The CPA Journal
THE VOICE OF THE PROFESSION 85th Anniversary 1930-2015
(/news/publications/the-cpa-journal)

Technology, Risk Management, and the Audit Process

Managing New Acquisitions in the Restarted Economy

Yigal Rechtman, CPA, CFE, CITP, CISM, and Guido Gabriele, Esq.

In Brief

As the U.S. economy continues to recover from the Great Recession, new technological developments are once again accelerating, as is corporate adoption of those developments. In this article, the authors discuss recent trends related to technological improvements, considerations in technology adoption and retirement, how to manage the attendant risks, and the implications for human capital.

* * *

The recovery of the U.S. economy since the Great Recession of 2007–2009 has been accompanied by exciting developments in technology. Many large companies have profited from this tech surge, often reinvesting revenue instead of distributing it to shareholders in the form of dividends. Small and mid-sized companies have experienced similar growth, albeit at a smaller scale. In particular, information technology and systems have enabled these companies to revitalize internal management and gain a competitive advantage. Some businesses and not-for-profit organizations have experienced organic growth, while others have grown via acquisition of remaining competitors or strategic partnerships, and the global economy has experienced similar trends based on technological adoption and adaptation. As with any great opportunity, however, this new surge in technology brings great risk.

The Risks of Investments in Technology

The technological booms and busts of the past two decades represent a cautionary tale; investment in a new technology is no less risky simply because one has adhered to prior "best practices." Less mature technology presents new, possibly greater kinds of risks. For example, switching to cloud-based operations for employees or deployment of a mobile app for customers may drive growth and provide a competitive edge, but it also expands the types of risk and potential impact of those risks, from employees suing for unpaid overtime to a breach of security perimeters that are now fully virtual. Still, many organizations that survived the Great Recession now have available cash on hand to grow or compete, and thus are driven to invest in technology.

(/cpaj-images/CPA.2016.86.5.016.uf001.jpg)

Though it is appealing to think about an acquisitionsolely in terms of the new intellectual property andintangible assets added to the acquirer's portfolio, there is more to the story.

Certain trends expected to manifest will shape how companies can best direct their technology investments. First, as new technology acquisition increases, the focus is likely to shift from generalized technology to specialized applications. In addition, as new technology is acquired, an increased disposal or warehousing of old technology is likely to follow. Finally, and perhaps most important, investment in human capital is necessary to make the best of new tools.

Technology Acquisition Risk

As many business owners and managers have found, the most efficient way to grow a business is by acquisition. In recent years, mergers and acquisitions have been on the rise, especially “boutique acquisitions” under $100 million. Though some acquisitions are primarily about securing talent and expertise, many also result in the incorporation of technological intellectual property that is integrated into the acquiring company's existing operations or launched as “new” products (Jacob Mullins, “2015 Will Be the Year of the Tiny Tech Acquisition,” *Business Insider*, Jan. 6, 2015, http://read.bi/2367PHq (http://read.bi/2367PHq)). Behind the curtain, these companies experience sudden growth in the complexity of their back-end systems as the new technology is integrated into the existing infrastructure. With that increase in complexity, the risk of unintended consequences also sharply rises.

Though it is appealing to think about an acquisition solely in terms of the new intellectual property and intangible assets added to the acquirer's portfolio, there is more to the story. In buying another company's assets and hiring its personnel, the acquiring company must also internalize its technology challenges. These challenges include varied integration issues and a plethora of common technology headaches: outdated servers, insecure configurations, incompatible software, and differing regulatory compliance requirements. For example,

an otherwise healthy company may, post-acquisition, find itself scrambling to become Payment Card Industry (PCI) compliant, needing to install new antivirus software on many workstations, or inheriting a bug list for internally developed software that cannot interface with the acquirer's financial reporting system.

Simply discarding the acquired company's hardware might seem like the easy answer, but such a break will likely be challenging from a cash flow perspective. In most cases, the acquiring company must incorporate the workstations, servers, firewalls, and software of the acquired company into its own infrastructure. The risk of internal unauthorized access to company data is therefore sharply and suddenly elevated, and this risk may reach outside the company to vendors and clients (e.g., through electronic data interchange interfaces or customer web portals). All of these technology risks are inherent to any acquisition and should not be ignored.

Software Specialization

Software specialization is another way for organizations to gain a competitive advantage. For example, the healthcare industry has seen a marked increase in the use of electronic medical records (EMR) in the past five years. At their best, EMR systems have the potential to deliver better patient outcomes and increased efficiency for providers. As a result, healthcare institutions are now working to integrate EMR into their alreadycomplex enterprise resource planning (ERP) systems (Mari M. Nakamura, Marvin B. Harper, and Ashish K. Jah, "Change in Adoption of Electronic Health Records by US Children's Hospitals," *Pediatrics*, vol. 131, no. 5, May 2013, http://bit.ly/1SUKYq3 (http://bit.ly/1SUKYq3)). ERP software has one key function—to get the right information to the right person at the right time. To achieve this goal with the maximum amount of EMR integration, some hospitals and similarly complex entities have turned to developing their own proprietary software internally or through a third-party development team. Some of these proprietary ERP software packages are written from scratch; others are crafted from highly configurable third-party software packages. In all cases, this trend has affected both large and complex hospital networks and smaller medical practices.

This search for differentiation and competitive advantage through highly customized, highly integrated software is not limited to the healthcare industry; it also exists in the communications, healthcare, government, not-for-profit, construction, and logistics sectors, to name just a few. And as with any burgeoning technology, with growth comes increased complexity and increased risk. Risk from specialized software first develops when a company fails to adhere to best practices during development or customization. Proper segregation of duties among the development team members is vital: the analyst, programmer, quality control department, and user should be discrete and sequentially responsible for their individual roles during the implementation process. Either in an attempt to launch new software quickly or by simple inattention, high-level managers often fail to implement such a segregation of duties. As a result, even flagship, mission-critical software products may lack basic quality and roll into production with potentially destructive bugs unnoticed.

Even if the development team follows best practices, other risks associated with specialized software may remain. More so than off-the-shelf software, internally developed or customized software packages may not be created with sufficient documentation or implemented with sufficient testing. In addition, third-party developers may functionally abandon commissioned software after moving on to new projects, making updates or bug fixes more difficult to come by. In highly regulated environments—especially those that may require audits of operational software—these risks can be significant.

Finally, failure to develop or customize software according to best practices may pose a risk that financial reports from the production side of the business will be inaccurate, as well as a risk that that these inaccuracies will not be not caught by the accounting and finance cycle managers in a timely fashion. In an effort to cut costs, a business may not spend the time and money required to add audit functionality to its internally developed software, leaving it entirely reliant on software that cannot be tested for accuracy. As a result, there is a real risk that profitability may be overstated (risk of failure) or understated (risk of lost opportunities).

As software and hardware security controls pro-tecting businesses' complex information systemshave improved, intruders have recognized thatpeople are the most vulnerable link in the chain.

Discarding Technology

The discarding of obsolete technology is a byproduct of acquiring new technology. Though many businesses hold on to technological assets far past their expiration date, it is generally accepted that most technology can be considered obsolete after only 18 months. In a period of accelerated growth, older technology is discarded even more quickly. Such discarded technology introduces the risk of data loss or unauthorized distribution of confidential data. Hard disks, workstations, servers, multifunction copiers, mobile devices, and many other technologies all may have sensitive data stored in their memory when discarded. For example, a recent study performed on used hard disks bought from eBay revealed that many contained data from the previous owners (Lucas Mearian, "Survey: 40% of Hard Drives Bought on eBay Hold Personal, Corporate Data," *Computerworld*, Feb. 10, 2009, http://bit.ly/1UQNph8 (http://bit.ly/1UQNph8)). Businesses must recognize the risks associated with decommissioning technology and ensure that the technology they discard is properly cleared of sensitive data before it is disposed.

Human Capital

The degree of risk associated with acquisition, adaptation, and disposition of technology is ultimately determined by the people interacting with that technology. Technology is at once harmless and useless until it is operated by a person, regardless of that person's job description and position. As such, managers and auditors must assess the risks of human use and misuse of any technology, both intentional and unintentional.

For example, many businesses are turning to remote access and telecommuting in hopes of increasing productivity and accommodating alternative work schedule needs. Though most regard this as a positive development, telecommuting is fraught with risks of unauthorized data access. Remote workers might store sensitive data on personal machines, share workstations with family, leave passwords in full view, or expose the business's assets to their unsecured personal networks. Businesses must therefore assess the risk of their remote workers' failure to comply with company security policies and enhance security accordingly. Tools such as encryption and training must be utilized to ensure that controls over *authentication* (knowing who is accessing data) and *authorization* (ensuring that the user has access to the right data and nothing more) are effective.

Technology professionals often express the opinion that people are not good at keeping data safe. As software and hardware security controls protecting businesses' complex information systems have improved, intruders have recognized that people are the most vulnerable link in the chain. Technology has become more complex, but human brains keep making the same mistakes. Rather than attempt to break encryption or find unpatched holes in software, hackers have turned to social engineering methods like phishing to trick workers into giving up information that would help them bypass security (Jack Wallen, "10 Social Engineering Exploits Your Users Should Be Aware of," TechRepublic, Jan. 27, 2016, http://www.techrepublic.com/blog/10-things/10-social-engineering-ploys-your-users-should-be-aware-of (http://www.techrepublic.com/blog/10-things/10-social-engineering-ploys-your-users-should-be-aware-of)). To make matters worse, information extracted from these methods (which include collection and aggregation of data from public sources) is compiled and made available in online black markets. Human capital may increase technological risk, but the workforce need not be replaced with robots just yet. A business that is aware of these risks can work to mitigate them, and the first step is, of course, a proper risk assessment.

Risk Management

In recent years, there have been an alarming number of high-profile security breaches, including at such large corporations as Target, Home Depot, Wyndham, Anthem Health, and T-Mobile. These breaches are particularly troubling because these companies presumably had the resources and opportunity to conduct a risk assessment and take steps to mitigate their data risks. It should be clear that the right time for a business to determine whether it is exposed to such a breach is always "now," and certainly not "after a breach." Managers and data owners should consider the probability of an adverse event and project its estimated financial impact. Risk can then be managed in one of four ways: avoid the activity that creates the risk, reduce the risk by mitigation, reduce the risk by sharing the consequences with others, or accept the risk. (For a complete discussion of risk management framework, see Yigal Rechtman, "Book Review: *Guide for Conducting Risk Assessments: Information Security*," *The CPA Journal*, March 2013.)

Risk management is often partially controlled by cost-benefit calculations. Managers must always contend with limitations on time, funds, and technology to manage risk within reason. The risk of new technology acquisition can be managed with testing and slow implementation cycles. The risk of poor development or configuration of new software can be reduced with policies and procedures that employ best practices in change management. Security risks can be reduced by proactively auditing information technology and shared by obtaining cyber-

security insurance. (For a detailed discussion of cybersecurity for CPA firms, see Yigal Rechtman, and Kenneth N. Rashbaum, "Cybersecurity Risks to CPA Firms," *The CPA Journal*, May 2015.) Auditors can measure the effectiveness of these controls in a Service Organization Controls (SOC) Type 2 report, providing assurance to management about the compliance of information technology with certain criteria and allowing the company to share the risk with the auditors who write the SOC reports. Proper policies and procedures, along with regular training and reminders, can also mitigate the risks associated with both new and existing technology.

Technology Risk and the Audit Process

U.S. GAAS (AU section 150, "Generally Accepted Auditing Standards," http://bit.ly/1qbSfbp (http://bit.ly/1qbSfbp)) requires auditors to assess the risk of financial misstatement, especially as it arises from the application and use of technology. The standards are general enough to include both the technology underlying internal controls in place for the preparation of the financial statements and that underlying the company's operations, provided that such technology is related to the production of financial results.

The classes of risks listed above can have a significant effect on an auditor's assessment of risks. For example, if a company has properly segregated duties with regard to the system development life cycle (SDLC) of a core system, then the risk associated with the system's design can be assessed as low. Tests of internal software development controls are likely to pass in such entities, and the reasonable reduction of risks enables the auditor to reduce the extent and nature of the auditing procedures and perform such procedures well before the year end.

The risks from new technology can also be relevant for understanding the growth opportunities associated with differentiation (or lack thereof), depending upon the company's degree of adaptation. As such, a sophisticated auditor can be in a position to develop better expectations and come up with fewer false positives when performing analytical procedures. When evaluating internal controls—either for testing or simply to understand the company's operations—it is helpful for auditors to understand the level of adaptation to new technology (e.g., new software, integration of mobile computing, a switch to cloud-based services) in light of risks associated with human interaction with that new technology. This understanding can assist auditors in complying with GAAS, in identifying situations where IT-based controls such as authentication and authorization can be improved, and in providing the company—with certain limitations—consulting services that aim to improve such deficiencies.

The current period of economic growth in the United States has ushered in a wide range of technological opportunities. At the same time, managers and auditors are well advised to consider the risks associated with these technological developments and apply their skill and knowledge to mitigate and manage these risks for overall organizational and practice success.

Yigal Rechtman, CPA, CFE, CITP, CISM is a senior manager for litigation support and forensic accounting at Grassi & Co., as well as an adjunct professor at the Lubin School of Business, Pace University, New York, N.Y. He is a member of The CPA Journal Editorial Board.
Guido Gabriele, Esq. is a litigation supervisor and technology consultant at Grassi & Co.