IT Risk Analysis—The Missing “A”

An accurate assessment of IT risk is essential for the development of a relevant and cost-effective IT control environment. Unfortunately, the tools and conceptual framework for IT risk analysis have often included only highly visible metrics, such as number of transactions, direct financial impact, and the effectiveness of disaster recovery and business continuity across the enterprise. These traditional markers are important and valid in the assessment of risk. However, this article explores the concept that IT risk is also driven by a more abstract but potentially powerful factor: the organization’s level of commitment to agile systems. The term “agile” is used here in the strategic sense—as the ability to adapt quickly and efficiently to business, regulatory and technical changes.

George Westerman and Richard Hunter, in their book IT Risk, break IT risk into four categories: availability, access, accuracy and agility (the four “A’s”). While most IT audit risk analyses include the first three categories, agility is sometimes ignored in spite of its strategic importance to the ongoing success of the organization. Agility, the ability to respond appropriately to the organization’s business needs, is the most “fuzzy” of the four risk categories, but may be the most important from the perspective of day-to-day delivery of results.

THE GROWTH OF RISK MANAGEMENT

The recent worldwide recession has brought an intense focus on methods to monitor, regulate and mitigate risk factors including, but certainly not limited to, operations, credit activities and market volatility. This attention is merely the latest manifestation of risk management efforts that have been ongoing for the last 70 years or more. The Basel Accords (I and II), which attempt to set worldwide standards for financial institutions’ capital reserves and risk-taking practices, are recent examples of global risk abatement efforts. Risk assessment practices have grown in sophistication, mathematical complexity and pervasiveness. Off-balance sheet exposure, collateralized debt obligations and many other factors are now routinely included in comprehensive risk models.

How does this new, invigorated culture of risk management affect the IT auditor’s day-to-day assessment of IT risk? Clearly, management now has higher expectations of the IT auditor’s work. For example, the chief information officer (CIO) may look for a more strategic view of IT risk, based on an in-depth understanding of the organization’s business and technology direction.

Questions asked may include the following:

• How can risk be addressed using a more integrated approach rather than as a series of unrelated threats?
• How can risk be addressed using a more integrated approach rather than as a series of unrelated threats?
• Is there a practical way to educate the rest of the organization, particularly senior management, on the longer-term, more strategic exposures?
• How can risk be addressed using a more integrated approach rather than as a series of unrelated threats?

TACTICAL VS. STRATEGIC RISK

The traditional focus of IT risk analysis has been on visible and tactical events. In terms of the Westerman-Hunter model, those events include breakdowns in computing resource availability, inappropriate access and inaccurate processing. Of course, mitigation of these well-known risks is essential for the continuity of any organization. However, longer-term and slow-developing risks, such as the failure to maintain agile systems, can present significant harm to profitability and efficient operations. Agility risk is strategic and develops over time. It may not be immediately visible and, hence, may be more difficult to evaluate and present to management.

Agility directly affects the organization’s ability to respond to technical, regulatory and competitive market changes. Agility risk may
come from lower-level, “nuts-and-bolts” factors or from improper strategic organizational structures. On the low end, for example, a legacy program might be written with hundreds of go-to statements. It may work perfectly well (after much debugging), but if it must be changed, the probability of failure is very high. Bad programming practices lead directly to nonagile systems. At the other end of the spectrum, an organization with high strategic agility risk may have siloed and disconnected applications, an excessive number of interorganizational links, and limited ability to change IT functionality within a reasonable time.

WHEN CHANGE IS CONSTANT: THE STRATEGIC VALUE OF AGILITY
In the 1990s, many progressive organizations implemented workflow systems as an important component of their business process management strategy. The benefits were and remain clear: structured movement of information with audit trails, straightforward authorization procedures and the ability to provide alternate paths if resources are temporarily not available. In an Oracle enterprise resource planning (ERP) system, for example, purchase orders flow from a lower-level initiator to a higher-level approver if the amount exceeds a predefined level, and other steps in the purchase-to-pay cycle follow. In a change control system, implementation of a program change cannot be put into production until a user/authorizer electronically approves the move.

In contrast, today’s for-profit and nonprofit businesses are increasingly compelled to go beyond the hierarchical, one-step-at-a-time processes tailored to workflow systems (although workflow systems continue to play a vital role in many core processes). In the marketplace, change is occurring at an exponentially increasing rate. Customers have the availability of the web, vastly more leverage than before and the flexibility to change providers easily. Hence, for many businesses, the ability to shift and be first to market is often more important than the capacity to produce cheap, standardized widgets. Product and service disruption is no longer an occasional event. Now disruption is nearly constant. Only agile firms can shift products, offerings, services and suppliers fast enough to maintain or increase market share. Increasingly, it is the nonroutine actions that drive competitive advantage. Thus, organizations with agile IT systems will thrive relative to other organizations when market conditions, governmental regulations, technology and other factors are the most disruptive.

THE PATH TO AGILITY
A strong, uniform, stable and predictable software platform may be the most essential element of an organization’s IT risk reduction program. And while a strong platform (software, hardware and methodologies) affects all areas of IT risk, it has a disproportionate effect on agility risk. Unfortunately, there is no simple formula for achieving the IT flexibility most firms need to respond to rapid change. Forward-thinking firms seeking to maximize agility encourage idea sharing, nonhierarchical decision making and full utilization of the entire organization’s mind space (including employees, contractors, vendors and customers). Such organizations often promote agility with human interaction tools.

Examples of these tools (mostly falling under the web 2.0 umbrella) include collaboration packages, information-sharing software (such as Microsoft’s SharePoint), wikis, blogs, alerting systems, hosted services for rapid change, social networks and even mashups. A number of organizations have used the spare cycles of millions of volunteer PCs to assist in problem-solving tasks. One example is the Folding@home project,3 which provides medical researchers with the equivalent of a massive supercomputer to solve difficult protein folding problems.

An organization without these capabilities runs the risk of delayed responsiveness to its customers and market conditions. In his book Dot Cloud: The 21st Century Business Platform Built on Cloud Computing, Peter Fingar notes that traditional companies are not only dramatically asymmetric in compensation, but also in availability of information.4 Workers may be uninformed about the business, unaware of the activities of other groups and unclear about the direction of the company. Top executives may (but not always) have access to vast amounts of detailed and summary data (e.g., business intelligence reports), whereas lower-level employees are often virtually in the dark. Organizations of the future must rely on crowd computing, taking advantage of the intelligence and knowledge of multiple groups, including employees, vendors, customers and others in relevant communities of interest.

EXCESSIVE FOCUS ON VISIBLE RISKS
There is an old joke about a partygoer who is hanging around a lamp post looking for his car keys. When asked why he is looking only in that one spot, he says, “it’s just common sense—the light is better there.” To a lesser extent, reviews of
enterprise risk have followed the same trajectory. Hurricanes, earthquakes, high-profile frauds and major accounting errors are visible. And while not everyone agrees on the particulars for a path to mitigation, there is at least consensus that, indeed, such events represent clear risks. For auditors, the lamp post light shining on highly visible risks is the brightest. Silent but corrosive agents of destruction may get overlooked because they are accretive and express themselves only over time. **Figure 1** illustrates the general relationship between categories of risk and their applicable time frames. Strategic risks, which may or may not be greater in magnitude than tactical risks, are less visible. Peter Weill and Jeanne Ross, in their book *IT Savvy*, note the effect when siloed, nonstandard and nonintegrated systems are proliferated:

> Many IT professionals are quite adept at making disparate systems look integrated, but the code required to link applications becomes increasingly complex. Over time, key systems have so many links to other systems that even small changes are time-consuming, expensive and risky.

**figure 1— relative Time frame for risk visibility**

The same lack of standardization mentioned previously can also be viewed from a platform perspective. If an organization commits scarce capital to developing specific IT capabilities, it needs to have assurance that the technological base or platform is stable and well defined. In the same sense that home builders need to work in a consistent metric—meters or feet—developers need assurance that the necessary technologies will be available and properly controlled so they can count on a set of capabilities. For example, assume an organization has a single, enterprisewide ERP system and needs to install a sales tax package, such as Vertex. If the new software requires a web services interface, all relevant applications can be linked to the package using the same interface. In contrast, for an organization with multiple ERP systems, installing the same package will require considerably more effort since multiple interfaces are needed. In addition, the risk of a sales tax calculation error increases with the number of unique interfaces required.

If IT auditors are to look beyond the standard three A’s of risk (availability, access and accuracy) and move into the realm of strategy (agility), the next question is—how? Traditional risk areas, such as disaster recovery and business continuity, are considered within scope of audit reviews. Looking at strategy is not as common. However, it is suggested as a direction of high payoff. In the next section, possible ways to introduce agility risk into the traditional availability portfolio of IT risk assessment are outlined.

**The Auditor’s Role in Assessing Agility Risk**

How do auditors use these concepts in their day-to-day work? Are strategic concerns only within the purview of senior management, or do they have a place in the auditors’ assessment of risk? In the past, perhaps they did not, but in the 21st century, organizational survival depends on agility. Its importance demands that it be included in any meaningful risk analysis.

Unfortunately, there is no canned prescription for the auditor’s review of agility risk. Certainly, there are IT functional bellwethers, pointing to the presence or absence of system flexibility, tool sets and appropriate information structures. **Figures 2 and 3** show example characteristics of organizations with low agility risk (desirable) and high agility risk (undesirable). These are suggestive only—real organizations vary so much that an “agility checklist” is not feasible or practical.

Auditors typically perform formal risk assessments to help develop annual audit plans. A weakness of many risk assessments is their reliance on a simplified model or a narrow perspective. For example, it is unlikely that a 1985
Figure 2—Characteristics of Organizations With Low IT Agility Risk (Successful Management of Agility Risk)

- New products, processes, geographic locations and acquired entities can be implemented without excessive cost, time or disruption to the rest of the organization or IT systems.
- Useful systems can be scaled and used by other divisions or subsidiaries without the risk of breakdown.
- Subsidiaries can be sold without undue cost of disposal.
- Systems are standards-based (e.g., for protocols, databases, middleware and other elements). New applications can be easily integrated into existing platforms.
- Development tools, database technologies, languages and other IT components are current, so that work can be outsourced if otherwise appropriate for the organization.
- Enterprisewide analytics, such as customer behavior summaries across all business units, can be readily obtained without unwieldy cross-reference tables or complex data extraction/refactoring over multiple systems.
- Software as a Service (SaaS) is used to provide off-the-shelf applications. For example, if an organization simply needs to pay its employees and does not use human resources/payroll to gain some strategic advantage over competitors, a generic package hosted and maintained by a third party may provide greater flexibility and possibly lower cost.
- Management is committed to the concept that new systems and changes to existing ones are made based on the long-term needs of the entire enterprise. Parochial systems and structures that do not integrate with other enterprise systems are discouraged. For example, multiple item numbers for the same physical product are not proliferated across multiple business units.
- An architecture of reusable software, algorithms and processes allows rapid but safe deployment of IT systems to meet immediate business needs. Service-oriented architecture (SOA) fits this model perfectly. However, even a partial implementation of the SOA concept speeds delivery by deploying pretested, shared computing components.
- A business model is used as the scaffolding for uniform IT systems. For example, a warranty claim process may be written in Microsoft Access and, due to acquisitions, must now scale from 50 to 500 users. Platforms not designed to scale beyond a certain number of users become risky at the margins of their capacity.
- Infrastructure is standardized, documented and properly architected to support business applications.
- Unstructured data (typically vital to rapid development) has a secure place in IT’s strategic architecture. For example, it is not left isolated on individual hard drives.
- IT systems have the ability to meet unforeseen customer actual demand, rather than merely matching forecasted demand. For example, factory production lines are linked to IT systems that are flexible enough to meet rapidly changing customer preferences.
- Rapid response/flexible tools and methods are a part of IT’s tool kit. For example, virtualization, cloud and/or crowd computing may be used, allowing rapid increases or decreases in transactions, information flow, etc.

Figure 3—Characteristics of Organizations With High IT Agility Risk (Poor Management of Agility Risk)

- Systems are not scalable and cannot accommodate rapid growth. For example, a warranty claim process may be written in Microsoft Access and, due to acquisitions, must now scale from 50 to 500 users. Platforms not designed to scale beyond a certain number of users become risky at the margins of their capacity.
- The subsidiary’s links into corporate systems are convoluted and nonstandard. As a result, the cost to separate the subsidiary and corporate systems may be significant; it could influence the divestiture business decision.
- Systems are not tied to the organization’s business model. Hence, the next acquisition represents a random and potentially permanent introduction of diverse databases, infrastructures, development environments, protocols and other technologies. High variability translates into higher IT costs and greater overall risk.
- Vendor software is needlessly modified in unique ways by multiple business units within the organization. As a result, custom code proliferates more than is necessary, increasing the time, cost and risk when entitywide changes and new releases are implemented.
- ERP systems are several releases out of date so that useful bolt-on packages cannot be installed without excessive cost and development time.
- There is poor interim visibility of inventory, orders, etc., across the organization due to the heavy processing required to standardize data in disparate formats.
- Application workflow is “hard coded.” New processes cannot be added without rewriting and extensive testing.
• Can security be integrated into the existing security system(s), or will a separate security directory need to be maintained? For example, can the package use Windows Active Directory, or does a separate, duplicated user directory need to be maintained?

CONCLUSION
Many important factors in the life of large organizations cannot be quantified or can be quantified only in simple “yes/no” or “big/medium/small” terms. That does not mean that such factors are unimportant. For example, morale, enthusiasm for one’s work and job flexibility all strongly affect enterprise performance, but are hard to measure. Agility falls in that same camp. It is fuzzy but important. Auditors should include it in their assessment tool kit.

The pace of change in business and society demands that organizations maintain IT systems that are agile. The ability to quickly change products and services, divest and acquire subsidiaries without excessive effort, scale systems up and down, implement “loose coupling” of data transmissions, and link new social computing elements is critical. The auditor should include an assessment of agility as part of a strategic review of IT risk. Only the paranoid and agile survive.9

ENDNOTES
1 Use of the term “agile” in this article is conceptual and applies generally across the enterprise. It is not referring to the specific development life cycle technique referred to as “agile development.”
2 Westerman, George; Richard Hunter; IT Risk, Harvard Business School Press, USA, 2007
5 Peter Weill and Jeanne W. Ross, IT Savvy, Harvard Business Press, USA, 2009, p. 73-74
6 “Web services is a standards-based suite of technologies (XML, SOAP, WSDL, UDDI) designed to support interoperable applications to application interactions over a network.” Project Maui Glossary, University of Iowa, USA, http://provost.uiowa.edu/maui/Glossary.html, accessed 25 November 2009
7 According to Wikipedia News (http://en.wikinews.org/w/index.php?title=Encyclop%C3%A6dia_Britannica_fights_back_against_Wikipedia,_soon_to_let_users_edit_contents&oldid=780255, accessed 29 November 2009), “Encyclopedia Britannica, the authoritative reference book first published in 1768, is planning to let readers edit its entries, Jorge Cauz, its president said Friday, as it battles to keep pace with online Internet encyclopedia projects like Wikipedia.”
8 Loose coupling refers to the ability of systems to communicate with each other without rigid adherence to data layouts, sequencing of transactions and other highly idiosyncratic configurations. For example, the use of XML helps enable loose coupling because that protocol carries its own instructions on how the data are to be used. Minor program changes do not automatically result in changes to the interface structure.
9 A slight variation on the quote from Andy Grove, former chairman of Intel, “only the paranoid survive.”