INTERNAL CONTROLS:

AICPA - INTERNAL CONTROL STANDARDS:

The information that follows is specific guidance from the American Institute of Certified Public Accountants Codification on Statements on Auditing Standards AU319 “Internal Control in a Financial Statement Audit”.

Internal control is a process effected by an entity’s board of directors, management, and other personnel designed to provide reasonable assurance regarding the achievement of objectives in the following categories: (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, and (c) compliance with applicable laws and regulations.

Internal Control consist of five interrelated components, which are:

- **Control environment** sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
- **Risk assessment** is the entity’s identification and analysis of relevant risks to achievement of its objectives, forming a basis for determining how the risks should be managed.
- **Control activities** are the policies and procedures that help ensure that management directives are carried out.
- **Information and communication** are the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.
- **Monitoring** is a process that assesses the quality of internal control performance over time.

CONTROL ENVIRONMENT:

Factors effecting the control environment include: integrity and ethical values, commitment to competence, board of director or audit committee participation, management’s philosophy and operating style, organizational structure, assignment of authority and responsibility, and human resource policies and practices.

**Integrity and Ethical Values:** The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of the entity’s ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management’s actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values.
and behavioral standards to personnel through policy statements and codes of conduct and by example.

- **Commitment to Competence:** Competence is the knowledge and skills necessary to accomplish tasks that define the individual’s job. Commitment to competence includes management’s consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

- **Board of Directors or Audit Committee Participation:** An entity’s control consciousness is influenced significantly by the entity’s board of directors or audit committee. Attributes include the board or audit committee’s independence from management, the experience and stature of its members, the extent of its involvement and scrutiny of activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management, and the interaction with internal and external auditors.

- **Management’s Philosophy and Operating Style:** Management’s philosophy and operating style encompass a broad range of characteristics. Such characteristics may include the following: management’s approach to taking and monitoring business risks, management’s attitudes and actions towards financial reporting (conservative or aggressive selection from available alternative accounting principles, and conscientiousness and conservatism with which accounting estimates are developed); and management’s attitude toward information processing and accounting functions and personnel.

- **Organizational Structure:** An entity’s organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. An entity develops an organizational structure suited to its needs. The appropriateness of an entity’s organizational structure depends, in part, on its size and the nature of its activities.

- **Assignment of Authority and Responsibility:** This factor includes how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring that all personnel understand the entity’s objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

- **Human Resource Policies and Practices:** Human resource policies and practices relate to hiring, orientation, training, evaluating, counseling, promoting, compensating, and remedial plans. For example, standards for hiring the most qualified individuals with emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior demonstrate an entity’s commitment to competent and trustworthy people. Training policies that communicate prospective roles and responsibilities and include practices such as training schools and seminars illustrate expected levels of performance and behavior. Promotions driven by periodic performance
appraisals demonstrate the entity’s commitment to the advancement of qualified personnel to higher levels of responsibility.

**RISK ASSESSMENT:**

Risk assessment for financial reporting purposes is its identification, analysis, and management of risks relevant to the preparation of financial statements that are fairly presented in conformity with generally accepted accounting principles. For example, Risk assessment may address how the entity considers the possibility of unrecorded transactions or identifies and analyzes significant estimates recorded in the financial statements. Risks relevant to reliable financial reporting also relate to specific events or transactions.

Risk relevant to financial statement reporting include external and internal events and circumstances that may occur and adversely affect an entity’s ability to record, process, summarize and report financial data consistent with the assertions of management in the financial statements. Once risks are identified, management considers their significance, the likelihood of their occurrence, and how they should be managed. Management may initiate plans, programs, or actions to address specific risks or it may decide to accept a risk because of cost or other considerations. Risks can arise or change due to circumstances such as the following:

- **Changes in Operating Environment:** Changes in the regulatory or operating environment can results in changes in competitive pressures and significantly different risks.
- **New Personnel:** New personnel may have a different focus on or understanding of internal control.
- **New or Revamped Information Systems:** Significant and rapid changes in information systems can change the risk relating to internal control.
- **Rapid Growth:** Significant and rapid expansion of operations can strain controls and increase the risk of a breakdown in controls.
- **New Technology:** Incorporating new technologies into production processes or information systems may change the risk associated with internal control.
- **New Lines, Products, or Activities:** Entering into business areas or transactions with which an entity has little experience may introduce new risks associated with internal control.
- **Corporate Restructurings:** Restructurings may be accompanied by staff reductions and changes in supervision and segregation of duties than may change the risk associated with internal control.
- **Foreign Operations:** The expansion or acquisition of foreign operations carries new and often unique risks that may impact internal control, for example, additional or changed risks form foreign currency transactions.
- **Accounting Pronouncements:** Adoption of new accounting principles or changing accounting principles may affect risks in preparing financial statements.
CONTROL ACTIVITIES:

Control activities are the policies and procedures that help ensure that necessary actions are taken to address risks to achievement of the entity’s objectives. Control activities have various objectives and are applied at various organizational and functional levels.

Generally control activities that may be relevant to an audit may be categorized as policies and procedures that pertain to the following:

- **Performance Reviews:** These control activities include reviews of actual performance versus budgets, forecasts, and prior period performance; relating different sets of data operating or financial to one another, together with analysis of the relationships and investigative and corrective actions; and review of functional or activity performance, such as a bank’s consumer loan manager’s review of reports by branch, region, and loan type for loan approvals and collections.

- **Information Processing:** A variety of controls are performed to check accuracy, completeness, and authorization of transactions. The two broad groupings of information systems control activities are general controls and application controls. General controls over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance. These controls apply to mainframe, minicomputer, and end-user environments. Application controls apply to the processing of individual applications. These controls help ensure that transactions are valid, properly authorized, and completely and accurately processed.

- **Physical Controls:** These activities encompass the physical security of assets, including adequate safeguards such as secured facilities, over access to assets and records; authorization for access to computer programs and data files; and periodic counting and comparison with amounts shown on control records. The extent to which physical controls intended to prevent theft of assets are relevant to the reliability of financial statement preparation, and therefore the audit, depends on the circumstances such as when assets are highly susceptible to misappropriation. For example, these controls would ordinarily not be relevant when any inventory losses would be detected pursuant to periodic physical inspection and recorded in the financial statements. However, if for financial reporting purposes management relies solely on perpetual inventory records, the physical security controls would be relevant to the audit.

- **Segregation of Duties:** Assigning different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets is intended to reduce the opportunities to allow any person to be in a position to both perpetrate and conceal errors or irregularities in the normal course of his or her duties.
INFORMATION AND COMMUNICATION:

The information system relevant to financial reporting objectives, which includes the accounting system, consists of the methods and records established to record, process, summarize, and report entity transactions (as well as events and conditions) and to maintain accountability for the related assets, liabilities, and equity. The quality of system-generated information affects management’s ability to make appropriate decisions in managing and controlling the entity’s activities and to prepare reliable financial reports.

An information system encompasses methods and records that:

- **Identify and Record** all transactions.
- **Describe on a Timely Basis** the transactions in sufficient detail to permit proper classification of transactions for financial reporting.
- **Measure the Value** of transactions in a manner that permits recording their proper monetary value in the financial statements.
- **Determine the Time Period** in which transactions occurred to permit recording of transactions in the proper accounting period.
- **Present Properly** the transactions and related disclosures in the financial statements.

Communication involves providing an understanding of individual roles and responsibilities pertaining to internal control over financial reporting. It includes the extent to which personnel understand how their activities in the financial reporting information system relate to the work of others and the means of reporting exceptions to an appropriate higher level within the entity. Open communication channels help ensure that exceptions are reported and acted on.

Communication takes such forms as policy manuals, accounting and financial reporting manuals, and memoranda. Communication also can be made orally and through the actions of management.
MONITORING:

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls on a timely basis and taking necessary corrective actions. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

Ongoing monitoring activities are built into the normal recurring activities of the entity and include regular management and supervisory activities. Managers of sales, purchasing, and production at divisional and corporate levels are in touch with operations and may question reports that differ significantly from their knowledge of operations.

In many entities, internal auditors or personnel performing similar functions contribute to the monitoring of an entity’s activities through separate evaluations. They regularly provide information about the functioning of internal control, focusing considerable attention on evaluating the design and operation of internal control. They communicate information about strengths and weaknesses and recommendations for improving internal control.

Monitoring activities may include using information from communications from external parties. Customers implicitly corroborate billing data by paying their invoices or complaining about their charges. In addition, regulators may communicate with the entity concerning matters that affect the functioning of internal control, for example, communications concerning examinations by bank regulatory agencies. Also, management may consider communications relating to internal control from external auditors in performing monitoring activities.
FINANCIAL STATEMENT ASSERTIONS:

- Existence
- Completeness
- Rights/Obligations
- Valuation
- Presentation/Disclosure

All transactions recorded must have these in order to be considered valid.
FRAUD:

Black’s Law Dictionary – a generic term that embraces all means by which humans can devise, which is resorted to by one individual to get advantage over another by false suggestions or by suppression of truth, and includes all surprise, trickery, cunning, dissembling, and any unfair way by which another is cheated.

US Supreme Court - a tort (a legal wrong) that meets the following conditions:
- Misrepresentation of a material fact
- The perpetrator knew it was false
- Made with the intention that the misrepresentation would be relied on
- The victim did rely on it and as a result suffered a loss

Institute of Internal Auditors – encompasses an array of irregularities and illegal acts characterized by intentional deception. It can be perpetrated for the benefit of or to the detriment of the organization.

AICPA – “a broad legal concept” that is distinguished from error depending on whether the action is intentional or unintentional.

Types of Fraud:
- Misrepresentation in financial reports
- False or overstated expense reimbursements
- False or overstated vendor invoices
- Check tampering
- Lapping of cash receipts
- Bogus credits
- Fictitious vendor
- Substitution
- Altering bank deposits
- Forging checks
- Kickbacks
- Bid-rigging
- Ghost employees
- Skimming
- Overstatement of payroll hours/effort
- Asset misappropriations / Stealing
- Theft / Larceny

Formula for Fraud:
- Incentive / Pressure to commit fraud
- Opportunities to commit fraud
- Attitudes / Rationalization
FRAUD - What You Should Know About the Sociological Factors that Cause Fraud

The key to dealing with fraud is to focus on prevention. It is much less expensive and more effective to prevent fraud from happening than it is to try to detect the crime. By the time the fraud is discovered, the money is usually already gone and chances are it will not be recovered. Furthermore, it is costly and time consuming to investigate a fraud.

But if we can prevent fraud from occurring in the first place, we avoid all those losses, and we save the time and effort of trying to reconstruct fraudulent transactions, track down the perpetrator, and reclaim missing funds.

In order to prevent fraud, we must first understand why it occurs. What causes people to steal from their employers or to "cook" the books? Most people would say fraudsters are motivated by greed, but generally speaking, greed is not the primary motivator.

To understand why employees, managers, and executives commit fraud, we must understand the fraud triangle.

The Fraud Triangle

Most people who commit fraud against their employers are not career criminals. The vast majority are trusted employees who have no criminal history and who do not consider themselves to be lawbreakers. So the question is, what factors cause these otherwise normal, law-abiding persons, to commit fraud?

The best and most widely accepted model for explaining why "good people" commit fraud is the fraud triangle. This is a model developed by Dr. Donald Cressey, a criminologist whose research focused on embezzlers, people he called "trust violators."

According to Cressey, there are three factors that must be present in order for an ordinary person to commit fraud. All three of these factors must be present at the same time in order for fraud to occur. The three factors are now referred to as:

- Pressure
- Opportunity
- Rationalization

Pressure

The first leg of the fraud triangle represents pressure, or what Cressey called a perceived non-sharable financial need. This is what motivates the crime in the first place. The fraudster has some financial problem that he is unable to solve through legitimate means, so he begins to consider committing an illegal act such as stealing cash or falsifying a financial statement as a way to solve his problem. The financial problem can be personal (too deep in personal debt) or professional (the person's...
job or business is in jeopardy). Examples of pressures that commonly lead to fraud include:

- Inability to pay one's bills
- Drug or gambling addiction
- Need to meet earnings to sustain investor confidence
- Need to meet productivity targets at work
- Desire for status symbols such as a bigger house, nicer car, etc.
- Non-shareable problems and the importance of status

Notice that Cressey did not say fraud is motivated by financial pressure, but instead by a non-shareable financial pressure. This is a very important distinction. Everybody has financial pressures, but not everybody commits fraud.

What constitutes a non-shareable need is completely in the eye of the beholder. One person could lose his rent money gambling and will be motivated by this problem to write a company check to cover his rent. Another person might suffer the same loss and not feel compelled to commit an illegal act.

Non-shareable problems all involve some sort of embarrassment, shame, or disgrace. More importantly, they all threaten the fraudster's status as a person who is trusted by others. In almost every fraud case, the fraudster's financial problem relates to status-seeking or status-maintaining. Consider the following examples:

- A CEO develops a new business plan. Unfortunately, the plan fails miserably, and sales plummet. Having just suffered through two previous bad quarters, the CEO is afraid that this latest disaster will cost him his job. Unable to face the shareholders and the board of directors and tell them the bad news, the CEO persuades the CFO to help him create fictitious sales to mask the losses. The CEO is convinced that they can increase sales and correct the books next quarter.

- A high-ranking financial officer experiences heavy losses in her personal investments. She feels unable to admit to her personal financial failures because this would hurt her status as a highly trusted person who is in charge of her company's finances. Therefore, she tries to resolve her personal financial problem in secret by writing company checks to a shell company she controls.

- A business manager's division suffers losses due an economic downturn. This puts her division in jeopardy of missing its earnings targets. Even though the losses were due to forces beyond her control, the manager, who has a history of business successes, fears being labeled a failure if she misses her goals. She records fictitious sales in order to maintain the appearance of success.

- A bank teller desires prestige symbols such as a nicer car, better clothes, jewelry, etc., but she cannot afford them on her salary. Because she cannot legitimately obtain these items, and because she is unwilling to "settle" for
less expensive counterparts, she begins stealing from her cash drawer to purchase these status symbols.

**Opportunity**

The second leg of the fraud triangle is opportunity, sometimes referred to as perceived opportunity, which defines the method by which the crime can be committed. The person must see some way she can use (abuse) her position of trust to solve her financial problem with a low perceived risk of getting caught.

It is also critical that the fraudster be able to solve her problem in secret. Remember that fraudsters are motivated by concerns over status. If a perpetrator is caught embezzling or falsifying financial information, this will hurt her status at least as much as the underlying problem she was trying to conceal. So the fraudster not only has to be able to steal funds, she has to be able to do it in such a way that she will likely not be caught and the crime itself will not be detected.

For example, if an employee has access to blank checks she may see an opportunity to forge a company check payable to herself. But that check might well be spotted during the reconciliation of the bank statement and she would be caught. In this case, even though there is an opportunity to steal the funds, there is no opportunity to steal them in secret. But suppose the same employee also reconciles the company's bank statement. Now, she can write a check payable to herself and then when the bank statement arrives she can destroy the fraudulent check and force the balance on the reconciliation. Now the person has a perceived opportunity to commit fraud.

**Rationalization**

The third leg of the fraud triangle is rationalization. As we stated already, the vast majority of fraudsters are first-time offenders with no criminal past. They do not view themselves as criminals. They see themselves as ordinary, honest people who are caught in a bad set of circumstances.

Because the fraudster does not see himself as a criminal, he must justify the crime to himself in a way that makes it an acceptable or justifiable act. This is known as rationalization. Common rationalizations include the following:

- I was only borrowing the money
- I was entitled to the money
- I had to steal to provide for my family
- I was underpaid/my employer had cheated me
- My employer is dishonest to others and deserved to be fleeced

While the perpetrator must rationalize the crime to himself before he commits the crime, after the act has taken place the rationalization will often be abandoned.

**When Does the Fraud Triangle Not Apply?**
The fraud triangle applies to most embezzlers and occupational fraudsters, but it does not apply to the "predatory employee"—the person who takes a job with the intent of stealing from his employer.

Also, as we stated earlier, while a rationalization is necessary for most people to begin committing fraud, the rationalization will often be abandoned after the initial act has taken place. Most frauds are not one-time events. They usually start as small thefts or misstatements and they gradually increase in size and frequency. As the perpetrator repeats the act, it becomes easier to justify until no justification is needed at all.

**What Does the Fraud Triangle Tell Us?**

Perhaps the most important lesson to be learned from the fraud triangle is that normally all three factors must be present for fraud to occur. If any one of the three elements is missing, fraud will normally not occur.

Cressey's model also tells us that concerns over status, not greed, is the primary motivator for occupational fraud.

**Why Sanctions Don't Deter Fraud**

We can also deduce from the fraud triangle that simply punishing people who are caught committing fraud is not an effective way to deter fraud. There are several reasons why this is so:

- Fraudsters only commit their crimes when there is a perceived opportunity to solve their problems in secret. In other words, fraudsters do not anticipate getting caught. The threat of sanctions does not carry significant weight with a fraudster because he never expects to face them.

- Fraudsters rationalize their conduct so that it seems legal or justified. Thus, they do not see their actions as something that is or should be sanctioned.

- Because fraudsters are primarily motivated by status, the greatest threat they face is that their crime will be detected. Detection will result in loss of status. Any sanctions that follow are only a secondary consideration.

**Building an Effective Deterrence Program**

The fraud triangle provides an outline for deterring fraud in any company. An effective deterrence program will directly target the three elements of the fraud triangle. Organizations should seek to:

1. Reduce pressures on employee that might push them into committing fraud.

2. Reduce perceived opportunities to commit fraud.

3. Dispel rationalizations for engaging in fraudulent conduct
FRAUD PREVENTION AND DETECTION:

Have a strong internal control system in place. Control environment and risk assessment is most important. Ensure that all transactions have more than one person involved from the beginning of the business process to the end. When risks are high due to the limitation of staff, closer supervision over the business process, independent reconciliations/reviews, and audits are important to compensate for control weaknesses.

_Fraud prevention_ is accomplished by:
- Segregation of duties
- Rotation of duties in positions susceptible to fraud
- Require employees handling financial transactions to take regular vacations of 2 weeks or more at one time and let someone else perform their normal responsibilities
- Adherence to organizational policies and procedures especially those concerning documentation and authorization of transactions
- Physical security over assets such as locking doors and restricting access to certain areas.
- Proper training of employees
- Independent reviews and monitoring of tasks
- Clear lines of authority
- Conflict of interest policies, which are enforced
- Regular independent audits of areas more susceptible to fraud

_Fraud detection_ is accomplished by:
- Independent reconciliations
- Inspections of documents (canceled checks)
- Employee complaints
- Discovery of unusual items that indicate follow-up is necessary
- Problems detected by audits
- Customer or vendor complaints, such as payments not being credited
- Unusual or unexplained report variances or financial statement trends
TYPES OF CONTROL ACTIVITIES: (PREVENTIVE – DETECTIVE)

Control activities are either preventative or detective.

**Preventive controls** are built in as part of the system and look at each transaction similarity to stop errors before they are recorded in the system. Preventive controls include segregation of duties, appropriate organizational lines of responsibility/authority, proper communication, signed statements/representations, written contracts/agreements, trustworthy employees, knowledgeable employees, performance management (work plans/ gaining commitment/ counseling/ monitoring/ evaluation), employee training/ reinforcement, supervision/oversight, independent authorization, documented accounting procedures and controls, adequate supporting documentation and records (including pre-numbered documents and the cancellation of documents), proper record-keeping procedures (including the timeliness of processing), budgetary accounting, physical security/control over assets and documents (including document control, safe deposits, timeliness of deposits and computer security), and pre audits of transactions (including matching of documents).

**Detective controls** are dependent on manual review of recorded information and are considered compensating controls when preventative controls are not in place. They require timely correction procedures. Detective controls include recalculations, checking control totals, analysis and review, independent reconciliations, follow up on questionable accounts/transactions, customer complaints/employee complaints, observations, rotation of staff, inspection of documents, confirmations, and post review/audits of accounts/transactions/exception reports/aging reports, etc.
INHERENT LIMITATIONS:

The effectiveness of internal controls is limited by:

- **People** – are responsible for making judgments, directing operations, and performing tasks. People have different levels of competency and are fallible. People have different skill sets and performance capabilities. People react to stress differently and make errors when distracted or placed in unreasonable conditions.
- **Organizational** – smaller organizations typically lack resources for having strong preventive controls. Larger organizations may have more decentralized environments. Both conditions require stronger monitoring over the processing, recording, summarizing, and reporting of transactions.
- **Circumvention or Collusion** - can result from the formation of close personal relationships, presence of dominate personalities were one persons work is being checked by another.
- **Deadlines or Unreasonable Conditions** – increases the likelihood of intentional exceptions due balancing issues or lack of information.
- **Control Override** - can result by allowing exceptions to existing policies or by subordinates following orders.
- **Tolerant Attitudes** – increases the likelihood of intentional exceptions due to tolerant attitudes that permit exceptions to occur.
- **Changing Conditions** - increases likelihood of unintentional exceptions due to changes in operations, systems, or people involved with the controls.
KEY CONTROLS:

- Honest and Competent People
  - Code of Ethics
  - Training
  - Hiring Practices
  - Performance Management
- Security
  - Assets
  - Data
  - Applications
- Written Policies / Procedures / Business Processes
  - Authorization
  - Documentation
  - Processing
  - Summarizing
  - Recording
  - Reporting
- Separation of Duties
- Supervision
- Independent Reconciliations (Post Audits)
  - Transaction Reports
  - Exception Reports
  - Vendor Reports
  - Ageing Reports
  - Budget Reports
NC STATE UNIVERSITY’S INTERNAL CONTROL:

Control Environment:
- Organizational Structure
  http://www2.acs.ncsu.edu/UPA/uniorgchart/index.htm
- Written Policies and Procedures
  http://www.ncsu.edu/policies/homepage.php
- State’s Oversight
  http://www.osc.nc.gov/
  http://www.osbm.state.nc.us/osbm/index.html
  http://www.ncauditor.net
  http://www.doa.state.nc.us/PandC/pandc.htm
  http://www.ga.unc.edu/publications/admin_manual/
  http://www.osp.state.nc.us/manuals/dropmenu.html
- Internal Audit
  http://www.ncsu.edu/internal_audit/
- HR Policies and Procedures
  http://www.ncsu.edu/human_resources/
- Central Office Oversight (Budget, Purchasing, Contracts and Grants, Controller’s Office)
  http://www.fis.ncsu.edu/budget/
  http://www7.acs.ncsu.edu/financialsvcs/index.html
  http://www.fis.ncsu.edu/controller

Risk Assessment:
- Compact Plan
  http://www2.acs.ncsu.edu/UPA/compactplan/index.htm
- Department Plans (Year-End Plan, Cash Management Plan)
- Performance Management Program
  http://www.ncsu.edu/policies/employment/performance_mngt_review/REG05.50.4.php
  http://www.ncsu.edu/human_resources/er/perfmgt.php
- Revisions to PRRs / Guidelines (Trust Funds, Journal Entries, Travel, Imprested Accounts)
Control Activities:

http://www.fis.ncsu.edu/controller/Procedures/default.asp
http://www.fis.ncsu.edu/controller/guidelines_ref/default.asp

Information and Communication:
- Financial Systems (GL, AP, AR)
- Human Resources System (HR, Labor Distribution)
- WEB Leave System / WEB Travel System
- Capital Asset Management System
- Core Receipt/Deposit System
- Other - Bookstore Systems / Food Services Systems / Vet Med / McKimmon

Monitoring:
- Supervision of Activities
- Analysis / Reporting
- Reconciliations
- Evaluations
- Outreach
- Internal Audit
DEPARTMENTAL INTERNAL CONTROL CYCLES:

- General Accounting and Reporting
- Cash Receipts and Deposits
- Imprested Accounts
- Accounts Receivable
- Fixed Assets
- Purchasing and Accounts Payable
- Payroll
Understanding Internal Controls

General Accounting and Reporting Cycle:

- **Risks**
  - Transactions not recorded
  - Transactions recorded wrong (amount/period/account)
  - Unauthorized transactions recorded
  - Unsupported transactions recorded

- **Controls**
  - Supervision of activities
  - Proper communication of policies/procedures
  - Proper training of staff
  - Numbered journal entries
  - Supporting documentation reviewed by the approver
  - Separation of duties between authorizing/processing/reconciling
  - Reconciliation of journals to Financials reporting
  - Maintenance and safeguarding of documentation
  - Documented management oversight of the process and review of journals
Cash Receipts and Deposits Cycle:

- **Risks**
  - Items lost/stolen/embezzled
  - Transactions not recorded
  - Transactions recorded wrong (amount/period/account)

- **Controls**
  - Supervision of activities
  - Proper communication of policies/procedures
  - Proper training of staff
  - Background check on new employees
  - Mandated vacations
  - Sequentially numbered receipts/deposit slips
  - Mail logs/copy of checks
  - Early restricted endorsement of checks
  - Locked box/ safe/ safeguarding procedures for undeposited receipt items
  - More than one person opening the mail
  - Separation of duties between receipting/recording/depositing/reconciling
  - Reconciliation of receipts/ mail logs/ copied checks to deposits
  - Daily deposits
  - Loomis pick-up
  - Reconciliation of deposit to Financials reporting
  - Maintenance and safeguarding of documentation
  - Documented management oversight of the process and review of revenues
Imprest Account Cycle:

- **Risks**
  - Items lost/stolen/embezzled
  - Transactions not recorded
  - Transactions recorded wrong (amount/period/account)

- **Controls**
  - Supervision of activities
  - Proper communication of policies/procedures
  - Proper training of staff
  - Background check on employees handling cash
  - Mandated vacations
  - Sequentially numbered checks/petty cash receipts/deposit slips
  - Locked box/safe/safeguarding procedures for undeposited cash items
  - Separation of duties between authorizing/processing/reconciling
  - Reconciliation of imprest account activities per bank to Financial reporting
  - Reconciliation of petty cash receipts/unspent cash to authorized amount
  - Maintenance and safeguarding of documentation
  - Documented management oversight of the process and review of activities
Accounts Receivable Cycle:

**Risks**
- Collections embezzled
- Transactions not recorded
- Transactions recorded wrong (amount/period/account)
- Collections not pursued
- Write off of accounts

**Controls**
- Supervision of activities
- Proper communication of policies/procedures
- Proper training of staff
- Background check on employees handling cash
- Mandated vacations
- Sequentially numbered charge slips/adjustment forms/write off forms
- Proper authorization procedures for charges/adjustments/write offs
- Reconciliation of daily receipts to collections
- Separation of duties between authorizing/processing/reconciling/answering billing complaints
- Immediate billing after services provided
- Monthly billing of outstanding balances
- Production of ageing report on receivables
- Reconciliation of interface systems
- Reconciliation of charges/collections to Financial reporting
- Maintenance and safeguarding of documentation
- Documented management oversight of the process and review of ageing report, adjustments made, write-offs and revenues
Fixed Assets Cycle:

- **Risks**
  - Acquisitions/items lost/stolen/embezzled
  - Transactions not recorded
  - Transactions recorded wrong (amount/period/account/location/condition)
  - Items not accounted for properly
  - Items impaired
  - Items misused
  - Items not safeguarded/insured

- **Controls**
  - Supervision of activities
  - Proper communication of policies/procedures
  - Proper training of staff
  - Sequentially numbered item tags
  - Numbered adjustment forms
  - Annual inspection, reconciliation and reporting
  - Proper authorization/processing procedures for changes/adjustments in location and condition
  - Documentation and proper approval of items transferred or held for home use
  - Separation of duties between authorizing/processing/receiving and reconciling inventory items
  - Maintenance and safeguarding of documentation
  - Documented management oversight of the process and review of adjustments made, write-offs and inventories
Purchasing and Accounts Payable Cycle:

**Risks**
- Items embezzled
- Transactions not recorded
- Transactions recorded wrong (amount/period/account)
- Items not received
- Items not properly approved
- Payments not made timely
- Payment of duplicate invoices
- Credits/Discounts not properly applied
- Purchasing and Contract requirements not followed
- Travel requirements not followed
- Expenditure guidelines not followed
- Improper charge to State/restricted funds

**Controls**
- Supervision of activities
- Proper communication of policies/procedures
- Proper training of staff
- Sequentially numbered vouchers/checks
- Proper authorization procedures
- Independent maintenance of the vendor file
- Supporting purchase order/invoice documentation
- Use of receiving/approval stamp
- Verification of travel compliance
- Reconciliation of invoice to purchase order/encumbering documentation/receiving documentation
- Separation of duties between authorizing/vendor approval/processing/receiving and reconciling
- Timely processing of invoices for payment
- Receiving verified before payment approved
- Reconciliation of charges to Financial reporting
- Maintenance and safeguarding of documentation
- Documented management oversight of the process and review of documentation, expenditures for the month/year
Payroll Cycle:

**Risks**
- Items embezzled
- Transactions not recorded
- Transactions recorded wrong (amount/period/account)
- Services charged not received
- Terminations not made timely
- Items not properly approved
- Payments not made timely
- Payment of duplicate items
- Calculations not made correctly
- Expenditure guidelines not followed
- Improper charge to State/restricted funds

**Controls**
- Supervision of activities
- Proper communication of policies/procedures
- Proper training of staff
- Independent HR office to process and approve new positions / hires
- Proper documentation and dept/college/VC authorization procedures
- Supporting employee personnel files with signed applications and approvals
- Supporting documentation for additional payments signed by employee and supervisor with description of work performed and time worked
- Hourly payments and additional payments recalculated
- Use of time records for part time/ temporary/ hourly paid employees signed by employee and approved by supervisor
- Use of leave recording system for full time employee with automated process for amounts earned and available and supervisory approval for leave taken
- Reconciliation of payroll registers to time records, supporting documentation for additional pay and departmental list of authorized employees and pay rates
- Separation of duties between authorizing/ processing/ reconciling
- Timely processing of payroll registers
- Time worked verified before payment approved
- Reconciliation of payroll registers to Financial reporting
- Reconciliation of payroll registers to Labor Distribution
- Maintenance and safeguarding of documentation
- Documented management oversight of the process and review of documentation, expenditures for the month/year
NC STATE UNIVERSITY’S CODE OF CONDUCT:

Organizational Code of Conduct, General Employee Conduct, Organization Records and Communications, Dealing with Outside People and Organizations, Prompt Communications, Privacy and Confidentiality:

Controller’s Office Code of Conduct:

North Carolina State University is a State supported institution and as such is held up to high standards of conduct in its service and business activities/functions. State agencies such as the University of North Carolina – Office of the President (UNC-OP), Office of State Budget and Management (OSBM), Office of State Purchasing and Contract (OSPC), Office of State Personnel (OSP), Office of the State Controller (OSC), and the Office of State Auditor (OSA) exercise oversight responsibilities and establish rules and regulations over the operations of the University. Management is responsible for and establishes controls and safeguards to ensure that such rules and regulations are complied with. As a State supported institution the University is also held up to close scrutiny by the public and is responsive to all questions regarding the use of State funds. Illegal acts are promptly reported to the State and to Campus Security. Management takes appropriate action to address all control weaknesses highlighted by self-evaluations and by internal or external audits. Provisions of the State Executive Budget Act are followed. Timely and accurate reporting is made to UNC-OP, OSBM, OSC and OSA. Information and assistance requested by the OSA is provided promptly. Journal entries made for financial reporting are supported with appropriate supporting documentation. The annual financial statements and tax returns are completed timely, are fairly stated in all material respects, and are in accordance with the established reporting standards. Decisions and responses to questions are done so with due care, competence, diligence, and without misrepresentation of the facts. Employees act with honesty and integrity and avoid relationships that would appear to be a conflict of interest. Employees interact with customers, fellow employees and others in a businesslike manner, using ethical behavior, proper communication, a professional attitude, and due respect. Employees are responsive to the need for security over information and computers. Employees are responsible for the assets and resources entrusted to them.

SPA Performance Appraisal Program:

http://www.ncsu.edu/policies/employment/performance_mngt_review/REG05.50.4.php

http://www2.acs.ncsu.edu/hr/docs/perfappraisal2002.doc

Conflicts of Interests:

http://www.ncsu.edu/policies/governance_admin/gov_gen/REG01.25.1.php

Outside Activities, Employment, and Directorships:

http://www.ncsu.edu/policies/employment/salary_admin/secondary_employ.php

Relationships with Clients and Suppliers; Gifts, Entertainment, and Favors; Kickbacks and Secret Commissions:

http://www.ncsu.edu/policies/finance/purch/basic_procurement_guidelines.htm

http://www.fis.ncsu.edu/materialsmgmt/staff/ethics.pdf

Organization Funds and Other Assets:


Use of Computers:

http://www.ncsu.edu/policies/informationtechnology/POI.08.00.1.php
QUIS / FEEDBACK

After studying and reviewing the information provided in this section, we have provided a quiz to reinforce the knowledge that you have gained. This is strictly voluntary. You may also provide us feedback as to how this section has helped you or how we could do better in providing you information by clicking on FEEDBACK. If you have questions that you would like for us to answer and consider publishing, you may contact the University Controller. Thanks for visiting our site and good luck on the quiz.

INTERNAL CONTROL ACCOUNTS QUIZ

Following is a series of questions that test your understanding of internal controls. You will need to print the quiz out and after completing the answers check you answers to the answer sheet. You can obtain the answer sheet by clicking on ANSWERS. If you have any question about the answer sheet, please let us hear from you by clicking on FEEDBACK.

1. Having internal controls guarantees that everything is done right.
   - True
   - False

2. Supervision is important to fraud prevention.
   - True
   - False

3. Only top management should care about internal control
   - True
   - False

4. The five components of internal control are: control environment, risk assessment, control activities, information and communication, and monitoring.
   - True
   - False

5. Training is not part of internal control.
   - True
   - False

6. The integrity and ethical values of an organization’s management is part of control environment.
   - True
   - False

7. Internal controls are done only one time.
   - True
   - False

8. New personnel, new or revamped information systems, and reorganizations do not present internal control risks.
   - True
   - False

9. Control activities are policies and procedures that help ensure that necessary actions are taken to address risks to achievement of the entity’s objectives.
10. Control activities include: performance reviews, information processing, physical controls, and segregation of duties.
   - True
   - False

11. The quality of system-generated information affects management’s ability to make appropriate decisions in managing and controlling the entity’s activities.
   - True
   - False

12. Communication is important to the internal control process.
   - True
   - False

13. Most fraudsters are first time offenders
   - True
   - False

14. Most frauds are detected by audits
   - True
   - False

15. A perceived non-sharable financial need is aka Pressure in the fraud triangle
   - True
   - False

16. A perceived opportunity is the method by which a crime can be committed
   - True
   - False

17. Rationalization is the perceived view that they are ordinary, honest people who are caught in a bad set of circumstances
   - True
   - False
QUIZ ANSWERS:

1. False - Internal control is a process designed to provide reasonable assurance, not absolute assurance.
2. True – Supervision is a key control.
3. False – Internal control affects everyone.
4. True – The five components of internal control are: control environment, risk assessment, control activities, information and communication, and monitoring.
5. False - Training is part of the control environment and an internal control.
6. True – Integrity and ethical conduct are essential elements of the control environment and part of internal control.
7. False – Internal control is a continual cycle of reevaluation and action.
8. False – New personnel, new or revamped information systems, and reorganizations do present internal control risks.
9. True - Control activities are policies and procedures that help ensure that necessary actions are taken to address risks to achievement of the entity’s objectives.
10. True - Control activities include: performance reviews, information processing, physical controls, and segregation of duties.
11. True – The quality of system-generated information affects management’s ability to make appropriate decisions in managing and controlling the entity’s activities.
12. True – Information must be shared up, down and across the organization to be useful in evaluating internal controls. Communication, both formally and informally is vital to a successful internal control process.
13. True – Most fraudsters are first time offenders with no criminal past (Refer to Fraud Triangle)
14. False – Most frauds are detected by tips; only approximately 10% is detected by some type of audit
15. True – Pressure is the first leg of the fraud triangle and is also know as perceived non-shared financial need.
16. True – Opportunity is second leg of fraud triangle; fraudster perceived method will be able to solve their problem in secret.
17. True – Rationalization is the third leg of fraud triangle; fraudster perceives themselves as ordinary and honest, but who are caught in a bad set of circumstances.