

Visual Learning Maps

Introductory Financial Accounting



Click to Go to the Website

VIRTUAL TEXT BOOK

INTERNAL CONTROL – 1 of 7

Internal Control is the constant attitude of guardians.

OBJECTIVES & PURPOSE

This vigilance concentrates on three operational realities.

1. Assets must be protected from theft and misuse. This responsibility is called **Safeguarding**.
2. **Reliable and Accurate** accounting records must be provided by the systems generating the records supporting the financial statements.
3. **Efficiency** and **Effectiveness** in items one and two above must be evaluated. Efficiency means
 - *“doing things right - correctly following procedures”;*Effectiveness means
 - *“doing the right things - are the procedures right? Do they need to be changed?”*

Also...

- Clear Audit Trail
- Affect on the quality of products and services
- Identification of, and response to, change

PRINCIPLES – Cornerstones of Planning & Implementing Controls

Define Responsibilities and Authorizations

Written practices include job descriptions and operational procedures for each employee and each task they perform. These are useful to the organization and to each person in the organization because they define:

1. How exactly to do the job
2. “Who” is specifically responsible for what?; and
3. “What” authorization(s) are required for normal processes and for exceptions to normal processes?

Unclear processing and responsibility procedures cause confusion and misunderstandings that lead to wastes time or inaccurate record balances.

INTERNAL CONTROL – 2 of 7

PRINCIPLES –continued

Ensure that Persons who have Physical Control over Assets are NOT Doing the Bookkeeping for those Assets – Segregation of Duties

- During the inventory count at a large appliance retailer, thousands of boxes containing refrigerators, stoves, washers, dryers and so on were counted and compared to inventory records – they matched. One of the auditors decided to walk across the tops of the boxes in the football field sized warehouse. After a short distance, the auditor fell through an empty box. Then all the boxes were opened. Only the boxes at the perimeters had appliances in them; which accounted for only 40% of the inventory.

Internal Control was weak. The warehouse manager had authority over all shipping and receiving AND was responsible for daily updating of the inventory records. The manager had his own business on the side - secret sales and carefully arranged delivery via the back door. He knew exactly what the inventory records should be; and of course did not record the back door *'shipments.'*

Ensure that One Person Does NOT Have Control Over a Complete Process – Segregation of Duties

- A bank loans manager who had authority to approve loans up to \$200,000 received the “Employee of the Year” award because he had created so much business for the bank, by making more than double the number of loans than any other manager. It turned out that “*created*” was literal. He had created hundreds of fictitious companies, each with their own bank account (at different banks) over which he had signing authority. He simply approved loans and transferred the funds into the phony company’s account.

The manager processed all the paperwork; had authorization over the release of funds; and was provided the check to deliver to the client. An internal auditor noticed that all the applicants had post office boxes for addresses. The Internal Audit Department descended upon the branch. The manager confessed. Only a small percentage of the missing millions were recovered because the manager had a gambling addiction.

THE LESSON IS:

Never let the people in charge of the candy keep the candy records!

Weak Internal Control around attractive assets is temptation. Remove it!

INTERNAL CONTROL – 3 of 7

PRINCIPLES –continued

Independent Verification – Internal and External

Smaller businesses generally do not have Internal Audit and / or Security departments. Large corporations do.

Smaller organizations must rely on two control oversight activities. The first is awareness of the owners about what is happening day-to-day; and their ability to recognize weaknesses. Second, the role of the external auditor becomes critical in examining, evaluating and reporting on the Internal Control systems. One of the levels of thinking auditors use is to ask, "*How would I commit fraud in this system?*"

In both smaller and larger organizations, the first step is to list the assets in their "*attractiveness*" order. Cash is always number one. The ranking of other assets varies from business to business. Inventory controls in a business selling sand and gravel will be fewer than a business that retails expensive jewelry. Another factor is "*the ease of walking*" factor. Watches *walk* easier than canoes. Can they *walk* out the back door or the front door? (The front door is shoplifting; the back door is shrinkage.)

No matter how small or large the business is, no matter how complex the system; the guardian's task is to physically prove or disprove the asset amount on the balance sheet by verification. The person performing the verification must be totally independent of the operation accounting for the asset **and** independent of the operation that has physical control of the assets. In one hand the verifier has the details of the asset record, whether it is gravel, gold bars or canoes, and with the other hand and eyes, the verifier physically counts the asset and records the count. The count is then compared to the records. Are they the same? If not, why not? How much is it out? A 3% inventory variance may be acceptable in the gravel business, because of other factors such as rain and wind. It is unacceptable in the vehicle business. If 3% of the cars are missing - where are they and how were they lost? Management must be informed and action taken to; 1) reconcile the difference (find the cars); and 2) determine if and what changes are to be made.

The more attractive and "*walk prone*" assets are the more often they should be verified. Surprise counts should occur as well as scheduled counts, depending on the asset. Vehicles at dealerships are counted monthly, but surprise counts occur several times a month. Large corporations even count their buildings every few years. Surprise counts are not usually used for buildings, but they are used in businesses for jewelry, fashion and sports ware, liquor, computers, pharmaceuticals, tires; and of course gold bars and petty cash –virtually in all goods in retail and wholesale distribution businesses.

INTERNAL CONTROL – 4 of 7

PRINCIPLES –continued

Information Technology Systems

Computer systems have evolved to a separate and significant area of responsibility for Internal Control Guardians. Management Information Systems are critical to decision making and running the business. Fraud, theft, and sabotage in this context can be devastating to a business; for three reasons:

- 1) People perceive that stealing digital information is not as immoral as stealing cash or goods
- 2) Code attacks are a constant threat; and
- 3) Network systems connected to the Internet are standard in business operations.

In addition to protecting hardware, it is a worrisome reality that systems and valuable data are susceptible to internal and external attack. Items under constant review are:

- Network vulnerability to viruses, worms & spam
- Password management & shared file structure
- Back up and disaster recovery procedures
- Remote access security
- Spy ware
- Integrated system processing without human judgment

Internal Audit, Security and IT departments

Not long ago, these departments were operationally separate. Internal Control strongly depends on these departments communicating regularly, conducting formal reviews; and cross training staff. Safeguarding assets and the accuracy of systems involves a spectrum of defenses that must be evaluated and changed as attacks change.

These departments must also keep up to date on statute and case law pertaining to Privacy Issues when considering covert surveillance on customers or using server software to track employee computer activities. Ethics, the Law, Union Agreements, and organizational policy are rarely operationally or philosophically synchronous.

INTERNAL CONTROL – 5 of 7

STANDARD CONTROLS

- Security Checks - Employees

More organizations are using security checks in the hiring process. Bonding employees who handle cash or valuable inventory has been commonplace for decades, now, security screening, both procedural and random, is standard.

- Cross Training Programs

People from all departments in an organization are regularly assigned to the Internal Audit Department for periods of one to three years. These people contribute their skill and detailed home department knowledge to Internal Audit and return to their home department with the learning experience of guardianship. The IT department regularly involves its staff with internal audits and internal audit reports.

- Equipment

Safes and vaults, time card imprinters, surveillance cameras, lighting, locks, building alarms, product sensor alarms, one-way mirrors, homing devices, magnetic swipe & digital grid scanners, infra-red and motion detection devices, Global Positioning System tracking, FM transmitters - are a just some examples of security tools widely used.

- Budgets & Variance Reporting

If fraud is committed internally through the books, mysterious figures will show up in departmental accounts – and will be investigated.

- Pre-numbered Printed Forms; and Automatically Assigned Sequential Numbers in Paperless Systems

Checks, invoices, inventory requisitions, receipts, journal entries, etc. increase accuracy; and provide audit trails for daily operations and auditors.

- Vacations

In operations where individuals prefer not to take vacations, supervisors should advise Internal Audit; this is an indicator that something untoward may be occurring. A policy should be in place to require vacations to be taken.

- Documenting History of Attempts

Training in the Internal Audit and Security departments has an important component of documentation of historical events pertaining to fraud and theft within the organization.

- Benchmarking

Organizations, often in different industries, compare Internal Audit, Securities and IT “best practices.”

INTERNAL CONTROL – 6 of 7

INTERNAL CONTROLS ARE NOT STATIC

No one has described any Internal Control system as *“It’s perfect; don’t touch it!”*

This requires continuous analysis and applied judgment as things and times change. Shoplifting would be greatly reduced if all customers were strip-searched before they left the store. This would tend to decrease sales and lawsuits would be costly. So, Internal Control strives for balance.

Examples of How Things Change

- Computer hardware and software upgrades require implementation testing AND Internal Audit review.
- New systems = new procedures; revised systems = revised procedures
- High staff turnover
- The advent of organized shoplifting has changed security measures and consequently, the cost
- Outsourcing
- Criminal charges in recent years against senior management foster cynicism throughout the organization; people think *“If the leaders have their hands in the cookie jar, why can’t I?”*

WHAT DOES BALANCE MEAN?

It means that the System of Internal Control provides **REASONABLE ASSURANCE** that assets are safeguarded and that the accounting records are accurate, dependable and reliable. Reasonable assurance means that Internal Control systems must balance the cost of controls with:

- 1) Their degree of effectiveness; and
- 2) Their affect on the business.

INTERNAL CONTROL – 7 of 7

A FEW MORE DANGERS

Collusion and Sabotage

Collusion is a secret pact between two or more persons to circumvent controls to commit fraud or an illegal act - a criminal conspiracy. Standard controls are designed for standard situations. Controls will generally not immediately identify these plots unless significant amounts are involved. In the longer term controls will uncover minor frauds.

Sabotage is the intentional and deliberate act to impair or destroy property. This can mean buildings or data. Security procedures focus on identifying situations and individuals that have the potential to commit sabotage; and prevent it. When sabotage occurs, controls are designed to: 1) Identify who had the capacity to do it; and 2) limit the extent of the damage.

Malicious Code

Malicious Code is a constant threat because creative hackers abound. It is generally an external attack, but can also arise internally – sabotage again.

Corporate Espionage

Security departments are actively engaged in detecting corporate espionage. Research and development costs reside on the balance sheet; therefore as assets, they are directly linked to the Safeguarding responsibility. Knowledge of new products, marketing and implementation plans do not appear on the balance sheet, nevertheless are valuable to the future of the business. Corporate espionage can be more devastating to a business than any other attack.

Here is a quote from a leading consultant in the field:

A growing number of intelligence gatherers regularly transgress ethical and even legal boundaries on behalf of corporate clients both here and abroad.

Such spooks—many of them former government spies who migrated to the civilian sector after the Cold War ended—will resort to every dirty trick in the book. They'll lie, misrepresent themselves, steal phone records and do anything they can to wiggle their way into your confidence. Perhaps even now they are shopping their specialized talents to your competitors. So, listen up and remember that forewarned is forearmed.

Imagination and paranoia are useful defensive mindsets in these realities.