In September 2009, the Public Company Accounting Oversight Board (PCAOB) published a report on the first-year implementation of Auditing Standard No. 5 (AS5) in an audit of internal controls over financial reporting. AS5 was adopted in 2007 with the intent to guide auditors in performing more risk-based, top-down audits in complying with the US Sarbanes-Oxley Act. In reviewing more than 250 audits performed by eight of the largest US public accounting firms, the PCAOB inspectors found that areas that merited improvement include risk assessment, consideration of fraud, entity-level controls and deficiency evaluation. Specific findings encompassed inadequate attention to risks arising from IT general controls (ITGCs), failure in identifying compensating controls that mitigate areas susceptible to fraud risk and inappropriate conclusions made on the severity of control deficiencies identified.1

These findings are especially poignant in today’s challenging economic times when organizations face heightened risks of fraud and cost cutting and layoffs create opportunities for asset misuse. That said, tried and true IT audit practices can go a long way in helping organizations better manage risks. To this end, this article presents an integrated risk assessment framework for IT auditors to scope and execute targeted audits that better address areas of heightened risk, identify pervasive issues and assist organizations in improving their overall risk profiles over time. While focused specifically on IT risks, the integrated risk assessment framework addresses the three elements of the fraud triangle described in the Statement on Auditing Standards No. 99 (SAS 99), Consideration of Fraud in a Financial Statement Audit. In examining four key risk factors—inherent susceptibility, keys to the kingdom, process maturity and organizational maturity—the framework can be a useful tool in identifying opportunities for fraud, such as an absence of effective internal controls; incentives for fraud such as adverse relationships between employees and companies; and rationalization of fraud, such as ineffective communication of ethics.

**INHERENT SUSCEPTIBILITY**

From a Sarbanes-Oxley compliance perspective, it is second nature for management and auditors to identify systems and data with financial reporting impact. In reviewing for inherent susceptibility to fraud, however, this view can be self-delimiting and may not account for the myriad ways in which an asset may be stolen or misused. Loss of intellectual property resulting from theft of source code or loss of competitive advantage arising from stolen customer data are some of the areas that IT auditors should consider in today’s economy. Industry surveys show that, faced with job uncertainties, employees are more likely to steal or misappropriate company assets. Privileged users with access to critical computing infrastructure such as computer networks and servers are another source of risk that merits concern. Consider a real-life incident in which a systems administrator planted a logic bomb on his/her company’s computer network and purchased a significant amount of put options for the company stock in anticipation of a stock price decline accompanying the damage. The logic bomb ended costing the company more than US $3 million in remediation efforts.2

Thus, in reviewing an asset’s inherent susceptibility to fraud, it is useful to look beyond conventional financial system or data precepts. The former does not account for the full spectrum of ways in which stolen or modified assets can be misused. The latter may not take into consideration the sheer enormity of damage that can result from illicit modifications of pervasive computing infrastructure accessible to a set of privileged users but not exclusive to any specific category of corporate data. With these considerations in mind, mundane ITGCs such as access controls are cast in a new light. Depending on the level of the assessed risk, IT
auditors may choose to increase the depth of testing in areas that are deemed especially susceptible to fraud. In a retail environment, this may mean an increased focus on point-of-sale technology. In a high-tech environment, this may mean identifying key infrastructure that has pervasive impact and privileged users who have access to these systems.

KEYS TO THE KINGDOM
Users who have privileged access have the ability to create an unauthorized account, access an existing shared account or compromise an existing account belonging to a different user. In addition, unlike end-user accounts, privileged users often share generic system accounts that are manufacturer-supplied by default, whether these are operating system root accounts or database administrator accounts. As a result of an ongoing trend toward IT outsourcing as a means to cut costs, privileged users increasingly take on the face of temporary employees, contractors, consultants and business partners—groups that are expected to have a lesser degree of loyalty to an organization when compared to internal employees. Perhaps what matters more is not the depth of access granted in any one singular system, but the breadth of access granted. Access to any one system may not raise a red flag, but when aggregated in an enterprise-wide view across multiple systems, it may be a cause of concern. Therein lies the rationale for the implementation of least privilege, minimal access to resources to perform one’s job. Segregation of duties, in the form of a role-based access control, is not a new concept—neither are controls over privileged accounts or passwords, for that matter. Still, it is not a sufficient deterrent against insider fraud. Pervasiveness of access across functions can be attained through collusion with another. In a review of insider cases associated with financial gain, the Computer Emergency Response Team (CERT) found that one-third of the cases of theft of information and half of the cases of modification of information involved collusion with at least one other insider.3

In reviewing the nature of access to key assets, one cannot help but return to the basics of IT audit. Who holds the keys (privileged users, temps, contractors or business partners), where the keys are located (unknown backdoor accounts), when the keys are changed (password changes), what keys are available to an individual at any given time (pervasive access across systems) and how the keys are used (collusion either with another insider or an external party) are some of the questions that need to be tackled. In a highly outsourced IT environment, IT auditors may choose to prioritize the testing of third-party controls such as account provisioning and service-level monitoring. In a smaller company environment in which root access to key systems is held by one or selected administrative users, more attention may be required of generic system accounts and frequency of password changes. In a larger organization, a single sign-on solution may come under scrutiny for its potential to unlock excessive system access with a single unauthorized account.

PROCESS MATURITY
A robust business process possesses the requisite checks and balances (or segregation of duties) that precludes any one individual from taking a transaction from start to finish without an additional pair of eyes. In assessing risks associated with transaction processing, auditors invariably perform an end-to-end review of key classes of transactions, examining the mix of upstream vs. downstream, automated vs. manual controls that impact accuracy, completeness and validity. Opportunities for fraud arise in part from the absence of these business controls. In 2008, news broke about a trader at a European bank who leveraged his former position at the risk management office to execute a series of fictitious transactions that cost the bank more than US $7 billion.4 A contributing factor includes a lack of controls over trade cancellation and trader supervision.5

The absence of process-level IT controls also gives rise to opportunities for fraud. Timely user deprovisioning, or the lack thereof, recurs time and again in numerous fraud incidents. At first glance, this seems obvious. If a user is no longer employed with an organization, why is access not disabled? In peeling back the layers, additional complexities await:

• If the user had privileged access to one or more systems—applications, operating systems, networks, servers, databases—the straightforward act of access disabling can become an administrative nightmare.

• What of backdoor accounts that the organization may not be aware of?

• Putting privileged access aside, what if there was a lag from the time the user was terminated to the time human resources (HR) was notified?
What about a lag from the time HR was notified to the time a request was made to IT to disable access?

What if IT incorrectly end-dated the terminated user’s enterprise resource planning (ERP) account in preserving referential integrity?

What if IT were too caught up in other, more pressing endeavors to disable access on a timely basis?

These questions and more surface the everyday realities that organizations face.

Inadequate user access procedures are not the only culprits that may give rise to fraud. More recently, software development life cycle (SDLC) procedures have come under scrutiny. Besides a possible compromise in data confidentiality resulting from an absence of controls over the use of live production data for testing, other SDLC-related risks that can arise include the introduction of trapdoors in new or modified code from a lack of code review. Seen in this light, the importance of IT change management controls is underscored. If software development is an emerging focus, the maturity of system and network monitoring processes have been traditional areas of concern. A plethora of tools exists in the market, including intrusion detection systems (IDS), configuration controls, security incident event management (SIEM) systems and data loss prevention (DLP) technologies. Yet, for all the hoopla surrounding real-time data capture and exception alerts, the devil is in the details when it comes to the implementation and maintenance of ongoing monitoring mechanisms. Put simply, the mere existence of audit logs is not a control; the review is. A straightforward yet targeted tracking of suspicious File Transfer Protocol (FTP) downloads from a key server may yield more rewards than a false sense of security derived from automated signature updates.

Inadequate backup procedures have been another area of concern. In February 2008, an unencrypted backup tape went missing from a financial institution containing Social Security numbers and bank account information on 4.5 million customers. Despite several high-profile data leaks due to missing or stolen tapes over the years, many organizations fail to encrypt backup tapes. With backup-to-disk and online backup services replacing tape as the traditional medium of choice, encryption remains a key control in mitigating data breach risks. Gaps in backup procedures can also hinder an organization’s ability to recover from data loss. CERT described a case in which the restoration of deleted files failed, not because of corrupted backup, but rather from a lack of backup testing in ensuring that data were properly recorded.

The absence of process-level business and IT controls gives rise to opportunities for fraud. In assessing fraud risks from a process perspective, areas to consider include the adequacy of checks and balances in key business processes, as well as the maturity of IT processes in user provisioning, development, monitoring and backup. The frequency of business controls that are tied to specific application, i.e., application controls, can be invariably high and depends on the number of transactions processed. Conversely, ITGCs in IT processes have a lower frequency, e.g., monthly, but may have a higher impact due to the underlying pervasive infrastructure. These considerations impact the amount of work to be performed for the IT audit. IT auditors need to audit where it truly matters (pervasive impact), but also determine the level of sampling necessary to obtain a level of comfort that the controls are operating effectively. The IT processes covered here merely scratch the surface. Other processes that merit further analysis include patch and configuration management. On the former, just as it may be a time-consuming process for organizations to disable all forms of privilege associated with a terminated user, it can be challenging to release security patches to key servers on a timely basis, especially if these are not all configured in the same manner. On the latter, even if organizations do not develop their own software, they need to pay attention to fraud risks arising from unchanged default configurations that come with a commercial off-the-shelf (COTS) program or Software as a Service (SaaS).

**ORGANIZATIONAL MATURITY**

Often, an over-focus on transaction or system minutiae, whether it be process approvals, system logins or configurations, fails to take into account the overall organization environment. An absence of overarching company or entity-level controls gives rise to opportunities for fraud. Entity-level controls such as security policy definition, timely update and periodic communication can go a long way toward mitigating risks arising from employee malice or negligence. Lack of security awareness, for instance, has been a key contributor to social engineering attacks. Users visiting web sites or receiving e-mail may be fooled into downloading malicious code. IBM’s ISS X-Force division reported greater sophistication in phisher attacks with the most popular subject lines comprising merely 6.25 percent of all phishing e-mails.

Another entity-level control to assess is preemployment background screening. Preemployment background screening has been traditionally performed for finance and accounting hires. To the extent that all insiders in a CERT study on IT sabotage exhibited personal predispositions, consideration should be given to prescreening IT hires who have privileged
access to key systems with pervasive impact. As an entity control, preemployment background screening can be useful in detecting any personal dispositions to fraud. In studying the psychology of the dangerous insider, the authors of “The Insider Threat to Information Systems; Psychology of the Dangerous Insider” describe the interplay among personal vulnerabilities, situational stress and the organization environment.10

The old adage “no smoke without fire” comes to mind. Fifty-seven percent of insiders in a joint US Secret Service and CERT study were called out for inappropriate behavior in the workplace prior to performing the insider incidents.11 The availability of avenues in an organization for reporting and addressing employee concerns or issues has an important bearing on how it in turn responds to insider risks. In analyzing compliance hotline reports from 1,328 organizations, the Network and BDO Consulting found that the reporting of fraud-related incidents increased from 10.9 percent of all complaints in the first quarter of 2006 to 21 percent in 2009.12 Whether formalized in whistle-blower procedures in support of the organization’s code of ethics or documented as part of general supervisor responsibilities, the reporting and handling of workplace issues cannot be underestimated. While the system monitoring of suspicious activities can be akin to finding a needle in a haystack, following up with reported issues in the workplace may very well avert a likely insider attack.

In assessing the maturity of entity-level controls, security policies and awareness, preemployment screening and avenues for reporting and handling workplace issues are all potential areas to review. Other areas that have not been covered in this article but are worth exploring further include the placement, alignment and effectiveness of the internal audit function within the organization. In reviewing the nature of entity-level controls within an organization, the IT auditor can make better decisions on the level of reliance on entity-level controls and correspondingly the level of testing to be performed on process-level controls.

INTEGRATED FRAMEWORK

In forming an integrated risk assessment framework, IT auditors need to appreciate the different interplay between two or more risk factors. Figure 1 provides a recap of various risk factors associated with fraud. Pervasiveness of access across applications in a smaller company, for example, may be compensated by an effective set of checks and balances in key business processes. On the other hand, tightened user provisioning and monitoring in a different organization may be undermined by an overall lack of employee awareness of security policy or social engineering threats. Similarly, the value of continuous system monitoring may be diluted by relaxed provisioning over system or database administrators who have the ability to modify audit logs. More important, multiple risk factors can combine to form a trajectory toward fraud.

Consider the following scenario:

• An organization prioritizes key system and data as part of its overall enterprise risk management, but does not take into consideration selected individuals with privileged access.
• The internal system environment is characterized by multiple shared-privileged accounts on various platforms.
• While checks and balances exist for business processes, IT processes in user provisioning and monitoring remain weak.
• Entity-level controls reflect gaps in awareness of security policies with preemployment screening conducted for finance and accounting hires only.
• After a recent round of layoffs, the organization increases its level of reliance on temps and contractors for IT support.

In this scenario, each individual observation may not be a cause of concern, but combined, they form a predisposing condition for fraud. This is a pervasive issue that IT auditors need to highlight for management. Rather than provide an itemized list inventorying a hodgepodge of seemingly unrelated concerns, IT auditors need to stand back and keep management apprised of the big picture. An integrated perspective leads to well-informed management decisions. In assessing its options, the organization may undertake a phased road map. That is, in the short term, it may prioritize controls over shared passwords associated with privileged accounts and access provisioning.
for IT temporary employees and contractors. Figure 2 reflects corresponding improvements in the nature of access (keys to the kingdom) and IT process maturity. Over the long run, the organization may invest in security awareness programs for employees, temporary employees and contractors, as well as selected system monitoring tools that track privileged users. Figure 3 reflects corresponding improvements in organizational maturity and IT processes.

CONCLUSION

The recent PCAOB report, on the one hand, indicates there is still progress to be made in performing risk-based audits that add value to an organization. Today’s uncertain economy, on the other hand, continues to challenge IT auditors to better assist organizations in managing fraud risk. In adopting an integrated risk assessment framework, IT auditors become better equipped in audit planning, execution and reporting in helping organizations mitigate fraud. By providing management with an insight into the interactions that can take place among one or more risk factors, IT auditors help management uncover systemic issues that truly matter.

As processes, systems or people change, IT auditors play a key role in helping organizations revisit and adapt their risk strategies.

ENDNOTES


5 S. Allen; “Controls Lessons From the Société Générale Fraud: What Patterns Emerge From Rogue Trading Incidents of the Recent Past?,” Banking Accounting & Finance, 1 October 2008


7 Op cit, Cappelli, et al


12 The Network and BDO Consulting; 2009 Corporate Governance and Compliance Hotline Benchmarking Report, USA, 2009