

The CPA Journal

Current Issue • About the CPAJ • Search the Archives • NYSSCPA.org

THE CPA AND THE COMPUTER

April 2002

Worst Information Technology Practices in Small to Mid-Size Organizations

By *Joel Lanz*

Implementation of the guidance on how to manage information technology remains a challenge for many small to mid-size organizations. Even some of the divisions and departments of large organizations still find effectively managing IT to be a challenge. In the current economic environment, the temptation to simply cut corners is great. Yet, knowing where to cut corners and where not to often differentiates successful organizations from the unsuccessful.

Four principles of a reliable system are identified in version 2.0 of the AICPA/CICA SysTrust Principles and Criteria for Systems Reliability:

- **Availability.** The system is available for use at times set forth in service-level statements or agreements.
- **Security.** The system is protected against unauthorized physical and logical access.
- **Integrity.** System processing is complete, accurate, timely, and authorized.
- **Maintainability.** The system can be updated when required while continuing to provide availability, security, and integrity.

Leveraging these principles encourages organizations of all sizes to realize the applicability, adaptability, and cost-effectiveness of available IT management guidance.

Available Guidance

Fortunately, various professional and industry groups have developed guidance to enable executives and their advisors to identify and facilitate implementation of cost-effective IT management strategies. The following are among the most commonly used:

- The AICPA and CICA’s jointly developed SysTrust is a professional service providing assurance on the reliability of systems. Four principles, with related criteria and illustrative controls, are used to determine whether the system is reliable. According to version 2.0, the service is designed to “increase the comfort of management, customers, and business partners with the systems that support a business or particular activity.”
- COBIT is released by the COBIT Steering Committee and the IT Governance Institute. Currently in its third edition, COBIT “helps meet the multiple needs of management by bridging the gaps between business risks, control needs and technical issues.”
- The Committee of Sponsoring Organizations (COSO) of the Treadway Commission publishes its Internal Control–Integrated Framework Report. This report describes the types of internal controls put in place to keep the company on course toward business goals.
- Other major studies include the Institute of Internal Auditor’s Systems Auditability and Control (SAC) Report, the British Standards Institute’s Information Security Management (BS7779), and the Federal Financial Institution Examination Council’s Examination Handbook.

Challenges

An organization’s inability to achieve business goals or desired returns from technology investments can result from a variety of challenges; too often, failure is explained by not implementing risk management strategies that do not initially appear to be cost-effective. Yet, adapting strategies to even partially mitigate well-known IT risks can pay off. The following challenges can be overcome by cost-effective solutions.

Abdication of responsibilities. As they do with non-technology issues, the board of directors and senior management have a responsibility to exercise appropriate oversight over technology functions. Unless they exercise these oversight responsibilities and ask the tough questions of the chief information officer, it is unlikely that technology risk will be adequately mitigated. Left unchallenged, the CIO might focus on issues impacting incentive compensation determination, including keeping systems up and running and implementing systems quickly. An appropriate organizational structure (and in a larger organization, a structure that includes independent monitoring) to review technology activities and strategies is crucial.

Inability to segregate activities. Like traditional financial functions, many strategies for mitigating IT risk require appropriate segregation of responsibilities. In some organizations there is no one besides the “IT person” who feels comfortable in taking on some of the responsibilities that need to be segregated. As a result, all activities are initiated, processed, and approved by one person. This risk can be reduced by using a well-documented process to facilitate random review by an appropriate executive.

Calculator mentality. In these environments, senior management views current technology as they did technology of the past, namely as calculators. This results in a

failure to manage, monitor, and make the investments necessary to leverage the business opportunity that technology can provide. Both management and IT should extend their capabilities beyond their existing comfort zones.

Putting out fires. In many environments, technology-related personnel need to focus on immediate problems and service delivery issues. There is often no time to plan ahead, which results in expending excessive time and resources to resolve problems. This challenge can be addressed by investing in user training and appropriate strategic IT planning to support business initiatives.

Information overload. Technology developments alone are enough to keep most IT groups busy. Add to that the numerous virus and other security warnings that come out daily and require immediate attention and it is easy to understand how the function can fall behind. Organizations should subscribe to appropriate IT security newsletters, such as those distributed free by The SANS Institute and the Computer Emergency Response Team (CERT).

Expectation gap. Executive management assumes that users have a certain level of technology ability and can solve certain problems on their own. Unfortunately, that is not always the case. It is not unusual for the technology function to divert resources to solve an immediate user need. In some cases, the function is called on to support products and resolve issues that have not been budgeted or planned for. As a result, what has been budgeted and planned for gets delayed or even postponed. To prevent this, organizations should establish, communicate, and enforce computer usage policies.

Inadequate training. Depending on the organization, the IT group may have obtained most of its skills on the job rather than through training. Although this is not necessarily a bad way of developing skills, given the pace of technological evolution, regular continuing education is imperative to the successful and efficient operation of any IT function. If organizations are to overcome this challenge, they need to keep their IT staff updated on the technology needed to support business objectives and operations.

Why Examine Worst Practices

Faced with the above challenges, organizations sometimes implement the worst practices identified below. A number of these practices could have been easily averted. In hindsight, organizations that adopted these worst practices would probably agree that the money, resources, and reputation lost were not worth the “expense” saved. Examining worst practices allows organizations to learn from each other’s mistakes and to identify alternative approaches to the IT problems that need to be addressed.

The NYSSCPA’s Emerging Technology Committee maintains an electronic forum to identify and discuss “Worst IT Practices.” Society members can participate in the forum on NYSSCPA.org. The following worst practices are taken from forum discussions as well as the author’s experience in evaluating IT functions of various sizes and sophistication in public and private accounting.

Availability-Related Worst Practices

No backup or appropriate off-site storage. Systems are relied upon to support critical operations and business processes. Yet, backups are not taken, and if they are, they are not maintained off-site. As a result, if a processing error or disaster occurs, the system can not be recovered. Lost revenues due to downtime are an obvious risk facing such an organization. The greater lost value, however, would be the damage to the organization's reputation. Scheduling backups during the day and maintaining daily copies off-site, even in a bank vault, is one way to avoid this practice.

Hiring the least expensive person. This worst practice ranges from not hiring the right person to hiring the right person and not updating their skills. A person meeting the bare minimum skills is hired to save on salary or because an appropriately qualified individual is not available in the market. As is true with most business functions, investing in the right technology person or team can sometimes compensate for other poor practices. Investing in the wrong person will cost the company many times more than the salary that is saved.

No periodic testing of business continuity plan. An obvious worst practice is not having a business continuity plan; however, a worse practice, and one that unfortunately is practiced by many organizations, is not to periodically test the plan. These organizations have a false sense of security; in reality, the plan that they are relying on may have design flaws or may not adequately consider day-to-day issues.

Not monitoring IT activity. Managing IT risk is actually not very different from managing other business operations. A key component of business operations is to periodically review activity reports to ensure that operations function as intended and planned. Various technology activity reports may be available for review, including transaction levels, capacity, and availability. If their importance is not prioritized, minimal review over IT activity and early warning signs may occur. The result will be system crashes and unavailable system resources, which could have been easily avoided.

Not knowing what has been paid for. This worst practice includes many day-to-day financial issues that users or IT professionals may not be aware of. These practices include overpaying for software licenses, not properly keeping track of IT assets, not verifying telecommunication or network charges, and paying for warranties on equipment that has already been disposed of. It is not unusual to realize savings of 10–20% when an IT expense review is performed. As with other expenses and cash disbursements, appropriate financial discipline and reconciliation is critical to ensuring that expenses are limited to actual business needs.

Security-Related Worst Practices

Not applying security patches. When security in a software application is exposed, the vendor releases a fix that patches the hole in the application. Vendors such as Microsoft generally notify customers by e-mail and make the patches available from the vendor's

website. Not vigilantly applying these patches is a worst practice. As the software's holes become widely known, the organization's exposure to external hacker attacks increases. To mitigate this exposure, patches and service packs provided by the vendor should be identified and updated in a timely manner.

Not monitoring security-related advisories and updates. In addition to monitoring vendor notices about security issues, organizations such as Carnegie Mellon's Computer Emergency Response Team (CERT) and the System Administration, Networking, and Security (SANS) Institute distribute free newsletters that provide guidance on recent security threats. Worst practice organizations ignore the threats identified by these organizations. A better practice would be to assign accountability for the issues identified, determine their business impact, take action, and reconcile notices to actions taken. This would significantly reduce the opportunity for a successful attack from an unauthorized party.

Leaving factory default settings unchanged. Many vendors ship applications to customers with default settings that facilitate use and implementation of the product. Customers define their own requirements, especially in the area of security, and change the default settings provided by the vendor to enhance security controls. Worst practice companies do not perform this exercise. They run the software as delivered from the vendor. Because these default settings are widely known, including settings for default passwords, unauthorized individuals can circumvent established controls.

Not enforcing need-to-have access. In the name of efficiency, some organizations lessen the "burden" of the security officer by granting the same level of access to all employees, regardless of their job function.

As a result, various segregation of duties strategies designed through organizational controls can be easily circumvented because the system does not enforce these controls. A variation of this worst practice is providing privileged-level access to too many individuals. These worst practices partially explain why approximately 70% of unauthorized system break-ins are from internal sources. To mitigate this worst practice, organizations should periodically review the security access list and assign access on a need-to-have basis only.

Not considering network security as important as physical security. Typical of this worst practice is the story of the organization that is aggressive in obtaining all keys given to a terminated employee or consultant. Yet that same organization does not take the necessary action to remove system access privileges to the network for these people. Removing computer system privileges should be part of the termination checklist process.

Integrity-Related Worst Practices

Not appropriately testing new applications. Pressed for time due to an organization's commitment or executive desire to achieve bonus targets, a worst practice organization

will implement a system without first testing it. This results in programming errors and conversion problems being uncovered while the new system is in production and when it is impossible to return back to the older system. By implementing this worst practice, organizations can assume they will spend an exponential amount of time fixing and reconciling the new system after production, rather than the fraction of the effort that could have been invested prior to implementation. Additionally, as errors get uncovered, it is unknown whether the source of these errors is the new system itself or whether the problem existed, undetected, in the old system. In these situations it is not uncommon for the organization's reputation to suffer as well.

Not reconciling and reviewing control reports. In this worst practice the organization does not review control reports produced by the system nor does it reconcile key transactions, including suspended transactions, which arise when the system can not appropriately post the transaction. As in the financial environment, these lists need to be reconciled and reviewed on a periodic and timely basis.

Customizing the system rather than the process. Today, many companies use off-the-shelf packages instead of developing a customized application from scratch. The benefits include the knowledge and expertise of how most companies in the target market handle the system processing of the business process being automated. Worst practice companies insist on doing things their way, however, and customize off-the-shelf packages even though it may not be cost-beneficial to do. This results in delayed implementation and increased cost of consultants to make the modifications. A better approach would be to study the requirements up-front and truly understand the need and the associated costs of these modifications so that a more effective development or purchasing decision can be made.

Failure to use what's available in the system. Worst practice organizations do not leverage the features available in their systems to effectively manage their business. These features can include editing checks for inaccurate or incomplete data entry, reporting capabilities that identify unusual transactions, and application security features to enforce organizational segregation of duty controls. When there is pressure to put a system into production, expediency often comes before utilization of features. The system is configured to minimize disruptions that could be attributed to the implementation team. Correcting this practice entails reviewing system capabilities and "fine-tuning" them to the need of the organization.

Users are not trained to use the system. No matter how good the computer system, it can not achieve its intended goals unless its users are adequately trained to use it. Worst practice organizations believe that because a system is available users do not need to be trained. The cost of user inefficiency in these organizations significantly exceeds the required training investment. Inadequate training can also lead to poor customer service and inaccurate processing.

Maintenance-Related Worst Practices

Not documenting operating procedures or custom applications. By not documenting key aspects of their operations or their applications, worst practice organizations unduly rely on their vendors. Over time, these vendors become more expensive because no one else can maintain the system. Another twist to this worst practice is the employee who can similarly hold the organization hostage to their demands. Not only can these risks be mitigated, but organizations can significantly enhance IT management effectiveness by documenting critical system functions.

Improperly managing vendors. In managing their vendors, worst practice organizations abdicate their responsibility and do not review, question, or supervise the work of their vendors. Organizational policy and expectations need to be properly communicated to vendors so that they can work with the organization toward desired business objectives.

Not getting help when it is needed. Probably the worst worst practice of all is not getting help when required. IT is a very complex field and requires numerous varieties of expertise. It is imperative that the requisite expertise be obtained when needed. The future of the organization's success depends on it.

Joel Lanz, CPA, a former Big Five partner, leads a CPA practice focusing on technology risk management and is an adjunct faculty member at Pace University. He can be reached at www.joellanzcpa.com

The author would like to acknowledge the contributions of fellow members of the NYSSCPA's Emerging Technologies Committee, including Bruce Nearon (chairperson), Ken Burstiner, Ford Levy, Dave Rauch, Walter Schmidt, and Daniel Tirone.

Editors:
Paul D. Warner, PhD, CPA
Hofstra University

L. Murphy Smith, DBA, CPA
Texas A&M University

[This Month](#) | [About Us](#) | [Archives](#) | | [NYSSCPA](#)

The CPA Journal is broadly recognized as an outstanding, technical-refereed publication aimed at public practitioners, management, educators, and other accounting professionals. It is edited by CPAs for CPAs. Our goal is to provide CPAs and other accounting professionals with the information and news to enable them to be successful accountants, managers, and executives in today's practice environments.

