BURZENSKI & COMPANY, PC
VETERINARY FINANCIAL ADVISORS

DO YOU KNOW WHERE YOUR INTERNAL CONTROLS ARE?
Checks and Balances to avoid Embezzelment

Preventing Fraud in Your Hospital

Gary I. Glassman, CPA
Burzenski & Company, P.C.
Tel. (203) 468-8133 Fax (203) 469-8515

Estimates of fraud in the United States

Consider the following estimates of fraud in the United States:

(i) Health agencies estimate fraud represents 10 percent of the nation's health care bill at a cost of $75 to $130 billion a year.

(ii) The tax gap, which is the difference between what people owe the government and what they pay, exceeds $200 billion a year.

(iii) The IRS estimates that electronic tax filing fraud costs the government billions of dollars a year. For example, in one 10-month period, fraudulent electronic returns increased 105 percent.

(iv) Thirteen percent of credit card sales resulted in loss due to fraud. For example, fraud losses at MasterCard exceed $300 million a year.

(v) Losses related to telephone fraud exceed $10 billion a year.

(vi) Some 60 percent of Americans have shoplifted. An estimated 200 million shoplifting incidents a year cost U.S. businesses almost $12 billion or about $150 per family per year.

The pervasiveness of dishonesty

Not only are the losses to fraud very high, but the estimates of the number of people who commit or would commit a dishonest act are also very high. Consider the following:

(i) The director of fraud and security for a large consulting company stated that of every 10 workers, three look for a way to steal, three would steal if given an opportunity, and four would usually be honest.

(ii) Two out of three college students admit to cheating on exams.

(iii) An Institute of Management study found that 87 percent of managers were willing to commit fraud if it would make their organizations look better.

(iv) A study of 400 people found that 47 percent of top executives, 41 percent of controllers, and 76 percent of graduate-level business students were willing to commit fraud by understating write-offs that cut into their company's profits.

What is the definition of fraud?

Fraud is defined as an intentional act of deceit for the purpose of gaining an unfair advantage that results in an injury to the rights or interests of another person. This can be accomplished through presentation of false or misleading information, suppressions of the truth, lies, tricks, and cunning. Fraud perpetrators are often referred to as white-collar criminals to distinguish them from criminals who commit violent crimes.

Three steps to fraud

To commit most frauds, a perpetrator must take three different steps: (i) the theft itself; (ii) converting the asset to personal use; and (iii) concealing the fraud.

1. Theft

Theft involves stealing something of value, such as cash, inventory, tools, supplies, equipment, or data. It can also be an intentional reporting of misleading financial information.

2. Conversion

The perpetrator converts the assets into a form that can be used personally. Conversion is usually required for all stolen assets except cash.

a. Stolen checks must be deposited to an account from which the perpetrator can withdraw funds.
b. Information (such as trade secrets or confidential company data) is often sold to someone such as a competitor.
c. Industry experts estimate that computer companies annually lose up to $200 billion in computer chips due to armed robbery and employee theft. In some circles, computer chips are better than gold. Their theft is being referred to as the crime of the electronic age.

Employees who steal computer chips must convert them to cash. A sophisticated black market exists, and the chips often change hands as much as ten times in three days. When some companies run short, they often end up buying their stolen chips back.

The following example illustrates the conversion practices discussed above:

Example: On the advice of its trusted manager, a brand-name carpet manufacturer approved purchase orders replacing looms described by a subsidiary as deteriorated past reconditioning. Instead of being discarded or sold to a dealer, the used looms, which were in perfectly sound condition, found their way to another building in a town close by, along with skilled workers to man them. In a short time, a new low-priced carpet maker was bidding against the original brand.

3. Concealment

The perpetrator must conceal the crime in order to avoid detection and to continue the fraud. Concealing a fraud often takes more time and effort and leaves behind more evidence than the actual theft does. Where there are checks and balances in the system, the perpetrator often must "cook the books" to avoid detection.

a. The theft of cash may require the employee to doctor the bank reconciliation and/or make false accounting entries to avoid detection.
b. Taking cash takes only a few seconds, but altering records to hide the theft can be more challenging and time consuming. One effective way to hide an employee theft is to charge the stolen item off to an expense account. For example, an employee could steal $10,000 and charge it off to miscellaneous expense. Or, a payroll clerk could add a fictitious name to the employee payroll records, intercept the paycheck, and cash it. The company would be missing funds, but the books would be in balance because there was a debit to wages expense and a credit to cash.

In the case of expense accounts, the perpetrator's principal exposure is limited to a year or less, because expense accounts are zeroed out at the end of the year.

If perpetrators chose to hide the theft by affecting another balance sheet account, they would have to continue to hide it. Hence, one of the most popular ways to cover up a fraud is to hide the theft in an income statement account.

One of the most effective ways to prevent the theft/conversion/concealment process is to have an effective system of internal controls. When such a system is in effect, fraud is made much more difficult. The internal control system must either be overridden or two or more perpetrators must collude with each other.

The nature and elements of fraud

A typical fraud has a number of important elements or characteristics.

(i) The perpetrator of the fraud must have gained the trust or confidence of the person or company being defrauded. This confidence makes it possible for the perpetrator to commit and conceal the fraud. For this reason, fraud schemes are often referred to as cons (from the word "CONfidence").

(ii) In contrast to most other crimes, a perpetrator uses trickery or cunning to commit the fraud rather than force. Instead of using a gun, a knife, or physical force to commit a crime, perpetrators use false or misleading information. The intent is to get someone to give them money or assets. They hide their tracks by falsifying records or other information about the asset.

(iii) Most frauds, once begun, are rarely terminated voluntarily by the perpetrator. The greed of the perpetrators is such that they continue to exploit the opportunity to obtain extra funds. The following factors can contribute to reasons why perpetrators may continue a fraudulent scheme:

  (a) They begin to depend on the "extra" income and cannot afford to stop.

  (b) When faced with the prospect of having additional money at their disposal, many move to a higher lifestyle that requires even greater amounts of money.

  (c) Most perpetrators will take as much money as they think their particular scheme or method will allow them to take. The amount taken is usually limited only by the success perpetrators have in concealing their actions or in the accidental or contrived opportunities the perpetrator is able to discover and/or create.

  (d) Some frauds are self-perpetuating. If perpetrators stop, their actions would be discovered, and they would get caught.

  (e) Fraud perpetrators rarely save or invest what they embezzle. In all of the cases that one particular fraud expert has investigated or read about, he has only uncovered two perpetrators that saved the money embezzled. One perpetrator converted the money to gold bullion and stashed it in his basement. The other put the money into trust funds for her grandchildren.

(f) If the perpetrators are not caught shortly after they begin, they typically become moreconfident of their scheme. Many get greedy and take larger amounts of money. These larger amounts are more prone to be scrutinized, and a scheme that might have gone undetected for some time is uncovered because the amounts taken rise to unacceptable levels. Such perpetrators usually make a mistake that leads to their apprehension. In time, the sheer magnitude of the amount of the fraud leads to its detection.

Example: At one auto repair shop, the accountant, a lifelong friend of the shop's owner, embezzled ever-increasing funds from the shop over a seven-year period. In the last year of the fraud, when the embezzler took over $100,000, the owner, facing bankruptcy, eventually had to fire the accountant and have his wife take over the bookkeeping. When the company began doing better, the wife began looking into the reasons for the recovery. She uncovered the fraud.

(g) The most significant contributing factor in most frauds is the failure to enforce existing internal controls.

(1) Internal Controls

We need good internal controls to prevent fraud. Most fraud occurs because of a lack of or monitoring of internal controls. The risk factors are:

- Inadequate internal control;
- Nonenforcement of internal control; and
- Inadequate monitoring of significant controls.

The most significant opportunity risk factor in most frauds is not enforcing existing internal controls. Other major factors are the absence of adequate internal controls and overriding existing internal controls.

Prevention Techniques

(a) Develop strong internal control – The best way to deter fraud is to design, implement, and enforce sufficient controls to make fraud difficult to perpetrate. The internal control system should include controls for authorizations, clear lines of authority, independent checks on performance, appropriate documents and records, and physical safeguards. Likewise, there should be a separation of duties between the authorization, custodial, and record-keeping functions. The lack of these controls is, itself, a risk factor.

Internal control should contain:

- Preventive controls to deter fraud;
- Detective controls to discover fraud soon after it occurs; and
- Corrective controls to remedy the problems caused by the fraud.

The overall responsibility for secure and adequate internal control lies with top management. Management must also establish procedures to ensure that the controls are complied with and enforced.

(b) Controls are much more effective when placed in a system as it is built, rather than as an afterthought. There should be controls to ensure enforcement of internal control and controls to ensure that internal control is not overridden.

(c) Management should be involved in the design and monitoring of controls.

(2) Risk Factor - Insufficient separation of duties

(a) Good internal control demands an adequate separation of duties. No single employee should be given too much responsibility. An employee should not be in a position to both perpetrate and conceal fraud. To achieve effective segregation of duties, the following functions must be separated:

(b) Authorization – Top management empowers certain employees to authorize transactions and make decisions. Authorizations are documented by signing, initialing, or entering a code on the transaction document or record. Employees who subsequently process the transaction should verify the presence of the appropriate authorization(s).

(c) Recording – This involves preparing source documents, maintaining journals, ledgers, or other files, preparing reconciliations, and preparing performance reports.

(d) Custody – This may be direct, as in the case of handling cash or maintaining an inventory storeroom, or indirect, as in the case of receiving customer checks via mail or writing checks on the organization's bank account.

If two of these three functions are the responsibility of a single person, problems may arise.

Prevention Technique

(a) Design and enforce internal control that incorporates adequate separation of duties.

(b) Design clear and proper authorizations procedures.

(c) Use the computer to help segregate duties – In modern information systems, the computer can often be programmed to perform one or more of the above-mentioned functions and, in essence, replace employees. For example, computer systems are now capable of recording a **digital signature** (or fingerprint), which signs a document with a piece of data that cannot be forged. The principle of separating duties remains the same; the only difference is that the computer performs the function rather than a human.

(3) Risk Factor - Inadequate safeguarding of assets

(a) If there are inadequate safeguards over assets, there is a good probability that some of them will "sprout wings and fly away." When people think about safeguarding assets they most often think of cash, checks, and physical assets, such as inventory and equipment. However, in today's world, one of a company's most important assets is its information. Accordingly, steps must be taken to safeguard both information and physical assets.

Prevention Technique

Design and implement adequate safeguards over physical assets. The following procedures are used to safeguard assets from such threats as theft, unauthorized use, and vandalism:

- Restrict access to physical locations, such as computer rooms and inventory storage.
- Restrict physical access to assets, thereby limiting the chances of loss. For example, cash registers, safes, lockboxes, and safety deposit boxes should be used to limit access to cash, securities, blank checks, and other paper assets.
- Restrict access to computer files and information by using passwords and security codes.
- Protect records and documents. Access to vital records and documents can be restricted by locking them in desks or file cabinets. Access to blank checks and documents should be limited to authorized personnel.
- Discarded paper documents should be shredded.
- Employees should be informed of the consequences of using illegal copies of software, and the company should institute controls to see that illegal copies are not in use.
- Closed-circuit televisions can be used to monitor areas where sensitive data or easily stolen assets are handled.

Processing of transactions

(4) Risk factor - No independent checks of performance

Not having independent checks on performance is a major risk factor.

Prevention Technique

Design and implement independent checks. Internal checks that evaluate the performance of each transaction processing function are an important control. The checks should be independent because they are more effective if performed by someone other than the person responsible for the original operation.

These independent checks include:

(a) Reconciliation of independently maintained records – For example, checking accounts should be reconciled to bank statements and subsidiary ledgers should match to their general ledger control account balances.

(b) Comparison of actual quantities to recorded amounts – For example, funds in a cash-register drawer should be reconciled at the end of each shift with the cash register tape.

(c) Batch totals – When records are grouped for processing, batch totals are created. The same control totals are generated by the computer during each subsequent processing step. Discrepancies between the totals would indicate that an error occurred during the previous processing stage.

(d) Independent review – Segregation of duties often results in two or more persons processing a transaction. In such cases, the second person should review the work of the first, performing such tasks as checking for proper authorization, reviewing supporting documents, and checking the accuracy of critical data items.

(5) Risk Factor - Inadequate record keeping

Maintaining inadequate documents and records also poses significant risk.

Prevention Techniques

(a) Require accurate records be kept and checked carefully for irregularities.
(b) Require properly designed documents that are used appropriately. The proper design and use of documents and records helps prevent fraud. Documents should:
(c) Be as simple as possible to minimize recording errors and facilitate efficient recordkeeping, review, and verification;
(d) Contain a space for authorizations or the receiving person's signature if they are used to initiate a transaction or transfer assets to someone else; and
(e) Be sequentially prenumbered so each can be accounted for. This reduces the likelihood of fraudulent use by dishonest employees.

(6) Risk Factor - Inadequate supervision

Fraud is more likely to occur when management fails to set up appropriate management oversight functions such as adequate supervision and monitoring of remote locations.

Prevention Technique

Develop and implement controls for ensuring effective supervision of employees. Effective supervision involves training and assisting employees, monitoring employee performance, correcting errors that occur, and safeguarding assets by overseeing employees who have access to them.

(7) Risk Factor - Employees with a criminal or questionable background

One control feature that is often lacking is a background check on all potential employees. To illustrate, consider the case of a large company that decided to check carefully the backgrounds of all potential employees. They screened 6,398 employees and rejected 851 (13.3 percent). This is in line with industry estimates that 10 to 15 percent of screened employees will be rejected. Most are rejected due to previous unsatisfactory employment, providing false information (education, employment, military, etc.), or a past criminal record.

Prevention Technique

Conduct background checks. Check potential employees, audit clients, and major vendors. One way to do so is to use an investigative agency, which can check:

- Underworld or questionable connections
- Financial history to determine credit history, heavy indebtedness, previous bankruptcies, or whether the principals are living beyond their means.

(8) Risk Factor - Management's own disregard for guidelines, controls, or regulatory authorities

When management fails to follow company controls and guidelines it sets a bad example for employees. Employees tend to see the company as having two sets of rules, one for them and another for management. When management lives by a different set of rules, employees focus more on what management does than what it says. In the employee's mind "What you do speaks so loudly I cannot hear what you say." As a result, it is easier for employees to rationalize their behavior by saying, "But management does it."

Prevention Techniques

A critical aspect of an organization's control environment is a management philosophy and operating style emphasizing honesty and adherence to controls.

(a) The more responsible management's philosophy and operating style, the more likely it is that employees will behave responsibly in working to achieve the organization's objectives.

(b) If management shows little concern for internal control and ethical behavior, employees are not likely to be as diligent or as effective in achieving specific control objectives. Management's philosophy and operating style can be assessed by answering questions such as:
- Does management take undue business risks to achieve its objectives, or does it assess potential risks and rewards prior to acting?
- Does management attempt to manipulate performance measures such as net income so its performance is seen in a more favorable light?
- Does management pressure employees to achieve results regardless of the methods required, or do they demand ethical behavior? In other words, do they believe the ends justify the means?

(c) Management should display and communicate an appropriate attitude regarding the internal control and financial reporting processes.

(9) Risk Factor - Assets highly susceptible to misappropriation

Assets such as cash and small, valuable items are vulnerable to theft and abuse.

Prevention Technique

Certain company assets are especially susceptible to misappropriation; take special care with them. Since employees with situational pressures are more likely to misappropriate them, special care should be taken with the following assets:
- Cash, especially where large amounts are on hand or processed;
- Inventory that is small and easy to move, has a high value or is in high demand; and
- Fixed assets that are small, marketable, or lack ownership identification.

(10) Risk Factor - Unclear policies and procedures

When policies and procedures are clearly spelled out, they act as a deterrent to potential perpetrators.

Prevention Technique

Publish a policies and procedures manual containing specific conflict of interest statements. A written policy and procedures manual is an important tool for assigning authority and responsibility in many organizations. The manual should spell out management policy with respect to handling specific transactions. In addition, it should document the systems and procedures employed to process those transactions. It should include a detailed listing of the organization's chart of accounts, along with sample copies of forms and documents.

(11) Risk Factor - Placing too much trust in employees

Opportunities arise when too much trust is placed in key employees who are not subject to the normal checks and balances that are so important to safeguarding company assets. Victimized employers are often heard saying, "I cannot believe that person would commit a fraud. That person was one of my most trusted employees."

Prevention Techniques

(a) Persons in positions of trust should be subject to more frequent and thorough accountability.
(b) Do not phase out checks and balances needed for proper controls.

(12) Risk Factor - No policy of mandatory vacations during which someone else performs duties

Many fraud schemes, such as lapping and kiting require the ongoing attention of the perpetrator. Therefore, employees should be required to take an annual vacation, during which time their job functions are performed by others. If mandatory vacations were coupled with a temporary rotation of duties, these types of ongoing fraud schemes would fall apart.

Prevention Techniques

(a) Set and enforce a policy that requires all employees to take an annual vacation.
(b) Have someone else perform the duties of the person on vacation. The ability to commit and conceal a fraud is thwarted when another person is required to perform the perpetrator's job. People who are not required to take a vacation are sometimes caught when they become sick or are not able to be present at work.

(13) Risk Factor - Lengthy tenure in a key job

Long-term employees who hold key positions may start to think of themselves as "above the law."

Prevention Technique
Rotate key employees periodically or transfer them to different functions. When employees are rotated it often leads to actions that bring misconduct to light.

(14) Risk Factor - Lack of support for company values

There should be an effective means of communicating and supporting company values or ethics.

Prevention Technique

Develop a code of ethics. This should communicate corporate values and motivate employees to live by it. Of particular importance is a formal company code of conduct addressing such matters as standards of ethical behavior, acceptable business practices, regulatory requirements, and conflicts of interest.

(15) Risk Factor - Inadequate training

Inadequate training of staff poses a significant fraud risk.

Prevention Technique

Develop and implement a training program that provides employees with needed skills. This should include fraud prevention and detection skills.

(16) Risk Factor - Inaction

Management's failure to correct known reportable conditions on a timely basis also makes an organization appear "fraud-friendly."

Prevention Technique

Design, implement, and enforce controls to ensure management's correction of known reportable conditions on a timely basis.

(17) Risk Factor - No audit trails

Knowing that there are no audit trails can further entice a potential perpetration.

Prevention Technique

Design and implement an accounting system with adequate audit trails.

(18) Risk Factor - Managerial carelessness or inattention to technical details

Prevention Technique
Train managers to adequately supervise subordinates and to pay attention to technical details.

(19) Risk Factor - Operating in a crisis or rush mode

During times of crisis, abnormal pressure, or rush jobs, there are additional opportunities to commit fraud.

For example, when a special project is being hurried for completion, the normal controls are often pushed aside, which results in the following:

- Signatures are obtained authorizing uncertain purchases;
- Reimbursements are made rapidly and with little documentation;
- Recordkeeping falls behind and cannot be reconstructed;
- Materials come and go rapidly and can easily be misplaced; and
- Ultimately, no one is entirely sure who is doing what.

Prevention Technique
Continue to enforce internal control at all times.

The following are some danger signs of embezzlement:

1. Unusual rise in accounts receivable write-offs.
2. Unexplained differences between physical inventory counts and inventory records.
3. Missing files.
4. An employee who never takes a vacation or days off. Maybe this person is super dedicated, or maybe the person can't take the chance of someone else taking over and finding out what he or she has been up to.
5. Extremely complicated accounting entries.
6. Unusual and unexpected decrease in profits.

Obviously, one or more of these signs does not necessarily mean an embezzler is at work. But a business owner should be alert to the possibility. You can deter thieving tendencies by close involvement in the company's day-to-day activities.

Weaknesses in controls

Some of the most commonly overlooked weaknesses that make embezzlement easier for the dishonest employee are as follows:

1. Checks received in the mail go directly to the person who records, posts them and prepares the deposits, with no independent record being made of the receipts.

2. Bank statements go directly to the person who reconciles them.

3. Checks and cash are allowed to accumulate before being deposited.

4. Cash sales are loosely handled and sales slips are not accounted for by renumbering.

5. There is no separate cashier to reconcile daily cash receipts with sales slips.

6. Cash register amounts are not compared with bank deposits.

7. Monthly statements are mailed by the very same person who works on accounts receivable without being checked by a superior and compared to the accounts receivable schedule.

8. Customers report discrepancies on their statements, but no one in authority attempts to reconcile them.

9. Accounts receivable are never confirmed with the customer.

10. Uncollectible accounts are simply written off without being first turned over to an attorney or collection agency for collection.

11. No one bothers to count and review petty cash because the fund is only a few hundred dollars.

12. Petty cash slips are made out in pencil and are not canceled after use.

13. No one cancels invoices, vouchers, supporting documents and checks to make sure they are not resubmitted for payment.

14. Invoices are often paid without the initials of the person who is supposed to authorize their payment.

15. The person authorizing payment of invoices does a perfunctory examination of the supporting documents: receiving reports, purchase requisitions, freight bills, etc.

16. Physical inventories are not compared to book inventory figures and differences are not satisfactorily explained.

17. Anyone with packages can walk out of the plant or other facility without question.

18. Payroll checks are distributed by the same person who prepares the payroll or maintains the time records.

19. The person signing payroll checks does not scrutinize the payroll, has little idea of its approximate total or who the employees are.

Some businesses may not have sufficient personnel to provide the desired segregation of functions, but if the proper procedures are carefully followed, they can reduce the possibility of losses due to employee dishonesty.

SOME COMMON METHODS OF EMBEZZLEMENT

Misappropriation of Cash Receipts

A. **Cash sales**

Covered by:

1. Not recording sales; destruction or omission of sales slips.
2. Tampering with cash register tapes; understating footings of cash sales reports.
3. Charging customers more than the duplicate slip shows.
4. Controversial charges collected, but reported as uncollectible.

B. **Collections on accounts and notes receivable**

Covered by:

1. Lapping (both of bank balances and – with currency collections – petty cash)
2. Kiting, or inter-bank check transfers.
3. Write-off of accounts as uncollectible.
4. Improper credits for allowances or discounts.
5. Entry in customers accounts only, concealed by:
   a. Over-footing of cash receipts and tampering with adding machine tapes.
   b. Tampering with bank statements, passbooks and customers' statements.
   c. Insertion of fictitious ledger sheets at time of an audit.
6. Reporting fake robberies of cash.

C. **Receipts of miscellaneous income and credits**

Covered by:

1. Not recording (including proceeds of illegitimate note executed to company bank).
2. Recording as an exchange item.

Misappropriation of Disbursements

A. **Cash on hand**

Covered by:

1. Cashing vouchers a second time.
2. Payment of the same expense out of petty cash and also by check.
3. Use of fictitious vouchers.
4. Raising amounts on legitimate vouchers.
5. Cashing worthless "exchange" checks.
6. Unauthorized borrowing by employees.
7. Unclaimed wages and dividends pocketed or check endorsements forged and cashed through the petty cash fund.
8. Transfer of cash from one fund to another at time of an audit.

B. **Cash with banks**

Cover by:

1. Fictitious creditors' invoices (checks cashed through petty cash, secret or falsely named bank accounts, or forged endorsements).
2. Increasing amounts on creditor's invoices; refund of excess pocketed or split with the creditor.
3. Paying creditor's invoices twice and appropriation of the second check.
4. Failing to record purchase returns, allowances, and discounts, and appropriating check or cash payments therefor.
5. Payment of fictitious refunds or allowances.
6. Increasing telephone and electric bills, etc., by employee's personal bills from the same utility.
7. Making off with the check properly drawn to the creditor.
8. Padding payroll rates, time, production or number of employees.

9. Fictitious advances to employees, and neglecting to deduct them from subsequent payrolls.

10. Duplicating payment for the same payroll or invoice by two checks signed by each of two authorized officers or partners.

11. Appropriating checks made out to "cash" or the bank, supposedly for creditor's account, payment of note or expense.

12. Buying improper disbursements in personal accounts of partners and officers.

13. Altering the name of a payee or increasing the amount of a check after signature.

14. Forging checks and destroying them on return by the bank, concealed by forced footings in the cash journal, or by raising amounts of legitimate checks.

15. Mingling cashier's funds with company funds and withdrawing company's funds after cashier's are exhausted.

16. Charging illegitimate withdrawals to fictitious customers' accounts.

Merchandise

A. Illegitimate removal of merchandise.
Covered by: 1. Overstatement of lists of physical inventory.

2. Unauthorized requisitions.

3. Entry only in stock records of fictitious purchase returns.

B. Reporting as received, items not received (usually associated with collusion between the creditor and the receiving clerk).

Miscellaneous

A. Undercharging customers through reduction in unit prices, quantities or calculation.

B. Allowing officer or employee free services or merchandise, or at reduced rate, when not entitled.

C. Manipulating financial showing to secure excessive commissions, bonuses or dividends.

BURZENSKI & COMPANY, PC
VETERINARY FINANCIAL ADVISORS

Internal Control Procedures
Cash

Control Objectives

1. Cash receipts are recorded accurately as to account, amount and period.
2. Cash disbursements are recorded accurately as to account, amount and period.
3. Cash disbursements are made for authorized and received goods and services.

	Yes	No
1. Are checks presented with the invoice or statements and signed by the practice owner?		
2. Are the use of signature stamps restricted or prohibited?		
3. Are checks not returned to the preparer after signing?		
4. Is mail opened by someone other than the bookkeeper and is the daily collection of accounts receivable independent of accounts receivable posting activity?		
5. Is adequate employee fidelity bond insurance maintained?		
6. Are checks made out to "cash" prohibited?		
7. Is access to the computerized accounting program limited?		
8. Is a daily shift cash-out performed which agrees to the computerized veterinary software?		
9. Are cash-out sheets printed, signed off on and approved by management?		
10. Are daily deposit tickets done which agree to the computerized veterinary software?		
11. Are restricted endorsement (e.g. for deposit only) placed on check remittances upon receipt?		
12. Are deposits made daily to the bank?		
13. Are credit card machines used which can batch process daily transactions and which have printers?		

BURZENSKI & COMPANY, PC
VETERINARY FINANCIAL ADVISORS

Internal Control Procedures
Invoicing and Accounts Receivable

Control Objectives

1. Sales represent valid transactions (i.e., products sold or services provided).
2. Sales of goods or services are recorded timely and accurately as to account, amount and period.
3. Cash receipts are properly applied to client accounts.
4. Client returns or other allowances are approved and recorded accurately as to account, amount and period.
5. All services rendered are appropriately approved for acceptance of credit risk, and doubtful accounts are recognized and provided on a timely basis.

	Yes	No
1. Are pre-numbered receipts or cash registers effectively used and controlled?		
2. Is the veterinary software password protected for limited access to change a client invoice, issue a credit, charge off a bad debt, or change any other part of a client record?		
3. Is the veterinary software password protected for limited access to print an entire client list?		
4. Are monthly statements sent and an aged accounts receivable listing prepared and reviewed?		
5. Are collection procedures established for accounts at 30 days, 60 days, 90 days and to the collection agency?		
7. Are exam room and hospital travel sheets utilized to determine accurate billing?		
8. Are estimates utilized and signed by clients for services rendered?		
9. Are payment agreement forms utilized for charging?		
10. Do authorizations for surgeries and other procedures indicate payment is expected at the time services are rendered?		
11. Are daily fee exception reports run for fee overrides?		
12. Are manual discounts prohibited or limited with proper approval?		
13. Have daily, monthly, and year-end close-out procedures been established for cut offs at the end of each accounting period?		
14. Have procedures been established to determine what reports to run for each reporting period and how they will be stored?		

BURZENSKI & COMPANY, PC
VETERINARY FINANCIAL ADVISORS

Internal Control Procedures
Inventory

Control Objectives

1. Acquisitions of inventory are authorized and properly recorded.
2. Movement and usage of inventory are recorded accurately as to account, amount and period.
3. Inventory is properly valued, and excess, slow-moving, and obsolete items are identified and accounted for on a timely basis.
4. Physical loss of inventory is prevented or promptly accounted for on a timely basis.

	Yes	No
1. Are inventories adequately safeguarded (limited access) and insured?		
2. Are computerized inventory records maintained?		
3. Is access to computerized inventory records limited?		
4. Are reconciliations done between physical counts and computerized records?		
5. Are physical counts of inventory performed at least yearly?		
6. Are packing slips matched with inventory received?		
7. Are packing slips matched with invoices before payment? Are discrepancies resolved?		
8. Are pricing changes made when vendors indicate price increases?		
9. Has a system for determining optimum inventory re-order quantities been established and/or maintained?		
10. Are inventory turnovers in times and days calculated?		
11. Does the owner/manager periodically assess whether excess, slow moving, obsolete inventory items are accounted for appropriately?		