UNDERSTANDING INTERNAL CONTROLS

COUNTY OF ORANGE
INTERNAL AUDIT DEPARTMENT

UNDERSTANDING INTERNAL CONTROLS

Table of Contents

Introduction 3

Understanding Internal Controls Objectives 5

Internal Control Defined 6

Internal Control Process 7

Control Environment 9

Risk Assessment 11

Control Activities 17
- Approvals 19
- Reconciliations 20
- Reviews 21
- Asset Security 22
- Segregation Of Duties 23
- Information Systems 25
  - General Controls 26
  - Application Controls 28
- Balancing Risks and Controls 33

Information and Communication 34

Monitoring 35

Appendix 36

INTRODUCTION

The purpose of *Understanding Internal Controls* is to assist employees in achieving the County's objectives. Internal controls serve to ensure the existence of basic and consistent business controls throughout the County and to define our responsibilities for them.

This guide is designed to satisfy the basic objectives of any business system. They address five interrelated components of a business system:

- **The organization's operating environment**
- **Its goals and objectives and related risk assessment**
- **Controls and related policies and procedures**
- **Its information systems and communication methods**
- **Its activities to monitor its performance**

Understanding Internal Controls provides an additional reference tool for all managers to identify and assess basic weaknesses in operating controls, financial reporting, and legal/regulatory compliance and to take action to strengthen controls where needed. By developing effective compliance programs, management can contribute to reducing the County's potential liability from fines and penalties that could be imposed for violations.

Understanding Internal Controls is based upon the internal control guidelines as recommended by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. COSO was formed to support the Commission's recommendation to develop additional, integrated guidance on internal control. This organizational approach provides the County with a common, accepted, and recommended reference point to assess the quality of its internal control systems.

SCOPE

Understanding Internal Controls applies to all the County's departments/agencies. The examples of control activities contained in this guide are not presented as all-inclusive or exhaustive of all the specific controls appropriate in each department. Over time, controls may be expected to change to reflect changes in our operating environment.

Understanding Internal Controls is designed to provide reasonable, but not absolute assurance for the accounting for and safeguarding of assets, the reliability of financial information, and the compliance with laws and regulations. Reasonable assurance is a concept that acknowledges that the cost of a control should not exceed the benefit to be derived from it.

The degree of control employed is a matter of good business judgment. When business controls are found to contain weaknesses, we must choose among the following alternatives:

- **increase supervision and monitoring;**
- **institute additional or compensating controls; and/or**
- **accept the risk inherent with the control weakness (assuming prior management approval).**

The guidance presented in this document should not be considered to "stand alone." This guide should be used in conjunction with existing policies and procedures, including those developed locally.

RESPONSIBILITY

Although management is primarily responsible for implementing internal controls, each department head, manager, and employee participates in establishing, properly documenting, and maintaining internal controls in each department/agency. All employees of the County are responsible for compliance with internal controls.

***UNDERSTANDING INTERNAL CONTROLS* OBJECTIVES**

The objectives of the *Understanding Internal Controls* document is to:

1. Convey to you that management is responsible for ensuring that internal controls are established, properly documented, maintained and adhered to in each department/agency.

2. Convey to you that all employees of the County are responsible for compliance with internal controls.

3. Give you the tools to establish, properly document, maintain and adhere to the County's system of internal controls.

INTERNAL CONTROL DEFINED

Internal control is a process, effected by an entity's board, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

Several key points should be made about this definition:

1. ***Internal control is a process.*** It's a means to an end, not an end in itself.

2. ***Internal control is effected by people at every level of a department/agency.*** Internal control is, to some degree, everyone's responsibility. Within the County, administrative officials at the department-level are primarily responsible for, and will be held accountable for internal control in their departments/agencies.

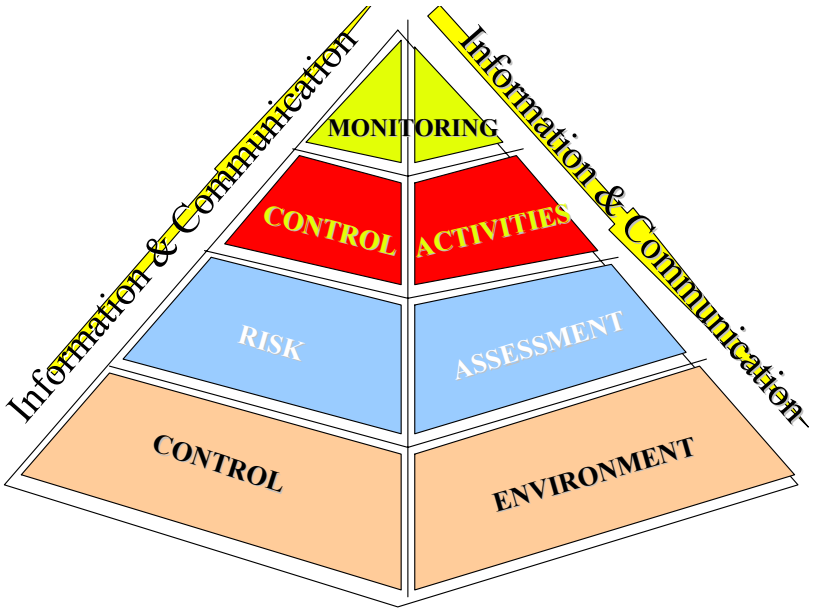
3. ***Internal control can provide only reasonable assurance -- not absolute assurance -- regarding the achievement of a department's/agency's objectives.*** Effective internal control helps a department/agency achieve its objectives; it does not ensure success. There are several reasons why internal control cannot provide absolute assurance that objectives will be achieved: cost/benefit realities, collusion among employees, and external events beyond a department's/agency's control.

4. ***Effective internal control helps an organization achieve its operations, financial reporting, and compliance objectives.*** Effective internal control is a built-in part of the management process (i.e., plan, organize, direct, and control). Internal control keeps an organization on course toward its objectives and the achievement of its mission, and minimizes surprises along the way. Internal control promotes effectiveness and efficiency of operations, reduces the risk of asset loss, and helps to ensure the reliability of financial reporting (i.e., all transactions are recorded and that all recorded transactions are real, properly valued, recorded on a timely basis, properly classified, and correctly summarized and posted), and compliance with laws and regulations.

INTERNAL CONTROL PROCESS

Internal control consists of five interrelated components as follows:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring



All five internal control components must be present to conclude that internal control is effective. The following diagram captures the internal control process and illustrates the on-going nature of the process:

CONTROL ENVIRONMENT

The control environment is the control consciousness of a department/agency; it is the atmosphere in which people conduct their activities and carry out their control responsibilities. An effective control environment is an environment where competent people understand their responsibilities, the limits to their authority, and are knowledgeable, mindful, and committed to doing what is right and doing it the right way; they are committed to following an organization's policies and procedures and its ethical and behavioral standards. The control environment encompasses technical competence and ethical commitment; it is an intangible factor that is essential to effective internal control.

The Board of Supervisors, County Executive Officer and departmental management enhance the County's and each department's/agency's control environment when they establish and effectively communicate written policies and procedures, a code of ethics, and standards of conduct. Moreover, the Board of Supervisors, County Executive Officer and departmental management enhance the control environment when they behave in an ethical manner – creating a positive "tone at the top" – and when they require that same standard of conduct from everyone in each County department/agency.

Who is Responsible?

The Board of Supervisors, County Executive Officer, and departmental management are responsible for "setting the tone" for the County. A control environment should be fostered that encourages:

- The highest levels of integrity and personal and professional standards,
- A leadership philosophy and operating style which promote internal control throughout the County, and
- An assignment of authority and responsibility.

CONTROL ENVIRONMENT TIPS

Effective human resource policies and procedures enhance the County's control environment. These policies and procedures should address hiring, orientation, training, evaluations, counseling, promotions, compensation, and disciplinary actions. In the event that an employee does not comply with the County's policies and procedures or behavioral standards, the County must take appropriate disciplinary action to maintain an effective control environment. **The control environment is greatly influenced by the extent to which individuals recognize that they will be held accountable**.

Listed below are some tips to enhance a department's control environment. This list is not all-inclusive, nor will every item apply to every department; it can, however, serve as a starting point.

- Make sure that the following policies and procedures are available in your department (hard copy or Internet access):

  - Administrative Procedures
  - Employee Handbook
  - Purchasing Manual
  - Personnel Memorandum

- Make sure that the department has a well-written departmental policies and procedures manual, which addresses its significant activities and unique issues. Employee responsibilities, limits of authority, performance standards, control procedures, and reporting relationships should be clear.

- Make sure that employees are well acquainted with County and departmental policies and procedures that pertain to their job responsibilities.

- Discuss ethical issues with employees. If employees need additional guidance, issue departmental standards of conduct.

- Ask employees to disclose potential conflicts of interest (*e.g.*, ownership interest in companies doing business or proposing to do business with the department).

CONTROL ENVIRONMENT TIPS (Continued)

- Make sure that job descriptions exist and correctly translate desired competence levels into requisite knowledge, skills, and experience; make sure that hiring practices result in hiring qualified individuals.

- Make sure that the department has an adequate training program for employees.

- Make sure that employee performance evaluations are performed at least annually. Good performances should be valued highly and recognized in a positive manner.

- Make sure that appropriate disciplinary action is taken when an employee does not comply with policies and procedures or behavioral standards.

RISK ASSESSMENT

I. DETERMINE GOALS AND OBJECTIVES

The central theme of internal control is (1) to identify risks to the achievement of an organization's objectives and (2) to do what is necessary to manage those risks. Thus, setting goals and objectives is a precondition to internal controls. If an organization does not have goals and objectives, there is no need for internal control.

At the county level, goals and objectives are presented in a strategic plan that includes a mission statement and broadly defined strategic initiatives. At the department level, goals and objectives must support the organization's strategic plan. Goals and objectives are classified in the following categories:

- ***Operations.*** These risks and related objectives pertain to the achievement of the basic mission(s) of a department and the effectiveness and efficiency of its operations, including performance standards and safeguarding resources against loss.
- ***Financial reporting.*** These risks and related objectives pertain to the preparation of reliable financial reports, including the prevention of fraudulent public financial reporting.
- ***Compliance.*** These risks and related objectives pertain to adherence to applicable laws and regulations.

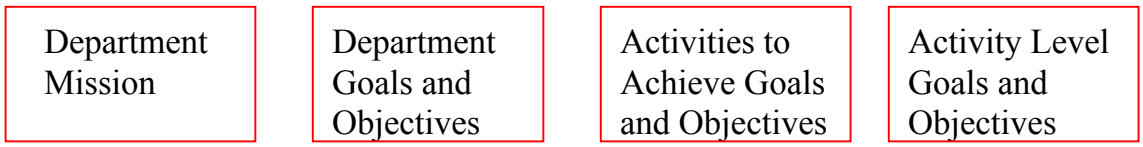
The following table illustrates these concepts:

Objectives	Classification
Payroll Provide service and support to the County.	
Processing-Compensation/Withholding Compensation rates and payroll deductions should be accurately and promptly entered into the payroll syst3m.	Operations (O)
Each accounting period, prepare journal entries for payroll deductions, and related adjustments.	Financial (F)
Processing-Authorizations Personnel management should properly and accurately maintain all compensation documentation.	Compliance (C)
An employee master file that is accurate and complete should be maintained.	O, F, C

RISK ASSESSMENT

A clear set of goals and objectives is fundamental to the success of a department.

Specifically, a department or work unit should have (1) a mission statement, (2) written goals and objectives for the department as a whole, and (3) written goals and objectives for each significant activity in the department (see diagram below). Furthermore, goals and objectives should be expressed in terms that allow meaningful performance measurements.



There are certain activities, which are significant to all departments such as: budgeting, purchasing goods and services, hiring employees, evaluating employees, payroll, and safeguarding property and equipment. Thus, all departments are expected to have appropriate goals and objectives, policies and procedures, and internal controls for these activities.

RISK ASSESSMENT

II. IDENTIFY RISKS AFTER DEFINING GOALS

Risk assessment is the identification and analysis of risks associated with the achievement of operations, financial reporting, and compliance goals and objectives. This, in turn, forms a basis for determining how those risks should be managed.

Who is responsible? To properly manage their operations, managers need to determine the level of operations, financial and compliance risk they are willing to assume. Risk assessment is one of management's responsibilities and enables management to act proactively in reducing unwanted surprises. Failure to consciously manage these risks can result in reduced assurance that goals and objectives will be achieved.

Risk Identification. A risk is anything that could jeopardize the achievement of an objective. For each of the department's objectives, risks should be identified. Asking the following questions helps to identify risks:

- What could go wrong?
- How could we fail?
- What must go right for us to succeed?
- Where are we vulnerable?
- What assets do we need to protect?
- Do we have liquid assets or assets with alternative uses?
- How could someone steal from the department?
- How could someone disrupt our operations?
- How do we know whether we are achieving our objectives?
- On what information do we most rely?
- On what do we spend the most money?
- How do we bill and collect our revenue?
- What decisions require the most judgment?
- What activities are most complex?
- What activities are regulated?
- What is our greatest legal exposure?

It is important that risk identification be comprehensive – at the department level and at the activity or process level-for operations, financial reporting, and compliance objectives – considering both external and internal risk factors. Usually, several risks can be identified for each objective.

RISK ASSESSMENT

Using our same example, the following table illustrates the concepts discussed so far. Note that the identified risks relate to the goals and objectives previously determined.

Goals and Objectives	Business Objective Classification	Risks
Payroll Provide service and support to the County community.		Transactions may not be processed or processed incorrectly.
Processing-Compensation/ Withholding Compensation rates and payroll deductions should be accurately and promptly entered into the payroll system.	Operations (O).	Financial statements may be misstated due to entry omissions, incorrect coding, duplicate journal entries, or improper cut-offs.
Each accounting period, prepare journal entries for payroll, payroll deductions, and related adjustments.	Financial (F)	Employment laws and regulations may be violated resulting in fines, penalties, or litigation.
Processing-Authorizations Personnel management should properly and accurately maintain all compensation documentation.	Compliance (C)	Incorrect data in the master file could result in incorrect wage payments.
An employee master file that is accurate and complete should be maintained	O, F, C	Payroll withholdings may be incorrect. Awards, incentives, recognitions, etc., may not be accurately reflected on the master file.

RISK ASSESSMENT

Higher Risk Transaction Types

Below are some types of transactions that **may** pose higher risks to departments:

- Petty cash (if high volumes are processed)
- Assets with Alternative Uses
- Cash Receipts
- Consultant Payments and Other Payments for Services
- Travel Expenditures
- Payments to Non-Vendors
- Equipment Delivered Directly to Department
- Purchase Exemptions (sole source)
- Payroll (rates, changes, terminations)
- Equipment On Location
- Software Licensing Issues
- Confidential Information
- Grants (meeting terms, not overspending)

These are transaction types that deserve a conscious risk review.

Quantitative & Qualitative Costs

When evaluating the potential impact of risk, both quantitative and qualitative costs need to be addressed. Quantitative costs include the cost of property, equipment, or inventory, cash dollar loss, damage and repair costs, cost of defending a lawsuit, etc.

Qualitative costs can have wide-ranging implications to the County. These costs may include:

- Loss of public trust
- Loss of future grants, gifts and donations
- Injury to the County's reputation
- Violation of laws
- Default on a project
- Bad publicity
- Public safety
- Public health

RISK ASSESSMENT

Risk Analysis. After risks have been identified, a risk analysis should be performed to prioritize those risks:

- Estimate the potential impact if the risk were to occur; consider both quantitative and qualitative costs.
- Assess the probability of the risk occurring.
- Determine how the risk should be managed; decide what actions are necessary.

Prioritizing helps departments focus their attention on managing significant risks (*i.e.,* risks with reasonable likelihood's of occurrence and large potential impacts).

RISK ASSESSMENT TIPS

Listed below are tips to guide a department through its risk assessment:

- Make sure the department has a mission statement and written goals and objectives.
- Assess risks at the department level.
- Assess risks at the activity (or process) level.
- Complete a Business Controls Worksheet (refer to the Appendix) for each significant activity (or process) in the department; prioritize those activities (or processes) which are most critical to the success of the department and those activities (or processes) which could be improved the most.
- Make sure that all risks identified at the department level are addressed in the Business Controls Worksheet.

CONTROL ACTIVITIES

Control activities are actions supported by policies and procedures that help assure management directives to address risk are carried out properly and timely.

***Who is Responsible*?** In the same way that managers are primarily responsible for identifying the financial and compliance risks for their operations, they also have line responsibility for designing, implementing and monitoring their internal control system.

Preventive & Detective Controls. Controls can be either preventive or detective. The intent of these controls is different. Preventive controls attempt to deter or prevent undesirable events from occurring. They are proactive controls that help to prevent a loss. Examples of preventive controls are separation of duties, proper authorization, adequate documentation, and physical control over assets.

Detective controls, on the other hand, attempt to detect undesirable acts. They provide evidence that a loss has occurred but do not prevent a loss from occurring. Examples of detective controls are reviews, analyses, variance analyses, reconciliations, physical inventories, and audits.

Both types of controls are essential to an effective internal control system. From a quality standpoint, preventive controls are essential because they are proactive and emphasize quality. However, detective controls play a critical role providing evidence that the preventive controls are functioning and preventing losses.

Control activities include approvals, authorizations, verifications, reconciliations, reviews of performance, security of assets, segregation of duties, and controls over information systems and are further explained as follows:

> ***Approvals, Authorizations, and Verifications (Preventive).*** Management authorizes employees to perform certain activities and to execute certain transactions within limited parameters. In addition, management specifies those activities or transactions that need supervisory approval before they are performed or executed by employees. A supervisor's approval (manual or electronic) implies that he or she has verified and validated that the activity or transaction conforms to established policies and procedures.
>
> ***Reconciliations (Detective).*** An employee relates different sets of data to one another, identifies and investigates differences, and takes corrective action, when necessary.

CONTROL ACTIVITIES

Reviews of Performance (Detective). Management compares information about current performance to budgets, forecasts, prior periods, or other benchmarks to measure the extent to which goals and objectives are being achieved and to identify unexpected results or unusual conditions that require follow-up.

Security of Assets (Preventive and Detective). Access to equipment, inventories, securities, cash and other assets is restricted; assets are periodically counted and compared to amounts shown on control records.

Segregation of Duties (Preventive). Duties are segregated among different people to reduce the risk of error or inappropriate action. Normally, responsibilities for authorizing transactions, recording transactions (accounting), and handling the related asset (custody) are divided.

Controls over Information Systems (Preventive and Detective). Controls over information systems are grouped into two broad categories – general controls and application controls. General controls commonly include controls over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance. Application controls such as computer matching and edit checks are programmed steps within application software; they are designed to help ensure the completeness and accuracy of transaction processing, authorization, and validity. General controls are needed to support the functioning of application controls; both are needed to ensure complete and accurate information processing.

Control activities must be implemented thoughtfully, conscientiously, and consistently; a procedure will not be useful if performed mechanically without a sharp continuing focus on conditions to which the policy is directed. Further, it is essential that unusual conditions identified as results of performing control activities are investigated and appropriate corrective action is taken.

CONTROL ACTIVITIES-APPROVALS (*Preventive*)

- Written policies and procedures
- Limits to authority
- Supporting documentation
- Question unusual items
- No "rubber stamps"
- No blank signed forms

An important control activity is authorization/approval. Authorization is the delegation of authority; it may be general or specific. Giving a department permission to expend funds from an approved budget is an example of general authorization. Specific authorization relates to individual transactions; it requires the signature or electronic approval of a transaction by a person with approval authority. Approval of a transaction means that the approver has reviewed the supporting documentation and is satisfied that the transaction is appropriate, accurate and complies with applicable laws, regulations, policies, and procedures. **Approvers should review supporting documentation, question unusual items, and make sure that necessary information is present to justify the transaction-before they sign it. Signing blank forms should not be done.**

Approval authority may be linked to specific dollar levels. Transactions that exceed the specified dollar level would require approval at a higher level. Under no circumstance should an approver tell someone that they can sign the approver's name on behalf of the approver. Similarly, under no circumstance should an approver with electronic approval authority share his password with another person. To ensure proper segregation of duties, the person initiating a transaction should not be the person who approves the transaction. A department's approval levels should be specified in a departmental policies and procedures manual.

CONTROL ACTIVITIES -RECONCILIATIONS (*Detective*)

- A reconciliation is a comparison of different sets of data to one another, identifying and investigating differences, AND taking corrective action, when necessary.
- For example, vouching charges in the statement of accounts to file copies of approved vouchers.

Broadly defined, a reconciliation is a comparison of different sets of data to one another, identifying and investigating differences, and taking corrective action, when necessary, to resolve differences. Reconciling monthly financial reports from the Auditor-Controller to file copies of supporting documentation or departmental accounting records is an example of reconciling one set of data to another. This control activity helps to ensure the accuracy and completeness of transactions that have been charged to a department's accounts. To ensure proper segregation of duties, the person who approves transactions or handles cash receipts should not be the person who performs the reconciliation. Another example of a reconciliation is comparing vacation and sick leave balances per departmental records to vacation and sick leave balances per the payroll system.

A critical element of the reconciliation process is to resolve differences. It does not do any good to note differences and do nothing about it. Differences should be identified, investigated, and explained – corrective action must be taken. If an expenditure is incorrectly charged to a department's accounts, then the approver should request that the Auditor-Controller post a correcting journal voucher; the reconciler should ascertain that the correcting journal voucher was posted. Reconciliations should be documented and approved by management.

CONTROL ACTIVITIES -REVIEWS (*Detective*)

- Budget to actual comparison
- Current to prior period comparison
- Performance indicators
- Follow-up on unexpected results or unusual items

Management review of reports, statements, reconciliations, and other information is an important control activity. Management should review such information for propriety, consistency, and reasonableness. Reviews of performance provide a basis for detecting problems. Management should compare information about current performance to budgets, forecasts, prior periods, or other benchmarks to measure the extent to which goals and objectives are being achieved and to identify unexpected results or unusual conditions which require follow-up. Management's review of reports, statements, reconciliations, and other information should be documented as well as the resolution of items noted for follow-up.

CONTROL ACTIVITIES-ASSET SECURITY

(***Preventive and Detective***)

- Security of physical and intellectual assets
- Physical safeguards
- Perpetual records are maintained
- Periodic counts/physical inventories
- Compare counts to perpetual records
- Investigate/correct differences

Liquid assets, assets with alternative uses, dangerous assets, vital documents, critical systems, and confidential information must be safeguarded against unauthorized acquisition, use, or disposition. Typically, access controls are the best way to safeguard these assets. Examples of access controls are as follows: locked door, key pad systems, card key system, badge system, locked filing cabinet, guard, terminal lock, computer password, menu protection, automatic call-back for remote access, smart card, and data encryption.

Departments that have capital assets or significant inventories should establish perpetual inventory control over these items by recording purchases and issuances. Periodically, the items should be physically counted by a person who is independent of the purchase authorization and asset custody functions and the counts should be compared to balances per the perpetual records. Missing items should be investigated, resolved timely, and analyzed for possible control deficiencies; perpetual records should be adjusted to physical counts if missing items are not located.

CONTROL ACTIVITIES-SEGREGATION OF DUTIES

(Preventive and Detective)

- No one person should...
  - Initiate transaction
  - Approve transaction
  - Record transaction
  - Reconcile balances
  - Handle assets
  - Review reports

- At **least** two sets of **eyes**

Segregation of duties is critical to effective internal control; it reduces the risk of both erroneous and inappropriate actions. **In general, the approval function, the recording function, reconciling function, and the asset custody function should be separated among employees**. When these functions cannot be separated, a detailed supervisory review of related activities is required as a compensating control activity. Segregation of duties is a deterrent to fraud because it requires collusion with another person to perpetrate a fraudulent act.

Specific examples of segregation of duties are as follows:

- The person who requisitions the purchase of goods or services should not be the person who approves the purchase.
- The person who approves the purchase of goods or services should not be the person who reconciles the monthly financial reports.
- The person who approves the purchase of goods or services should not have custody of checks.
- The person who maintains and reconciles the accounting records should not have custody of checks.
- The person who opens the mail and prepares a listing of checks received should not be the person who makes the deposit.
- The person who opens the mail and prepares a listing of checks received should not be the person who maintains the accounts receivable records.

CONTROL ACTIVITIES-SEPARATION OF DUTIES EXAMPLES

The box below identifies some of the potential key (and high risk) transaction types with guidelines for separating duties.

TRANSACTION TYPE	WHO INITIATES	WHO AUTHORIZES	WHO RECORDS	WHO RECONCILES	CONTROLS (CUSTODY)
Purchase of Goods (1)	Issues Requisition **Person A**	Approves P.O./ Invoice **Person B**	County Records **Auditor-Controller**	Budget Report **Person B or C**	Receives Goods **Person A or C**
Purchase of Services (1)	Issues Requisition **Person A**	Approves Payment & Verifies Receipt of Services **Person B**	County Records **Auditor-Controller**	Budget Report **Person B or C**	Disburses Check **Auditor-Controller**
Cash Receipts (1) (2)	Opens Mall, Lists Checks, Restrictively Endorses **Person A**	Approves Deposit Order **Person B**	County Records & Department Records **Accounting & Auditor-Controller**	Bank Account/ Budget Report & Deposits to Checklist **Person B or D**	Safeguards and makes the Deposit **Person C**
Payroll	Employee's Time Report	Approves Time Report & Payroll Data Changes **Person A**	County Records **Auditor-Controller**	Budget Report Review **Person B**	Distributes Payroll Checks **Person B or C**
Inventory (3)	Issues Requisition **Person A**	Approves P.O./ Invoice **Person B**	County Records & Department Records (Issues & Receipts) **Accounting & Auditor-Controller**	Departmental Records to Budget Reports & Physical Counts **Person B or C**	Receives & Disburses Goods **Person A**

(1) If the same person authorizes and reconciles, additional monitoring is necessary.
(2) No receipts should be received directly by Person B
(3) Physical counts should not be under the **control** of persons responsible for custody or recording.

CONTROL ACTIVITIES -INFORMATION SYSTEMS

County employees use a variety of information systems: mainframe computers, local area and wide area networks of minicomputers and personal computers, single-user workstations and personal computers, telephone systems, etc. The need for internal control over these systems depends on the importance and confidentiality of the information and the complexity of the applications that reside on the systems. There are basically two categories of controls over information systems:
(1) General Controls and (2) Application Controls.

CONTROL ACTIVITIES-GENERAL CONTROLS (*Preventive and Detective*)

General Controls

General controls apply to entire information systems and to all the applications that reside on the systems.

General Controls Include:

- ♦ Access Security, Data & Program Security, Physical Security
- ♦ Software Development & Program Change Controls
- ♦ Data Center Operations
- ♦ Disaster Recovery

General controls consist of practices designed to maintain the integrity and availability of information processing functions, networks, and associated application systems. These controls apply to business application processing in computer centers by ensuring complete and accurate processing. These controls ensure that correct data files are processed, processing diagnostics and errors are noted and resolved, applications and functions are processed according to established schedules, file backups are taken at appropriate intervals, recovery procedures for processing failures are established, software development and change control procedures are consistently applied, and actions of computer operators and system administrators are reviewed. Additionally, these controls ensure that physical security and environmental measures are taken to reduce the risk of sabotage, vandalism and destruction of networks and computer processing centers.

Finally, these controls ensure the adoption of disaster planning to guide the successful recovery and continuity of networks and computer processing in the event of a disaster.

The County Data Center performs many general control functions for departments in the County. They functionally support the general control functions at the County for networks, network-based applications, mainframe and mainframe-based applications. For example, the County Data Center makes backup copies of files residing on the mainframe and local area networks. They perform the security management function for the network by requiring personal identification codes and passwords to log on to the network and access certain files and subdirectories. When the County Data Center develops or modifies an application for a department, they do the design, programming, testing, documentation, and installation of the application. The County Data Center may also

install and run virus detection software to periodically scan both network servers and personal computers connected to the network for files infected by known viruses.

CONTROL ACTIVITIES-APPLICATION CONTROLS

(*Preventive and Detective*)

Applications are the computer programs and processes, including manual processes, that enable us to conduct essential activities: buying products, paying people, accounting for revenues and expenditures, and forecasting and monitoring budgets

Application Controls

Application controls apply to computer application systems and include input controls (*e.g.*, edit checks), processing controls (*e.g.,* record counts), and output controls (*e.g.*, error listings), which are specific to individual applications.

Application Controls Include Programmed Procedures within Application Software:

- Input Controls (Data Entry)
  - -Authorization
  - -Validation
  - - Error Notification and Correction
- Processing Controls
- Output Controls

They consist of the mechanisms in place over each separate computer system, which ensure that authorized data is completely and accurately processed. They are designed to prevent, detect, and correct errors and irregularities as transactions flow through the business system. They ensure that the transactions and programs are secured, the systems can resume processing after some business interruption, all transactions are corrected and accounted for when errors occur, and the system processes data in an efficient manner.

Electronic Data Interchange, Voice Response, and *Expert Systems* are types of applications that may require certain controls in addition to general application controls.

When a department decides to purchase or to develop an application, department personnel must ensure the application includes adequate application controls: (1) input controls, (2) processing controls, and (3) output controls.

CONTROL ACTIVITIES-APPLICATION CONTROLS

(*Preventive and Detective*)

Input controls ensure the complete and accurate recording of authorized transactions by only authorized users; identify rejected, suspended, and duplicate items; and ensure resubmission of rejected and suspended items. Examples of input controls are error listings, field checks, limit checks, self-checking digits, sequence checks, validity checks, key verification, matching, and completeness checks.

Processing controls ensure the complete and accurate processing of authorized transactions. Examples of processing controls are run-to-run control totals, posting checks, end-of-file procedures, concurrency controls, control files, and audit trails.

Output controls ensure that a complete and accurate audit trail of the results of processing is reported to appropriate individuals for review. Examples of output controls are listings of master file changes, error listings, distribution registers, and reviews of output.

If a department has applications that are critical to its success, then department personnel must ensure that application controls reduce input, processing, and output risks to reasonable levels.

CONTROL ACTIVITIES -APPLICATION CONTROLS

(Preventive and Detective)

Application Controls: End User Computing

Twenty years ago, an information systems professional was needed to operate a computer. Today department personnel can obtain and use information on the computer themselves. Some of the common applications used by departments are word processing, desktop publishing, spreadsheets, database management systems, graphics programs, electronic mail, project management, scheduling software, and mainframe-based query systems that are used to generate reports. In addition to computer applications, departments use other information systems applications such as voice mail.

Advancing technology enables departments to purchase or develop information systems and applications, shifting certain general control responsibilities from the centralized information systems department to end-user departments. This often happens in the move from the mainframe to a client-server environment.

The end-user department becomes responsible for segregation of duties within the department's information systems environment, backup and recovery procedures, program development and documentation controls, hardware controls, and access controls. If a department has end-user information systems that are critical to its success, then department personnel must ensure that application & general controls reduce information systems risks to reasonable levels.

CONTROL ACTIVITES

Using our same example, the following table illustrates the concepts discussed thus far. Note that the control activities address the risks previously identified.

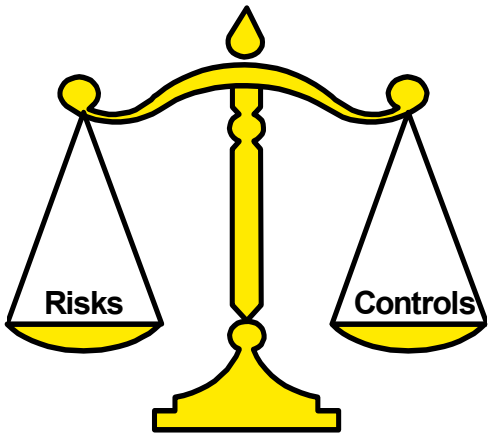
OBJECTIVES	RISKS					CONTROL ACTIVITIES		
	*O, F, C	DESCRIPTIONS	Impact	Proba-bility	Total	DESCRIPTIONS	In place	Planned
Payroll Provide service and support to the County.								
Processing-Authorization To ensure compensation rates and payroll deductions / withholdings are authorized in accordance with management's policy.	O, F	(1) Employees may receive compensation that is not authorized by management and subject the County to penalties or criticism.				(1) Supervisory personnel conduct reviews of compensation (including premium pay) regularly.		
	C	(2) State labor and employment laws and regulations may be violated.				(1,2) The payroll calculation procedures are in compliance with the Orange County Merit System Selection Rules and Appeals Procedures, MOU's, the Personnel and Salary Resolutions, and state laws.		
	C	(3) Interest and penalties may be incurred when remittance to the appropriate taxing entity is inaccurate or untimely.				(3) Establish and communicate County guidelines to develop, summarize and report tax information by required deadlines. (3)Tax remittances are reviewed and authorized by management.		
Processing-Compensation and Deductions / Withholding To ensure compensation rates and payroll deductions are accurately and promptly entered into the payroll system.	O, F	(1) Pay rates or deductions may be unauthorized or inaccurate due to deliberate or accidental errors.				(1) Initial pay, deductions, benefit elections, and any subsequent additions or changes are reviewed and authorized by management.		

OBJECTIVES	RISKS					CONTROL ACTIVITIES		
	*O, F, C	DESCRIPTIONS	Impact	Proba-bility	Total	DESCRIPTIONS	In place	Planned
Processing-Compensation and Deductions / Withholding *(Continued from previous page)* To ensure compensation rates and payroll deductions are accurately and promptly entered into the payroll system.	O, F	(2) Transactions may not be entered into the system in a timely manner, creating avoidable morale issues.				(1) Supervisory review, verification, and approval of inputs to the payroll system are performed. (2) Payroll processing schedules are established to ensure payroll adjustments are input timely.		
Recording To ensure journal vouchers for payroll, payroll deductions / withholdings and related adjustments are prepared and recorded for each accounting period.	F	(1) Financial statements may be misstated due to entry omissions, incorrect coding, duplicate journal vouchers, or improper cut-offs, which may affect the external perception of County operations.				(1) Transactions are classified according to the County's *Chart of Accounts*. (1) Coding instructions, cut-off procedures and closing schedules have been developed, documented, and communicated.		
	O, F	(2) Errors and omissions may go undetected and uncorrected adversely affecting payroll control, payroll funding, or managerial reports.				(1,2) Fluctuation analyses are performed for recurring entries. (1,2) Supervisory personnel review, verify, and approve journal vouchers.		

*Denotes whether risk and related objective is operational, financial or compliance.

CONTROL ACTIVITIES

BALANCING RISKS AND CONTROLS



To achieve goals, management needs to effectively balance risks and controls. By performing this balancing act "reasonable assurance" can be attained. As it relates to financial and compliance goals, being out of balance causes the following problems:

Excessive Risks	**Excessive Controls**
Loss of Assets	Increased Bureaucracy
Poor Business Decisions	Reduced Productivity
Noncompliance	Increased Complexity
Increased Regulations	Increased Cycle Time
Public Scandals	Increase of No-Value Activities

In order to achieve a balance between risk and controls, internal controls should be proactive, value-added, and cost-effective.

INFORMATION & COMMUNICATION

Information and communication are essential to effecting control; information about an organization's plans, control environment, risks, control activities, and performance must be communicated up, down, and across an organization. Reliable and relevant information from both internal and external sources must be identified, captured, processed, and communicated to the people who need it – in a form and timeframe that is useful. Information systems produce reports, containing operational, financial, and compliance-related information that makes it possible to run and control an organization.

Information and communication systems can be formal or informal. Formal information and communication systems – which range from sophisticated computer technology to simple staff meetings – should provide input and feedback data relative to operations, financial reporting, and compliance objectives; such systems are vital to an organization's success. Just the same, informal conversations with customers, suppliers, regulators, and employees often provide some of the most critical information needed to identify risks and opportunities.

When assessing internal control over a significant activity (or process), the key questions to ask about information and communication are as follows:

- Does our department get the information it needs from internal and external sources – in a form and timeframe that is useful?
- Does our department get information that alerts it to internal or external risks (*e.g.,* legislative, regulatory, and developments)?
- Does our department get information that measures its performance – information that tells the department whether it is achieving its operations, financial reporting, and compliance objectives?
- Does our department identify, capture, process, and communicate the information that others need (*e.g.*, information used by our customers or other departments) – in a form and timeframe that is useful?
- Does our department provide information to others that alerts them to internal or external risks?
- Does our department communicate effectively – internally and externally?

Information and communication are simple concepts. Nevertheless, communicating with people and getting information to people in a form and timeframe that is useful to them is a constant challenge. When completing a Business Controls Worksheet for a significant activity (or process) in a department, evaluate the quality of related information and communication systems.

MONITORING

Monitoring is the assessment of internal control performance over time; it is accomplished by ongoing monitoring activities and by separate evaluations of internal control such as self-assessments, peer reviews, and internal audits. The purpose of monitoring is to determine whether internal control is adequately designed, properly executed, and effective. Internal control is adequately designed and properly executed if all five internal control components (Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring) are present and functioning as designed. Internal control is effective if the Board of Supervisors, the CEO and departmental management have reasonable assurance that:

- They understand the extent to which operations objectives are being achieved.
- Published financial statements are being prepared reliably.
- Applicable laws and regulations are being compiled.

While internal control is a process, its effectiveness is an assessment of the condition of the process at one or more points in time.

Just as control activities help to ensure that actions to manage risks are carried out, monitoring helps to ensure that control activities and other planned actions to effect internal control are carried out properly and timely and that the end result is effective internal control. Ongoing monitoring activities include various management and supervisory activities that evaluate and improve the design, execution, and effectiveness of internal control. Separate evaluations, on the other hand, such as self-assessments and internal audits, are periodic evaluations of internal control components resulting in a formal report on internal control. Self-assessments are performed by department employees**;** internal audits are performed by internal auditors who provide an independent appraisal of internal control.

Management's role in the internal control system is critical to its effectiveness. Managers, like auditors, don't have to look at every single piece of information to determine that the controls are functioning and should focus their monitoring activities in high-risk areas. The use of spot checks of transactions or basic sampling techniques can provide a reasonable level of confidence that the controls are functioning.

APPENDIX

COUNTY OF ORANGE
STANDARDS FOR BUSINESS CONTROLS
(Indicate Activity)

OBJECTIVES	BUSINESS OBJECTIVES	RISKS	EXAMPLES OF CONTROL ACTIVITIES	CONTROLS IN PLACE YES (Y)/NO (N) COMMENTS		CONTROL REVISIONS
Review each objective listed for the activity and make any needed additions or deletions. Goals and objectives should be clearly defined and measurable. Indicate if the objective is Operational (O), Financial (F), and/or Compliance © in the next column.	O, F, C	Review the risks listed for each objective and make any needed Changes, (i.e., list risks with reasonable likelihood of occurrence and large potential impacts).	For each risk, listed are examples of control activities to manage the risks and help ensure that the actions to manage the risk are carried out properly and in a timely manner.	**Y / N**	For each example of a control activity, indicate a Yes (Y) or No (N) if the control activity is in place., identify the control activity here. In addition, identify sources of information, methods of communication, and monitoring activities.	List all control revisions planned to correct any control deficiencies or revised controls for the new system.