

Unmasking IT Fraud: Practical Applications of SAS-99

Joel Lanz and Edward M. Patrisso

Heightedened concerns about fraud require that financial executives proactively identify risks of material misstatement due to fraud. Even without the materiality threshold, most enterprises aggressively seek to minimize the occurrence of fraud and the resultant market and reputation embarrassments that can occur. At financial institutions, in addition to the cost of funds and personnel-related expenses, information technology (IT) represents a significant area of resource focus, whether capitalized or expensed. Compared to other functions or departments, IT is unfamiliar to many financial, accounting, and audit executives (financial executives). Sometimes, due to the perceived complexity of IT, financial executives ignore the potential fraud and cost-management opportunities that exist.

When IT fraud is considered, financial executives, as well as current professional literature, limit their consideration of IT-related fraud to computer security. With significant financial allocations (sometimes but not always budgeted), use of external resources, complexity, and general unfamiliarity or direct experience with the management of IT department operations, however, financial executives face many challenges in applying traditional financial control strategies in the IT department. This article focuses on one of the most frequent fraud risks in the IT department: vendor fraud. It shows how the guidance provided in a recent auditing standard can assist financial executives to minimize the incidence of these frauds. In addition to practical guidance in mitigating the risk of IT vendor fraud, we present a case study in detecting this type of fraud.

Vendor Fraud Challenges in the IT Department

Vendor fraud in the IT department is both similar to and different from vendor frauds committed in other departments of the financial institution. The financial institution's vendors can commit it alone or IT vendors can facilitate the commission of the fraud by an employee of the institution.

IT vendor fraud requires the presence of three conditions identified in the appendix to Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit Summary* (SAS-99), which are generally present when material misstatements due to fraud occur.¹ Exhibit 1 identifies the identified condition, its description per SAS-99, and examples of its application to IT-vendor-related fraud.

Another similarity to traditional fraud is that IT vendor fraud can be categorized in the same manner as traditional occupational fraud. According to the Association of Certified Fraud Examiners, there are three major categories of occupational fraud: (1) asset misappropriations; (2) corruption; and (3) fraudulent statements, as shown in Exhibit 2.²

Yet, IT fraud is different from traditional fraud. Discounting the information security phenomenon, IT department fraud is seldom emphasized in professional literature and journals. This could be, in part, because the highly

Joel Lanz is a principal of a niche CPA technology governance and risk management practice in Jericho, NY. He can be reached at jlanz@bankingcpa.com.

Edward M. Patrisso is currently a vice president and chief internal auditor for a major international commercial bank. He can be reached at edmpat2@aol.com.

Unmasking IT Fraud

technical jargon used to describe the resources compromised are typically beyond management capability (especially in smaller to midsize institutions) to supervise or verify.

Because of the technical complexity, enhanced reliance and trust is placed on employees, vendors, and consultants involved with IT, resulting in incentives and corruption opportunities. Finally, as IT can represent a significant expense item on the typical financial institution's income statement, certain frauds can be easily camouflaged.

Reviews of General Controls May Not Identify Exposure to IT Vendor Fraud

Per generally accepted auditing standards (GAAS), general controls consist of "policies and procedures that relate to many applications and support the effective

functioning of application controls by helping to ensure the continued proper operation of information systems."³ An example that illustrates management ignorance or indifference to IT department issues is the internal audit coverage typically provided to IT departments. Unlike financial and operational audit areas, many financial institutions provide coverage for IT department controls in a single audit normally referred to as a general controls review (GCR). In a typical GCR, an auditor will review the organizational structure of the IT department, controls over system development and changes, security administration, selected logical security elements, and the business continuity plan. Except for evaluating the adequacy of insurance coverage, financial budgeting and management of the IT department is seldom included within the scope of the GCR.

Contrast this with the audit coverage provided to financial and operational areas. Typically, internal audit

EXHIBIT 1

Conditions That Underlie Fraud

Condition Fraud	SAS-99 Description	Examples of IT-Vendor-Related
Incentives or pressures	Profitability, contract and other third-party expectation performance, personal financial challenges, or performance targets	<ul style="list-style-type: none"> • Manipulating payment terms invoicing to avoid expenses that can reduce bonus payments • Providing financial kickbacks or other soft benefits to the IT decision maker
Opportunities	Arise from the nature of the industry, ineffective monitoring by management, complex or unclear accountabilities, and deficient control practices	<ul style="list-style-type: none"> • Failing to invoice in accordance with contract terms • Manipulating performance measures to show compliance • with service-level agreements and avoid penalties
Attitude and rationalization	Arise by allowing and justifying the fraudulent act to exist	<ul style="list-style-type: none"> • Careless attitude in executing purchasing responsibilities for the financial institution • Manipulating expenses to compensate vendor for initial customer-acquisition investments • Justifying pressure and poor compensation by misappropriating technology assets

procedures would include some review of budget vs. actual expenses and further investigation of significant variances. Due to the large scope of GCRs, these procedures, even if designated within the scope of the audit, would be rated as low risk and frequently omitted from most GCRs. At best, these procedures may be included as part of an institution-wide purchasing review. Even then, because the team assigned to the review typically does not have the requisite understanding of technology processes, inadequate coverage over IT purchases usually results.

Auditing Tools to Test for IT Vendor Fraud

In issuing SAS-99, the American Institute of Certified Public Accountants (AICPA) attempted to provide the accounting profession with background, perspective, and selected tools to specifically assist in the prevention or detection of financial-related fraud. Financial executives can leverage this guidance to identify current practices that could facilitate IT vendor fraud. When designing IT vendor fraud prevention or detection programs, financial executives should include the requirements to emphasize professional skepticism, to brainstorm potential fraud risks, and to communicate with executive management and the audit committee.

Emphasize Professional Skepticism

Financial executives typically have a way of asking tough questions or doing a gut check on the operations for which they are responsible. The new SAS emphasizes the need for financial executives to question activities and not take things for granted. This probably requires that these executives not only rely on the organization's chief technology officer, but also question the need for and methods of procuring technology resources.

Brainstorm Potential Fraud Risks

Perhaps one of the biggest changes to audit procedures relating to the new SAS is the requirement that the audit team identifies potential areas of fraud risk and discusses how fraud can be committed, prevented, and detected. Financial executives should perform a similar exercise focusing on IT purchases and the engagement of vendors that do not have to comply with the financial institution's policies.

Communicate with Executive Management and the Audit Committee

The SAS requires expanded communications with executive management and board committees on the subject of fraud. Getting executive management buy-in on policies and enforcing these policies can dramatically improve the ability to minimize fraud. When necessary, business units and management need to take ownership

EXHIBIT 2

Categories of Occupational Fraud

Category of Fraud	Description	Examples of IT-Vendor-Related Fraud
Asset misappropriations	Misusing an organization's assets	<ul style="list-style-type: none"> • Unauthorized copying of software • Unauthorized selling of the financial institution's technology resources
Corruption	Wrongful use of influence in a business transaction in order to produce some benefit	<ul style="list-style-type: none"> • Improperly influencing vendor selection • Undisclosed conflicts of interest with vendor • Facilitating identity theft
Fraudulent statements	Falsifying financial statements	<ul style="list-style-type: none"> • Inflated invoices or payments • Intentionally misclassifying as assets or expenses

of technology procurement decisions and better understand what is being purchased.

Case Study: Applying the SAS to Detect an IT Vendor Fraud

During a routine internal audit of a financial institution's IT department, the auditors made a shocking and almost unbelievable discovery. The vice president of IT was receiving hundreds of thousands of dollars through an elaborate and extensive kickback scheme. He was doing this by purchasing systems-related equipment and assets and hiring system consultants. Most of these expenditures were unjustified and unnecessary. He succeeded with this fraudulent activity for almost two years.

The audit began as any other, but leveraged guidance provided in SAS-99 and its predecessors (including exposure drafts). The audit team conducted a preliminary meeting with key members of the IT department. The vice president of IT was confident and quick with responses to our inquiries. We provided him with an extensive list of documentation that we would need to obtain during the audit. Risk is consistently assessed at high for the IT department; therefore, audits are usually performed on a 12- to 18-month cycle. At this time, we were conducting a GCR in addition to an annual technical audit.

General controls are the policies and procedures that govern the structure and control of the IT department. Weak general controls can seriously diminish the reliance on the entire system environment and put an institution at risk. Two parts of the general control program are: (1) a review of IT expenses and the procurement procedure; and (2) a review of the usage and hiring of IT consultants.

Our review of the procurement procedure included determining if the policies and procedures were adequate and adhered to when purchasing things, such as hardware, software, PCs, printers, and any other system-related equipment. We needed to ensure that independent bids were being received when applicable and that the bank was receiving the best price. In addition, the justification for all purchases needed to be documented and approved at the proper level. Payment should only be made by the accounting department after all expenses have been properly approved and after matching all purchase orders to the applicable invoice. Next, all assets must be compared to the shipping documents and invoices when received. Finally, the serial number of the item must be recorded on a fixed-asset

inventory report. It is important for the location of the assets to be recorded so they do not "disappear" over time.

Our review of the IT consultants was also very straightforward. We wanted to ensure they were under contract and that the contract terms were adequate. They all are required to sign an information privacy agreement informing them of the penalty for disclosing confidential information to which they would be privy. Background/security checks had to be made on all consultants before beginning work and being granted any access to systems or the premises. If the consultant was hired through a consulting agency, adequate due diligence needed to be conducted on the agency to gain confidence with the agency's validity and business practices. Once employed, all consultants need to maintain detailed time records of their assignments and the hours worked on those assignments. These time records must be approved by the direct manager and matched to the agency's bill. The rate charged by the agency also needs to be the contracted rate and the total charge recalculated for accuracy.

The Red Flags

We began our audit of purchases by selecting a sample of 15 items from the fixed-asset inventory list and obtaining the related invoices and payment documentation. When we received the invoices from the accounting department, we realized 12 of the 15 were from the same vendor. The types of purchases included PCs, servers, printers, cable wires, and even service contracts. The vendor name was not one that any of us recognized. We felt this could be a coincidence, so we selected an additional 15 items for review. As fate would have it, 13 of these 15 were from the same vendor. We now had approximately 80 percent of our sample of invoices being from the same "unknown" vendor. Before the audit was completed, we had reviewed 125 invoices.

There were several red flags as the audit was being conducted. We were initially suspicious during our inquiry process with the vice president of IT. Many of his responses were inconsistent and did not make much sense. When questioned as to the reason he provided so much business to this one unknown vendor, he informed us that an institution of this size (\$16 billion in assets) was "too small" to deal directly with the major vendors, such as Compaq, IBM, and so forth. He stated that these companies only dealt with Fortune 500 companies; therefore, we needed to use the services of a purchasing agent to

obtain the equipment for us. As we were not born yesterday, we knew this was not accurate.

In many cases shipping
documents never existed and . . .
the vendor “walked” equipment
over to the office.

When we asked him the reason for not obtaining bids for the purchases in accordance with the bank’s procurement process, we were informed that bids were only required for major projects, such as reconfiguring the computer room. While the IT department’s procurement procedures were vague, we did know that this was not the intended interpretation of the bank’s policy.

After beginning to review the invoices in detail, we noted in some cases the equipment purchased was being sent directly to the home of the vice president of IT. For the assets being sent to the office, we were informed that shipping documents were being thrown away when the asset was received. After further questioning of the staff, however, we were informed that in many cases shipping documents never existed and that the vendor “walked” equipment over to the office for the majority of the deliveries. The staff also informed us that in many cases the purchase orders were only cosmetic in order for the invoice to be paid by the accounting department. The purchase orders were actually generated after the invoice came in for payment.

The vice president of IT was also responsible for maintaining the inventory of system assets, which were very vague and impossible to trace to actual equipment. The list did not contain a detailed description or a detailed location of the assets.

We then learned that three consultants employed by the bank were also being paid through this same unknown vendor. We felt there was no way that hiring consultants through a third party could be cost-effective. When we questioned the vice president of IT, he informed us that he did not know where to find consultants, so this vendor was hired to locate consultants to suit the company’s needs. All of the consultants were with different agencies; unbeknownst to them, they were being paid through a third party. All of the consul-

tants had been working for the bank for several years. After researching the payment history for these consultants, we noticed that the bank actually was paying these consulting agencies directly in the past and had only begun to pay them through the third party over the past year and a half. This again discredited the explanation of the vice president of IT.

A review of the time sheets used by the consultants revealed that they were very generic and did not contain the name of any agency. All three of these consultants were from different agencies, yet all used the same generic time sheets. The vice president of IT informed us that this was the way his previous superior wanted it. Several of his actions were blamed on a previous executive, who had retired from the bank more than two years before.

The invoices used for the consultant payments were also generic for each consultant and appeared as if they could easily be PC-generated. A review of the invoices for the past year revealed that they were all in sequential order with no breaks, suggesting either our bank was their only client or we had our own invoice numbering system from the vendor. The vice president of IT informed us that the invoices were in sequential order based on his request. This made it easier for him to “control.” We, however, could not determine how this was benefiting him based on his processes.

As the audit continued and we began to research deeper, we realized two other consultants were being paid through another third-party vendor. Again, invoices and time sheets were generic. As a matter of fact, they looked exactly like the invoices and time sheets being used for the first third-party vendor.

We obtained the check register and reviewed a large sample of the canceled checks to the vendors. In all cases, the checks were payable to the vendor personally in his name and not the company name on the invoices. Finally, the checks were being sent to a post office box across the street from the bank. Based on the address on the invoices, this vendor resided on the other side of town. Many post offices were located closer to the alleged office of the vendor.

How the Audit Team Reacted to the Red Flags

Needless to say, we reacted very quickly to the red flags. We did not necessarily know whether we had fraud yet, but we certainly knew something was not right or at least not efficient and cost-effective. We notified senior management and the audit committee immediately. We

constantly sent them new information, as new data became available.

We attempted to gain our own pricing for the consultants and found that the phone number indicated on the invoice was not in service. The company was not listed in the yellow pages or through directory assistance. We attempted to visit the address indicated on the invoices and found it was an apartment building. According to the doorman, no one by the name of the vendor had ever occupied an apartment in that building.

We obtained a Dun & Bradstreet (D&B) report on the vendors and all of the agencies involved. The D&B report on the vendor in question revealed a company of a similar name; however, it indicated a completely different line of business.

We requested that due diligence be conducted on all agencies and vendors involved. The documentation received from the vendor was extremely suspicious. The certificate of incorporation did not appear to be on the usual type of paper, there was no evidence of a seal on it, and it did not list the officers of the company. In addition, the vendor did not supply the financial statements we had requested, stating that its accountant was traveling.

The bank hired a private investigator to research the personal life and history of the vice president of IT and the vendor in question. After accumulating all of our information and documenting the inconsistencies and false statements of the vice president of IT, the chief auditor and senior general manager interviewed him. The vice president was visibly nervous as he was questioned. We documented his responses; he pleaded ignorance to most questions. The chief auditor and senior general manager then met with the bank's attorney to determine how to proceed legally.

Details of the fate of the vice president of IT remained confidential; needless to say, he was terminated immediately. While he never confessed to wrongdoing, he also never denied any and never aggressively questioned the reasons for his termination.

Ultimately, we learned that the primary vendor that received 80 percent of the bank's IT business was a longtime associate of the vice president of IT (more than 10 years). The second vendor turned out to be related to the vice president of IT and was an associate of the first vendor.

In a nine-month period, the bank paid the primary vendor \$1.1 million and the secondary vendor \$400,000 in expenses for supplies, equipment, and consultants of the total \$1.9 million IT expense. None of the money was ever recouped, mainly because the documentation

was so poor that it was difficult to determine which purchases were legitimate and which were not.

Neither vendor had any other clients besides the bank. Neither vendor had any other employees. Both vendors "went out of business" immediately.

How the Fraud Was Committed

Roughly 80 percent of the bank's IT equipment and supplies was being purchased through one vendor. The bank was employing five out of seven consultants through two different third parties, both of which were not legitimate and appeared to be funneling funds back to the vice president of IT.

Vague procurement procedures allowed for various interpretations. The vice president of IT never implemented a true procedure to require independent bids for major purchases. He purposely maintained an ambiguous asset inventory, so assets could never be traced. He was the sole individual responsible for approving the purchases and receiving the assets when they arrived. This allowed him to ship assets to his home, to neglect to tag the assets, or to authorize the bank to pay for assets that were never received.

No official records were maintained. The vice president of IT did not maintain shipping documents. He had his staff create purchase orders for cosmetic purposes only, after the equipment was already purchased and received.

He never informed human resources when consultants were starting an assignment or being released. He was solely responsible for hiring and terminating consultants himself. He was solely responsible for negotiating and maintaining the consultants' contracts. He was solely responsible for approving their time sheets and verifying their hours. He had been submitting approved time sheets to accounting for payment of hours and even days that the consultants never worked.

Why the Fraud Succeeded

This fraud would not have succeeded in a well-controlled environment. The vice president of IT was successful because all levels of management trusted him; therefore, he was rarely questioned. When questioned, he was a smooth talker and appeared to have a viable answer for everything. He indicated that senior executives no longer with the organization had granted him complete authority. Since these executives were no longer with the bank, they could not be

questioned. When his own staff, lower-level managers, or auditors questioned him, he would become belligerent, concealing his acts with intimidation.

The vice president of IT had full control over locating and hiring consultants. He never obtained independent bids from vendors. He had very little oversight from his superiors and he intentionally maintained poor documentation.

Basic Control Deficiencies

This fraud was a textbook example of the result of poor internal controls. There was no segregation of duties. The vice president of IT had ultimate control and *carte blanche* capability.

Human resources was never aware of the hiring or releasing of IT consultants and, therefore, could not control them or obtain due diligence on the vendors.

The bank had no centralized purchasing function. Each department was responsible for its own purchases, thus allowing for too much control by the purchaser.

Purchasing authority was concealed through ambiguous and vague procurement procedures (*e.g.*, no system for obtaining bids, no control for delivery checks of assets). The bank's approval process for assets focused on correctness of payment rather than approval of the actual purchase. There was no vendor management procedure in place (*e.g.*, approving vendors, conducting due diligence).

Despite these deficiencies, this fraud happened primarily due to extremely poor oversight and control by the accounting department. Where was the accounting department during this period? Accounts payable is any institution's final line of defense. The accounting department must control the expenses in accordance with the institution's policy, ethically, and in the best interest of the institution.

The accounting department never required the necessary standard documentation, such as purchase orders and shipping documents. It did not require confirmation of the receipt of the asset. It did not validate the claims of the vice president of IT with his superiors that he was in

fact granted *carte blanche*. It did not question the high level of volume to one vendor. It did not question the checks being made out to an individual personally. It did not question the mailing of the checks to a post office box across the street from the office. These were all red flags that should have immediately been detected and questioned by the accounting department. The controller informed us that accounting staff members took the vice president's word at face value. Accounting staff members also indicated that they were aware of consultants being paid for hours that they did not work. When they questioned the vice president of IT, they were informed that they were wrong and needed to mind their own business.

Adequate Controls Are Essential

Two very valuable lessons should be learned from this case study. First, at smaller companies, management often will say, "Those recommendations are great in a perfect world, but we just aren't staffed to implement those types of controls." No matter how small or how large a company is, adequate internal controls can be implemented. It is much easier to implement them with a larger staff; however, it is still possible with a small one. Without solid controls, the risk of loss greatly outweighs the possible minor inconvenience of an added check and balance. Second, functions that are charged with the responsibility to manage risk must have the intellectual integrity not to accept easy answers or to dismiss something because it requires the involvement of a specialist. By rigorously applying the fundamental practices of risk management, they can often overcome the bullying that can lead to frauds, such as that identified in this article.

Notes

1. Codification of Statements on Auditing Standards Section AU316.85.
2. *2002 Report to the Nation: Occupational Fraud and Abuse*, Association of Certified Fraud Examiners, p. iii.
3. See AU 319.45.