

EDUCAUSE Center for Applied Research

Research Bulletin

Volume 2005, Issue 17

August 16, 2005

Managing Your IT Portfolio Risk: The Trailing Edge You Don't Want to Admit To

Peggy G. Rogers, University of California

Richard N. Katz, EDUCAUSE



Overview

Colleges and universities are complex enterprises. In many ways, they resemble small towns and cities more than corporate enterprises. As comprehensive environments charged with the education, care, feeding, life safety, and personal growth of members of their communities, colleges and universities build, acquire, and accumulate a wide array of information systems. There have been many articles, presentations, and studies on strategies for enterprise resource planning (ERP) applications—this is not one of them. While the enterprise-wide student, financial, and human resource applications rightfully demand much of our attention and budget, the smaller administrative departmental or niche applications cannot be ignored. These smaller systems look after the myriad roles played by the academy: housing systems, endowment investment and accounting systems, hazardous materials tracking systems, and the like.

With the explosion in application technologies over the past decade, many large institutions have been unable to avoid supporting a growing number of administrative application environments. Over time, central IT organizations find themselves supporting administrative applications on multiple platforms, database management systems, and programming languages. If we also include the technologies used locally within schools or departments, the range of technologies most likely increases. Managing such complex environments often means mitigating the inherent risks of complexity. Risks can be obvious, such as technical obsolescence, lack of vendor support, and so forth. Risks can also be subtle, such as the economic risk of maintaining unnecessary software licenses and skills scarcity.

The EDUCAUSE Center for Applied Research (ECAR) study of IT leadership in higher education¹ highlighted the fact that a great many technical IT workers will exit higher education and the workforce within the next three to five years. With the inevitable wave of baby boomer retirements looming, looking seriously at the many technologies currently being supported is becoming more urgent. The situation of a rapidly shifting workforce is exacerbated by the fact that in some ways, the distribution of IT worker ages and of IT skills is bimodal: many IT workers age 40 and over often know PL1, COBOL, JCL, MVS, and other tools of the mainframe era. IT workers under age 40 have been trained in a client-server or Web era, and their skills revolve around C, C++, Java, Visual Basic, J2EE, WebSphere, .Net, and similar languages and environments. This bimodal distribution of IT skills places many higher education technical environments at risk.

Highlights of Managing IT Portfolio Risk

Evaluation and remediation of the risks posed by trailing edge or obsolete systems is a critical component of an enterprise risk management (ERM) strategy. Enterprise risk management is the process of planning, organizing, leading, and controlling the activities of an organization in order to minimize the effects of risk on an organization's operations. ERM looks at risks broadly. In higher education environments, risks include

financial loss and loss of customer goodwill, the institution's reputation, aging technologies that will limit future architectural choices, and more.

In the specific context of aging information, we think of risk management chiefly in terms of portfolio theory. Many higher education IT environments are decades old, including systems that were purchased or developed over the span of many years. As with a financial portfolio (or portfolio of campus housing) most institutional IT portfolios consist of superstars (killer apps), workhorses (higher education's counterpart to cash cows), and the trailing edge. The trailing edge of IT portfolios contains systems that are old and serviceable and those that are dogs—systems or even environments that pose a risk to ongoing effective operations.

What Do We Mean by Risk?

For our purposes, a technology should be considered at high risk if the likelihood of being unable to continue to support the production environment for applications has become too high due to

- minimal vendor support for the technology, and/or
- loss of explicit or tacit technical knowledge within the institution.

A variety of circumstances can lead to a lack of vendor support. In the best of circumstances, the vendor provides customers with a long lead time for phasing out older technologies. For example, IBM provides customers with clear indications of their plans for continuing or discontinuing ongoing support of various products. Often, however, the fate of technologies is closely tied to the fate of the vendor or to the vagaries of the volatile technology market. Some technology companies do not survive, and their products disappear quickly from the market. Other products or companies are bought by competitors, bringing uncertainty about the future of specific product lines. Managers of technology organizations must keep abreast of both official and implicit possible removal of vendor support for technology products.

Staff turnover and the possible loss of valuable institutional and technical knowledge are certainly not new issues for IT organizations. What looms ahead in the near future, however, is the retirement of the baby boom generation. As documented in the recent ECAR research study on IT leadership in higher education, the number of older technology workers in higher education is large: "Fewer than 5 percent are under the age of 31, and 25.1 percent are under 41. Almost 40 percent are over 50."²

Although some institutions have successfully retrained older workers in newer technologies and many older individuals have made the leap on their own, many organizations have a generation gap, with older staff supporting older technology while younger staff deploy and support the newer technology. And, while some older employees may be willing to learn newer technologies, it is unlikely many of the younger generation are willing to learn older technologies. With this generation gap lies the risk of losing all knowledge of specific older technologies in the foreseeable future.

Review Policy and Determine the Scope of Evaluation

An essential part of any ERM program should be an effort to ensure that there is policy to guide the institution's investment in and attention to the trailing edge of the IT technology portfolio. How far behind the current vendor release is it acceptable to be? To the extent that the institution's notions about risk and about the institution's tolerance for risk can be codified, the downstream governance of an ongoing effort to manage the portfolio will be eased. This is no different from most institutions' board investment committees, where it is a standard practice to articulate and codify an investment philosophy that will guide a program. Such policy guidance can also go far in moving recalcitrant system users or technical diehards off the dime when their risky but beloved systems come under review.

As with any project, an important first step is to establish the scope of the project. For reviewing older technologies, one determining factor of scope is organizational—will this review include institution-wide, centrally supported technology only, or will it include technologies used within an individual school or department? Depending on the size of the institution, an enterprise-wide review could be too ambitious—some more well-defined context might be more realistic.

Another aspect of the scope of the review is which technology is included. For administrative applications there are three basic supporting technologies:

- platform/operating system;
- database management system or (more generally) data file structures; and
- programming languages.³

An initial risk assessment for older technologies might look at platforms first, followed by data file structures and finally programming languages. Or, all three might be included in one review. Of course, some application environments, especially for smaller applications running on one or more workstations, might combine the programming language and database management system into one tightly coupled technology, making it impossible to separately evaluate one from the other.

Identify At-Risk Technologies

Once the overall scope is established, the next step is to identify those technologies considered at risk. It is important to keep the key goal in mind: identification of technologies that pose a serious risk of being infeasible to support in the foreseeable future. This is not an exercise in identifying technologies that might be considered either out of date or politically incorrect. If we attempted to keep all administrative applications within the realm of currently accepted modern technology, we would find ourselves doing nothing but conversion, migration, and replacement projects—essentially running in place like Alice and the Red Queen:⁴

“Now! Now!” cried the Queen. “Faster! Faster!” And they went so fast that at last they seemed to skim through the air, hardly touching the ground with their feet, till suddenly, just as Alice was getting quite

exhausted, they stopped, and she found herself sitting on the ground, breathless and giddy.

The Queen propped her up against a tree, and said kindly, “You may rest a little now.”

Alice looked round her in great surprise. “Why, I do believe we’ve been under this tree the whole time! Everything’s just as it was!”

“Of course it is,” said the Queen, “what would you have it?”

“Well, in our country,” said Alice, still panting a little, “you’d generally get to somewhere else—if you ran very fast for a long time, as we’ve been doing.”

“A slow sort of country!” said the Queen. “Now, here, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!”

When consulting members of the IT organization to identify at-risk technologies, it will be important to distinguish between technological bigotry and the identification of areas of genuine risk.

Identify Target Technologies

The flip side of identifying at-risk technologies is to identify target technologies for replacing those that are at-risk. For organizations with a clearly defined strategic direction for administrative applications, this will be a simple task. For other organizations that have developed various islands of technology, this may be more difficult. There are generally three possible solutions for an application that relies on at-risk technology—migrate the code, replace the application, and outsource the support.

Migrate the Code

In some cases it may be possible to retain a large portion of an existing application and migrate the code to run on a different platform, with a different database management system, and so forth, which is often the most cost-effective approach. This approach can meet with some resistance, however—some may argue that the migration effort is nonproductive because it may not result in an application that fully embraces newer technology. The key goal, however, is mitigation of risk, not achieving a uniformly modern technical environment.

Replace the Application

Another option is to rewrite the application in-house or buy a vendor package. The complete replacement of an application certainly solves the reliance on at-risk technology. In some cases, this may be the only viable alternative. This route should not be taken lightly, however. The rule of thumb among migration software experts is that the development of a replacement application will take four to eight times the resources of a migration effort.⁵

If a complete replacement of the application is the only alternative, then the project must be treated as any new development project, following the organization's standard development procedures. One difference is the motivation for the development—normally a departmental or niche application is developed for one or more functional offices, at their request and probably with their funding. In this case, the motivation is coming from risk avoidance and mitigation. If the customer has no immediate needs for enhancements or is unwilling or unable to assist in funding the project, then the scope of the development project should be kept to replacing current functionality only.

Of course, as with any new application development project, there will be a “build or buy” decision—is there off-the-shelf packaged software that meets this business function? Or is this a unique function requiring in-house development? It is possible that at the time of original development there were no off-the-shelf solutions but that a cost-effective package may now fit the need adequately, providing a relatively painless replacement path.

Outsource the Support

If the primary problem with the at-risk technology is the loss of knowledgeable staff rather than inherent risks in continued support of the vendor software, then outsourcing the support for the application may be an option.

Inventory At-Risk Applications

Once the at-risk technologies have been identified, the following steps are required.

Find Them

The first step is to find all production applications that rely, either directly or indirectly, on these technologies. Some institutions keep a comprehensive list of all production applications across platforms, making this inventory step reasonably easy. Other institutions treat some platforms less formally than others and may need someone to do some sleuthing to find out what applications are currently in production on every platform.

What do we mean by relying “indirectly” on an at-risk technology? An example at one institution is a client-server production application distributed to multiple Windows desktops in one functional office. The runtime code was compatible with newer releases of Windows—no problem. However, the development environment required to perform any maintenance to the code was restricted to running on the Windows 95 operating system, a platform that had been identified as at risk and to be eliminated.

Sometimes problems exist in interface files, even where the core application does not make use of any at-risk technology. One application identified in an at-risk review is a system that tracked mail costs and forwarded these costs to an internal recharge application. Although not well documented, one key interface was a hand-off of a PC diskette (soon to be at-risk hardware) that was translated to the required format using a DOS-based program (DOS was also identified as an at-risk platform to be eliminated from direct use by production applications).

Describe Them

While a complete review of every detail of every production application is not necessary (nor would it be cost-effective), the inventory must be more than simply a list of application names, or worse yet, acronyms. At the very least, identification of the production applications must include

- the platform or platforms on which the application runs;
- all file structures used, including database management system (DBMS) software and any other proprietary file structures (does anyone have IDMS files?);
- programming languages; and
- a brief description of the function of the application plus, if possible, some categorization of size of application—for example, how many separate processes are there? This type of information will help in the next step of determining options for removal of the at-risk technology.

Decide What to Do with Them

The next step is to look at each application and decide what option or options will remove the at-risk technology. Although one analyst should be in charge of this process, the task may best be handled by a small team. This team should also come up with a best guess for cost (primarily staff hours required) for each option for every application.

Once every application is reviewed and options are determined, a summary of the estimates and required staff time should be prepared.

The Need for Buy-In

The real work is tackling the tasks required to remove the at-risk technologies. Before the work begins, however, there must be sufficient buy-in from different segments of the organization if the project is going to succeed.

IT Management

First, management must review the recommendations and determine how the work will be funded. Can we do this? And, what is our target completion date? Are there any hard deadlines for any particular at-risk technologies? For example, if a major software license will expire, has management decided that it will not be renewed?

IT Staff

Analysts and programmers do not always completely agree with management decisions, nor is it necessary for most projects that they do. However, emotions may run surprisingly high with an at-risk review. If some staff members feel their livelihood is threatened because the technology with which they are most comfortable has been identified as at-risk and to be eliminated, it may be difficult to get cooperation. These are also the staff members most likely to have expertise that is critical to the success of the

project. While it may not be possible to ever get wholehearted support of the project from these staff members, some time spent early in the planning stages with these staff members may help ameliorate their concerns.

Customers

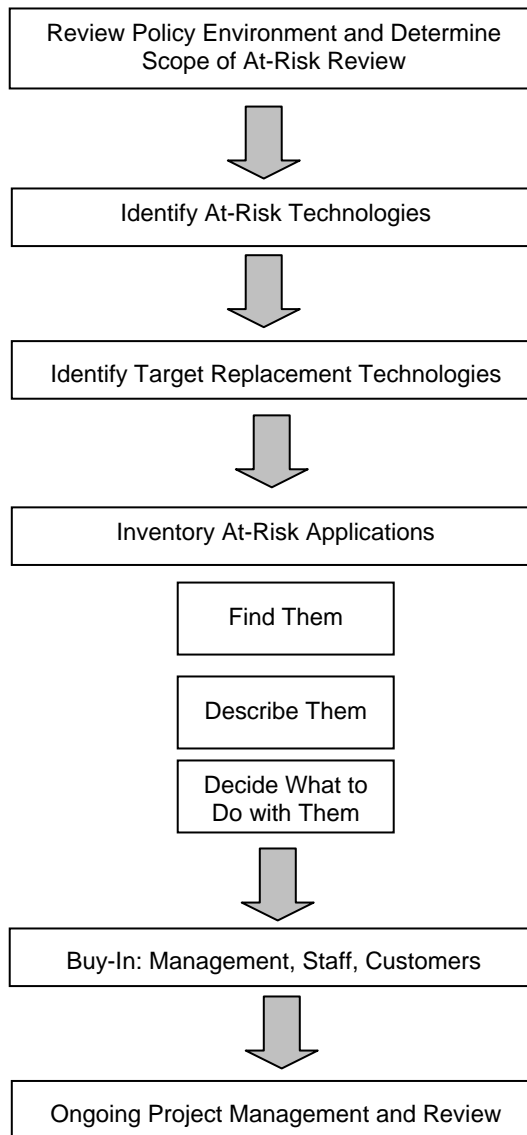
Normally with an IT project, the customers are key participants, often providing all or part of the funding and certainly making many of the decisions. However, for an at-risk project, this may not necessarily be true. If the best option for removing an application's dependency on an at-risk technology is a behind-the-scenes migration (for example, from one DBMS to another), the customers may not be affected. In fact, such a migration project is most successful if the customers do not notice any changes.

Of course, if the application is fully dependent on an at-risk technology (for example, an application written in FoxPro, when FoxPro has been identified as at-risk technology), then it is likely that the application will need to be replaced. In this case, the customer, of course, must be consulted. IT management must decide on plans for funding before approaching the customers. The chances of customers being thrilled to pay for a replacement system because IT has decided the technology is at-risk are slim at best. If, however, the customer was contemplating replacement in any case, then a jointly funded project may be the best approach.

Ongoing Project Management

Once the work is under way to migrate, replace, or outsource support for all applications relying on at-risk technology, the project or projects must be managed the same as any other systems development project. This includes oversight by a project manager to ensure progress is being made and periodic reports to higher level management. If the original estimates prove faulty, then the overall project plan must be revisited and adjusted.

Figure 1. Diagram of Steps to Take



What It Means to Higher Education

Chief information officers (CIOs) play a number of roles, including a key and increasingly common role as a manager of a portfolio of institutional operating systems, applications, and other information technologies. CIOs as portfolio managers have three key objectives:

- build resources in ways that promote the ability to innovate (flexibility);
- maintain a current suite of proven technology to “run the business” at service levels that are appropriate to the institution’s priorities; and

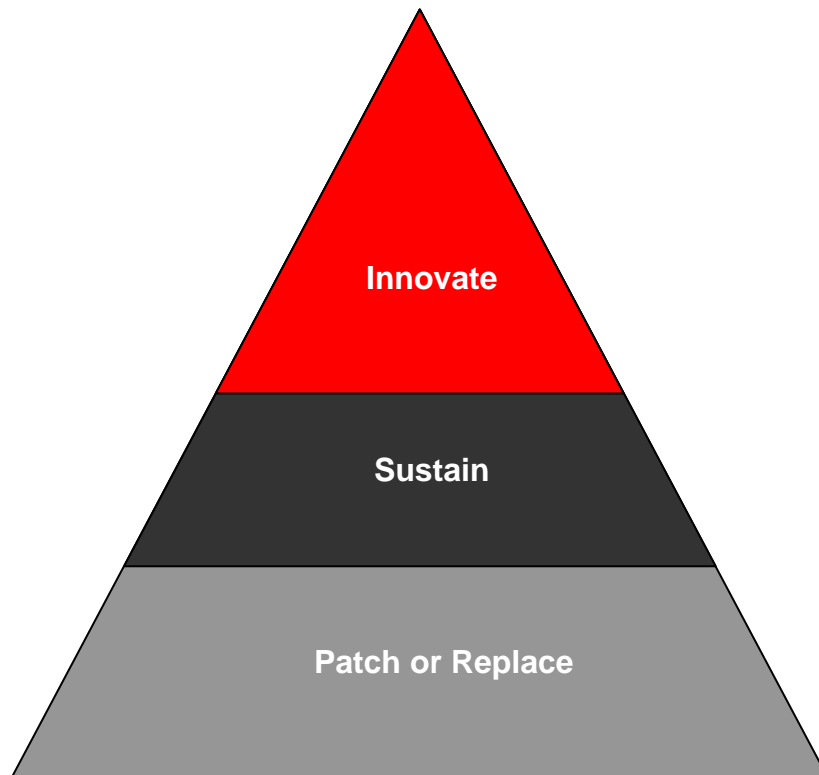
- reduce the number and criticality of those trailing-edge applications, operating systems, and technical environments that may place the institution at risk.

Viewed another way, the CIO must balance investments across platforms that

- can lead an institution into its future (for example, high-performance networking, VoIP, e-portfolio, and so forth);
- ensure regulatory compliance and effective operations; and
- keep the floor from collapsing under the institution.

These tasks put the CIO in the company of the campus architect, facility manager, fleet manager, and chief financial officer, who must also worry about how much maintenance can be deferred before levels of risk become unacceptably high. In IT management, shorter life cycles make portfolio management even trickier, as Figure 2 illustrates.

Figure 2. An Investment-Oriented View of the IT Portfolio



Every institution should develop a process, a governance system, and an investment philosophy to address at-risk systems. In Fortune 100 companies today, it is commonly assumed that 40 percent of the IT dollars are to be targeted toward innovation-seeking investments, while 60 percent are to be devoted to maintaining current operations. ECAR's recent study of IT funding reveals that higher education IT managers are putting a worrisome share of their investment dollars into remediating the trailing edge of technology.⁶ This deferred maintenance issue is not creeping—it is galloping.

Key Questions to Ask

CIOs and other leaders of the institution should ask themselves the following:

- Do we have a policy that ensures the currency of our technical portfolio? Does this policy identify the institution's tolerance for risk?
- What is the current state of the IT portfolio of operating systems and applications?
- Which systems are at risk? What is the nature, intensity, severity, and imminence of those risks?
- What are the costs of remediation? What are the costs of failures to act? Costs can be related to
 - ♦ economics (high maintenance costs, the risk of failure);
 - ♦ service performance;
 - ♦ architectural and competitive positioning (can we move IT to “the next level”?);
 - ♦ adaptability (can we build a workforce of technical generalists with islands of isolated and obsolescent technology?);
 - ♦ integration (how much energy will we invest integrating obsolete systems with new systems?);
 - ♦ skills (will COBOL programmers always be around?); and
 - ♦ reputation (not only the reputational risk when systems fail, but the risk of operating an IT environment that is unattractive to the next generation of IT superstars we need in order to remain competitive).
- What leadership support, governance, staffing, and financial investments will need to be organized to manage the trailing edge of technology effectively?

Where to Learn More

- R. N. Katz et al., *Information Technology Leadership in Higher Education: The Condition of the Community* (Boulder, Colo.: EDUCAUSE Center for Applied Research, Research Study, Vol. 1, 2004),
<<http://www.educause.edu/LibraryDetailPage/666?ID=ERS0401>>.

- P. J. Goldstein, *Information Technology Funding in Higher Education* (Boulder, Colo.: EDUCAUSE Center for Applied Research, Research Study, Vol. 7, 2004), <<http://www.educause.edu/LibraryDetailPage/666?ID=ERS0407>>.
- M. Jeffery and P. J. Goldstein, "IT Portfolio Management for Colleges and Universities: Balancing Risk/Return for Strategic Results" (Boulder, Colo.: EDUCAUSE Center for Applied Research, Research Bulletin, Issue 3, 2005), <<http://www.educause.edu/LibraryDetailPage/666?ID=ERB0503>>.

Endnotes

1. R. N. Katz et al., *Information Technology Leadership in Higher Education: The Condition of the Community* (Boulder, Colo.: EDUCAUSE Center for Applied Research, Research Study, Vol. 1, 2004), <<http://www.educause.edu/LibraryDetailPage/666?ID=ERS0401>>.
2. Ibid., p. 38.
3. While this research bulletin focuses on operating systems, database management systems, and programming languages, we note that vulnerabilities on in terms of network penetration and information transport should also be part of the institution's risk assessment.
4. L. Carroll, *Through the Looking Glass (and What Alice Found There)*; available online at <<http://www.literature.org/authors/carroll-lewis/through-the-looking-glass/index.html>>.
5. C. Burgess, Manager of Data Warehouse and Corporate Systems, University of California Office of the President, personal communication.
6. P. J. Goldstein, *Information Technology Funding in Higher Education* (Boulder, Colo.: EDUCAUSE Center for Applied Research, Research Study, Vol. 7, 2004), <<http://www.educause.edu/LibraryDetailPage/666?ID=ERS0407>>.

About the Authors

Peggy G. Rogers (peggy.rogers@ucop.edu) is a Systems Analyst and Project Leader at the University of California Office of the President. Richard N. Katz (rkatz@educause.edu) is Vice President of EDUCAUSE and Director of ECAR.

Copyright 2005 EDUCAUSE and Peggy G. Rogers and Richard N. Katz. All rights reserved. This ECAR research bulletin is proprietary and intended for use only by subscribers. Reproduction, or distribution of ECAR research bulletins to those not formally affiliated with the subscribing organization, is strictly prohibited unless prior permission is granted by EDUCAUSE and the authors.