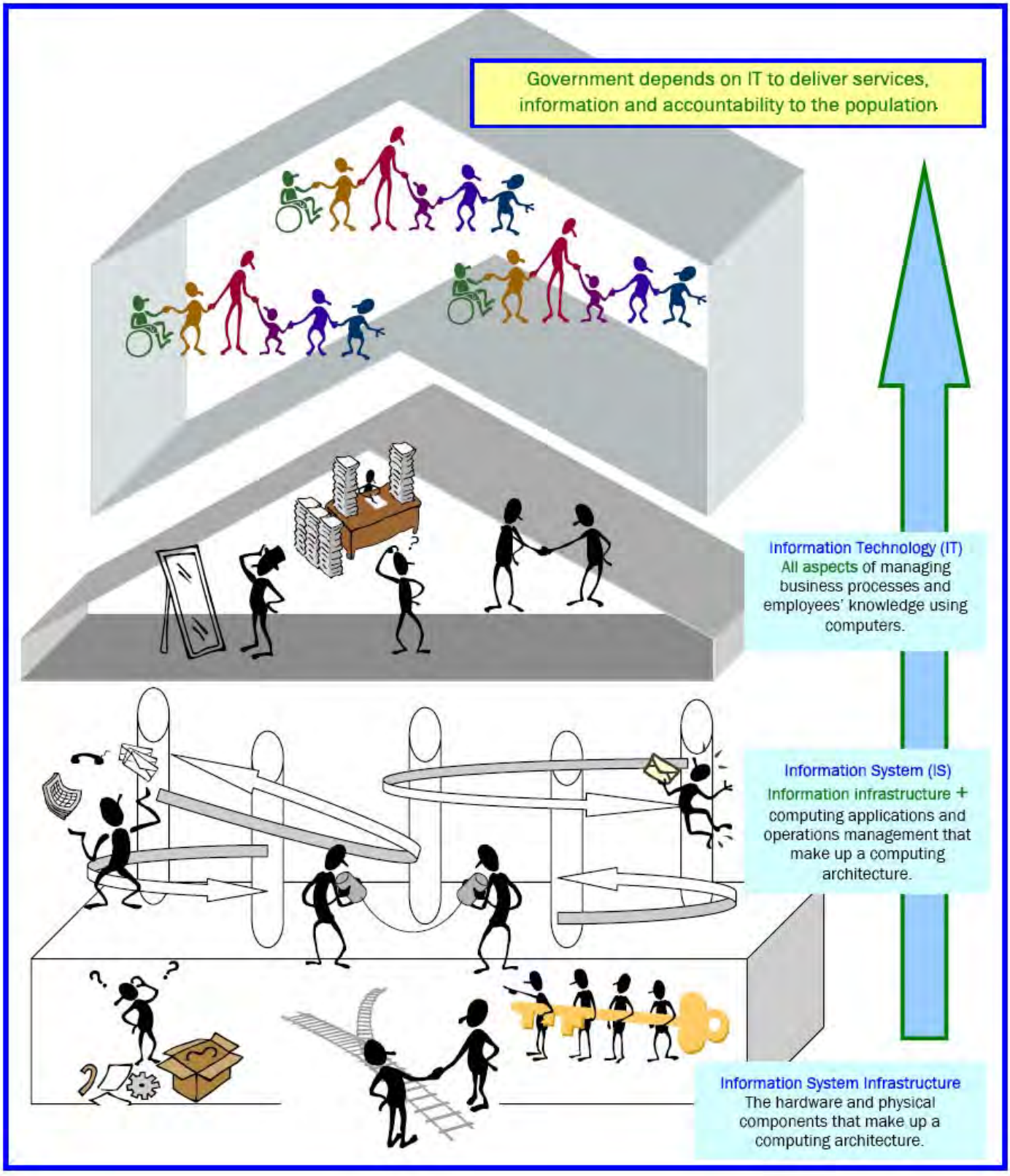
OPEGA
Guidance

Legislative
Oversight
Guide

Statewide Planning and Management of Information Technology

Guide No. IS-01-06

December
2006


Government depends on IT to deliver services, information and accountability to the population
Information Technology (IT)
All aspects of managing business processes and employees' knowledge using computers.
Information System (IS)
Information infrastructure + computing applications and operations management that make up a computing architecture.
Information System Infrastructure
The hardware and physical components that make up a computing architecture.

Introduction

Information technology (IT) forms the foundation of 21st century government operations and policy development. It underlies government's ability to:

- deliver services;
- assimilate and share knowledge;
- manage finances and other resources;
- direct and monitor program performance;
- report transparently to the public for democratic decision-making; and
- maintain public trust by virtue of authentic accountability.

The State of Maine's Executive Branch has historically planned and managed IT in a fragmented and uncoordinated manner. This situation is not financially or operationally tenable. Examples of the consequences of Maine's fragmented IT planning and management are[1]:

- costly failures in new systems implementations;
- expensive retrofitting of new systems due to lack of proper planning and safeguards in the early stages of system design;
- significant lost opportunities for deep vendor discounts and synergistic investment;
- undesirable levels of exposure to security and business continuity risks;
- inability to account for IT expenditures;
- underutilized and often unreliable data and information;
- employees struggling to do their jobs while hampered by out-dated or problematic systems; and
- an IT culture of "operational expediency."

An organizational transformation began in 2005 with the establishment of the Office of Information Technology (OIT), putting Maine in a strong position to benefit from an enterprise approach to IT planning and management. This approach has two major objectives. The first is to treat IT as a major capital asset for strategic investment. Since the year 2000, Maine has spent more that $500 million on IT and cannot give an account of return on this investment. The second is to maximize the return on IT investment by increasing systems interoperability and data compatibility. The goal is to develop a financially sound system that processes high quality information for service delivery, management decision making, and accountability.

Systems Interoperability: the electronic capability of systems to work together.

Data Compatibility: the ability to relate data from different systems based on common definitions and coding.

During a performance audit of Statewide Planning and Management of Information Technology, the Office of Program Evaluation and Government Accountability (OPEGA) identified a number of areas presenting significant risks related to the IT transformation. A key observation OPEGA offered was the need for strong leadership from the Executive Branch and equally strong oversight from the Legislative Branch as OIT moves forward.

[1] Other driving factors are insufficient and inconsistent levels of funding, and considerable complexity due to dedicated funding of federal programs.

The Legislature has responded by assigning primary oversight of Statewide IT, including the Office of Information Technology, to the Joint Standing Committee (JSC) on State and Local Government – a JSC versed in Maine's processes for managing large capital assets. All legislative committees, however, have some degree of oversight responsibility in this area as the Departments under their jurisdictions utilize and implement new technologies.

Summarized in this *Legislative Oversight Guide for Information Technology* are areas that warrant the Legislature's focused attention over the next few years. The *Guide* does not include all topic areas, nor complete coverage of any particular topic. Instead, it is meant to assist the State and Local Government Committee, and all legislators, in quickly becoming familiar with immediate oversight needs, as they develop deeper familiarity with all of the issues.

For specific topic areas, this *Guide* offers:

- Discussion – that provides background information, describes challenges and risks, and notes management actions underway that need support and oversight.
- Key Questions – that legislators in oversight roles should consider asking.

For a deeper understanding of these and other topics, legislators can refer to the full OPEGA report on *Statewide Planning and Management of Information Technology* that was issued in January 2006. The report is available on OPEGA's website at www.maine.gov/legis/opega or can be obtained by contacting OPEGA at (207) 287-1901. Copies are also available in the Law and Legislative Reference Library. Other documents of interest are listed below.

Key Documents:

2006 February
The New Enterprise Office of Information Technology, OIT's 2005 Annual Report.

2005 May
CIO Memorandum to All Commissioners: IT Restructuring.

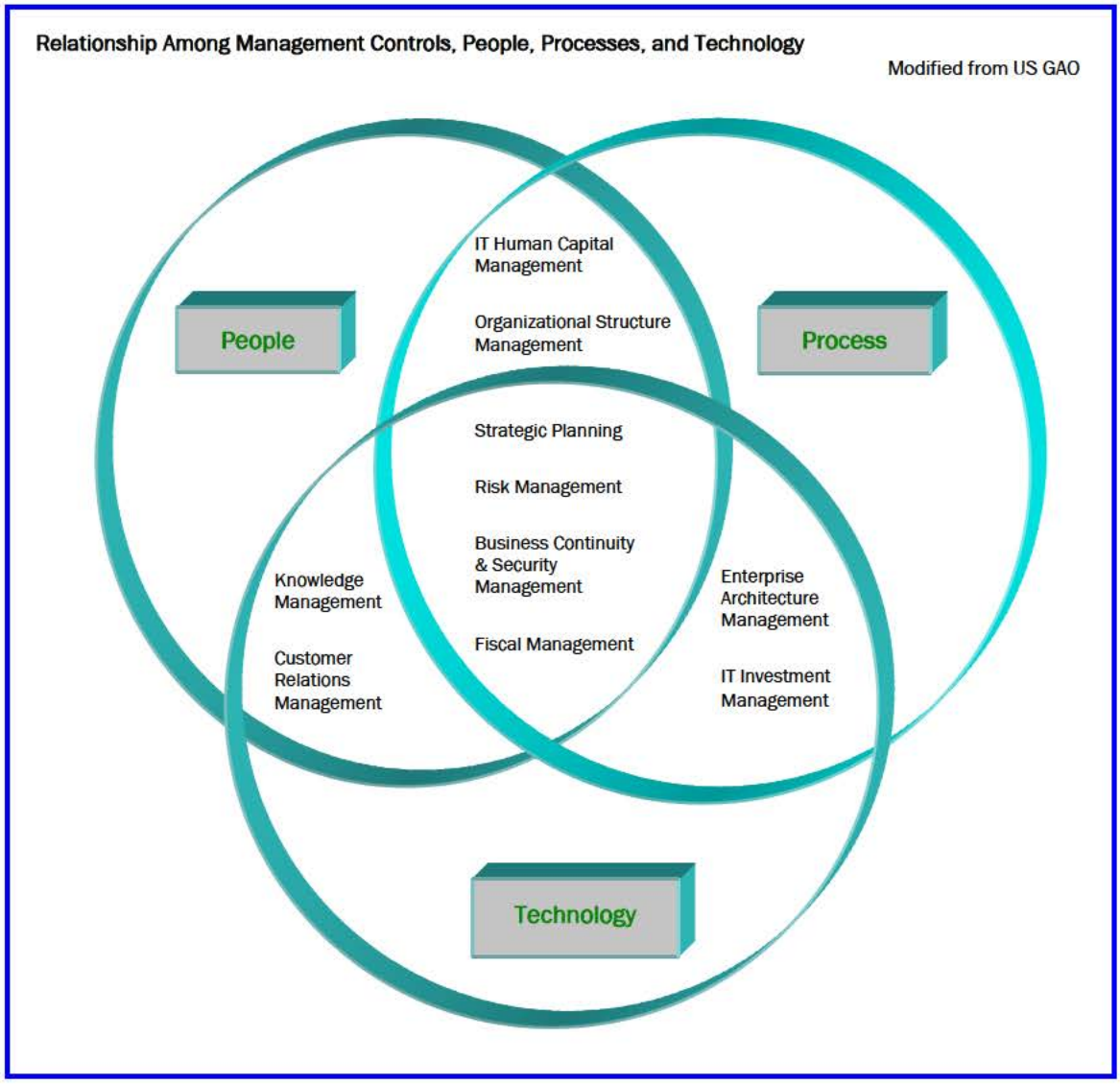
2005 January
Governor's Executive Order: *An Order Concerning Effective Application of Information Technology*.

2004
Maine's CIO's IT Management Plan.

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

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

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 the figure below.



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. The following table describes Maine's current status with respect to these core areas of focus.

High-Level Management Controls

largely underway	observable progress made using explicit strategies
underway but unstable	implementation strategies modified based on testing and feedback
very early stages	planning and testing possible strategies
aware but not yet underway	action pending other priorities
area of concern	progress is hindered by resistance to change, system complexity, and/or resource limitations

Institutional Practice	Definition	IT Current Status
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
Strategic Planning	establishing the agency's mission and vision, including core values, goals, and approaches/strategies for achieving the goals	underway but unstable
Organizational Structure Management	aligning operational responsibilities with business and mission goals and objectives, and maintaining an accountability framework	underway but unstable
Risk Management	addressing potential events or situations that threaten the successful achievement of organizational objectives	very early stages
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
IT Investment Management	selecting and controlling IT spending so as to maximize return on investment and minimize risk	aware but not yet underway
Customer Relations Management	focusing an organization's operations on how to best satisfy customer needs	area of concern
Fiscal Management	budget formulation and execution, financial control and acquisition that enables an organization to track its use of material resources	area of concern
Enterprise Architecture Management	developing, maintaining, and using an explicit blueprint for operational and technological change	area of concern
Knowledge Management	capturing, understanding, and using the collective body of information and intellect within an organization to accomplish its mission	area of concern

As the Office of Information Technology (OIT) transforms the State of Maine's IT into a true enterprise, they must unravel extensive tangles of expedient and cost-compromised "fixes" that make up existing systems within each individual Department. OIT must reach core IT elements that need to be integrated, and processes that need to be aligned. Unraveling the undocumented systems that currently support the Executive Branch will be time consuming and unavoidably disruptive to operations.

Organizational resistance to the significant changes accompanying transformation to an enterprise approach is typical and expected. Supporting OIT with resources and leadership will be critical as that organizational resistance continues to challenge the Executive and Legislative Branches' ability to persevere and achieve long-term benefits. Organizational resistance is expressed in many ways. Key expressions for the Legislature to be on the alert for include:

- **OIT adds an unnecessary layer of administrative overhead.**

  Actually, the costs of administrative overhead may be reducible in the long run, once the existing disorder is resolved; but until then, the work of transforming into an enterprise must be heavily managed and administered. Shortcuts here will

undermine success, and failure at this stage will prohibit another attempt in the near future. Maine cannot afford to disinvest in the enterprise transformation.

- **OIT is charging us more to do work that we can do ourselves for less.**

  OIT is actually exposing the many hidden costs that have not been transparent to Departments (or anyone else) in the past. Additionally, no baseline exists for past IT expenditures, meaning there is no way to validate the perspective that IT is costing more than it did before. Also, allowing Departments to "do it themselves" is how the current situation developed. While individual Departments may be able to meet their own IT needs more cheaply in the short-term, results of that approach have been costly to the State as a whole.

  The perception, however, that OIT is costing Departments more means that Departments may seek work-arounds to avoid OIT related costs and OIT involvement in projects. For example, a policy exists requiring that all IT expenditures over $250,000 be reviewed by OIT. There is high risk that Executive Branch Departments, accustomed to solving their IT needs in an expedient, cheap, ad hoc manner will parse up projects into components that each cost less than $250,000 dollars, in order avoid OIT's review processes. However, these projects quickly add up – it only takes four such projects to spend a million dollars – and can lead to non-strategic investments and poor project management, as they have in the past. (See the Investment and Project Management sections of this Guide).

- **OIT has taken the best people out of the Department, the ones who know how to keep things up and running, and is not providing adequate support.**

  This statement may be true, but the appropriate response is not to return to the past arrangement. Because existing information technologies in the Departments are not documented, the State is dependent on crucial knowledge residing in the minds of certain individuals. It is incumbent upon OIT to rely on these individuals to successfully transform to an enterprise, and capture the knowledge that is currently isolated and vulnerable.

  The better response is to focus instead on how to continually improve OIT's Customer Support. OIT does need to prioritize Departmental needs, and rework customer support approaches so that operations experience maximum support and the least amount of disruption possible. Nevertheless, a certain amount of disruption is inevitable as OIT becomes firmly established. Continuing improvement in Customer Support should be expected.

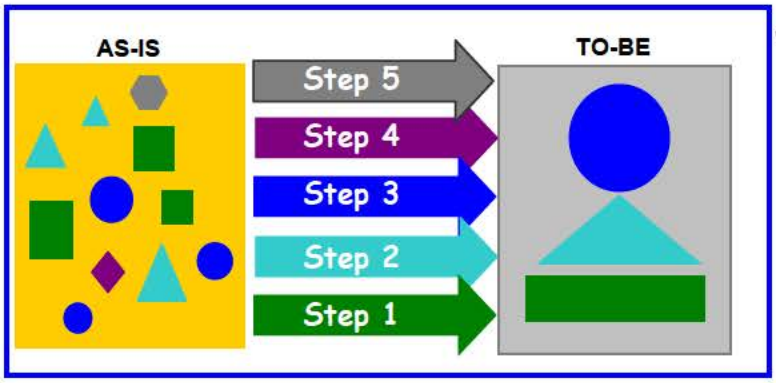
- **The cost of changing is too high. OIT is already over budget.**

  Actually, the opportunity cost of not changing is far higher. The evolution of IT across the State, left to continue on its historic path, presents greater risks than the State can tolerate. The true cost of the transformation to an enterprise cannot accurately be predicted. In certain ways the IT transformation is akin to rehabilitating an old New England farmhouse (that has been added onto, room by room, over generations), into an energy-efficient, structurally sound, community center that has the potential to grow in the future. Like the old farmhouse, each restorative change exposes unanticipated challenges. But unlike the old farmhouse, tearing it down and starting anew is not an option.

Enterprise Architecture (EA) Management & Knowledge Management

Discussion

- Enterprise Architecture refers to an organizational blueprint that defines – in business terms and in technology terms – how an organization as a whole: (a) operates today, (b) intends to operate in the future, and (c) intends to invest in technology to transition to that future state. Maine is in the early stages of developing an enterprise architecture to guide IT development.



- In April of 2006, OIT began developing a plan and schedule for completing a picture, or map, describing the "as is" and "to be" environments of the enterprise. OIT was then planning to articulate the steps for transitioning to the desired future state, and metrics for measuring enterprise architecture progress, quality, compliance, and return on investment.

- The seemingly overwhelming and resource-intensive task of documenting Maine's "as-is" IT state is a prominent barrier to future progress. The goal of producing an EA is currently being threatened by the need to keep Departmental IT experts available to help end-users. Only certain individuals know enough about how undocumented Departmental systems operate to keep them running. These same people are required for EA development. Because EA underpins the entire IT transformation, OIT is strategizing how to transfer knowledge for end-user support to help desk personnel before turning full attention to the EA. For a period of time Departmental IT experts will overlap with end-user support – an unavoidable cost. In the long run, these experts will be able to focus on engineering larger gains in efficiency by aligning technology and business processes across the State. Consequently, a first oversight priority may be to follow up on OIT's strategy to accomplish this task.
- Knowledge Management refers to an organization's activities to capture, understand, and apply the collective body of information and intellect within an organization to accomplish its mission. It is closely aligned with EA management, because both focus on systematically identifying an organization's information sharing needs. Done well, employees across the state will easily be able to leverage one another's expertise, and statewide information will be available by geographic, demographic, economic, and environmental groupings.
- OIT's Technology Exchange Forum formed a Data Dictionary Subcommittee in September of 2006. This Knowledge Management committee will create a set of recommendations for more effective and efficient future data exchanges.

Key Questions

- Q How is OIT progressing in terms of finding new end-user support so that Department IT experts can be available for EA development?
- Q How will progress in EA development be reported to the Legislature?
- Q What are the State's high priority data exchange needs? How is the work of the Data Dictionary Subcommittee progressing?

Investment Management

Discussion

- Investment Management refers to selecting and controlling IT spending to maximize return on investment (ROI) and minimize financial risk. Historically, Maine has not treated IT as a set of major capital assets requiring disciplined investment management. Instead, Maine's fragmented method of financing IT and capturing related expenditures has diluted asset management, governmental control, and accountability, without creating economic efficiencies.
- Historically, accounting structures and practices have not allowed the Executive Branch or the Legislature a clear view of IT budgets and expenditures across the State as a whole, or by any specific Department, program, or statute. IT budgets, appropriations, and expenditures have been treated as components that support separate programs in the various Departments. This has hindered the State's ability to effectively manage IT investments on an enterprise-wide basis. The CIO is now working with the State Controller and State Budget Officer to modify the use of account code structures to enable full capture and reporting of Executive Branch IT budgets and expenditures.
- OIT has developed a rate structure that reflects actual costs, and a process to bill for services they provide to agencies. This is a nexus of organizational resistance to the enterprise transformation because it requires Departments to plan for IT needs and account for previously hidden costs they are not yet accustomed to managing. The Legislature may want to focus oversight on this resistance to ensure OIT's success in accomplishing this critical change.
- OIT has formed a Portfolio Review Committee (PRC) to evaluate major projects prior to their inception for project risk, strategic alignment, and sound business investment criteria. All proposed or requested capital investments in Executive Branch IT, estimated to exceed $250,000, are supposed to be reviewed and approved by the PRC before moving forward. OIT intends to use the Enterprise Architecture to guide investment decisions and allow the enterprise to leverage its resources.

Key Questions

- Is OIT able to clearly articulate Statewide IT expenditures? What are they? Are there projections for future expenditures? How will OIT track expenditure trends?
- How is OIT managing costs for IT services within each Executive Branch Department? What is the current rate structure? How will the structure be reviewed and updated? How frequently?
- Are Executive Branch Departments bringing proposed and requested capital investments in IT to OIT's PRC? What controls are in place to ensure that this happens?
- What is the criteria OIT's PRC uses when making investment decisions? How is it updated? How will the Legislature know when it has been updated?
- How is OIT tracking ROI and reporting ROI to the Legislature?
- How is OIT making investment decisions when a thorough enterprise architecture is not yet in place?
- How will IT projects under $250,000 be controlled to assure project risks are minimized and investments make sense?

Project Management

Discussion

- 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. The need for strong project management has often gone unrecognized, resulting in inadequate efforts to build strong IT project management skills within agencies, or to assure that those individuals assigned as IT project managers have strong IT project management capabilities. Similarly, IT project management capabilities have not always received proper consideration when selecting vendors to contract for IT projects.
- A formal Project Management Office (PMO), under the new OIT, aims to improve the quality and depth of project management (PM) and reduce the risks associated with large development projects and system implementations. The new PMO has been educating OIT staff in new PM methods and the consequences of poor PM. Department and PMO staff, managing significant IT projects, must now successfully complete training in the adopted Ten-Step method that OIT provides quarterly.
- Through the portfolio review process (described in the previous section), OIT will identify PM needs for large system projects. It remains unclear what criteria will be used to determine PM needs for particular projects, or how those needs will be met.
- Since only projects that are proposed to cost more than $250,000 dollars are going to the Portfolio Review Committee, it is unclear how strong project management for endeavors under $250,000 will be assured.
- OIT has assigned Agency[2] IT Directors, who report to OIT, to be responsible for assessing IT contracts with vendors and monitoring vendor progress. However, OIT's objectives to assure quality project management may conflict with the need to minimize costs faced by Departments funding IT initiatives.

Key Questions

- Is the capacity for OIT to provide PM improving? Are resources adequate to fulfill training needs?
- What projects is the new PMO supporting at this time?
- Is OIT tracking all current projects? Does OIT have adequate resources to monitor them all?
- What IT contracts is OIT overseeing? Who is monitoring PM on these contracts?
- How is PM adequacy being monitored on projects that cost less than $250,000?
- How is the Legislature being kept apprised of progress on IT projects in various Departments?
- What institutional practices are in place to regularly monitor and audit the State's PM capabilities?

[2] "Agency" here refers to Departments.

Risk Management – Security – Business Continuity

Discussion

- Historically, Maine State leaders have not employed a risk management approach to making IT decisions, whether those decisions are related to IS infrastructure investments or to specific IT projects. It is essential that State leaders recognize the high-risk nature of IT and actively engage in managing IT risks by regularly performing risk assessments and establishing cost effective controls. OIT plans to include a risk assessment component in their Portfolio Review Process.
- OPEGA's audit of Statewide IT Planning and Management included a baseline risk assessment of Maine's IT environment. The audit determined that: only 1% of the IT environment was highly controlled; only 11% had a satisfactory (medium) level of control; and the remaining 88% had an undesirable (low) level of control. At the conclusion of the audit, OPEGA provided the CIO with a recommended 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 was engaged in strengthening risk management prior to OPEGA's audit and responded to the audit by committing to constructing a risk management plan that builds on OPEGA's work, mitigates or eliminates priority risks, and measures the effectiveness of OIT's risk management process. OIT also committed to implementing an on-going internal audit process to measure the effectiveness of established risk management procedures and controls. Currently, OIT claims that resources are too constrained to maintain an ongoing internal audit function. The Legislature may want to carefully consider this situation. It is highly unconventional for a large IT operation not to be subjected to regular internal audits.
- The OPEGA audit identified high priority areas of risk, and with OIT, identified actions to remedy inadequacies. These included security controls to reduce the risk of loss or damage to the IS infrastructure, the applications it supports and the data that resides in those applications. It also included business continuity plans (BCPs) that prescribe how the enterprise, and each Department within it, will continue to perform critical functions and provide needed services if, indeed, the infrastructure, applications, and/or data are not available for extended periods of time.
- OIT has agreed to consolidate Departmental IT security policies into a single policy based on the National Institute for Standards and Technology (NIST) as specified in the Federal Information Security Management Act (FISMA) and the Health Insurance Portability and Accountability Act (HIPAA). The timeframe for implementing this important work is currently unclear. Because Departmental IT systems are not documented, security assessment must be performed on each system before a plan for upgrade and alignment can be determined.

Key Questions

- What are the current information security high priority issues?
- Does OIT have plans in place to devise a clear and uniform set of security policies and procedures for the enterprise? How will the policy be implemented?
- What are the statuses of the BCP plans?
- What are the statuses of disaster recovery plans?
- How is risk management handled in the portfolio review process? How can we be assured that this risk management strategy is working effectively?
- When is the next risk assessment and IT audit scheduled to take place? How will the results be reported to the Legislature?
- Are OIT's risk management efforts adequately resourced?