

INTERNAL CONTROLS

Why Do We Need Strong Internal Controls?

To protect yourself & your employees

Goal

Protect your Assets

- From the time assets are received to the time they are booked
- To the point in which assets are removed from your system / books

What Do I Need to Do?

- Assess the Level of Risk
 - Qualitative / Quantitative
 - Political Risk
 - Local Newspapers
- Identify Reasonable Controls
- Determine Benefits of Controls
- Implement Controls
- Document the Controls and the Performance of the Controls
- Monitor the Controls

Tips

- There are no Absolutes
- Keys to Good Systems of Control
- Strong Documented Policies
 - Many entities have controls in place, but they have not formalized or documented in policies or as procedures.
- Monitoring / Enforcement of Policies - Must be Documented *Ex. Checklist for Review*
- Documentation of any Deviations from Standard Practice / Policy

Accounts Payable/ Cash Disbursements

Common Risks:

- Checks Processed by unauthorized Personnel
- Payments Made Based on Invalid or Unapproved Invoices
- Payments to Fictitious or Invalid Vendors
- Misuse of Hand Drawn Checks

A good control system has these duties segregated:

- Setting Up Vendors
- Creating / Approving POs
- Processing Invoices
- Issuing Operating Checks

Examples of Controls

- Access to Electronic Signature is limited.
- Review of Voided Checks
- Review of Voucher Packages
 - Purchase Orders
 - Invoices (Recalculation)
 - Receiving Reports
- Approvals Prior to Payment
- Authorization for Creation of POs or Payment Request
- Password-ed Check printer
- Check Stock Locked up
- Review of New Vendors
- Payments / Encumbrances should be recorded daily
- Reconciliations

Accounts Receivable/ Cash Receipts

Common Risks:

- Misappropriation of Funds Prior To Posting to the Accounting Records
- Not Crediting Appropriate Accounts Receivable, Duplication of Revenue
- Diversion of funds to improper accounts

A good control system has these duties segregated:

- Establishing Bank Accounts in Entity's Name
- Receiving Cash,
- Depositing Cash
- Recording Cash
- Reconciling Cash

Examples of Controls

- Sequential / Pre-Numbered Receipts
- Separation Between Individuals Receiving Money (Via Mail or In Person) and Individuals Posting to the General Ledger
- Separation Between Receiving Money and Depositing Money
- Establish number of days acceptable to hold receipts
- Establish maximum amount of cash that can be held in vault
- Petty Cash Procedures
- Check-Cashing Procedures
- Post BANNER daily
- Reconciliations

Payroll / Benefit Disbursements

Common Risks:

- Theft Due to Ghost Employee
- Check to Terminated/Inactive Employee
- Unauthorized Payroll Changes
- Undetected Mathematical or Data Entry Errors Due to Lack of Oversight
- Manipulation of Withholding Balances

A good control system has these duties segregated:

- Setting up New Employees
- Setting up Direct Deposit Information
- Making Payroll Changes
- Processing Payroll Checks

Examples of Controls

- Thorough review of Initial Input
- Review sample of monthly salaries
- Pay adjustments must be Approved/Reviewed by Payroll Director
- Calculations of employee salaries outside of system; Reviewed by Payroll Director
- Payroll reports compared to initial salary calculations; Review of new employees added
- Distribution of checks by someone outside of Payroll
- Review of exception reports

All Controls should be Documented, Monitored, and Reviewed on a regular basis by the Institution

Credit Card/Purchasing Cards

Common Risk:

- Circumventing Expenditure Controls

Examples of Controls:

- Strong Policy
 - Allowable Vendors by Dept
 - Thresholds
 - Allowable Items
- Voucher Packages
 - Matching Receipts to Statement
- Monitoring
 - Electronic File by Cardholder

Access Controls

Common Risk:

- Access Point
 - Doors to a System/Data
 - Via Computers, Networks, Applications, Database
- Inadequate Separation of Duties (*Rights in System do not agree to established separation of duties structure.*)

Examples of Controls

- Physical
 - Doors, Locks
 - Card Keys
- Logical –
 - Passwords
 - Alphanumeric,
 - Expiration Periods,
 - Lock-Out
- Virus Protection
- Firewalls
- Patch Management

Environmental Controls

Common Risk:

- Loss of Data Due to Environmental Factors such as Power Loss, Fire, or Water

Examples of Controls

- Fire Suppression, Extinguishers, etc.
- Temperature Detection
- Moisture Detection
- Uninterruptible Power Sources or Generators

Disaster Recovery Planning

Common Risk:

- Loss of Data Due to Disaster. Disaster could include anything from loss of equipment due to viruses to loss due to tornado, flood, hurricane, or terrorist threats.

Examples of Controls

- Strong Policy Required
 - Consider:
 - Recovery Team and Contact List
 - Staffing assignments and needs
 - Identifying Critical Systems
 - Order of Restoration of the Critical Systems
 - Equipment Needs / Vendor Contacts
 - Alternative Policies and Procedures
- Review Policy Periodically
- Communication of Policy to Staff