

## Chapter 9

### REVIEW OF CONTROLS

<u>Section</u>	<u>Contents</u>	<u>Page</u>
900	Control Concepts	9-1
901	Primary Objectives of Control	9-1
902	Control - Management's Responsibility	9-2
903	Control - Auditor's Responsibility	9-2
904	Basic Elements of Internal Control	9-2
905	Review and Evaluation of Internal Controls	9-3

## Chapter 9 - Review of Controls

### 900. Control Concepts

1. Control is defined by the Institute of Internal Auditors (IIA) as "any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved." (International Standards for the Professional Practice of Internal Auditing – Glossary)
2. Controls are designed to:
  - prevent undesirable events from occurring;
  - detect and correct any undesirable event that may have occurred; or
  - direct/encourage a desirable event to occur.
3. Variants of the term control include, but are not limited to: administrative control, internal accounting control, internal control, management control, operational control, and output control. These terms reflect different objectives management wishes to achieve. The methodology for evaluating controls is consistent for all of the control variants.
4. The control environment is the attitude and actions of the board and management regarding the significance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:
  - Integrity and ethical values
  - Management's philosophy and operating style
  - Organizational structure
  - Assignment of authority and responsibility
  - Human resource policies and practices
  - Competence of personnel.

### 901. Primary Objectives of Control

According to the IIA (PA2110.a2), the internal audit activity should evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

1. reliability and integrity of financial and operational information;
2. compliance with policies, procedures, laws, regulations, and contracts;
3. safeguarding of assets;

4. effectiveness and efficiency of operations.

#### 902. Control - Management's Responsibility

One of the tasks of a board of directors is to establish and maintain the organization's governance processes and to obtain assurances concerning the effectiveness of the risk management and control processes. (PA2120.A1-1)

#### 903. Control - Auditor's Responsibility

1. The internal audit activity performs audit work and gathers information in order to evaluate the adequacy and effectiveness of the risk management and control processes.
2. All of the University's systems, departments, offices and activities are subject to evaluation by Audit and Management Services.

#### 904. Basic Elements of Internal Control

An effective auditor must acquire the ability to recognize and evaluate the major controls for each activity and then develop the necessary audit procedures to test their effectiveness. Some of the basic elements which contribute to good internal control are:

1. An organizational structure which is well-balanced and systematic.
2. Careful separation and delineation of duties and responsibilities between individuals who:
  - initiate or authorize transactions,
  - execute the transactions, and
  - have responsibility for the assets, liabilities, revenues, or expenses resulting from transactions.

There should be a segregation between the functions of record keeping and custodianship.

3. Maintenance of accurate information, records and reports adequate to the activity's needs.
4. Properly qualified personnel.
5. Arrangement of duties so that one employee's work compliments that of another employee.
6. Establishment of written operating procedures to clarify duties and responsibilities.
7. Periodic reviews of the system of internal control at timely intervals.

## 905. Review and Evaluation of Internal Controls

1. Policy - For audits requiring an evaluation of the adequacy of controls, a review should be conducted in accordance with procedures included in this manual.
2. Purpose - The review should enable the auditor to determine whether controls are adequate to provide reasonable assurance that:
  - information generated will be reliable and complete;
  - Federal, State, University and departmental requirements will be complied with;
  - assets will be properly safeguarded; and
  - goals and objectives will be accomplished in an efficient manner.
3. Procedures for Evaluating Internal Controls - For each process included in the scope of the audit, the auditor should complete the Risk/Control Matrix (Exhibit 9-1) to document the evaluation of controls. Procedures for preparing the matrix are listed below.
  - A. Assess the level of risk associated with each control objective by completing the “Ranking of Control Objectives” section on the Risk/Control Matrix. Each control objective should be ranked as one of the following:
    - (1) High Risk refers to situations where a major exposure exists if the control objective is not in place.
    - (2) Medium Risk is that risk which is considerable in nature, but may not constitute a major threat.
    - (3) Low Risk refers to situations where an exposure exists if the control objective is not in place, but the exposure does not by itself represent a major potential for material misstatements of financial data or significant adverse effects.

The Risk/Control Matrix includes the following standard control objectives:

- (1) Authorization - All transactions should be approved by responsible personnel, in accordance with their specific or general authority, before the transaction is recorded.

Examples of authorization controls include:

- review and approval
- requiring authorized signature

- endorsement or authorizing symbol
- electronic signature
- authorization password

(2) Accuracy/Completeness of Information - All transactions should be accurate (i.e., mathematically correct), consistent with the originating transaction data, and recorded in a timely manner. Also, all transactions should be included in the accounting records.

Examples of accuracy controls include:

- reconciliation procedures
- recalculation procedures
- control amount and account totals (manually kept)
- visual format checks
- visual pricing checks
- pre-printed and pre-coded forms
- simultaneous preparation
- batch control register
- batch control totals
- hash control totals
- run-to-run totals
- check digit verification
- data entry dual keying
- numeric edit checks
- range or reasonableness checks
- dependency checks
- existence checks
- format checks
- mathematical accuracy checks
- prior data matching
- error suspense files
- error processing time and date stamps
- error reports

Examples of completeness controls are:

- reconciliation procedures
- pre-numbered documents
- serially numbered transactions
- batch serial numbers
- batch control registers
- document control counts
- sequence checking
- processing completeness checks
- batch control totals

- hash control totals
- run-to-run (transaction count) totals

(3) Validity of Information - All (recorded) transactions should fairly represent the economic events that actually occurred.

Examples of validity controls are:

- review of authorization signatures
- verification of transaction purpose
- review of transaction legitimacy
- review for compliance with Federal, State, University and departmental requirements (laws, policies and procedures, directives, regulations, etc.)

(4) Segregation of Duties - Segregation of duties ensures that responsibilities are assigned to individuals in such a manner so that no one individual or department can control all the phases of processing a transaction. Segregation helps prevent or detect an individual from perpetuating or concealing errors/irregularities (e.g., fraud).

Examples of activities that should be performed separately are:

- authorization of transactions
- recording of transactions
- custody of assets
- accountability of assets

(5) Physical Security of Assets - Access to physical assets and information systems should be controlled and properly restricted to authorized personnel.

Examples of physical safeguards are:

- safes or vaults
- locked cabinets or doors
- storerooms with custodians
- security access controls
- dual control measures

B. Identify and document risks related to the process by reviewing ARMICS<sup>1</sup> documentation, departmental procedures, compliance information, and other materials obtained during the preliminary survey. (Note - All risks and controls identified in ARMICS documentation should be included in the Risk/Control Matrices prepared by AMS.) Also, note any relevant compliance references on the Risk/Control Matrix.

---

<sup>1</sup> Agency Risk Management and Internal Control Standards

C. For each risk identified, rank impact as high, medium or low. Consider the following risk factors when assessing impact:

- impact of service delays
- impact of unreliable information
- magnitude of resources controlled
- impact of adverse publicity
- confidentiality of information

D. Identify and document control procedures that contribute to the management (e.g., avoidance, reduction, sharing) of each risk. Control procedures may be detective, corrective, or preventive in nature. After identifying the control procedures, determine which control objective(s) each control procedure helps achieve.

The auditor should identify and document weaknesses when, in the auditor's judgment, risks are not adequately mitigated by the control procedures. If necessary, audit findings should be written and cross referenced to the Control Matrix Worksheet. (See Chapter 12: "Nature and Presentation of Audit Findings and Recommendations".)

The auditor should also determine whether the department has adequately documented operating and control procedures in written policies and procedures. Finally, the auditor should determine whether the performance of control procedures is evidenced by the department.

E. For each risk identified, rank likelihood as high, medium or low. When assessing likelihood, consider control procedures as well as the following risk factors:

- control environment:
  - extent of management planning and review
  - adequacy of policies and procedures
  - pressure on management to meet objectives
  - extent of government regulation
  - experience level of management
  - management's receptivity to audit reports and recommendations
  - history of errors and irregularities
- complexity of operations
- changes in operations
- level of processing sophistication

F. Discuss risks, impact ratings, likelihood ratings, control procedures and weaknesses with the department head and/or other staff in the department. Also, inquire whether any risks have been excluded. (*Note - The auditor may submit a draft of the Risk/Control Matrix to the department head for discussion purposes; however, the*

*“Preliminary Conclusion”, “Departmental Assessment” section, and auditor references on the final page of the matrix should be deleted before sending the matrix to the department head.)*

- G. After making any necessary revisions to the matrix based on discussions with the department head, complete the “Preliminary Conclusion” section on the Risk/Control Matrix to document whether controls are adequate. When developing the conclusion, the auditor should evaluate the residual risk (i.e., the risk remaining after considering control procedures), consider the ranking of control objectives, and determine whether the objectives have been met.
- H. Submit the Risk/Control Matrix to the Audit Director for review and approval.
- I. Submit the Risk/Control Matrix along with a cover memo (Exhibit 9-1a) to the department head and request that he/she complete the “Departmental Assessment” section to document whether he/she concurs with risks, impact ratings, likelihood ratings, control procedures and weaknesses noted. *(Note – Auditor references on the final page of the matrix should be deleted before sending the matrix to the department head.)* If the department head disagrees with the above information, discuss the matrix with him/her and consider revising the matrix.
- J. If controls are determined to be inadequate, send a memo (Exhibit 9-2) communicating the opinion on controls to the Vice President. Copies of the memo should also be sent to the Assistant/Associate Vice President (or Dean) and the department head.
- K. Identify control procedures to be tested and indicate audit program references in the appropriate column on the Risk/Control Matrix. If existing controls for a process are determined to be inadequate during the evaluation of controls, then audit test procedures should, in most instances, not be performed. Also, refer to Table 1 in the matrix for a guideline to use when identifying controls to test.
- L. Finally, design specific audit tests to ensure that control procedures are effective (i.e., functioning as intended). The Risk/Control Matrix, audit program and time budget must be approved by the Audit Director before beginning fieldwork. After fieldwork (testing of the controls) has been completed, a final conclusion should be prepared to state whether controls are adequate and functioning as intended. The final conclusion should be documented in the fieldwork working papers.

See Section 804 and chapters 10 - 12 for procedures related to the audit program and fieldwork.