W-5 Readings and Notes

- *Planning for Public Information Systems*

  As Rose (2005) has pointed out, the fragmentation inherent in American federalism does constitute an obstacle to planning for integrated e-government services at a national level and, as a corollary, for innovations in e-governance often to arise in smaller countries from Estonia to Singapore, where this obstacle does not exist. Before we can discuss the different IT planning processes, it is important to discuss the individuals typically charged with leading IT planning processes – Chief Information Officers (CIOs).

  Federal CIO

  The Chief Information Officer role became widespread under the "Reinventing Government" initiatives of the 1990s. The vision of the CIO position is that this officer would report directly to the department head and play an inner-circle role in departmental planning. Since 1998 the OMB and CIO Council have issued an annual strategic plan that sets goals, objectives, and targets for IT. CIOs must accept the mandated federal enterprise architecture for IT, as prescribed by OMB, or suffer budgetary consequences. The average tenure for a CIO since 2004 has declined to 2 years.

  Assessing the Federal CIO role a decade after Clinger-Cohen

  A 2006 forum sponsored by the Professional Services Council brought to light numerous criticisms of the implementation of the Clinger-Cohen Act of 1996. Speaking at the forum, William Cohen, a co-author of the Act, lamented that ten years later, the power of federal CIOs is still not respected and understood. Some at the forum attributed this to the fact that CIOs often rose from technical ranks and were not well-prepared to take on strategic leadership roles. Others noted that rather than being accepted into the inner leadership policy-making circle along with departmental chief financial officers, CIOs instead have tended to be looked upon narrowly, as the person who runs the local area network and making sure e-mail works (Miller, 2006n). There was little talk at the forum about how the OMB has eclipsed the CIO Council created by Clinger-Cohen, but the pessimism at the 2006 re-assessment of the Clinger-Cohen Act was a clear indication that the original vision had fallen well short in the view of CIOs themselves.

  Collaboration skills top role requirements

  There is increasing recognition that CIOs and even program managers need "people skills" even more than technical skills. John Sindelar, acting associate administrator of GSA's Office of Government-wide Policy, noted at a 2006 conference of federal executives that future managers would need collaboration skills more than ever in a government more reliant on networking. Specifically, with consolidated LOB (Lines-of-Business) enterprise software being emphasized by OMB and the Bush administration, who noted that would-be managers of such projects are ruled out if there had been a record of past collaboration

problems. Sindelar called on government to alter civil service laws to support and require skills in knowledge sharing and flexible collaboration (Kash, 2006b).

State-level CIOs

For over a decade, the National Association of State Chief Information Officers (NASCIO) promoted the concept that the state CIO position should be at the cabinet level, reporting directly to the governor. In Arkansas, California, Indiana, North Carolina, New Mexico, Ohio, and West Virginia, changes were made in 2004-2005 period to have the CIO report to the governor. In this context, it is perhaps surprising to some that in 2005, NASCIO reversed its stand, ceasing to favor gubernatorial direct reporting by the CIO. The central problem which had emerged was that cabinet status brought politicization to the office of the CIO, even to the extent of their forced turnover (like other cabinet positions) when elections brought in new governors. Several state CIOs left office after the 2004 elections. Rethinking organizational structure, in 2004-2005, Iowa, Wisconsin, Kentucky, and Nebraska switched from gubernatorial reporting for the CIO to departmental reporting, and Virginia switched to reporting to an IT investment board (Peterson, 2005). Many state-level CIOs now believe that greater stability and control may be achieved without cabinet-level political status. Currently, about 50 percent of state CIOs are considered Cabinet-level, but about 30 percent report directly to their Governor.

Planning Mandates: The Federal Enterprise Architecture (FEA)

The key document for federal enterprise architecture policy was a 2000 revision of OMB Circular A-130. This revision required all federal agencies to submit an enterprise architecture (EA) document in conjunction with capital planning, IT investments, and related matters. The document required coverage in five areas:

- A business reference model
- Information of business process flows
- Description of software applications for processing information
- The data model for agency information systems
- A description of the agency's technology infrastructure

The objective of the EA initiative was to make inter-departmental information transfer more compatible and efficient, to encourage multiple re-use of IT data and application resources, and to improve security levels. It was also expected that IT under EA would become more scalable and thus new systems might be integrated more economically.

The ultimate purpose of the FEA is to achieve cost savings and performance efficiencies. For instance, the Interior Department used its enterprise architecture (EA) analysis to group programs performing similar functions for similar lines of business, and then identified over 100 programs as "redundant" (Jackson, 2006e). This conformed to the OMB's directive to use EA to identify cost savings.

The Data Reference Model

Creating common data definitions across federal agencies proved a daunting task. In 2004, the initial Data Reference Model (DRM) was met at the agency level with considerable resistance and/or indifference as managers reported difficulty seeing how it could be used to define data in specific agency contexts. Seeking to meet a Dec. 17, 2005 deadline established by the E-Government Act of 2002, the CIO Council, at the behest of the Office of Management and Budget, created DRM Version 2.0 at the end of 2005. The main innovation was heavy use of an Extensible Markup Language (XML) schema for data description. The Council hoped the Version 2.0 would usher in a new era of federal-level data sharing, continuing to cite Recreation One-Stop as a poster child for use of the system (Thormeyer, 2005f). However, even though the new DRM version provided five levels of data definition specificity, acknowledged not all levels would be needed for any given agency, and failed to spell out which levels would be compulsory and which optional, it remained an open question whether the new DRM would actually promote data integration and sharing or merely be an additional OMB-generated paperwork hoop for agency-level CIOs to have to jump through. Some even called the new version a "step backward" toward even greater agency discretion over data definitions and formats. Optimists cited it as a more flexible set of tools to promote data interchange.

Federal Transition Framework (2006): OMB Seeks to "Facilitate" Centralization

In 2006, Richard Burk, chief architect for the OMB, described to a reporter how enterprise architecture would be used in the future. The intent, he noted, could be seen by agencies using enterprise architecture more and as a result spending less of their discretionary budgets on IT. The OMB's Federal Transition Framework (FTF), released in July 2006, was intended to enforce a standard way for agencies to describe and share information about cross-agency IT initiatives promoted by the OMB. By September, 2006, some 15 cross-agency initiatives were promoted in the FTF catalog. Starting with FY 2009 agency budget submissions, agencies would have to use the FTF to describe their IT efforts. The purpose, Burk states, was to find a way to "facilitate" agency adoption of cross-agency IT initiatives, long a goal of the OMB, which had become increasingly hostile in the last decade to single agency owned systems tailored to agency needs. A "strong enterprise architecture" was one which demonstrated close acceptance of the cross-agency initiatives in the FTF catalog, and agencies not demonstrating such close acceptance were "immature" in terms of their enterprise architectures, in the language of the OMB (Miller, 2006k).

Strategic Planning

Strategic planning is seen within government as a solution to the problem of massive IT failures For instance, in early 2006 a GAO report criticized the Defense Department's Global Information Grid (GIG) project, a massive attempt to weld a variety of programs and systems, including communications satellites and next-generation radio, into an Internet-like, but secure, worldwide network. The GAO found GIG was "being managed in a stove piped and bungled manner" (Onley, 2006a), with no one ultimately accountable in spite of its estimated cost of $34 billion over five years. The GAO predicted that decentralized management would lead to interoperability problems, which have plagued DoD in the past. The GAO called for creation of an office of Deputy Secretary of Defense for

Management, to oversee strategic planning and enterprise architecture development as well as information technology and financial management within DoD.

Strategic planning for IT takes many shapes and forms, Garson (2007) suggests seven steps:

1. Creating a planning structure
2. Auditing information systems
3. Defining goals
4. Evaluating proposals
5. Composing annual plans
6. Obtaining administrative and political approval
7. Implementing the plan, evaluating outcomes, revising the plan

Further, GAO has identified 24 specific agency practices to evaluate planning.

Standardizing Federal Strategic Planning

In early 2006, the CIO Council was considering methods to standardize strategic planning throughout the federal government. The vehicle for accomplishing this would be the Strategic Markup Language (StratML), developed by the CIO Council's XML Community of Practice. Since its inception, StratML has grown and now has three parts (http://xml.fido.gov/stratml/), the most recent signed by President Obama in May 2013. Adopted by the Chief Financial Officer's Council, which represents the federal officials most often responsible for developing agency strategic plans, the purpose of StratML is to identify and enforce the use of common terminology across all federal strategic plans, securing agreement on such terms as mission, vision, values, goals, and stakeholders.

Use of StratML helps to eliminate inter-agency inconsistencies, such as one agency issuing "strategic vision" statements and another issuing a "strategic plan." Moreover, StratML helps to assure agencies conform to the OMB's Federal Enterprise Architecture when issuing planning documents in compliance with information resource management objectives required by the EGovernment Act of 2002. StratML was expanded to enforce common terminology with regard to planning documents required by the Government Performance and Results Act of 1993 (Jackson, 2006b).

Strategic Planning and the Federal Budget

Strategic planning is enforced through the requirement that agencies submit their budgets to the President via the Office of Management and Budget, using OMB forms which specify such things as reporting conformity to the Federal Enterprise Architecture.

Enterprise Resource Planning: Background

Enterprise resource planning systems, after a checkered start in the private sector in the late 1980s and early 1990s, were widely adopted in the public sector in the late 1990s. By the 2000s, transition from agency-specific to enterprise software was the primary reform thrust of the U.S. Office of Management and Budget as well as of many states and

localities. Efforts were made to unify financial, human resources, payroll, procurement and other departmental software systems into single jurisdiction-wide systems. Enterprise software offered three central promises:

- That enterprise-wide software systems would be less expensive than multiple departmental systems.
- That consolidation of databases would improve management decision-making.
- That reliance on large ERP software vendors would assure critical systems remained state of the art, never obsolete.

Where ERP was sometimes seen as a relative failure when first introduced, by the mid-2000s it had grown into a $100 billion industry with many public sector jurisdictions at all levels reliant upon it. Enterprise resource planning originated in the private sector to consolidate financial, HR, and other systems into a supersystem which would supposedly save costs. Initial efforts often were not highly successful in the private sector. Despite this, a number of states and cities have applied ERP with varied success. For example, Florida became a leader in ERP with its efforts to replace legacy systems. However, salaries were cut to pay the contractor for the new system. It is debatable if there are actual savings.

A prominent example of state-level ERP was that completed by the Commonwealth of Pennsylvania in 2005, integrating database applications across 50 state agencies. Taking three years and $140 million to complete, the project is commonly cited as an on-time, on-budget success story delivering almost immediate reductions in payroll processing and other transaction costs (Wagner and Antonucci, 2004).

Enterprise Resource Planning Problems and Failures

In March 2006, the Government Accountability Office issued a report, Financial Management Systems: Additional Efforts Needed to Address Key Causes of Modernization Failures. Evaluating ERP efforts in the IRS, Defense Department, and elsewhere, the GAO found continuing problems in ERP requirements management, testing, data conversion, system interfaces, and risk and project management. The report came after widespread publicity about over-budget, behind-schedule ERP projects from vendors such as CGIAMS, Oracle Corporation, and SAP America Inc.

ERP problems are illustrated by the following quotation from Government Computer News illustrates:
“The graveyard of failed enterprise resource planning projects is littered with critical analyses by the Government Accountability Office and agencies' inspectors general. From the Veterans Affairs Department's late, lamented Core Financial and Logistics System to the Interior Department's bungled Financial and Business Management System, agency officials have spent plenty of time explaining to Congress and the public why millions of dollars were wasted on yet another doomed project” (Government Computer News, 2006c).

Like the private sector before it, the public sector has found that ERP is not a panacea. While experiences vary greatly, it can be noted that the three ERP promises are mirrored by three ERP problems (Kavanagh and Miranda, 2005):

Purchase of ERP systems, while expensive, can be overshadowed five times over by costs of contract maintenance and services. Evidence for improved decision-making is spotty at best, with many public managers reliant on agency-specific data systems and specialized business intelligence software not part of ERP systems. Even where ERP systems are relied upon, it is primarily to consolidate departmental data silos without much transformation of underlying business processes. Instability in the ERP industry has left public managers wondering whether it is wise to put all one's eggs in a single vendor partnership.

Moreover, ERP problems and failures are not uncommon in government. In 2005, a General Accounting Office report faulted the NAVY for wasting $1 billion on four different ERP systems which were redundant, incompatible, and did not meet Navy specifications (Songini, 2005a). For its part, the Navy at this writing claimed that problems of system integration would be solved if they were given 6 additional years, to 2011.

Problems of ERP stability are illustrated by Cook County, Illinois (Chicago), which in 1999 opted for ERP software from J. D. Edwards, Inc., which was later bought out by PeopleSoft, which required expensive upgrades to prevent obsolescence. Peoplesoft was then bought out in 2004 by Oracle Corporation, causing Cook County to consider if it could afford Oracle's upgrade price tag. The initial commitment to ERP had proved to be a slide from one set of cost-benefit calculations to a much different one. Moreover, as Scott Dulman, director of Worldwide Government Marketing for Business Objects noted, "After investing millions of dollars to optimize their business processes, many governments are finding that ERP alone can't do the job" (quoted in (Kavanagh and Miranda, 2005: 39). Business Objects is a system to integrate data from multiple ERP systems as well as agency-specific systems, so public managers can obtain the kind of timely information originally promised by ERP systems alone.

A second example of the difficulties of creating a successful ERP system is illustrated by the Interior Department's Financial Business Modernization System. After two years of work, Interior cancelled its contract with BearingPoint, Inc., which in turn sued Interior for breach of contract. Among the problems were difficulties with field offices linked by satellite or dial-up connections, the need for infrastructure upgrades to run the software, and the resistance of field offices to a centralized financial system (Dizard, 2006o).

Public-sector ERP projects have upfront costs ranging from $10 to $500 million (Perlman, 2005). However, this is the tip of the ERP iceberg. Customization, consultants, data conversion, training, testing, maintenance, and other costs can easily be greater, even ten times greater, than the initial systems outlay. Return on investment can often take years (Minahan, 1998: 120; Koch, 2002) and productivity can go down, not up, when ERP is implemented (Robb, 2004),

Causes of ERP Problems

The enterprise-wide ERP approach is one of one-size-fits-all software consolidation. As such it was the main thrust of President Bush's Management Agenda under the OMB. It had come under increasing criticism not only from federal unions, but also from Congress. Some members of Congress reportedly gave credibility to departmental feedback that the ERP "initiatives shut down perfectly good IT systems in favor of inferior ones" (Miller, 2006p).

The larger the scope, the greater the problems in implementing one-size-fits-all enterprise systems. In summer 2006, the Department of Defense acknowledged this by announcing that it was "too big" to implement a single enterprise architecture for all DoD agencies. Instead it planned to implement a federated strategy (called the Business Mission Area Federation Strategy) under which agencies only had to adhere to enterprise-wide data sharing standards tying agency enterprise architectures to the DoD enterprise architecture and specifically to the Global Information Grid being build by the DoD. This system of "tiered accountability" was seen as a "process of consultation with" not "dictation to" DoD agencies, which would still have to present IT projects costing over $1 million to a business mission-specific review board before the investment could go ahead. The DoD federated model set a precedent for those opposed to OMB-dictated government-wide ERP lines-of-business systems (Onley, 2006c).

In trying to account for ERP failure, some commentators have placed emphasis on the fact that large-scale IT efforts, such as ERP involves, are typically led by IT departments. Yet evidence suggests that successful projects tend to be led by business/operating departments, whose ownership of the process is essential to buy-in and success (Essex, 2006). Making IT systems serve business processes is both a commonly-cited ERP design principle but in practice is also a common ERP failure.

Yet another problem in ERP implementation is outsourcing, engendering the possibility of having to go through a series of ERP vendors. For instance, the Interior Department sought to create an ERP to accomplish budgeting, financial management, acquisitions, information management, property management, travel, and other tasks, consolidating dozens of existing programs and systems it described as a "hodgepodge" (Dizard, 2006e). In 2006, a $100 million ERP contract was awarded to IBM, to be implemented between 2006 and 2012. IBM, however, was given only a one-year contract with five additional option years because of Interior's prior experience, which had led it in 2005 to terminate its contract with former ERP integrator, BearingPoint, for being over-budget and behind schedule. In essence, Interior had been forced to write off its two-year, $63 million, ERP efforts with BearingPoint and start over, at least partially, with a new vendor. While all may go well subsequently, putting years 2-6 on option implicitly held out the possibility of further vendor displacements in this massive, long-term project.

Funding

Another failure factor in ERP implementation is inconsistent funding. Being large-scale, ERP projects frequently entail unexpected needs and cost overruns. Unless the department's chief executive officer and chief financial officer are fully behind the ERP project, and prepared for additional funding as needed, failure may ensue. Moreover, ERP is typically implemented by IT departments, which typically lack easy access to control over the department's funding resources.

Shared service provider centralization: Answer to ERP failure?

As the greater complexity and difficulty of developing enterprise resource planning (ERP) software became apparent, the federal government established "centers of excellence" also called "shared services providers," to back up struggling departments and to prevent

such major ERP disasters as the Defense Department's Business System Modernization initiative and the Department of Homeland Security's Emerge2. Some shared services providers are private sector (ex., IBM, SAP Public Services) while others are governmental. The Interior Business Center (IBC), formerly the National Business Center (NBC), run by the Interior Department is one such governmental center. Its former director, Doug Bourgeois, described the typical situation: "Invariable, the question that such agencies ask when they approach us is, 'This is bigger and more complex than we thought it was going to be. Can you take it over for us? Can you manage it? Can you host it for us?' (Dizard, 2006b). As a result, over 20 agency ERP projects had floated into IBC control by early 2006, with others wishing to do so but refused due to IBC limitations.

Because of the high risk, frequent failures, and high price of ERP developed under agency control, the Office of Management and Budget moved to promoting development of ERP systems through shared service providers/centers of excellence rather than through agencies on their own. Also, the OMB became increasingly hostile toward customization of ERP software because customization was seen as a failure factor. Career-oriented agency CIOs, for their part, found pleasing their constituents through customization was not worth the career-busting price of being tagged with an ERP failure.

In January 2007, the OMB released draft guidelines designed to encourage agencies' moving to shared-services financial management software established by the OMB Financial Systems Integration Office (FSIO). Agencies were mandated to report baseline and subsequent performance data for input into FSIO's database, for use by the OMB, the Chief Financial Officers Council, sharedservices providers, agencies, and possibly the public. It is expected this database will be used to identify high- and low-performing agencies in the Financial Management Line of Business, and thus to encourage competition among shared-services providers as well as to allow comparison of in-house versus shared-services costs of providing financial management services (Mosquera, 2007n).

To further put pressure on agencies with large legacy financial management systems, in summer 2006, the OMB issued a requirement that agencies with 10 or more employees must either operate a financial systems complying with the Financial System Integration Office or compete their systems with public and privatesector sharedservices providers under OMB Circular A76. While using the A-76 process to compete, government jobs with private sector vendors had been using the policy from the beginning of the Bush Administration. What was new was having a government shared-services provider from one agency competing for another agency's jobs. The bottom line was that the burden of proof that existing systems were "best value and lower risk" rested with the agency, in a process judged by the OMB and where the OMB (and the Bush administration to which it was responsible) strongly presumed the shared-services government-wide model was better (Miller, 2006w).

Why do agencies find ERP risky and fraught with failure? IBC former head Doug Bourgeois answered: "The most valuable lesson [agencies] learn when they fail [is to limit customization]. Every organization comes in [saying], 'We are unique, we need unique requirements. ...' " (Dizard, 2006b). Sam Mok, a chief financial officer (CFO) who had implemented ERP systems at the Labor, State, Defense, and Treasury departments found not one went smoothly. "If you look at some of the spectacular system failures, which some CFOs lost their jobs over, and I've talked with them, they should have been an SOB

and said no [to customization]. They might still be on the job. But if you try to accommodate [requests for customization], at the end, they were left out and hung to dry by themselves," Mok said (Dizard, 2006b).

Not only is customization of ERP software a very major initial expense, Gupta (2000: 16) points out that it is an expense which comes back again and again whenever the ERP has a major upgrade, and which are recurrent. Upgrades are themselves another example of ongoing ERP costs beyond initial layout, but reprogramming customized modules to be interoperable with the upgrades escalates the cost. ERP design, ironically, can be a driver of customization. Precisely because it is enterprise-wide in scope, ERP can blur lines of responsibility. Vendors blame faulty management, CIOs blame line administrators, administrators blame vendor system design and the central IT shop. To settle the disputes, the agency head may well be pressured to going back to the vendor for expensive customization as the seeming best way to solve the problem in a form of what Perlman (2005) calls "scope creep."

The central implementation problem with ERP is that it is, by definition, a one-size-fits-all software strategy. The success depends upon agencies foregoing customization of software to fit their own agency practices and needs, and instead changing agency practices and foregoing satisfaction of unique needs in order to adapt to the requirements of standardized software. Bluntly, ERP stands traditional software design on its head: instead of designing software to meet expressed user needs, users are expected to change to adapt to predetermined standard software requirements. At the price of sacrificing customization, agencies are supposed to benefit even more by reaping economies of scale through use of enterprise-wide software.

When ERP is mandated and agencies are forced to adapt, do they in fact change their ways? McCoy Williams, director of Financial Management and Assurance in the Government Accountability Office, answered "No," finding agency failures were often traced to failure to change business processes. "Agencies are putting in new systems, but they're doing things the same way as before," he stated (Dizard, 2006b). On the other hand, numerous ERP success stories exist as well, but little in the way of hard data on long-term effectiveness of the ERP strategy. In the meantime, some departments and agencies are moving in the OMB direction. The Department of Agriculture, the Department of Labor, and the Environmental Protection Agency, for instance, moved financial management to OMB-designated centers of excellence in 2006.

In September 2006, under the Office of Management and Budget's Financial Management Line of Business consolidation initiative, the OMB and the General Services Administration finalized their guidance on financialmanagement systems. The core of the guidelines required that any federal agency which planned to replace or substantially modify their financialmanagement systems had to do so by turning over their financial operations to a sharedservices provider (or become one themselves) or to a private financial services vendor (Thormeyer, 2006l). Thus, in 2006 the U. S. Department of Labor awarded Mythics Inc. of Virginia Beach, Va., a fiveyear, $5.3 million contract to provide financialmanagement services. In principle, an agency might be allowed to be an exception to the rule if it could demonstrate its own financial management system provided "best value and lowest risk," but it was clear this countered administration policy, was difficult to prove, and the burden of proof was on the agency.

One of the issues associated with the OMB's shared-services provider strategy is that most federal providers (COEs: "Centers of Excellence"), unlike corporate counterparts, are barred from retaining and reinvesting earnings under the Economy Act of 1932, amended in 1988 (ex., the Interior Department's National Business Center). This is a critical disadvantage since bringing a major new department under financial or human services shared-services requires a substantial up-front investment not easily handled by an agency bound by annual fiscal year funding. Under the Government Management and Reform Act of 1994 (GMRA), however, some units (ex., the Treasury's Bureau of Public Debt) were allowed to be organized as franchise funds, which allow retention and reinvestment of up to 4% of their earnings - less flexibility than the private sector, but still more than most federal shared-services providers. Thus, the OMB shared-services providers do not compete on a level playing field. Rather there are three tiers of relative advantage, from Economy Act COEs at the bottom, to GMRA agencies in the middle, to private providers in the most advantaged position to compete for shared services contracts (Miller, 2006u).

The track record of the shared-services strategy

The Office of Personnel Management became the first large federal agency to contract with a shared-services provider when it signed with the Bureau of Public Debt's Administrative Resource Center (ARC) to provide financial management Line of Business services, as encouraged by the OMB. In late 2006, after having expended some $400,000 on planning and piloting, OPM decided that what ARC had to offer was not consistent with OPM's financial management needs. Consequently, they cancelled the contract and sent it out for re-competition among other federal and private sector providers, again relying on OMB guidance in developing their request for proposals. Putting the best spin on this shared-services failure, OMB stated that it showed the desirability of "fully competing financial management services instead of just looking at the public sector providers' skills and choosing one" Miller, Jason (2006t).

Federal Enterprise Architecture

The Federal Enterprise Architecture (FEA) is the primary planning framework used by the OMB for IT planning and budgeting. FEA is based on five reference models:

- Performance Reference Model (PRM)
- Business Reference Model (BRM)
- Technical Reference Model (TRM)
- Service Reference Model (SRM)
- Data Reference Model (DRM)

The federal CIO Council, which runs the Solutions Exchange program to highlight best IT practices, in 2005 served notice that any future "best practices" would have to be standards-based or based on commercial software. That is, software systems not conforming to "enterprise architecture" standards by definition could no longer be considered "best practices." The Council's purpose is to encourage enterprise-wide, but modularized systems, components of which might be shared among agencies through

CORE (Miller, 2005k). CORE is the Component Organization and Registration Environment, a software registry and component exchange run by the OMB's Federal Enterprise Architecture (FEA) office.

It may be noted that an ERP strategy is controversial, given that in the past the larger the IT system initiative, the more likely failure. Europe's Organization for Economic Cooperation and Development (OECD) is among the public sector bodies which endorses an opposite strategy. In 2001, the OECD issued a policy position paper endorsing "dolphins", not "whales," as an IT implementation strategy. They wrote: "Very large projects, i.e. expensive, longterm and complex initiatives, often fail. A radical approach, increasingly adopted in the private sector, is to avoid large projects altogether, opting for small projects instead. One expert has called this change a shift from "whales" to breaking big projects into small modules ["dolphins"]. Rather, it involves a shift to a different way of working and thinking, with total project timeframes of no more than six months, technical simplicity, modest ambitions for business change, and teamwork driven by business goals... large IT projects should be avoided wherever possible...Where big projects are unavoidable, they should be divided up into selfcontained modules that can be adjusted to changes in circumstances, technology and requirements" (OECD, 2001: 2).

That is, some jurisdictions believe greater effectiveness can be obtained through smaller, more targeted IT initiatives rather than through large, generalized enterprise-wide solutions. There is some argument that special-purpose systems are also more secure than systems built for generalized use. For instance, when the Federal Aviation Administration was criticized over security in 2005, one of its defenses was that "because parts of their system are custombuilt with older equipment, specialpurpose operating systems and proprietary communication interfaces, chances for unauthorized access are limited" (Thormeyer, 2005d). Similarly, industry experts responsible for critical infrastructure security planning acknowledge that as one moves from legacy systems to standardized platforms and public networks such as the Internet, there will be higher exposure to cyberattack (Jackson, 2005a).The large-scale/small-scale architecture debate is complex. The OECD report mentioned above, while endorsing small-scale architecture, also endorses standardized commercial software rather than customized software, for instance. It is logical to assume that the more generalized the task, the more appropriate a large-scale solution, and vice versa. Thus, one would expect enterprise software to be more satisfactory for generalized tasks like payroll and less satisfactory for tasks like case management, where localized agency variables are prominent. Assessing large-scale/small-scale strategies must be undertaken on an empirical, contingent basis, not on the basis of ideological assumptions that one approach or the other always is more cost effective.

Portfolio Management

This approach manages IT investments and sets priorities among projects. It is considered a planning "best practice." Portfolio Management takes a holistic view of hardware, software, and human resources.

5 Stages of the Portfolio Management Process

- Creating Investment Awareness

- Building an Investment Foundation
- Developing a Complete Investment Portfolio
- Improving the Investment Process
- Leveraging IT for Strategic Outcomes

This planning approach requires top management support, buy- in by stakeholders, a strong evaluation component, and a way to eliminate redundancy. Although portfolio management of IT investment is now a long-standing federal government policy, implementation is altogether a different matter. In 2005, a General Accountability Office study of the Department of Health and Human Services (HHS) found that for some 90% of information technology investments, appropriate executive oversight was lacking (Mosquera, 2005d). The GAO found no comprehensive IT investment management process in either HHS or in its largest agency, the Centers for Medicare and Medicaid Services (CMS). The GAO made several recommendations which might have affected HHS's FY 2006 budget for IT of some $5 billion. The GAO called for establishment of written procedures for IT system selection, implementation of a regular IT tracking and review system, and that agency-level business representatives be included on the HHS IT investment review board. Although HHS had been using portfolio management software, the GAO found a systematic portfolio management approach was not implemented. Moreover, there were no standard procedures for monitoring and overseeing the development and operations at state-level Medicaid management information systems.

In late 2005, a George Washington University survey of portfolio management practices in federal agencies found that most federal administrators were aware of it, almost half claimed to be using it, but when details were examined, few federal administrators were actually using it. On the positive side, the survey found almost half of CIOs said they did "manage projects as a portfolio" and 88% said they planned to do so. But in fact, over half of the 59 federal CIOs surveyed stated that they did not centrally track IT projects and that their IT staff did not understand measurement strategies such as return on investment. Two-thirds said they did not attempt to track project benefits. Overall, the study found agencies sorely lacking in training of IT staff in cost estimating, costbenefit analysis and project management (Miller, 2005l).

Risk Management

Risk Management is a planning specialty that has increasingly become more professionalized during the last two decades. Risk analysis is a broad category and is basically a subset of strategic planning. Essentially there are many forms of IT risk – physical, liability, outsourcing of IT functions, security, workplace injury, etc. In addition, ergonomic factors have become a major issue for reducing IT risk (equipment usage, repetitive factors).

As funding becomes tighter in any given area, Congress and agency decision-makers are apt to prefer the tighter justifications provided by risk and needs assessments, as opposed to allocating funds based on population formulas or the like. Starting in January 2006, for instance, the Department of Homeland Security started requiring specific risk assessments in its grant competitions, abandoning its prior reliance on formula-based allotments (Lake, 2006).

The Office of Management and Budget produces a quarterly “at risk” report on IT projects. In summer 2006, some 79 projects were listed, totaling $2.2 billion in investment risk. The Government Accountability Office had indicated the “at risk” report was conservative, and was underestimating risk. The GAO urged augmenting the “at risk” reports with projects on the “Management Watch List,” a broader listing, though as noted by a GAO report, this, too, was based largely on self-reporting by the agencies and may have underestimated risk. A number of projects whose problems had been cited in recent GAO evaluations were not on the OMB risk or watch lists, for instance (Thormeyer, 2006j).

Starting with FY 2002, the Office of Management and Budget initiated the Management Watch List, designed to track missioncritical IT projects that are behind schedule and over budget. The Watch List requires projects to be classified “high risk” by agencies if:
1) The agency has not demonstrated the ability to manage complex projects
2) The projects have unusually high development, operating and maintenance costs
3) The projects are addressing deficiencies in an agency’s ability to perform missioncritical business functions
4) The project’s delay or failure would affect an agency’s essential business functions.

These broad criteria allow very diverse reporting by agencies. For instance, in FY2006 the Veterans Affairs Department reported 33 Watch List projects, compared to only 6 by the Department of Defense, even though the DoD IT budget is 17 times that of the VA. Due to such wide variations in reporting, the OMB Watch List system has come under criticism by Government Accountability Office auditors (Thormeyer, 2006i). For its part, the OMB has defended the “flexibility” of its approach and resisted GAO’s call for creating an aggregated governmentwide list of high risk projects by consolidating the Watch List with its quarterly high-risk reports. OMB’s uncharacteristic defense of agency autonomy could be motivated, critics say, by a desire not to create an official hit list of IT projects for budget-conscious congressional committees which in recent years have become more resistant to pricey IT initiatives.

Summary

Ideally, organizations engage in planning to achieve objectives that further the organization’s goals and fulfill its mission. In economically adverse times, the reality is that planning becomes more defensive and targeted to survival. A study of successful federal IT projects found that IT success was associated with transformational leadership and with strategic planning by public managers. Without a vision, the agency fails. At the same time, Sociotechnical theory appears to offer the most regarding transformational leadership in strategic planning by focusing on the importance of the human factor in IT success.

Needs Assessment

The main purpose of a needs assessment is to identify organizational problems (internal and external) and potential solutions. A thorough needs assessment can re-energize an organization as quickly as a poor one can damage it. At its core, needs assessment attempts to differentiate between needs and wants, and our text recommends a four stage process:

1. Collecting information

2. Identifying and prioritizing problems
3. Researching alternative possible solutions
4. Seeking consensus on proposed solution

Information collection involves reviewing existing policies, analysis of records transactions, interviews with key staff, and brainstorming. In addition delphi methodologies are often used to query experts, form focus groups of employees and clients to facilitate electronic discussions and, in some cases, public hearings.

Problem identification and prioritization forms a baseline against which improvement can be measured. The gap between current practice and desired level of performance is identified. A key aspect of the problem identification stage for IT is answering the question of whether technology can even serve to meet the needs of the problem, or is it outside the scope of technology?

Problem prioritization involves ranking problems in terms of importance to the mission of the agency. Facilitators can help with this by doing clustering of problems first, and then further dividing and ranking these. This is the point where it is important to identify actual needs versus wants. Researching solutions involves an examination of constraints, alternative solutions, mandates, purchasing regulations, and a review of best practices. Often researching IT options includes vendor conferences, exploration of peer groups or agencies.

Following the research phase, agencies engaging in needs assessment should be able to draft a functional specifications document – if done correctly, this becomes a purchasing specification, and is vendor or brand independent. It should spell out in great detail the capabilities and outcomes of the system(s) needed.

The last step in conducting a needs assessment is to seek consensus. At its core a good needs assessment is a form of organizational development, that is, the process engages multiple stakeholders and the resulting assessment accounts for their needs. In the end, the needs assessment must “sell” the recommendations to top management and for this reason must be framed as a planning document and not as a technical evaluation.

Many agencies have found it helpful to include the development of a pilot program or prototype IT system before full implementation. Planning for a phased implementation can aid consensus building in that it allows users to experience the look and feel of a new system even thought it may not be fully functional. These can be valuable in obtaining feedback as the implementation process progresses.

Governments not infrequently associate needs assessments with consulting experts. For instance, the methodology of Oktibbeha County, MI, in conducting a needs assessment for food security information systems, listed such needs assessment phases as interviewing key food security personnel, observing daily operations, examining records, surveying IT experts, and developing a systems prototype - all reasonable steps, but notably omitting any mention of surveying clients and end users! (Gareau, 2004)

Needs assessments are a common prelude to instituting training programs in public administration. An example is Virginia’s Emergency Management Training Analysis and Simulation Center, which offers needs assessment services for agencies considering training employees for homeland defense (Lipowicz, 2005h).

Feasibility Studies

A feasibility study analyzes a business problem and has three broad dimensions: operational, economic, and technical. What is needed may not be feasible, and what is feasible may not be needed. Needs assessment should be coupled with feasibility studies in order for both to be effective. In addition, feasibility studies do not ensure that projects match agency missions, and do not establish need. They simply bridge strategic planning and needs assessment on the one hand, and practical concerns of the project manager on the other hand. Feasibility studies are routinely used as part of IT implementation in such agencies as the IRS (Mosquera, 2005e) and the Navy (Gerin, 2005).

- BACKNEXT

Build Info:Server Time:

Users present begins here

Toggle users present panel Number of users present:2