to the agencies' key business initiatives.

**OIT Enterprise Technology Services** - Many of the services directly provided or managed under the old organization were done at the individual agency level. Under the new organization, these services will be coordinated as part of an enterprise delivery structure, replacing the old Bureau of Information Services which went out of existence in July of 2005. Management level staff now directs each of these service areas:

| | | |
|---|---|---|
| Client Technology | Application | Radio |
| Operations | Network | |

**OIT Policy, Administrative and Strategic Planning** - Policy level services, administration, performance management, project management services and e-government are important functions which need to be reorganized and focused. The new enterprise organizational model calls for OIT leadership in:

| | | |
|---|---|---|
| Performance and Administration | e-Government Services | Project Management Oversight |
| IT Enterprise Security | IT Policies and Strategies | |

The new OIT organization is specifically designed to address concerns about management and planning; resource deployment and utilization; and redundancies that have grown in the prior organizational structure. The objective is to move in the direction of standardizing resources and services wherever possible and allowing them to be shared across multiple agencies. The goal is to move from a culture of "operational expediency" to one of "managed services".

Strategic planning process focused on critical business and IT issues facing the State is underway. OIT is utilizing its central authority to strategically direct resources.

OIT is also undertaking a strategic planning process to identify, prioritize and address critical business and IT issues facing the State of Maine. Some issues will only be resolved with changes in agency business practices and/or additional funding by the Legislature. However, the new organization will utilize its greater consolidated authority to strategically direct its resources. The new enterprise leadership is arranging human resources, capital assets and expenditures such that resources can combine to solve common system problems across all agencies.

As a result of the IT Management Plan and OIT consolidation, two groups were created to work with the Chief Information Officer:

Two advisory bodies have been created to work with the CIO -- the Executive Steering Committee and the CIO Council.

- The Executive Steering Committee – a group of high level state government leaders responsible for providing strategic direction by way of aligning IT operations with state governmental business needs. (This group has only recently been formed as part of the consolidation effort, but has begun to have formal meetings.)
- The CIO Council – a group of State government technology leaders who facilitate communication and advise the CIO. (It has been operating for nearly one year.)

Both groups conduct formal meetings with published agendas and recorded minutes.

# Conclusions

The purpose of OPEGA's review was to determine whether information technology across the State is being planned for and managed in a way that:

- maximizes the effectiveness and efficiency of Maine state government; and
- keeps exposure from associated risks at an acceptable level.

OPEGA has formed the following conclusions as a result of its work:

State's historical approach to planning and managing IT has not been adequate for some time now. State is currently exposed to an unacceptable level of IT-related risk.

A. For some time now, the State's historical approach to the planning and management of information technology (IT) has not been adequate to maximize the effectiveness and efficiency of State government nor to keep risk at an acceptable level. The State has shown a tendency to lag behind the rest of the country in adopting innovative information system practices or technology in many areas.[3] Instead, an IT culture of operational expediency has been created by:

   - an organizational structure with fragmented IT functions "silo-ed" within each agency;
   - chronically constrained financial and human resources;
   - rapidly changing technology;
   - constantly shifting and increasing policy/regulatory demands; and
   - failure to treat IS infrastructure, IS managed data, and employee knowledge as the major capital assets that they are.

   Planning, risk management, and sound policies and procedures have been put on the back burner in this culture. As a result, the State is currently exposed to an unacceptable level of IT-related risk.

   1. Physical security and environment controls are inadequate to properly protect hardware and software from damage or destruction.
   2. System access security protocols do not meet industry standards.

3 A notable exception to this is the development of e-government capabilities through the State of Maine website where Maine has been recognized as a national leader. This effort is spearheaded by a separate organizational unit called InforME. InforME receives it direction from a 17 member Board consisting of: the Secretary of State; Chief Executive Officers from several State agencies; the State's Chief Information Officer; the State Librarian; a representative from both the House and Senate; a representative from the Judicial Branch; and 8 representatives from various organizations outside of State government.

3. The State is not adequately prepared to continue its operations in the event of a significant emergency affecting the availability of key information systems or infrastructure.
4. System implementation projects have a tendency to be behind schedule, over budget and/or the systems have significant weaknesses when implemented.
5. Inefficiencies and a lack of meaningful performance data exist because of the inability to share or compare information among different information systems.

OIT consolidation is poised to significantly improve situation through enterprise approach, but strategic plan needs to include additional best practice elements. In addition, enterprise does not currently include Judicial and Legislative branches.

B. The organizational transformation that began in July 2005 with the establishment of the Office of Information Technology is poised to significantly improve the planning and management of information technology as it takes an enterprise approach across the State's Executive branch. The new OIT organizational structure logically follows IT functions with areas of responsibility, lines of authority and communication clearly defined. The OIT Directors and Managers are experienced, committed to providing quality IT services and very enthusiastic about the IT consolidation. The CIO has already recognized and developed plans to address many of the root causes of the unacceptable risk exposures. OIT's approach also already incorporates many of the key elements from the best practice models for planning and managing IT in government.

   OPEGA did note, however, there are some additional elements that need to be incorporated into the CIO's strategic plan in order to truly manage Executive branch IT from an enterprise perspective.

   OPEGA also noted that the enterprise within the CIO's jurisdiction does not include the Judicial or Legislative branches. This is in keeping with the traditional separation of the three branches of government, but the State as a whole could benefit even more by including all three branches within the enterprise. Existing technology is readily available to create explicit boundaries between governmental branches while allowing the State to act more cost-effectively and securely.

Success of transformation efforts depends on CIO's capabilities and support from Executive and Legislative branches. Related risks need to be monitored and managed by leaders in both branches but Legislature has no real mechanism for doing so.

C. The transformation to an enterprise approach is key to realizing a strategic plan for IT that has the potential to vastly improve the effectiveness and efficiency of State government. It will likely be another 3-5 years before the full benefits of the transformation are realized. The success of transformation efforts is heavily dependent on the capabilities of the CIO and support from both the Executive and Legislative branches. There are risks related to the transformation itself that need to be monitored and well managed by leaders in both branches. In particular, the potential for significant leadership change as a result of the normal political process is a serious risk. OPEGA noted that currently there is no mechanism through which the Legislature can focus on support and oversight of the long-term, enterprise-wide strategic plan and the transformation required to accomplish it.

# Findings and Observations

OPEGA discussed its recommended management actions with the Chief Information Officer and the Commissioner of the Department of Administrative and Financial Services. OPEGA also considered alternative solutions presented by management. Management actions noted in this report were agreed upon as a result of these exchanges. If agreement was not reached, OPEGA's recommendation and Management's response are reported separately.

**Finding** - a situation where actual or potential deficiencies in internal control elements may expose the State to significant potential risks.

**Observation** - a situation where opportunities for improving effectiveness or efficiency exist.

Findings and observations include management actions and OPEGA's recommendations for possible legislative action.

OPEGA's recommendations for possible legislative action are also presented with the relevant observations. They should be referred to other appropriate legislative bodies for consideration.

## Enterprise Architecture Management

Maine is only beginning to develop an enterprise architecture to guide IT development. OPEGA has three findings or observations important to evolving to the next stage of maturity.

Enterprise Architecture refers to an organizational blueprint that defines – in business terms and in technology terms – how an organization as a whole operates today, how it intends to operate in the future and how it intends to invest in technology to transition to that future state. Maine is at Stage 1 of the Enterprise Architecture Management Maturity Framework (see Background section and Appendix B for more detail) and is only beginning to develop an enterprise architecture to guide IT development. Maine's CIO is acutely aware of the need for an enterprise architecture and is using the results of the NASCIO Assessment in September 2004 as a baseline from which to measure progress in developing one.

OPEGA has the following three findings or observations that are important to assuring that Maine's enterprise architecture evolves to the next stage of maturity.

### *Finding 1. Enterprise Architecture*

**Finding 1**
Descriptions of "as is" and "to be" environments have not yet been developed.

OIT has not yet developed a picture or map that describes the "as is" and "to be" environments of the enterprise, as well as specific steps for transitioning from the "as is" to the "to be". Such a picture or map is critical to establishing a foundation for on-going enterprise architecture management.

Management Action
OIT will create descriptions of "as is" and "to be" environments. CIO will provide regular updates on progress to oversight and advisory bodies.

Management Action

The CIO will assign responsibility for creating descriptions of the "as-is" and "to-be" environments to the new Policy and Strategic Planning Unit. The descriptions will be in terms of business, performance, information/data, application/service and technology. The "as-is" and "to-be" pictures will include steps for transitioning to the desired future state and related metrics for measuring enterprise architecture progress, quality, compliance and return on investment. Work on developing these descriptions will begin by April 1, 2006 and the Unit will first establish a plan and schedule for a completed product.

The CIO plans to provide regular updates on enterprise architecture progress to the Executive Steering Committee, CIO Council, Commissioner of DAFS and the Governor. The CIO will also provide progress reports to the legislative Joint Standing Committee tasked with oversight of OIT, which is currently the Committee on Appropriations and Financial Affairs.

## *Finding 2. Policies and Procedures*

Finding 2
Written policies and procedures are either non-existent, inadequate or inconsistent across the Executive branch in a number of IT areas.

Written policies and procedures are either non-existent, inadequate or inconsistent across the Executive Branch in a number of IT areas including:

- documentation management and standards;
- information security;
- network and firewall configuration requirements and change processes;
- network, systems, and application security logging and monitoring;
- incident response and management;
- system software updates and configuration changes;
- database administration;
- help desk operations, and
- anti-virus software.

This is a reflection of the historic approach to planning and managing IT where decision-making around these areas occurred in individual agencies operating for the most part independently. These agencies also had varying levels of resources to devote to developing policies and procedures which often have been given low priority.

Management Action
Standardized policies and procedures will be developed, communicated and implemented across the enterprise. High priority issues will be addressed first; others as time and resources permit.

Management Action

OIT will develop standardized policies and procedures and work to see that they are communicated and implemented across the enterprise. OIT will first establish these policies and procedures for high priority issues and will establish others as time and resources permit.

OIT has identified the following efforts as high priority and will address them during 2006:

- framework for policy development that supports the organization and facilitates implementation and compliance;
- consolidated security policies and procedures for enterprise;
- risk analysis of proposed projects;
- tracking current projects by Project Management Office;
- standards for document preparation and management;
- incident response and management procedures; and
- network and firewall configuration and change control procedures.

The CIO has assigned responsibility for developing these efforts to specific individuals, who are currently in the process of determining reasonable timeframes for completion. Those due dates will be provided to OPEGA by April 1, 2006. In the meantime, when weaknesses are uncovered and problems arise, management takes remedial procedural action immediately. Gaps in existing policy are identified for future correction.

## *Observation 1. State as the Greater Enterprise*

Observation 1
Enterprise approach is currently focused on Executive branch and does not include the Judicial or Legislative branches; some improvement opportunities will not be realized.

The move to an enterprise approach is currently focused on the Executive branch and does not include the Judicial or Legislative branches. The largest gain from an enterprise approach does lie within the Executive branch, however, there are other improvement opportunities that will not be realized until the whole of State government is treated as the enterprise. These include:

- sharing data to develop dynamic information;
- developing systems that can provide meaningful performance measures and allow them to be linked with financial data;
- gaining efficiencies in capturing, maintaining and making use of data that originates through one branch but has uses or implications for activities in others;
- improving decisions about where the State needs to invest in IT;
- leveraging purchasing power; and
- improving management of IT risk management across the entire State.

**Recommendation**
State's Constitutional Officers and representatives from Judicial and Legislative branches should continue to actively participate on CIO Council.

**Recommendation**
Judicial and Legislative branches should explore opportunities to contract with OIT for services.

**Recommendation**
Legislature could establish specific group to manage enterprise architecture and IT investment for whole of State government but not until Executive branch transformation has matured.

Recommendations

A. The State's Constitutional Officers and representatives from the Judicial and Legislative branches are currently invited to participate on the CIO Council. At a minimum, all of these individuals should be encouraged to actively participate. Although this Council serves only in an advisory capacity to the CIO and the CIO has no authority over the other branches, it is currently the only forum established for any sharing of information, strategies and plans related to IT development across the entire State.

B. As OIT matures, Judicial and Legislative branches should explore opportunities to contract with OIT for services (which they may outsource) as an alternative to directly contracting with entities outside State government. The possible benefits of contracting with OIT would include items in the preceding bulleted list, and more.

C. Legislation could be enacted to establish a specific group tasked with developing and managing an enterprise architecture and investment management strategy for all three branches of State government. The legislation would need to require cooperation among the three branches with the goal of coming to agreement on plans that incorporate the needs of all. Membership of this group would need to include the Executive branch CIO and his counterparts in the Judicial and Legislative branches. OPEGA does not recommend that this action be taken until the Executive branch transformation has matured. Otherwise, the legislation could serve to take momentum from the Executive branch transformation that is underway and seriously delay the expected benefits and gains from that effort.

## Investment Management

Maine does not treat information systems as major capital assets requiring disciplined investment management. OPEGA has two findings related to sound investment management practices.

Investment Management refers to selecting and controlling IT spending so as to maximize return on investment and minimize risk. Maine does not treat information systems as major capital assets requiring disciplined investment management. Maine's historical model of financing information systems and capturing IT expenditures has diluted asset management, governmental control and accountability without creating economic efficiencies. Consequently, Maine is at Stage 1 of the IT Investment Maturity Model (see Appendix A for more detail). Proper investment management is critical to moving the State from the "as is" to the "to be" environment within the enterprise architecture.

OPEGA has the following two findings related to developing sound investment management practices.

# *Finding 3. Finance and Accounting*

**Finding 3**
Current accounting structures and financial practices do not provide view of IT budgets and expenditures across the State as a whole, or by any specific activity, program or statute.

Current accounting structures and financial practices do not easily allow the Administration or the Legislature a clear view of IT budgets and expenditures across the State as a whole, or by any specific agency, program or statute. IT budgets, appropriations and expenditures are typically only reviewed and reported as components of separate programs in various agencies. This hinders the State's ability to effectively manage IT investments on an enterprise-wide basis.

## Management Actions

**Management Action**
CIO will pursue feasibility study on establishing IT as a specific "program" within the Executive branch.

1. By July 2006, the CIO will pursue a feasibility study to determine the advisability of OPEGA's recommendation to establish IT as a specific "program" within the Executive branch for budgeting, appropriation, expenditure and oversight purposes. The CIO will involve the State Budget Officer, the Commissioner of DAFS and the State Controller in this study. The purpose of establishing IT as a "program" would be to make transparent:
   - all of the costs associated with information technology in the Executive branch;
   - the IT investment decisions being made;
   - the funding sources supporting the "program";
   - the resources assigned to the "program"; and
   - the strategies, plans, goals, objectives and performance measures of the "program".

**Management Action**
CIO will initiate effort to modify account code structures to enable full capture and reporting of Executive branch IT budgets and expenditures.

2. The CIO will work with the State Controller and State Budget Officer to modify account code structures enabling full capture and reporting of Executive branch IT budgets and expenditures. The goal of these modifications would be to assure that adequately detailed financial data is readily available for use in managing the enterprise architecture and IT investments, as well as monitoring performance and progress related to information technology. This will be accomplished by July 2006.

**Management Action**
OIT is developing rate structure and billing process for OIT services provided to agencies that reflects actual costs. OIT plans to assist agencies in developing IT budgets.

3. The CIO and OIT's Performance Management and Administration Office are currently developing a rate structure and billing process for OIT services provided to agencies that reflects actual costs of providing specific types of services. The structure and process should facilitate agency budgeting of these costs as well as actual expenditure tracking. The results will be communicated to agencies so that they fully understand how the rates were derived and what charges they can expect from OIT for IT services. OIT also plans to assist agencies in developing their budgets relative to IT during the normal agency budgeting process for fiscal years 2008 and 2009 commencing in July 2006. For those agencies whose legacy IT is under-funded, the CIO will specifically work to align future sources of funds with existing and projected business requirements.

**Recommendation**
Judicial and Legislative branches should explore establishing IT as specific "program".

Recommendation

For the same purposes as the Executive branch, OPEGA also recommends that the Judicial and Legislative branches explore the possibility of establishing Information Technology as a specific "program" within their respective branches.

## *Finding 4. Investment Decision-making*

**Finding 4**
Decisions on IT investments have not been made from enterprise perspective or by centralized State entity.

Decisions on IT investments to date have not been made from an enterprise perspective or by using a coordinated process. Consequently, there are few mechanisms in place to assure that such investments are the best use of the State's resources or are being made in a way that will lead to increasing effectiveness and efficiency in State government.

Management Actions

**Management Action**
OIT's enterprise architecture will be used to guide IT investments.

**Management Action**
Proposed or requested capital investments in IT will be reviewed and approved by OIT's Project Review Committee.

1. In April 2006, OIT's Policy and Strategic Planning Office will begin developing an enterprise architecture. Once completed, that architecture will be used to guide investments in information systems and allow the enterprise to leverage its resources.
2. Proposed or requested capital investments in IT will be reviewed and approved by OIT as it strives to move the Executive branch from the "as is" to the "to be" environment within the enterprise architecture. OIT has formed a Project Review Committee to evaluate major projects prior to their inception for project risk, strategic alignment and sound business investment criteria. This committee is currently testing its evaluation plan on several project proposals in order to refine the process and develop a formal procedure.

## Risk Management

Maine has not employed risk management approach in making IT decisions. OPEGA has one finding which highlights the need for sound risk management practices.

Maine state leaders have historically not employed a risk management approach in making IT decisions, whether those decisions are related to IS infrastructure investments or to specific IS projects. It is essential that state leaders recognize the high risk nature of IT and actively engage in managing these risks through risk assessment and establishment of cost effective controls. Under the new consolidated organization structure, OIT should be positioned to establish an effective risk management process that will assure IT risks across the Executive branch are adequately managed. At the time of OPEGA's review, OIT already had plans to address many risk exposures that had resulted from past IT planning and management practices.

# *Finding 5. Risk Assessment and Audit*

**Finding 5**
Risk assessment found one percent of IT environment highly controlled; eleven percent satisfactorily controlled; remaining 88% had an undesirable level of control. State is exposed to unacceptable level of risk.

The risk assessment, based on the industry-standard COBIT framework, determined that only one percent of the IT environment was highly controlled. Only eleven percent had a satisfactory (medium) level of control. The remaining 88% of the IT environment had an undesirable (low) level of control. As a result, the Jefferson Wells team identified 7 issues that pose a high level of potential risk to the State of Maine, 11 medium-risk issues and 3 issues that were considered low risk. JWI also noted that remedying the high risk and medium risk issues would likely require a significant budgetary investment as well as a significant amount of time for documenting and implementing new policies, procedures and processes.

**High level of control** = extensive resources have been allocated to reduce the impact of risk

**Medium level of control** = minimal resources have been allocated to reduce the impact of risk if it occurs, however more resources could be applied at minimal-moderate costs

**Low level of control** = inadequate resources have been allocated to reducing the impact of risk if it occurs, and the effort to mitigate the risk may have a moderate to high cost

**JWI Risk Assessment – Nov 2005**

The specific issues noted by JWI have been incorporated into the other findings and observations in this report so that individual attention can be brought to them. However, the overall results highlighted the need for more formal and continuous activities aimed at assessing and mitigating risks.

## Management Action

**Management Action**
OIT will construct risk management plan that builds on risk assessment results and works to mitigate or eliminate priority risks. Plan will include on-going internal audit process and assessing risks on specific projects.

OPEGA has provided the CIO the detailed methodology and results of the risk assessment performed by JWI. The CIO has also been provided a suggested three year audit plan for specific IT reviews that should be conducted to get a more detailed look at areas of concern identified in the risk assessment.

OIT's Policy and Strategic Planning Office will construct a risk management plan that builds on the JWI risk assessment, works to mitigate or eliminate priority risks and measures the effectiveness of OIT's risk management process. As part of this plan, OIT will develop an on-going internal audit process to measure the effectiveness of established risk management procedures and controls. OIT will also continue to cooperate with OPEGA on its reviews and other external audits of IT policies, procedures and practices with the goal of using them to improve its processes and performance.

As previously described, OIT has already formed a Project Review Committee to evaluate major projects prior their inception. Assessing the risks associated with specific projects is a critical component of the process.

Recommendation
OPEGA should establish a schedule of IT reviews to include in future OPEGA work plans.

Recommendation

OPEGA also recommends that the legislative Government Oversight Committee:

- direct OPEGA to establish a schedule of independent IT reviews to be included in future OPEGA Annual Work Plans; and
- support OPEGA in obtaining funding to hire IT audit consultants that would likely be needed to accomplish these reviews.

## Project Management

Weak or inconsistent project management has been root cause of problems for system implementation problems. OPEGA has 2 findings related to improving project management across the enterprise.

Projects for implementing new information systems or major upgrades have often been behind schedule, over established budgets or have resulted in systems that have serious weaknesses when implemented. One recurring root cause for this has been weak or inconsistent project management. A formal Project Management Office (PMO) has been created under the new OIT to improve the quality and depth of project management and reduce the risks associated with large development projects and system implementations.

OPEGA has the following two findings that are related to assuring improved IT project management across the enterprise.

### *Finding 6. Enterprise-wide Project Management*

Finding 6
There has been little effort to ensure that individuals managing IT projects, whether State staff or vendors, have strong project management capabilities.

The need for strong project managers has often not been recognized as a factor critical to the success of major IT projects. Consequently, there has been little concerted effort to build project management skill sets within agencies or to assure that those individuals assigned as project managers have strong project management capabilities. Similarly, project management capabilities are not always given proper consideration when selecting contracted vendors to assist with IT development projects. A prime example of this is the Maine Claims Management System project (MECMS).

Management Action
OIT staff will be educated in project management methods. OIT will support agencies by providing project management skills and knowledge.

Management Actions

1. The new OIT Project Management Office (PMO) will educate OIT staff in new project management (PM) methods and the consequences of poor PM. The PMO will support agencies by providing project management skills and knowledge in large system projects. Agency and PMO staff managing significant IT projects must now successfully complete training on the adopted Ten-Step PM that will be provided quarterly by the PMO. The PMO currently sponsors

Management Action
Enterprise-wide policy and procedure requiring agencies to engage OIT's PMO on their system needs or problems will be established.

Management Action
OIT now has responsibility for contracting with system development vendors; project management capabilities will be a consideration in selecting vendors.

discussion groups, outside speakers, and is facilitating PM professional development. OIT Project Managers will also be assisted in obtaining professional PM certification. The PMO will begin providing Project Sponsor training sessions, which are a component of the Ten-Step PM training, in March 2006. A pilot session was held with Department of Labor sponsors in November 2005.

2. OIT is developing an enterprise-wide policy and procedure requiring agencies to engage OIT's PMO **prior to formulating a solution** to their system needs or problems. The PMO will communicate this policy to all agencies by April 2006.
3. Effective January 2006, OIT has responsibility for contracting with vendors working on system development projects as well as managing the resulting contracts. The CIO has directed Project Proposal Evaluation Teams to consider the vendors' project management capabilities during the vendor selection process and build appropriate project management requirements into contracts.

## *Finding 7. System Development Life Cycle (SDLC)*

Finding 7
State of Maine lacks effective System Development Life Cycle (SDLC) process and attendant project management methodology.

The State of Maine lacks an effective System Development Life Cycle (SDLC) process and the attendant project management methodology. IT capital projects for the development and acquisition of large scale information systems are, therefore, put at a significant risk of failure. While some larger information system projects have succeeded and could be used as models, other projects have had very serious and visible implementation problems. Adherence to a formal SDLC serves as a system of controls over the project so that steps and considerations important for success are not overlooked.

Management Action
OIT PMO has adopted the Ten Step PM methodology; will be adopting a SDLC methodology.

### Management Action

The OIT Project Management Office has adopted the Ten Step PM methodology and is developing supporting policies and procedures for implementation by March 2006. In addition, OIT's Policy and Strategic Planning Office will be assigned responsibility for selecting and adopting a SDLC methodology. This will be accomplished during 2007.

## Security and Business Continuity

Security controls reduce risk of loss or damage to IT assets. Business continuity plans assure continued operations if risk occurs. OPEGA has 3 findings regarding weaknesses in these areas.

Security controls are put in place to reduce the risk of loss or damage to the IS infrastructure, the applications it supports and the data that resides in those applications. Business continuity plans prescribe how the organization will continue to perform its critical functions and provide needed services if, indeed, the infrastructure, applications and/or data are not available for periods of time.

OPEGA has the following three findings related to security and business continuity weaknesses.

## *Finding 8. Physical Security*

**Finding 8**
Risk assessment identified weaknesses in physical access security controls, particularly in regard to the State's primary data center.

The risk assessment performed by JWI identified a number of weaknesses in physical access security controls, particularly in regard to the State's primary data center. Specifically, JWI noted policy and procedure concerns with:

- physical access request and approval;
- granting building access and creating access key cards for secure areas;
- authorization forms, documentation and information maintained on individuals who had been issued access key cards;
- regular review of the appropriateness of current badge access capabilities for individuals with active key cards; and
- vulnerabilities related to the physical location of the data center.

### Management Actions

JWI and OPEGA have shared the details of the identified weaknesses with the CIO. Based on these details, the OIT Security Officer has developed an action plan to address the physical access weaknesses in order of priority as determined by the degree of risk associated with each. This action plan was submitted to OPEGA on January 9, 2006. As discussed in that plan, the following actions have been taken, or are planned, to strengthen physical access security controls.

**Management Action**
OIT Security Analyst has rewritten Access Control Policy for building housing the primary data center.

1. The OIT Security Analyst has rewritten the Building Access Control Policy for the building housing the primary data center. OIT is co-located with another State agency at this facility and the policy must address the needs of both agencies. These agencies are working together to implement the new building access policy. Building employees will be given formal training on the new policy once it is approved by the appropriate departmental management.

**Management Action**
OIT Security Analyst will develop complete set of procedures for administering the Access Control Policy.

2. After consulting with OIT Enterprise Operations and the other affected agency, the OIT Security Analyst will also develop a

complete set of procedures for administering the Building Access policy. All building supervisory staff will be given formal training on the new building access procedures once approval has been given by the appropriate departmental management. The OIT Security Analyst will incorporate specific recommendations from the JWI risk assessment into this set of procedures to further assure that:

- lost, missing, stolen, altered, or revoked access cards are properly dealt with and purged from the access control system;
- complete and accurate records are kept of key-card access levels and assignments;
- duties are properly segregated in safeguarding new blank key card stock separate from the security office that creates the access key cards;
- access to secure areas is limited to those individuals whose job responsibilities require such access; and
- access badges issued to contractors are related to specific contracts and have an expiration date associated with the expiration date of the contract.

**Management Action**
Access Request Form has been modified.

3. The OIT Security Analyst has redesigned the Access Request Form for the primary data center building. The Access Request Form has been modified so that the employee signs to acknowledge receipt of the access badge. This includes all access badges issued regardless of whether the badge authorizes access to high security areas.

**Management Action**
All generic access cards have been removed from access control system at the primary data center facility.

4. OIT has removed all generic access cards from the access control system at the primary data center facility.

**Management Action**
OIT is reviewing physical vulnerabilities of the primary data center and is mitigating these risks wherever possible.

5. OIT has begun reviewing the physical vulnerabilities presented by the location of the primary data center and is mitigating these risks wherever possible. A proposal for closed circuit cameras has been placed before the Bureau of General Services. Irregularly timed perimeter monitoring will also be assigned to the current security/OIT staff to identify suspicious activity.

**Management Action**
OIT will review active access key cards quarterly after implementing new access control system.

6. OIT will select and implement a new access control system which will provide the reporting capabilities necessary to facilitate regular reviews of active access key cards. This new system will be in place within FY 06. Once the new software is in place, a quarterly review process will be adopted with policies and procedures developed to support that process. The quarterly review will include auditing the list of active access key cards against the records of cardholders and their access capabilities. Key cards with minimal activity will also be investigated for possible deactivation.

**Management Action**
Physical access security controls will also be implemented at OIT's hot site/auxiliary data center.

7. OIT will seek to implement as many physical access security controls as possible at OIT's hot site/auxiliary data center. This data center is also co-located with another State agency. OIT does not control either the access control system for that building, or access to the great proportion of that facility. However, OIT will develop and implement new procedures to control access to the OIT computer room there.

**Management Action**
Key card control security will be added to IT facilities wherever possible.

**Management Action**
Procedures have been implemented to help ensure that all access key cards issued to departing OIT employees are deactivated.

**Management Action**
OIT will develop single IT Security Policy based on ISO Standard 17799 and develop procedures to implement policy; monitor compliance enterprise-wide.

8. Wherever possible and as changes are made, key card control will be added so there is a record of access to all State of Maine data centers, server rooms, communication and electrical cabinets. The reorganization of the IT function in the Executive branch will facilitate implementation of this recommendation. OIT personnel will be onsite wherever there is a data processing facility. Where these facilities are located in a building managed by another agency, OIT will work closely with that agency to ensure that only authorized persons have access to the voice and data network and computing equipment. While OIT considers the security of this equipment to be very important, securing it will likely be a long-term goal associated with data center consolidation. The equipment will ultimately be secured best by removing it to a remote computing site under the close control of OIT.
9. OIT has implemented a "check-out" procedure for all OIT employees. These procedures will help ensure that all access key cards issued to departing employees are collected or deactivated. OIT will develop a mechanism for ensuring these procedures are employed by other agencies using the current Agency Information Technology Directors.
10. By August 1, 2006, the OIT Security Officer will consolidate agency IT Security Policies into a single policy based on ISO Standard 17799 and develop procedures to implement and monitor compliance with that policy. ISO 17799 is an internationally recognized generic information security standard that represents a comprehensive set of controls comprising best practices in information security.

## *Finding 9. System Security*

**Finding 9**
System access controls do not measure up to industry standards. Procedures are inadequate or inconsistently applied; firewall rules are not well documented.

The results of the JWI risk assessment suggest that system access controls do not measure up to industry standards. Procedures regarding password security for administrative accounts, password enforcement, password encryption and data security were inadequate or inconsistently applied across the enterprise. In addition, the firewall rules being used by the State were not well documented, thus preventing JWI from fully evaluating the adequacy of the State's policies on firewall configuration. The firewall protects the system from unwanted intrusion by enforcing a set of rules; blocking some traffic and allowing other traffic. Firewalls also inspect the traffic as it passes through the open ports.

**Management Action**
New IT Security Policy will clarify that established password policies and procedures apply to whole Executive branch.

<u>Management Actions</u>

1. As previously mentioned, the OIT Security Officer will consolidate agency IT Security Policies into a single policy based on ISO Standard 17799 and develop procedures to implement and monitor compliance with that policy. This policy will make it clear that established password policies and procedures apply across the whole Executive branch.

**Management Action**
Plans are being developed to ensure password policies are enforced and passwords are encrypted.

**Management Action**
Independent audit of firewall rule set will be conducted and will produce improved documentation.

2. The OIT Policy and Enterprise Groups have begun meeting to develop plans to ensure that:
   - password policies are enforced across the entire network; and
   - passwords are encrypted when stored or included in data streams.
3. The OIT Security Officer plans to conduct an independent audit of the firewall rule set. One product of that review will be improved documentation of the rule set that will be available for examination in subsequent reviews.

## *Finding 10. Business Continuity Planning*

**Finding 10**
Business Continuity Planning is inadequate across the Executive branch IT environment.

Business Continuity Planning (BCP) is inadequate across the Executive branch IT environment. Some business continuity plans do exist, but even they are weak and would most likely fail if relied upon in an actual emergency. Consequently, in the event of a natural or man-made disaster, there is not an effective plan in place to guide the recovery of the Executive branch IT systems and services. This could seriously impact the State's ability to continue to perform functions and provide services to the public.

**Management Action**

**Management Action**
OIT will facilitate BCP by consolidating data centers; assessing current plans; identifying weaknesses and recommending remedies. Effort will require significant financial and human resources.

To improve business continuity planning, OIT will:

- consolidate and standardize data centers to make the technology portion of continuity planning easier and less expensive;
- assess current Continuity of Operations Plans (COOP) of the individual agencies in the context of the new enterprise approach;
- conduct a gap analysis to identify and prioritize shortfalls; and
- recommend actions to remedy inadequacies.

The Enterprise Security Office at OIT is responsible for the technology elements of COOP planning and will require a corresponding investment of time and resources from the respective business agency managers to ensure a successful outcome. This effort is expected to require a significant commitment of financial and human resources.

**Recommendation**

**Recommendation**
Each agency, in all three branches of State government, should also develop its own Business Continuity Plan.

OPEGA further recommends that each agency, in all three branches of State government, also develop its own Business Continuity Plan. The plan should detail how operations will be continued if critical information systems and/or the agency's current physical location(s) are unavailable for an extended period of time.

## Knowledge Management

Maine has not treated knowledge as an asset and has yet to adopt "knowledge management" practices. OPEGA has 5 observations regarding opportunities for improved knowledge management.

Knowledge management refers to capturing, understanding, and using the collective body of information and intellect within an organization to accomplish its mission. Maine has not treated knowledge and the information that supports it as an asset. Consequently, Maine has yet to adopt modern "knowledge management" practices that would help the State capitalize on that asset to achieve gains in effectiveness and efficiency.

OPEGA has the following five observations related to opportunities for improving knowledge management.

## *Observation 2. Performance Management*

**Observation 2**
Inadequate attention has been given to designing information systems that create accountability and are themselves accountable.

Inadequate attention has been given to designing information systems that create accountability and are themselves accountable. This is a major root cause of the State's failure to employ performance budgeting practices. Information systems across the enterprise have not been designed to capture or produce data, in a useable form, that allows the State to:

- adequately evaluate the performance of programs and activities;
- compare that performance to financial and human resources that are being committed to that program or activity; or
- to do the same for the information systems themselves.

This is primarily due to the past lack of agency capacity to define measures, and the lack of a single entity responsible for monitoring the accountability of information systems.

**Management Action**
OIT will investigate and make recommendations for assimilation of knowledge management into the enterprise to improve performance monitoring and increase accountability.

### Management Action

The CIO will direct the Policies and Strategies Office, the PMO, and the Performance and Administration Office of the OIT to investigate and make recommendations for assimilation of knowledge management into the enterprise to improve performance monitoring and increase accountability. This effort will include consideration of the following OPEGA recommendations:

A. Design new or upgraded systems to collect or produce data needed for effectively monitoring performance of programs, functions or activities. These features should also link performance data to allocated resources. Both management and legislative needs require consideration in this process.

B. Use automated tools to establish and monitor performance metrics for information systems across the enterprise. Such information will be

necessary to manage the enterprise architecture and related investments by helping to identify systems with poor performance – both from a technological standpoint and in terms of meeting the needs of the business operations they support. OIT should include a function that is responsible for this type of activity.

**Recommendation**
Legislative bodies responsible for oversight of information system implementations should take an interest in system design.

Recommendation

OPEGA further recommends that legislative bodies responsible for oversight of information system implementations take an interest in whether, and how, the system is being designed to provide accountability, and allow the impact of enacted legislation to be evaluated.

## *Observation 3. Enterprise Data Management*

**Observation 3**
Ability to combine data from different sources or systems across the enterprise is very limited. Same data is also often duplicated in several systems.

The ability to combine data from different sources or systems across the enterprise is very limited. This limitation is due both to differences in the way data is captured and coded in various information systems (data compatibility) as well as a lack of electronic capabilities to easily bring the data together and analyze it (systems interoperability). As a result, it is difficult to convert data into information that can answer specific questions or help inform decisions about particular demographic or geographic groups. For example, data related to "at-risk" youth in Maine resides in Corrections, Health and Human Services and Education. The data from systems in each of these areas would need to be looked at in a combined fashion in order to answer questions about how well the State is addressing that population or complying with related regulatory requirements.

In addition, the same data may be getting captured in multiple systems, all with different field names, data formats and codes. This means there is duplication of information across the enterprise and it may not be easy to determine which pieces of duplicated data are most current or valid.

Management Actions

OIT is addressing the need for data consolidation, integration and exchange as an important long-term strategic objective. It is very difficult to make the needed changes in existing systems. There are, however, data exchange methods that offer some ability to manage data sharing between applications with the data being duplicated, but linked, in each participating system. Long-term efficiencies can be better addressed by designing new systems to share common data as part of their initial design. OIT is taking the following actions to address this issue.

**Management Action**
OIT will develop data standards to begin codifying common data elements across multiple information systems.

1. As part of its enterprise architecture, OIT will develop data standards to begin codifying common data elements, their formats, meanings

**Management Action**
New systems will be evaluated for common data elements that can be shared or architected as a common resource rather than duplicated.

**Management Action**
OIT is investigating tools to assist in exchanging data between existing "legacy" applications.

and sources across multiple information systems. This work will begin in April 2006 and build on work begun in the former Behavioral and Developmental Services several years ago.

2. As opportunities arise, new systems will be evaluated to see if common data elements can be shared or architected as a common resource rather than duplicate data. Several agencies have already begun projects to consolidate key customer data within their organizational domains. OIT will investigate the feasibility of consolidating this data further into a multi-agency "Customer Relationship Management (CRM)" module.
3. OIT is investigating tools to assist in exchanging data between existing "legacy" applications. The goal is to provide documented standard linkages between systems that can be maintained as the cooperating applications change over time.

## *Observation 4. Best Practices & Emergent Technology*

**Observation 4**
Professional development opportunities for IT staff have been limited thus limiting exposure to new ideas and technologies.

Professional development opportunities for IT staff in the Executive branch have been limited by resource constraints. Consequently, these individuals may not be receiving enough exposure to emerging or proven concepts, approaches or innovations in information technology outside of Maine State government. Such exposure is critical to helping Maine stay current.

**Management Action**
OIT will facilitate professional development program to keep technical staff current and assure emerging trends are assimilated to support the business.

**Management Action**

The Policy and Strategic Planning Office will facilitate a professional development program looking for "to-be" opportunities for the enterprise architecture. The program will ensure that technical staff remains current within their skill sets, and that new and emerging technical trends are appropriately assimilated to support the business.

## *Observation 5. Knowledge as a Capital Asset*

**Observation 5**
The wealth of accumulated knowledge possessed by OIT staff may be lost as they choose to retire or otherwise leave State government.

The IT staff in the Executive branch, particularly at the management level, has many years of knowledge and experience working in the State's IT environment. The wealth of accumulated knowledge these individuals posses may be lost as they chooseto retire or leave the State for other reasons.

Management Action
Succession planning and knowledge transfer were considerations in hiring initial enterprise management team for OIT and will extend throughout the enterprise.

Management Actions

Succession planning and knowledge transfer for senior management were considerations during the hiring of the initial enterprise management team for OIT. This focus will be extended throughout all disciplines within the enterprise.

At the PMO, specific training in succession planning is underway starting with the Director. A career ladder is being established for those working directly in the office and tangentially in the agencies. OIT will build upon activities such as Maine Fusion Conferences to develop an ongoing series of professional seminars in IT and management.

## *Observation 6. Knowledge Management Techniques*

Observation 6
State's IT is not yet being well utilized to share knowledge around particular topics.

The State's IT is not yet being well utilized to help bring together cross-organizational groups, within or outside of the State, that need to share knowledge around particular topics. In the knowledge management framework, these groups are called "communities of practice". Some examples of "communities of practice" are:

- professional organizations;
- groups of engineers working on similar problems; and
- gatherings of first-time managers helping each other cope.

Communities of practice are currently aiding knowledge sharing in an *ad hoc* manner through technology-based mechanisms that provide remote learning opportunities, electronic libraries and on-line forums.

Explicitly using technology to foster "communities of practice" and provide better ways of sharing knowledge could also help to reduce the risk of significant knowledge loss the State is facing with a maturing workforce. For example, retirees could continue to provide knowledge to former co-workers by becoming part of on-line forums on subjects that were previously their area of expertise.

Management Action
OIT will work to increase use of technology for information sharing over time as resources permit.

Management Actions

OIT will work to increase the use of technology for information sharing over time and as resources permit. OIT expects to:

- investigate the feasibility of appointing a Chief Knowledge Officer to coordinate the management of the State's information assets;
- advocate that Data Stewards and Product Managers be designated by the business units to provide on-going support, training and product planning for important information assets; and
- continue to foster the introduction and use of technology to facilitate knowledge management and information sharing whenever opportunities arise.

## Leadership and Oversight

Potential changes in IT leadership create risk that enterprise transformation will be disrupted before it is fully mature. OPEGA has 2 observations related to assuring transformation continues.

Many organizations, including other states, have implemented plans for consolidating IT and have realized the benefits of their consolidation efforts. After several attempts, the State of Maine is experiencing a successful transformation to an enterprise approach through consolidating IT across the Executive branch. One of the most recognized reasons for success is the leadership of the current CIO and the support the CIO is receiving from the Commissioner of the Department of Administrative and Financial Services and the Governor. The possibility of changes in leadership creates a risk that the transformation will be disrupted before it has a chance to fully mature. Meaningful and continuing oversight of IT activities from an enterprise perspective would help assure that this area of high risk for the State continues to be properly planned for and managed.

OPEGA has the following two observations related to assuring that the State continues planning and managing IT from an enterprise perspective and reaps the ensuing benefits.

### *Observation 7. Leadership & Succession Planning*

**Observation 7**
Political process creates risk that frequent short-term leadership changes will interfere with long-term strategic planning for IT. CIO may change as early as January 2007.

The reality of the political process is that changes in IT leadership may occur with every new administration. The potential for frequent short-term leadership changes will always present some risk in an area like IT that requires more long-term strategic planning. The current CIO may change with administration as early as January 2007. A potential change in leadership at that particular time presents an increased level of risk as OIT will still only be 1 ½ years into its transformation effort.

**Management Action**
CIO has initiated two pronged approach to mitigate the risk of change in leadership:

- strengthen OIT management team; and
- create new widely supported strategic plan.

#### Management Action

The CIO has initiated a two pronged approach to mitigate the risk of a change in leadership. The first prong is to strengthen the OIT management team, through education, experience and authority, to create leaders who can maintain the current transformation effort if the CIO changes. The second prong is to create a new Strategic Plan which will be widely supported by agency leadership and will provide on-going direction for the efforts of the enterprise technology governance team.

In addition, two groups, the Executive Steering Committee (government business) and CIO Council (government technology and management), have been established to work with the CIO in an advisory capacity. These groups should also help bring continuity to the transformation effort over time.

Recommendation
Legislature should further mitigate this risk through:

- active support and oversight;
- OPEGA reviews; and
- legislation requiring CIO to have certain qualifications.

Recommendation

In addition to the CIO's efforts, OPEGA recommends that the Legislature further mitigate this risk through:

- actively providing legislative support and oversight from the responsible Joint Standing Committees of jurisdiction;
- continuing independent reviews by OPEGA of various aspects of information technology; and
- enacting legislation that requires individuals appointed to the position of Chief Information Officer to have particular knowledge and capabilities in both information technology and leadership arenas.

## *Observation 8. Legislative Oversight*

Observation 8
Legislative oversight activities devoted exclusively to the State's information technology are absent.

Legislative oversight activities devoted exclusively to the State's information technology are absent. Each JS Committee performs some oversight of information systems as it relates to the agencies and/or programs within its jurisdiction. However, there is not one legislative body assigned responsibility for overseeing the planning and management of the IT enterprise.

Oversight of State-wide IT issues would serve as an important control over the risk of potential financial loss related to lack of coordination. Also, given the tendency of government to lack long-term management continuity, an oversight structure is needed to provide a stable guiding force that will transcend leadership changes. Sustained legislative attention is vital to reinforce the link between accountability for returns on technology related investments and the satisfaction of real public needs. The legislative body tasked with oversight of State-wide IT efforts should understand the environment in which technology operates, and the particular demands that accompany government automation projects.

Recommendation
Legislature should support any actions taken Administration to establish IT as a specific "program".

Recommendations

A. The Legislature should support any actions taken by the Administration to establish IT as a specific "program" for budgeting, appropriation, expenditure and oversight purposes. As previously discussed in Finding 3, the CIO is exploring the feasibility of taking this approach to finance and accounting for IT.

B. The Legislature should assign responsibility for oversight of this "program" to either the JS Committee on Utilities and Energy or the JS Committee on State and Local Government. The Utilities and Energy Committee would be most familiar with the concepts, approaches and risks involved in planning and managing enterprise-

**Recommendation**
Legislature should assign responsibility for oversight of enterprise-wide IT to either Committee on Utilities and Energy or Committee on State and Local Government.

wide infrastructure which is similar in nature to Telecommunications and Electricity. The State and Local Government Committee is also an option as it is already familiar with the State's processes for managing investments in other large capital asset areas.

# Acknowledgements

OPEGA would like to thank the Chief Information Officer and the numerous individuals from the Office of Information Technology, the Secretary of State's Office, the Treasurer's Office and the Attorney General's Office who worked diligently to provide the vast amount of written documentation requested during this review. Their cooperation and willingness to share their time and knowledge provided for more valuable results.

## *APPENDICES*

A.1. Best Practice Model: Enterprise Architecture Management -

A.2. Best Practice Model: IT Investment Management

A.3. Best Practice Model: Knowledge Management

A.4. Best Practice Model: Risk Management

B. Highlights of the Shifting Technological and Policy Environment Of Information Systems Development

C. Maine's IS Infrastructure Development

D. Key Excerpts from the CIO's Management Plan for 2004 – 2005

E. Bibliography and Guidance

F. Acronyms

## Appendix A. 1 Enterprise Architecture Management

Developing, implementing and maintaining an enterprise architecture (EA) is basic to both organizational transformation and IT management. A properly managed EA can clarify and help optimize the interdependencies and interrelationships among an organization's business operations and the underlying information systems.

An **enterprise architecture** is an organizational blueprint that defines–in business terms and in technology terms–how an organization operates today, intends to operate in the future, and intends to invest in technology to transition to this future state.

The GAO has developed an Enterprise Architecture Management Maturity Framework (EAMMF) for use in assessing the maturity of EA practices in the federal government. The EAMMF is a life cycle model where the stages are cumulative; in order to attain a higher stage of maturity, the organization must have institutionalized all of the requirements for that stage in addition to those for all of the lower stages. The EAMMF is three dimensional as it defines four Critical Success Attributes that apply to each Stage and specific Core Elements related to each Attribute within each Stage. Key features of the GAO's Enterprise Architecture Management Maturity Framework (EAMMF) are presented in Figure 6.

- **Stage 1: Creating EA Awareness** – The organization does not have any plans for developing an architecture or has plans that do not demonstrate an awareness of the value of an EA. There may be some EA activity, but efforts are ad hoc and unstructured, lack institutional leadership and direction, and do not provide the necessary management foundation for successful EA development.
- **Stage 2: Building the EA Management Foundation** – The organization recognizes that the EA is a corporate asset and vests accountability for it in an executive body representing the entire enterprise. EA management roles and responsibilities are assigned; plans for developing EA products are established; and the necessary resources are committed.
- **Stage 3: Developing the EA** – The organization focuses on developing architecture products according to the selected framework, methodology, tool, and established management plans. The products are to describe the current ("as-is") and future ("to-be") states and the plan for transitioning from the current to future state (the sequencing plan). The organization is also measuring its progress against plans, addressing variances and reporting on progress.
- **Stage 4: Completing the EA** – The organization has completed its EA products and they have been approved by the CIO and the EA steering committee or investment review board. An independent agent has assessed the quality of the EA products and evolution of those products is governed by a written EA maintenance policy.
- **Stage 5: Leveraging the EA to Manage Change** – The organization has secured senior leadership approval of the EA products as well as a written institutional policy requiring that IT investments comply with the architecture, unless an explicit waiver is granted. Decision-makers are using the EA to identify and address ongoing and proposed IT investments that are conflicting, overlapping, redundant or not strategically linked. The organization measures EA benefits or return on investment and adjustments are continually made to both the EA management process and the EA products.

**Figure 6. Summary of EAMMF Version 1.1: Maturity Stages, Critical Success Attributes, and Core Elements**

~*A Framework for Assessing and Improving Enterprise Architecture Management* (Version 1.1), GAO Executive Guide; GAO-03-584G, 2003

| | Stage 1: Creating EA awareness | Stage 2: Building the EA management foundation | State 3: Developing EA products | Stage 4: Completing EA products | Stage 5: Leveraging the EA to manage change |
|---|---|---|---|---|---|
| **Attribute 1: Demonstrates commitment** | | Adequate resources exist.<br>Committee or group representing the enterprise is responsible for directing, overseeing or approving EA. | Written and approved organizational policy exists for EA development. | Written and approved organizational policy exists for EA maintenance. | Written and approved organizational policy exists for IT investment compliance with EA. |
| **Attribute 2: Provides capability to meet commitment** | | Program office responsible for EA development and maintenance exists.<br>Chief architect exists.<br>EA is being developed using a framework, methodology, and automated tool. | EA products are under configuration management. | EA products and management processes undergo independent verification and validation. | Process exists to formally manage EA change.<br>EA is integral component of IT investment management process. |
| **Attribute 3: Demonstrates satisfaction or commitment** | | EA plans call for describing both the "as-is" and "to-be" environments of the enterprise, as well as a sequencing plan for transitioning from "as-is" to "to-be".<br>EA plans call for describing both the "as-is" and "to-be" environments in terms of business, performance, information/data, application/service and technology.<br>EA plans call for business, performance, information/data, application/service and technology description to address security. | EA plans describe or will describe both the "as-is" and "to-be" environments of the enterprise, as well as a sequencing plan for transitioning from "as-is" to "to-be".<br>Both the "as-is" and "to-be" environments are described or will be described in terms of business, performance, information/data, application/service and technology.<br>Business, performance, information/data, application/service and technology descriptions address or will address security. | EA products describe both the "as-is" and "to-be" environments of the enterprise, as well as a sequencing plan for transitioning from "as-is" to "to-be".<br>Both the "as-is" and "to-be" environments are described in terms of business, performance, information/data, application/service and technology.<br>Business, performance, information/data, application/service and technology descriptions address or will address security.<br>Organization CIO has approved current version of EA.<br>Committee or group representing the enterprise or the investment review board has approved current version of EA. | EA products are periodically updated.<br>IT investments comply with EA.<br>Organization head has approved current version of EA. |
| **Attribute 4: Verifies satisfaction of commitment** | | EA plans call for developing metrics for measuring EA progress, quality, compliance, and return on investment. | Progress against EA plans is measured and reported. | Quality of EA products is measured and reported. | Return on EA investment is measured and reported.<br>Compliance with EA is measured and reported. |

maturity

Note: each stage contains all elements of previous stages.

## Appendix A.2 IT Investment Management

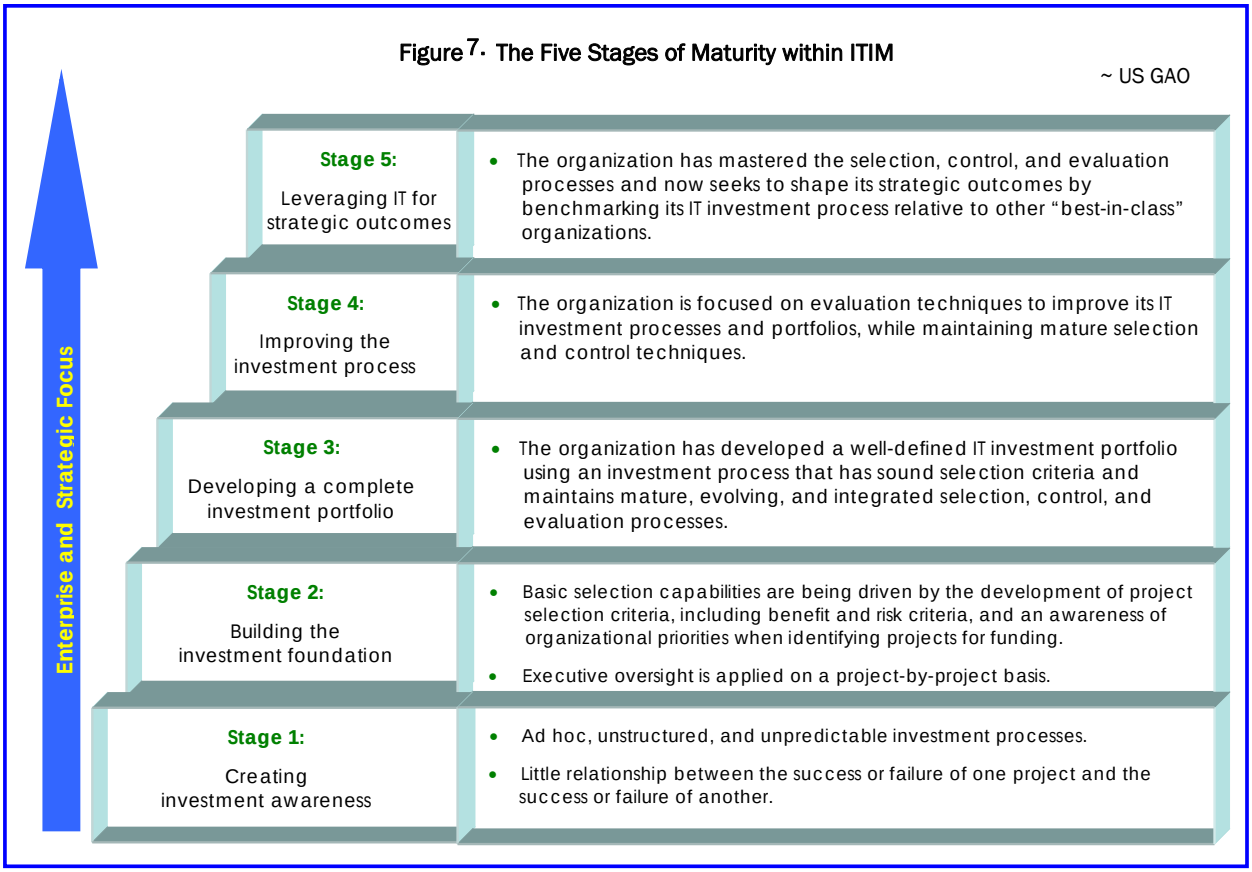
An organization's practices for managing its investments in IT impact its ability to successfully manage an enterprise architecture. Financing information technology, therefore, must be restructured in a way that will support the EA. This includes employing portfolio-based capital planning and investment control practices. Investing in IT without considering the EA often results in systems that are duplicative, not well integrated and unnecessarily costly to maintain and interface.

> "Based on our experience, employing ITIM and EAMMF in concert can greatly increase the chances that an organization's operational and IT environments will be pursued in a way that optimizes mission performance."
>
> GAO, 2003

The GAO has developed an Information Technology Investment Management (ITIM) model to use in concert with the EAMMF. Key features of this model are presented in Figure 7[4].

Figure 7. The Five Stages of Maturity within ITIM

~ US GAO




4 *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, GAO/AIMD-10.1.23, 2000.

## Appendix A.3 Knowledge Management

In the 1990's, as both the federal government and the private sector began adapting to the "Knowledge Age," it became apparent that organizational culture change was in order. The Knowledge Age is signified by the dominance of knowledge-based products and services in the market place.

Over the past decade and a half, knowledge-centric organizational cultures with explicit knowledge management practices emerged. Knowledge management is closely aligned with enterprise architecture management, because both focus on systematically identifying the information sharing needs of organizations. The relationships between: technology, information, knowledge and mission performance are depicted in Figure 8.

> "Knowledge Management is really not a new concept. It simply incorporates and makes sense of many things we already know and accept with a new twist. Knowledge management requires data sharing at an enterprisewide level and bridging local islands of information."
>
> **~ Shereen Remez, US CKO, 2000**

Figure 6.8. nowledge Management Relationships


Knowledge management is an updated set of approaches to strategically using intellectual assets. Familiar processes influenced by knowledge management include: taxonomy for data compatibility, information integrity and quality, monitoring and evaluation, research and development, training and education, multi-media communications, and tracking emerging technology and best practices.

Figure 9. KM Terms Defined


**Wisdom** – knowledge in context such that it can be appropriately applied in action.

**Knowledge** – information in context such that its significance is understood.

**Information** – data in context such that it influences perception.

**Data** – discrete, unorganized observations.

Knowledge-centric organizations designate Chief Knowledge Officers (CKOs) who play a complementary role to CIOs. While CIOs focus much of their activity on physical infrastructure and computer applications, CKOs focus their efforts on data, information and knowledge with the goal of developing and maintaining an organization that acts wisely. Figure 9 depicts the CKO's focus.

## Appendix A 4 Risk Management

The principal goal of risk management is to ensure that an organization is able to meet its mission and objectives in the face of uncertainty. Risk management involves assessing risks and implementing the most cost effective controls to keep exposure from risk to an acceptable level. Risk management practices should be woven into enterprise architecture and investment management decisions to assure that the organization properly considers and addresses:

- the growing risks directly related to IT specific objectives;
- IT-related risks that affect achievement of business objectives throughout the organization; and
- opportunities for IT to provide controls over risks related to business objectives.

Very simply, risks are events or situations that threaten the achievement of an organization's objectives through loss, failure or missed opportunities. Risks can arise from a variety of internal and external sources and can change over time. For example, IT failure was not a significant risk until IT began playing a substantial role in operations.

Controls are mechanisms used by an organization to:

a. prevent these events from occurring;
b. detect that they did occur so proper action can be taken; and/or
c. reduce the impact to the organization if the event does occur.

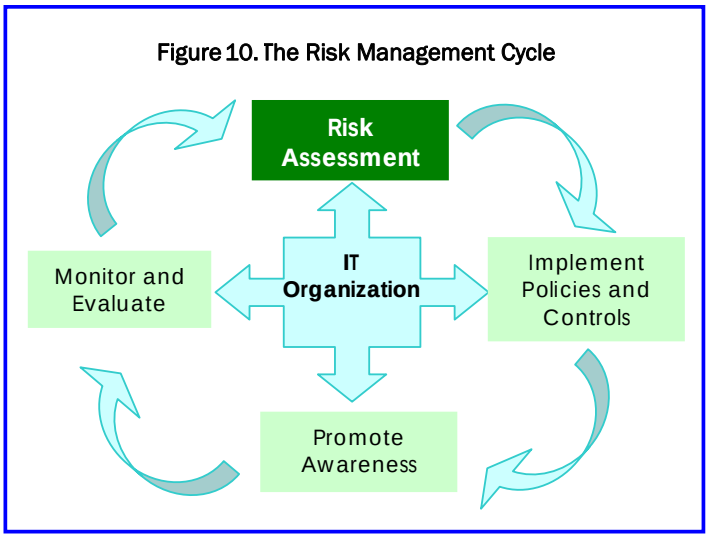
There is a broad range of mechanisms that might be employed to address risk (beyond the strictly financial). Many of these fall into familiar categories but are not always thought of as controls when identifying ways to reduce exposure to risk. Individual controls vary in their potential effectiveness and in the cost that is associated with implementing them. Typically, a variety of controls are used in conjunction with one another to address a particular risk. The group of controls used by an organization is collectively referred to as a system of internal control. Some examples of controls include:

<table>
<tr><td>quality assurance processes</td><td>internal and external audits</td><td>budgeting and forecasting processes</td><td>employee performance evaluation systems</td></tr>
<tr><td>supervision and oversight</td><td>organizational design</td><td>strategic planning;</td><td>employee training and education</td></tr>
<tr><td rowspan="2">reconciliations, comparisons and edits</td><td>policies and procedures</td><td>physical safeguards</td><td rowspan="2">definition and communication of mission, goals and objectives</td></tr>
<tr><td>status reporting;</td><td>customer surveys</td></tr>
</table>

Risk management, then, is about striking the proper balance between risk and controls to keep an organization's exposure to an acceptable level, at a cost the organization can afford. It involves having a continuous process of:

- identifying actual and potential risks;
- assessing the likelihood that each risk will occur and the impact(s) to the organization if it does;
- deciding what combination of controls should be employed to bring the organization's exposure from this risk to an acceptable level;
- implementing the controls; and
- monitoring whether the controls employed continue to be adequate and effective.

This continuing cycle of activity is illustrated in the Figure 10.




All elements of the risk management cycle are important, but risk assessment provides the foundation for other elements. Since risks and threats change over time, it is important that organizations periodically reassess risks and reconsider the appropriateness and effectiveness of the controls they have selected.

Critical to this process is properly assessing the likelihood of each risk occurring and the impact to the organization's objectives if it does. As illustrated in Figure 11, risks that are very likely to occur and would significantly impact achievement of the objective would be identified as highest risk. Conversely, those risks that rarely occur and would have little or no impact would be considered the lowest risks. Other risks would fall on the gradient in between. By properly assessing risks, the organization is in a better position to prioritize where limited resources should be applied to establishing controls. More resources should be devoted to controls for high risks than for low risks.

Decisions about how many resources to devote to controls also require an understanding of what is considered an "acceptable level" of exposure for the organization. Different organizations have differing risk appetites in terms of the exposures they are willing to bear. Some organizations could easily recover from a $100,000 loss and are willing to leave this level of risk uncontrolled. However, such a loss would put other organizations out of business and they are likely to establish controls that reduce such financial exposures.


In organizations where the risk management practices are mature, risk management is also done on a "enterprise-wide" basis. The risk management process is on-going at all levels of the organization and in relation to all of the organization's activities. All managers have an understanding of the organization's risk appetite and an evaluation of risk becomes a part of nearly every decision that is made.

## Appendix B. Highlights of the Shifting Technological and Policy Environment of Information Systems Development

| Technology Advances | Federal Legislation |
|---|---|
| **1960s** | |
| **Mainframe** users shared a pool of "dumb" terminals and had to rely on centralized printing and storage resources. | **Brooks Act** - called for centralized oversight of federal information technology acquisitions by the General Services Administration (1965)<br>**Freedom of Information Act (FOIA)** (1966) |
| **1971 – 1975** | |
| **Personal computer** and powerful applications were developed allowing for a new era of computer users who did not understand computer systems. | **Privacy Act** (1974) |
| **1976 – 1986** | |
| Ethernet standards were developed which provided a means of linking together computers from different manufacturers. **Networks** expand. | **Paperwork Reduction Act (PRA)**- applied life cycle management principles to information management and focused on reducing the government's information-collection burden. (1980)<br>**Competition in Contracting Act** (1980)<br>Significant **rewrite of FOIA** (1986) |
| **1987 – 1991** | |
| All the pieces in place to develop distributed systems and **enterprise architecture**. | **Computer Security Act** (1987)<br>**Chief Financial Officers Act** (1990) |
| **1992 – 2002** | |
| The **World Wide Web** takes off; portable computers are widely used; and Interactive Voice Response (IVR) services automate routine processes and transactions.<br><br>Huge advances in **imaging** and printing products are made with digitalization.<br><br>Publishing to the www becomes generally accessible. | **Government Performance and Results Act (GPR)** - required that agencies set strategic goals, measure performance toward those goals, and report on their progress. Effective implementation of the GPR hinges on agencies' ability to produce meaningfully integrated information to manage performance and measure results. (1993)<br>**Government Management Reform Act** - agenda to remedy the government's lack of useful, relevant, timely, and reliable financial information. (1994)<br>**Amendments to the PRA** - required 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. (1995)<br>**The Clinger-Cohen Act** - elevated former information resources manager positions to executive-level CIOs, who became accountable for: strategic IT functions such as developing architectures, managing portfolios, and measuring the performance of information technology investments. Among other things, the Clinger-Cohen Act also (1) required senior executive involvement in IT decision-making, (2) imposed much-needed discipline in acquiring and managing technology resources, (3) called for the redesign of inefficient work processes before investing in technology. (1996)<br>**Electronic Freedom of Information Act Amendments** (1996)<br>**HIPAA Act** with "administrative simplification" provisions that required the Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions. (1997) |
| **2003 – present** | |
| Information Technology becomes focused on management issues for reducing cost and complexity of systems.<br><br>**Wireless** technology becomes significant. | **E-Government Act** (2002) |

## Appendix C. Maine's IS Organizational Development

| State-Wide Information Services | | | State Agencies |
|---|---|---|---|
| organization | enterprise operations | agency services | |
| **1971 – 1976** | | | |
| The administrative unit, Central Computing Services (CCS), was established in The Bureau of Accounts and Controls under The Department of Finance and Administration. | Finance and Administration began depending on computer controls for financial risks; management focused on training human resources. | Planning Office, Finance and Administration, Maine State Retirement System, Lottery, Inland Fisheries and Game, and legislative tracking, were automated by CSS. | Many agencies develop their own administrative units for information management. |
| **1976 – 1987** | | | |
| CCS became the Bureau of Central Computing Services (BCCS) and the Computer Services Advisory Board (CSAB) was established. | First report on all data processing plans and activities (the enterprise) due; challenges to long-term planning a focus; change management system initiated to track performance issues.<br>Efforts are made to produce "standards" for departments and develop disaster recovery plans. | Produced large data processing applications for agencies.<br>Began migrating IS to new networking, database and teleprocessing techniques.<br>Connected agency management to email; mainframe upgraded; graphics capacity improved and report writing packages developed. | Agencies challenged to turn long lists of "data" into "information" for decision-making. |
| **1987 – 1992** | | | |
| The Office of Information Services (OIS), Bureau of Data Processing (BDP), Advisory Committee for State Telecommunications and the Policy Review Board were established. The BCCS and CSAB were dissolved. Division of Telecommunications added. Changed "Information Systems Division" into "Customer Service Division".<br>Service model, with BIS as one of many potential contractors to provide services to agencies heavily promoted. | Released report on strategic directions for mainframe and networking computers; developed security guidelines; worked on disaster recovery plans for agencies; first issue of statewide database management strategy released; OIS business plan completed. | Network security system installed; began GIS planning; developed MFASIS, Medicaid Claims Processing, MCJUSTIS and other applications. | OIS created technical management steering committee established to plan products and standards.<br>OIS conducted strategic planning with several agencies.<br>Proliferation of outsourcing became noteworthy. |

**Maine's IS Infrastructure Development** (continued)

| State-Wide Information Services | | State Agencies | |
|---|---|---|---|
| organization | enterprise operations | agency services | |
| **1992 – 1996** | | | |
| OIS and BDP reorganized into the Department of Data Processing (DDP) and the Bureau of Information Services (BIS). Moved GIS from Department of Conservation to DDP. Combined Operations Division and Network Control Services to create "Network and Computer Services" Division.<br>Attempted to use "Total Quality Management" (TQM) approach to extend the existing services model of consulting for agencies | Created inter-agency project teams to plan future IS directions.<br>Developed a disaster recovery planning guide for agencies to create their own plans.<br>Coordinated disparate agency systems to work with a central hub for email systems, e-government, and web presence. | Focused on the federally required "Family Assistance Management Information System" (FAMIS) that integrated service delivery and reporting on: Medicaid, Food Stamps, Welfare, Employment and Transitional Services.<br>Enabled the MFASIS data warehouse; expanded MCJUSTIS; began inmate phone system for prison; automated tax system, highway tolls and voicemail systems. | Agencies struggle with data storage issues and continue to outsource without enterprise framework.<br>Agencies demand relational databases; telecommunications and network connection.<br>Contracting increases as Agencies work to comply with new federal information security requirements. |
| **1996 – 2000** | | | |
| Established the Office of the CIO<br>DDP abolished and BIS organized into 3 Divisions. | InforME e-government project is launched and began winning multiple national awards for e-government.<br>Strategic plan for technology development released. | Began work to overhaul the financial system for Y2K compliance. Began processing school food vouchers over the internet; developed bar code reading capacity.<br>Developed call management systems for BMV.<br>Initiated an "enterprise-wide" helpdesk and telecommunications support services. | Focused on www development and technical upgrading. |
| **2001 - 2003** | | | |
| Office of the CIO was separated from DAFS/BIS.<br>Authority for policy was vested in the Information Systems Policy Board (ISPB). | | | |
| **2003 - present** | | | |
| Current Chief Information Officer (CIO) was appointed.<br>Governor's Executive Order merges BIS into the Office of the CIO, making this office accountable for statewide IS and IT infrastructure development. | IT governance and management plans released with steps to apply best practices to Maine's IT activities. Plans emphasize enterprise architecture, investment management and accountability.<br>CIO has the National Association of Chief Information Officers (NASCIO) evaluate Maine's IT operations to determine baseline in "Enterprise Architecture Maturity Model". | Wireless technology deployed. | Bureau of Motor Vehicles has a license renewal computer breakdown.<br>Department of Health and Human Services goes "live" with the new Medicaid Claims Management System (MECMS), which is highly unstable; CIO brought in to manage related contract service and implements a successful stabilization plan.<br>See OPEGA audit. |

## Appendix D. Key Excerpts from the CIO's Management Plan for 2004 – 2005

| Key Issues | Strategies |
|---|---|
| **IT governance** | |
| An enterprise must be well governed to be well managed.<br>• IT governance structure is weak; CIO's responsibilities extend beyond scope of authority.<br>• No defined processes for enterprise IT oversight.<br>• Funding and procurement mechanisms do not work in concert to facilitate enterprise IT management. | Merge the Office of the Chief Information Officer (CIO) with the Bureau of Information Services (BIS), creating the Office of Information Technology (OIT). This new governance structure will provide effective counsel to guide the enterprise forward, improve collaboration to begin to break down silos and provide the opportunity to better leverage IT investments across all levels of government; critical gains given the current fiscal environment and increased security concerns. |
| **IT strategies** | |
| • No cohesive enterprise IT strategy for achieving business objectives.<br>• Long-term planning incomplete for supporting rollout of enterprise initiatives.<br>• Enterprise IT investment not being managed as a portfolio.<br>• New and emerging technologies are being explored in an ad hoc manner while priorities, resource allocation, and trade-offs are being made in isolation.<br>• New pressures on old business processes. | • Actively foster shared applications development, use and maintenance.<br>• Consolidation and collaboration of IT services where appropriate in order to allow agencies to focus on their core missions.<br>• Implementation of the Portfolio Management Policy to improve planning within agencies.<br>• Enterprise oversight and review of department/agency portfolios to identify opportunities for collaboration and prioritize funding.<br>• Development of a method to measure value added for all new IT initiatives. |
| **IT Infrastructure** | |
| The growing pains experienced by agencies as they transition from local to shared infrastructure needs to be eased. This IT Management Plan will facilitate decision making and dispute resolution surrounding such issues as defining the shared infrastructure, how it should be paid for, and when its use is mandatory.<br>• Insufficient resource allocation to disaster recovery, security and business continuity planning.<br>• Ongoing maintenance and replacement requirements are not well funded; compete with new initiatives for funding.<br>• Infrastructure growth is not guided by a comprehensive enterprise plan that is tied to a business strategy.<br>• Infrastructure (networks/data centers) is fragmented and duplicative.<br>• Management practices and operational procedures are inconsistent. | • Undertake consolidation and modernization of the IT infrastructure under the OIT, in line with the strategic objectives and supported by an analysis of total cost vs. expected benefits.<br>• Review and update all infrastructure standards and policies.<br>• Develop best in class performance measurements and deploy them throughout all IT organizations for consistency in reporting.<br>• Build new funding model that will address required infrastructure maintenance upgrades and development.<br>• Review enterprise level opportunities such as email, procurement and desktops. |

## Appendix E Bibliography and Guidance

Specific criteria and industry best practices for internal controls, planning, and management of information technology (IT) investments:

2000 November
*Management of Federal Information Resources*, Office of Management and Budget (OMB) Circular A-130.

2000 July
*Preparing and Submitting Budget Estimates*, Office of Management and Budget (OMB) Circular A-11.

2000 May
*Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, GAO/AIMD-10.1.23.

1999 January
*Federal Information System Controls Audit Manual*, GAO United States General Accounting Office GAO/AIMD-12.19.6.

Best practices and key institutional management controls that facilitate operational change to results orientation and increased accountability:

2005 September
*Chief Information Officers Responsibilities and Information and Technology Governance at Leading Private-Sector Companies*, GAO-05-986.

2005 August
*IT Management Frameworks: A Foundation for Success*, National Association of State CIOs, Research Brief.

2003 April
*A Framework for Assessing and Improving Enterprise Architecture Management* (Version 1.1), GAO Executive Guide; GAO-03-584G.

2002 January
*Human Services Integration: Results Of A GAO Cosponsored Conference On Modernizing Information Systems*, GAO-02-121.

2001 October
*Human Capital: Attracting and Retaining a High-Quality Information Technology Workforce*, GAO-02-113T.

2001 February
*Maximizing the Success of Chief Information Officers: Learning From Leading Organizations*, GAO-01-376G.

2001, February
*A Practical Guide to Federal Enterprise Architecture*, Chief Information Officers Council, version 1.0.

2000 November
*Determining Performance and Accountability Challenges and High Risks*, GAO-01-159SP.

Resources recommended by the Customer Management Community (CRM)-Forum, an independent forum for CRM research conducted by private industry experts and consulting firms, including Deloitte Research and Gartner Group:

2003
*Issues of Knowledge Management in the Public Sector*, Xiaoming Cong and Kaushik V. Pandya, University of Luton, UK.

2001 August
*Managing Knowledge @ Work: An Overview of Knowledge Management*, Chief Information Officers Council.

2001 August
*Metrics Guide for Knowledge Management Initiatives*, Chief Information Officer, Department of the Navy.

2000 July
*GAO: Supporting Congress for the 21st Century*, GAO/T-OCG-00-10.

2000 March
*Efficient and Effective Government for the 21st Century*, GAO/T-OCG-00-9

Guidance and Tools:

2003 September
*The Federal Enterprise Architecture Program Management Office: How to Use the Performance Reference Model,* Version 1
http://www.whitehouse.gov/omb/egov/documents/How_to_PRM.PDF

2003 April
*Implementing the President's Management Agenda for E-Government,* E-Government Strategy,
http://www.whitehouse.gov/OMB/egov/2003egov_strat.pdf

2005 June
*Budget Justification and Reporting Requirements for Major IT Investments, Planning, Budgeting, Acquisition, and Management of Capital Assets,* OMB Circular No. A-11.
http://www.whitehouse.gov/omb/circulars/a11/current_year/s300.pdf

- reporting requirements for an agency's IT Investment Portfolio.
  http://www.whitehouse.gov/omb/circulars/a11/current_year/s53.pdf
- principles of budgeting for capital asset acquisitions.
  http://www.whitehouse.gov/omb/circulars/a11/current_year/app_j.pdf
- selected OMB guidance and other references regarding capital assets.
  http://www.whitehouse.gov/omb/circulars/a11/current_year/app_k.pdf

## Appendix F Acronyms

**AITD**
Agency IT Director

**BCCS**
Bureau of Central Computing Services

**BCP**
Business Continuity Planning

**BDP**
Bureau of Data Processing

**BIS**
Bureau of Information Services

**BMV**
Bureau of Motor Vehicles

**CCS**
Central Computing Services

**CIO**
Chief Information Officer

**CKO**
Chief Knowledge Officer

**CMC**
Customer Management Community

**COBIT**
Control Objectives for Information and Related Technologies

**COOP**
Continuity of Operations Plans

**CRM**
Customer Relationship Management

**CSAB**
Computer Services Advisory Board

**DAFS**
Department of Administrative and Financial Services

**DDP**
Department of Data Processing

**DHHS**
Department of Health and Human Services

**e-**
electronic-

**EA**
Enterprise Architecture

**EAMMF**
Enterprise Architecture Maturity Management Framework

**FAMIS**
Family Assistance Management Information System

**FOIA**
Freedom of Information Act

**GAO**
Government Accountability Office

**GIS**
Geographic Information System

**GOC**
Government Oversight Committee

**GPRA**
Government Performance and Results Act

**HIPAA**
Health Insurance Portability and Accountability Act

**IS**
Information System

**ISO**
International Organization for Standardization

**ISPB**
Information Services Policy Board

**IT**
Information Technology

**ITIM**
IT Investment Management

**IVR**
Interactive Voice Response

**JS**
Joint Standing

**JWI**
Jefferson Wells International

**KM**
Knowledge Management

**MCJUSTIS**
Maine Criminal Justice Information System

**MECMS**
Maine Claims Management System

**MFASIS**
Maine Financial & Administrative Statewide Information System

**NASCIO**
National Association of State Chief Information Officers

**OCIO**
Office of the Chief Information Officer

**OIS**
Office of Information Services

**OIT**
Office of Information Technology

**OMB**
Office of Management and Budget

**OPEGA**
Office of Program Evaluation & Government Accountability

**PM**
Project Management

**PMO**
Project Management Office

**PRA**
Paperwork Reduction Act

**SLDC**
System Development Life Cycle

**TANF**
Temporary Assistance to Needy Families

**TQM**
Total Quality Management

**www**
World Wide Web

**Y2K**
Year 2000