

## **Maricopa Risk Assessment Process (MRAP):**

### **What it is**

Recent mandates and rapidly changing internal and external environments point to a need for a preventive framework with which to assess and manage risk (opportunities and exposures). In the Fall of 1999, the Vice Chancellor for Business Services launched the Maricopa Risk Assessment Process (MRAP) initiative under the direction of the Governing Board. The goal of MRAP is to embed ongoing assessment of risk into Maricopa's culture. Emphasis is placed on "tone at the top" which is predicated on ethical values, integrity, and competence. The MRAP philosophy fosters continued evaluation of effectiveness and efficiency of organizational leadership, systems, and strategies.

### **Where we are**

In October 2000, the Maricopa Risk Assessment Plan (MRAP) was identified as an internal assessment process within the framework of the MCCC Strategic Plan. Also, in the months of September and October 2000, management and implementation strategies for MRAP were reviewed with members of the Chancellor's Executive Council and Administrative Services Group. Since then, the Business Services Support Team has identified the strategies for roll-out to the colleges and departments. These strategies include the following:

- building support for the vision by getting the word out
- developing a shared understanding of risk concepts
- discovering new and improved tools (best practices)
- conducting pilot(s) with supportive work group(s)
- assigning remaining risks to a responsible department or process expert

Potential MRAP facilitators were trained on use of the Resolver Ballot voting tool in December 2000. Within the next few months, we plan to conduct pilot risk assessments as well as build support by getting the word out.

# MARICOPA COMMUNITY COLLEGES INTERNAL AUDIT & MANAGEMENT ADVISORY SERVICES

## THE IMPORTANCE OF INTERNAL CONTROL

### WHAT IS INTERNAL CONTROL?

---

Internal control is a process. It should provide reasonable assurance for the achievement of these primary objectives:

Effective and efficient operations;  
Financial and other reporting data are reliable;  
Compliance with laws and regulations.

For example, activities to safeguard, or make more efficient or effective use of assets are internal controls. Assets include funds, buildings, equipment, supplies and people. Internal control can be as simple as locking your desk, or as complicated as requiring multiple levels of passwords to access information systems.

### WHO IS RESPONSIBLE FOR INTERNAL CONTROL?

---

In the past internal control was considered an arena reserved for accountants and auditors. Today, the concept of control is very broad. It encompasses all the elements of the organization including its resources, systems, culture, and corporate ethical values. Everyone in the organization plays a role.

This new understanding of control has emerged as organizations address the realities of downsizing, information technology and turbulent change. Furthermore, it has resulted in accounting pronouncements that require organizations, units and departments to conduct their own risk assessment, evaluation of internal controls and redesign of processes and controls as are needed.

***Everyone is responsible***

Everyone is responsible for internal control. Boards, executives, department heads, managers and supervisors are responsible for maintaining an adequate system of financial and administrative controls throughout the organization. They set the "tone" by influencing the control consciousness of employees and communicating an administrative philosophy that includes integrity, ethical values and competence. Employees are responsible to thoughtfully, conscientiously, and consistently execute the control activities in place. Further, it is essential that employees can and do communicate upward any unusual conditions identified as a result of performing control activities. The conditions should be properly assessed and appropriate corrective action taken by management.

## **WHY ARE INTERNAL CONTROLS NEEDED?**

---

Controls are simply good business practices. A sound system of controls reduces risk. Taking risks is often the key to innovation and growth. Risk can also adversely affect an organization's ability to achieve objectives and execute strategies. Thus it is important to distinguish between "good" and "bad" risk and find tools to manage any "bad" risk identified. Effective control provides mechanisms to identify, analyze and manage risks.

## **ARE THERE TYPES OF CONTROL?**

---

A sound system of controls will include certain common control activities:

- Segregation of duties
- Approvals and Authorizations
- Verifications and Reconciliations
- Reviews and Monitoring
- Security of Assets and Records

### **Segregation of Duties**

Segregation of duties is critical to effective internal control; it reduces the risk of both erroneous and inappropriate actions not being detected. No one department or individual should handle all aspects of a transaction from beginning to end. In general, the approval, accounting/reconciling, and the asset custody functions should be separated among employees.

For example,

- The person who requisitions the purchase of goods or services does not approve the purchase.
- The person who approves the purchase of goods or services does not reconcile the monthly financial reports, or obtain custody of checks.
- The person who opens the mail and prepares a listing of checks received does not make the deposit.

### **Approvals and Authorizations**

Actions and transactions must be approved by persons with designated authority before they can occur. The approver certifies the transaction is appropriate, accurate and complies with policy, laws and regulations. For example, if this control were not in place, requisitions and purchase orders could be created for inappropriate or fraudulent goods and services.

### **Verifications and Reconciliations**

Simple verifications and reconciliations help ensure that information is complete and accurate. Differences must be investigated and corrective action taken when necessary. Example: Receipts for travel are verified for accuracy.

### **Reviews**

Managers should review reports, statements, reconciliations and comparisons of financial and performance indicators. Reviews provide a basis for detecting problems. Management's review and any problems or resolutions identified should be documented. If this control were not in place managers would be unaware of accounting and account coding errors and budget overruns.

### **Security of Assets and Records**

Access to equipment, inventories, securities, cash and other assets is restricted. Assets are periodically counted and compared to amounts shown on control records. Security over non-physical assets will include system software passwords and long distance access codes.

### **WHAT ABOUT UNNECESSARY CONTROL ACTIVITIES?**

---

Poor or excessive internal control activities reduce productivity, increase the complexity of processing transactions, increase the time required to process transactions and add risk to the achievement of the organization's objectives.

### **DO SOUND INTERNAL CONTROL ACTIVITIES HAVE LIMITATIONS?**

---

Internal controls provide only *reasonable* assurance objectives are achieved. Managers or other employees may choose to ignore policies and procedures when faced with time and resource constraints. Also, Individuals acting collectively may misappropriate assets and conceal information to prevent detection. This is called collusion.

# COLLEGE CASHIER'S OFFICES INTERNAL CONTROL STRUCTURES AND POTENTIAL CASH HANDLING FRAUDS IN THE MCCC CD ENVIRONMENT

Department of Internal Audit

## **Basic Controls and Procedures**

The decision to prevent and detect fraudulent activity within the business environment begins and ends with internal controls and related procedures. Therefore the keys to counter such fraudulent activity involve establishing an appropriate control structure and ensuring that controls are operating as intended and that compensating controls are in place when other controls break down. Obviously controls can take the form of being preventative or detective in nature but all should seek to achieve the following objectives with regards to the entire control structure:

- Minimize exposure to individuals with a predisposition or motive to commit fraudulent activities. This can be achieved through the appropriate screening of employees and the adequate discipline of employees apprehended.
- Reduce the available opportunities and methods for fraud.
- Increase the probability of detection when frauds do occur, such as conducting spot checks and unannounced reviews.
- Determine that established controls are being followed as the failure to do this negates an otherwise well defined internal control structure.

## **Delegation of responsibility, authority and accountability**

Effective delegation of decision making is not only sound management but also good crime prevention. When responsibility and accountability cannot be fixed, neither can blame. This can be appealing to a dishonest employee as well as an unnecessary temptation for an honest one.

## **Separation of duties**

Another critical fraud control is adherence to the separation-of-duties principle. More often than not, implementation of this concept is more a matter of administrative changes than of any cash outlays. There are four concepts to this principle:

- No individual should have total control over every phase of any significant transaction or sensitive job.
- Work flows should proceed from one person to another so that, without duplication, the work of the second acts as a check upon that of the first.
- Those who authorize the use of assets should not also be responsible for their custody.
- Recordkeeping and bookkeeping activities should be separated from the handling and custody of assets.

Due to the relative small size of several of the College Fiscal Offices, there are not enough employees in some cases to divide responsibilities in a manner that would otherwise be desirable. In these cases assignment of dual responsibilities for a given task as well as job rotation among the staff will help to minimize undetected fraud.

### **Six common myths about fraud**

According to the February 1990 Journal of Accountancy, statistics illustrate that U.S. employees steal about \$120 billion annually with the average bank embezzlement garnering \$125,000. Fraud is not foreign to the government and higher education sectors anymore than it is to big business. Higher Education feels it is immune due to the type of environment in which we operate, however, that leads to the first myths concerning fraud.

- Myth No 1. --- Most People Will Not Commit Fraud
- Myth No 2. --- Fraud Is Not Material
- Myth No 3. --- Most Fraud Goes Undetected
- Myth No 4. --- Fraud is usually well concealed
- Myth No 5. --- Prosecuting Fraud Perpetrators Deters Others

### **References:**

White Collar Crime, Library of Congress, Copyright 1994  
Journal of Accountancy, February 1990

# POTENTIAL CASH HANDLING FRAUDS IN THE MCCCC ENVIRONMENT

Department of Internal Audit

## RECEIPTS PROCESSING

### **1. Removing small amounts from cash funds and registers.**

#### Scenario

Cashier's Office Employee: Cash is pocketed rather than retained in cash drawer/register. Although drawer is short at the end of the day, it is impossible to identify any one person as responsible for shortage and is thus determined to be an error in change making. Little additional effort is made and the cycle continues.

#### Control Attributes:

- Individual cash drawers/ windows and the related responsibility assigned to specific employees rather than accessed by multiple employees during workday/ shift.
- Appropriate follow-up investigation into minor deviations shortages/ surpluses in cash drawers reconciliations at end of day.
- Batch numbers assigned to specific shifts/ employees to ensure responsibility placed for transaction processing.
- Cash and check payments stored securely during working hours.
- Supervisor reviews and approves each batch as it is closed resulting in limited follow-up and immediate attention if errors are identified.
- Reconciliation and verification of payment and refund documents performed by supervisor (individual other than one who prepared).
- Cashier's Office employees handling cash appropriately supervised.

**2. Failing to record "cash/check" receipts (in total) for tuition, fees, or other receipts creating overages in cash funds and pocketing overages.**

Scenario

Cashier's Office Employee: Payments received at the window are recorded as partial payments unknown to the student/ payor. Receipts are not issued unless questioned, giving reason that "the computer is down," "canceled check will serve as your receipt" or issuing unauthorized receipts (self designed). Receipts could be lapped to cover accounts.

For receipts other than tuition and fees, WIZ tickets not created giving reason as "time constraints." As such these are set aside and not validated until end of day. Validation not completed on all WIZ tickets. Rely on lapping or depositors lack of reconciliation to conceal.

Control Attributes:

- Individual cash funds (register, petty cash funds, vault) and the related responsibility assigned to specific employees rather than accessed by multiple employees during workday/ shift.
- Individual cash drawers/ windows and the related responsibility assigned to specific employees rather than accessed by multiple employees during workday/ shift.
- Personal check receipt created and remitted to third party (student) (depending on college) for payment received. Receipt illustrates payment processed and account balance adjusted to reflect payment received.
- Financial institutions may have accounts established under College name or pseudonym which are not properly authorized. College Departments/ Units which have the authority to collect cash may use these unauthorized accounts improperly.
- Payments controlled by batch number and data entry occurs immediately when payment made in-person. Receipt copies used to balance to payments received.
- Restrictive endorsement placed on personal checks upon receipt.
- Personal checks received for payment required to be made payable to College name.
- Cash and check payments stored securely during working hours.
- WIZ ticket created in presence of depositor/ payor ensuring correctness of deposit, account number and signed by preparer.
- Third party (non-student) receives validated WIZ ticket as a receipt of amount paid or deposited.
- Cash transmittal document (i.e. deposit slip) is required to be presented by depositor/ payor. Necessary especially if the Cashier's Office cannot process WIZ transactions immediately.

**3. Failing to make regular bank deposits or depositing only part of the money.**

Scenario

Cashier's Office Employee: Deposits are "borrowed" for the personal benefit of employee by shorting deposits or not depositing regularly. Lapping could occur to cover shortages for extended durations.

Control Attributes:

- Weekly "Cash Count Reconciliation" is performed by an individual different than the one who prepares the bank deposit reducing the opportunity to conceal deposit shortages (through supplementing deposit with funds from the vault).
- Bank deposit prepared by individual other than those directly processing cash receipts.
- Signature from armored car representative ensures deposit delivered to bank intact.
- Reconciliation of total WIZ tickets to cash register "control tape" performed by supervisor.
- Locked mail bag ensures transaction documents delivered to the District Office intact.
- Reconciliation of bank statement performed by individual other than individual who prepared bank deposit.

## REFUNDS PROCESSING

### **1. Identifying "undeliverable" Student Refund Checks (credit balances) and converting them to demand checks for personal benefit.**

#### Scenario

Cashier's Office Employee: Refund checks sent by mail are returned undeliverable to the Fiscal Office due to incorrect address and are not claimed by students. Cashier's Office employee opening mail retains check. Student's account is already adjusted to show that refund has been paid. The check is forged and cashed (QuickCash - No ID) or secondarily endorsed and deposited.

Alternatively, the Cashier's Office employee responsible for "automatically" disbursing refunds identifies this undeliverable check, alters student address to deliver to perpetrator's P.O. Box number as the "revised" address. Address of student returned to original address. (Depending on College - Cashier's Office employees have access to alter student demographic information)

#### Control Attributes:

- Person opening mail is not also responsible for its processing. Should not be the same person as the one responsible for refund preparation and disbursement. Individual opening mail creates log of receipts to be used in reconciliation of mail received and checks processed (Lock box technique).
- Students usually claim refunds unless amount is insignificant (moved out-of-state).
- Cashier's Office employees (depending on College) should not have update access to SIS to modify student addresses, names, telephone numbers.
- Supervisory approval of refund disbursement is required to ensure propriety of processing prior to disbursement of funds. Review would include examination of demand checks and POS tapes for possible improprieties.
- Refunds are not "automatically" processed for students in an overpayment status. In-person or written requests for refund are required to process disbursements.
- The employees who create the demand refund checks are not responsible for mailing (distributes) them.
- Reconciliation of bank statement might detect forged signature discrepancies/ similarities or a possible secondary endorsement by College personnel on canceled checks (depending on how check processed by perpetrator).

**2. Student refunds "not yet claimed" of which student is unaware or believes to be carried over to next semester. Converted to demand checks for personal benefit.**

Scenario - Demand Check

Cashier's Office Employee: Refund checks are "automatically" processed (depending on College, may be after certain days in semester) by individual within Cashier's Office. Address of student is modified by Cashier's Office employee (depending on College - access may be available) to deliver check to perpetrator's P.O. Box/ other address.

Demand check prepared and disbursed to incorrect address (Conversely, this demand check could just be held out of mailing if same individual creating checks is responsible for mailing). Check is forged and cashed (QuikCash - No ID) or forged and secondarily endorsed. Student's account has been adjusted to show "no refund due" and the student's address is returned to original address. Check stub could be destroyed removing evidence of address modification.

Scenario - Credit Card

Cashier's Office Employee: Refund "credits" to credit card accounts may be assigned to a perpetrator's credit card account using false credit card account number and expiration date but adjusting unsuspecting student's account to a refund paid status. POS input could be performed directly by perpetrator and after batch reconciliation, POS receipt could be destroyed removing evidence of improper credit card account credited.

Note 1: Either of these scenarios could involve unsuspecting Cashier's Office employees contacted by telephone to send refunds directly to perpetrator. Perpetrator (Cashier's Office Employee) could obtain all necessary information to convince authenticity of student identity and posing as student, over the telephone, have check mailed to perpetrator's address(es). Address could be modified and returned to original address after check received. Check stub and/ or POS receipt could still be destroyed as Cashier's Office employee would have access to such documentation.

Note 2: Either of these scenarios could also be perpetrated by a Registration Office employee if performed over the telephone. Perpetrator could obtain all necessary information to convince authenticity of student identity and posing as student, over the telephone, have check mailed to perpetrator's address(es). Address could be modified and returned to original address after check received.

Control Attributes:

- Cashier's Office employees (depending on College) should not have update access to SIS to modify student addresses, names, telephone numbers.
- When processing telephone refunds, an attempt is made to ensure credit card refund processed against an appropriate credit card account ( matching refund to original credit card number).
- Verification of telephone refund recipients includes asking for identifying information of greater substance than just Social Security Number, birthdate and address (i.e. Mother's maiden name). Such identifying information could be obtained upon registration.
- Supervisory approval for refunds is required to ensure propriety of processing prior to disbursement of funds.
- Responsibility for processing of individual refunds can be traced to specific Cashier's Office employees through the use of employee initials on supporting documentation or batch transactions assigned by operator ID and ensured through password access.
- Refunds are not "automatically" processed for students in an overpayment status. In-person or written requests for refund are required to process disbursements.
- The employees who create the demand refund checks are not responsible for mailing (distributes) them.
- Up-to-date student residence information is used to mail information directly to the student.
- Reconciliation of bank statement might detect forged signature discrepancies/ similarities or a possible secondary endorsement by College personnel on canceled checks (depending on how check processed by perpetrator).

## DEMAND CHECKS

### **1. Blank Checks inappropriately obtained and processed through check signing machine for personal benefit.**

#### Scenario

Cashier's Office Employee: Perpetrator (Cashier's Office employee) takes demand checks from the bottom of the check stock box to avoid immediate detection. Checks processed through the check signing machine and taken completing additional information away from Office and cashing.

#### Control Attributes:

- Employee that prepares checks and has access to check signing machine is not the same employee that approves the signature machine/ check stock reconciliation thereby reducing the opportunity for falsification.
- Access to the unused checks, check signing machine and signature plates is restricted when not in use.
- Unissued checks locked up; numerically accounted for in log; access restricted to limited number of designated personnel (depending on college).
- Checks issued and recorded in pre-numbered order; sequence accounted for.
- Voided checks defaced.
- Control over access to check signing machine, signature plates and the usage of such.
- Reasonable limits on amounts that can be paid through use of a demand check.
- Recording signature machine control totals and reconciling to check control totals to ascertain that all checks signed are properly accounted for.
- Prohibiting checks written to "Cash" or "Bearer."

## PETTY CASH PROCESSING

### **1. Petty Cash Vouchers Improperly used to charge personal purchases or falsely supported for reimbursement for personal benefit.**

#### Scenario - College Department Employee

##### College Department Employee:

Manager of a department at the College signs voucher for requestor to purchase office supplies. Administrative support purchases personal items along with purchases of office supplies. Manager follow-up is limited and original sales receipt presented to Cashier's Office is limited in detail. False sales receipts may be also supplied and cash pocketed directly.

#### Scenario - College Department Manager:

Manager of a department at the College signs voucher and performs personal purchases directly with limited knowledge of "Requestor" or "Unit Head." Original sales receipt presented to Cashier's Office is limited in detail. False sales receipts may be also supplied and cash pocketed directly. No departmental knowledge of fraudulent act.

Note: If greater deception was necessary at the departmental level, Petty Cash Voucher signatures could be forged with reliance placed on the minimal account reconciliation performed by the Manager/ Unit Head to conceal transactions.

##### Control Attributes:

- Managerial review of purchases made with Petty Cash at departmental level is appropriate to ensure funds used properly.
- College Department Manager cannot conspire to independently misuse public funds due to some upper level of supervisory review. Requirements could stipulate that all such purchasing is process through lower level requests and thus supervisory review would be more readily available.
- Petty Cash Voucher approval signatures required including Dept Head, Unit Head and Fiscal Agent.
- Original sales receipts required to close out voucher. Dates on the sales receipt as well as all supporting documentation reviewed for propriety by the Fiscal Agent representative.
- Limitations placed on the number of vouchers allowed to be outstanding to one department at any one time.
- Number of days which Petty Cash Voucher may be outstanding is limited procedurally.
- Access to blank Petty Cash Vouchers is restricted.

## MISCELLANEOUS

### **1. Blank Student Identification Cards (ID) are obtained by students/ employees in order to create false IDs.**

#### Scenario

Students/ College Employees/ Others:

Blank ID cards are taken from the stock of such cards maintained at the Student Activities Offices/ Campus Security. Such ID cards are used to make fraudulent IDs acceptable as formal identification by the Fiscal Office, Fitness Center, Library and Sporting Events. ID cards could be sold to non-students for unauthorized access or used in refund schemes to obtain inappropriate refunds from the Cashier's Office.

Control Attributes:

- Adequate supervision is employed in situations where work study students create IDs and have access to blank cards.
- Inventory of blank ID cards in stock is regularly performed. (depending on College).
- Student ID is processed only with review of alternate formal picture ID (i.e..State Drivers License, Military ID) (depending on College). Requirements should ensure that more than just the students Name and Social Security Number be necessary to ensure a registered student's identity prior to creating ID
- Student ID should not be considered as acceptable identification for most College fiscal transactions (including disbursement of refund checks and student loan checks) (depending on College).
- Access to blank ID cards restricted under lock and key (depending on College).

### **2. Safe Combinations and Door Keys "sold" to non-employees or non-authorized employees.**

#### Scenario

Cashier's Office Employees: Employee sells safe combination and door keys to non-employees or non-authorized employees resulting in robbery occurring during business or non-business hours due to ease of access.

Control Attributes:

- Safe combination restricted to necessary supervisory employees.
- Combination of safe changed once each year and whenever person having combination is no longer employed in the Cashier's Office.

## PHYSICAL SECURITY CONTROLS

- Cash and Checks maintained overnight in a locked safe with combination lock.
- Manual "Hold-Up" panic alarm system to alert campus security.
- Burglar Alarm utilized to secure building and Cashier's Office.
- Cashiering Office opened and closed only when a second person is present to observe the general area.
- Safe locked during business hours between withdrawals and deposits.
- Cash drawers lockable requiring key entry to which individual employee has only access. Drawers locked when window closed.
- Safe restricted to storage of funds related to the operation of the Cashier's Office only.
- Security windows/ glass installed for the safety of Cashiering personnel.
- Cash counted in an area not visible to customers or others from outside the office.
- Exterior doors have automatic door closers and are key code operated.
- Door keys restricted to necessary employees; doors to Cashier's Office locked.
- Security cameras installed.
- Locked deposit bags.

## Risk and Control Self-Assessment Process Best Practices

Risk & Control Self Assessment (RCSA) denotes a process where work groups of process experts identify the objectives they should be meeting and the adequacy of their processes or other mechanisms in place to meet those objectives. RCSA leads process experts to collectively identify and evaluate risks and controls and/or develop action plans relating to them.

- Preliminary meeting with manager or supervisor
  - ✓ Discuss scope
  - ✓ Identify participants
- Meet Individually with Participants
  - ✓ Discuss processes, risks
  - ✓ Identify areas of concern
- Confirm direction with manager or supervisor
- Conduct RCSA meeting
  - ✓ Provide control background
  - ✓ Identify risks
  - ✓ Rank risks
  - ✓ Develop action plans to address risks
  - ✓ Target action plan implementation dates
- Issue preliminary report for review
- Develop final report with department
- Issue final report document

### Common elements for effective RCSAs:

- Aim for Groups of 10-16 key participants
- Interviews reduce department time investment
- Interviews increase risk identification over surveys
- Actual RCSA session should be about 4 hours
- Adapt to the department's culture and hours
- Utilize electronic anonymous voting tool to identify risk areas, and rank risks
- Develop action plans and implementation dates during session
- Engage individuals with ability to implement action plans in session
- Issue preliminary report within week
- Follow-up on action plans
- Identify preferred equipment/support software
- Never show up without food

# **MRAP** *Maricopa Risk Assessment Process*

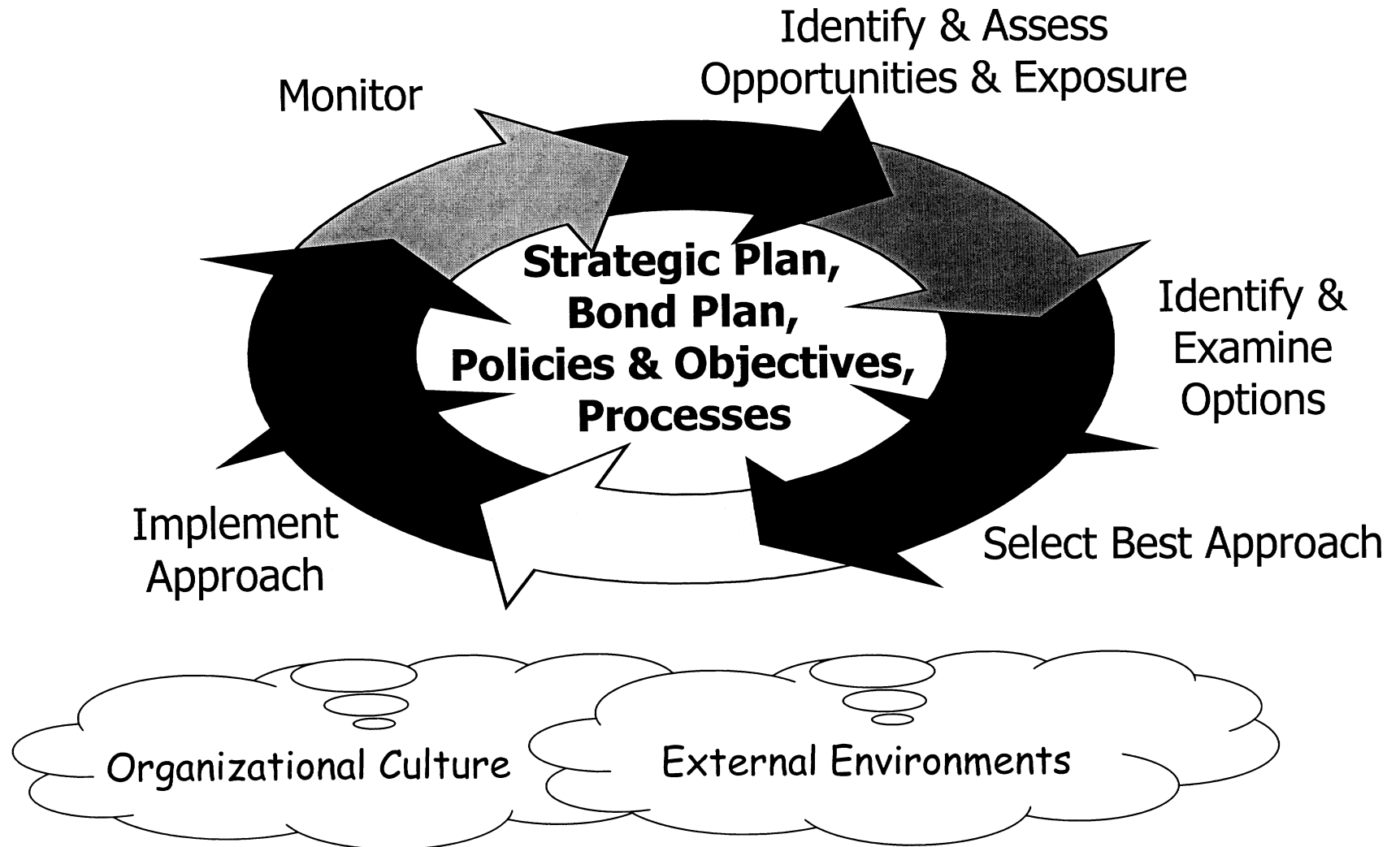
## **The 10 Universal Business Risks**

- (A)** Destruction or Loss of Assets
- (B)** Competitive Disadvantage and/or Public Dissatisfaction
- (C)** Fraud or Conflict of Interest
- (D)** Erroneous Management Policies and Decisions
- (E)** Erroneous Financial Records
- (F)** Unacceptable Accounting Principles
- (G)** Business Interruption
- (H)** Government Criticism or Legal Action
- (I)** Excessive Costs
- (J)** Deficient Revenues

*Source: Sally Dix, Director of Internal Audit  
Airtouch Communications*

# ***MARICOPA RISK ASSESSMENT PROCESS (MRAP)***

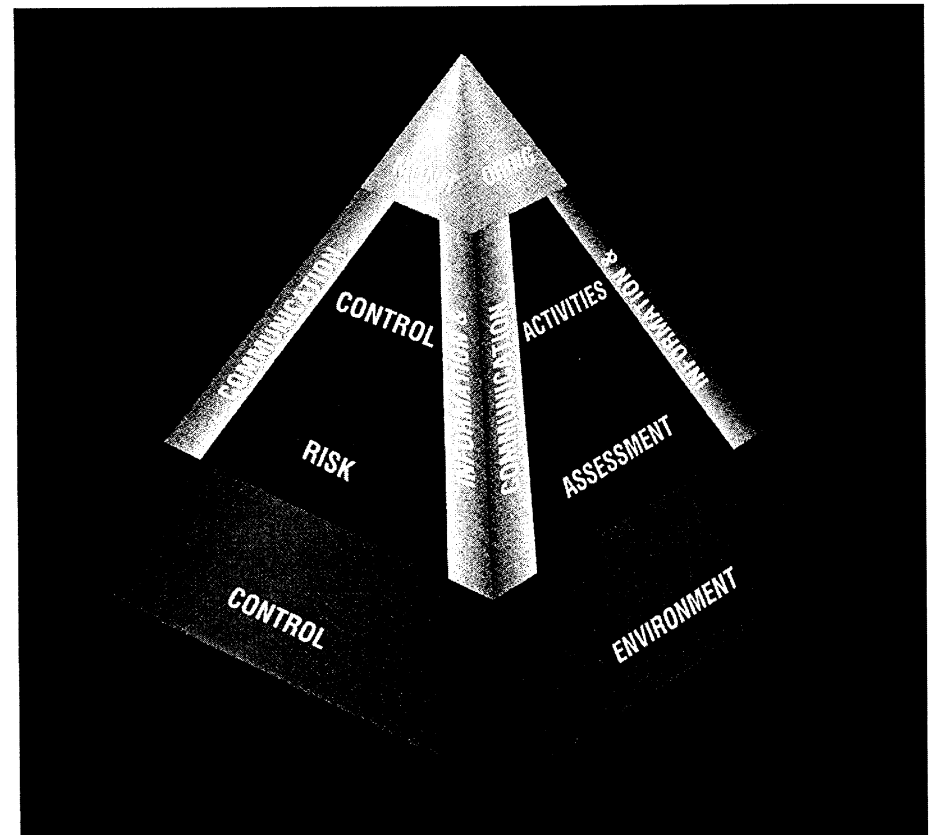
## ***RISK MODEL***



# The COSO Model

The Five Components:

- Business or Control Environment (*the tone of the organization*)
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring



**Maricopa Assessment Process (MAP)  
Business Services Support Team  
Pre-selected Assessment Questions**

**1. Control Environment**

1.1 Does MCCCCD have an entity-wide, up-to-date strategic plan that is used to direct its day to day and future operations?

Do colleges and district office departments have a vision, mission and set of objectives that link closely and meaningfully to the district-wide mission, vision and goals?

1.2 Is there a written code of conduct/ethics statement for employees, reinforced by training, communication and requirements for written statements of compliance?

Do we communicate the basic fabric/core values of MCCCCD throughout MCCCCD?

1.3 Do Board and CEC members set a day-in, day-out example of high integrity and ethical behavior?

1.4 Do employees feel they can raise difficult issues or deliver "bad news" to any level of MCCCCD? I.e., are there established processes for communicating issues?

Is it clear that fraud and other inappropriate behavior will not be tolerated? Are consequences defined and clearly communicated? Are consequences applied uniformly?

1.5 Are risks identified and candidly discussed with the Board and CEC?

1.6 Are performance and incentive compensation targets reasonable and realistic?

Are complete background checks performed before hiring new employees?

Are job descriptions accurate and up to date? Do they include all major expectations?

Is there a statement in every job description of the employee's responsibility for internal controls?

1.7 Assignment of responsibility: Do we identify who can handle what?

**2. Risk Assessment**

2.1. Are ongoing risk assessment processes are in place?

Do we evaluate risks in a timely manner with a reasonable degree of professional skepticism exercised by appropriate levels of management, i.e., do we ask the right questions at the right time?

Are we more proactive and preventive vs. reactive and corrective?

Are actions readily taken to mitigate risks identified and are overall strategies for managing important risks established?

Are the assignments and activities needed to implement the strategies identified and communicated to the responsible employees?

2.2. Does the risk management function encompass all areas of potential risk to MCCCCD? Should it?

2.3. Does MCCCCD have processes in place to ensure business continuity in the event of major internal or external disaster or failure?

Does MCCCCD need a total disaster recovery or business continuity plan?

2.4. Are steps identified, communicated and taken to properly secure the information systems?

## **Pre-selected Assessment Questions (Cont'd)**

### **3. Control Activities –**

3.1. Does management periodically assess the effectiveness of the control within colleges, programs, departments and activities?

Are the results communicated to the Board and the CEC?

3.2. Do staff other than managers see control activities as part of their responsibility?

3.3. Does everyone demonstrate that they understand and accept their control responsibility?

3.4. Are control activities designed as an integral part of the introduction of new systems and processes?

### **4. Information & Communication**

4.1. Is sufficient, relevant information communicated in a timely manner to the appropriate employees to enable them to perform their assigned responsibilities?

4.2. Are information needs and related information systems reassessed as objectives change or as reporting deficiencies are identified?

4.3. Is trust actively promoted between employees, supervisors and departments?

4.4. Is there a way to communicate suspected risks, deficiencies, and improprieties through someone other than a direct supervisor?

Are employees protected from retaliation?

Is there a process for internal and external complaints to be taken seriously, investigated and acted upon?

### **5. Monitoring**

5.1. Does the Chancellor ensure periodic assessment of the effectiveness of the internal control system and communicate the results to the CEC and to the Board?

5.2. Is effectiveness monitored against targets and indicators? Do follow-up procedures ensure that appropriate change or action occurs?

5.3. Are assumptions behind objectives periodically challenged?