Audit Manual

Process and Activities

October 2016
# Table of Content

**Introduction**  
3

**Strategic Aim**  
4

**Chapter 1 – Audit Engagements**

- Financial audits  
5
- Compliance audits  
5
- Information systems audits  
5
- Operational audits  
5
- Investigative audits  
6
- Consulting engagements  
6

**Chapter 2 – Internal Controls**

- Definition  
7
- Internal control components  
7
- Objectives of internal controls  
8
- Levels of controls  
9
- Type of controls  
9
- Control tools  
11

**Chapter 3 – Audit Process**

- What is an audit engagement?  
13
- Audit process  
13
- Entrance conference  
13
- Preliminary research  
14
- Risk assessment  
14
- Audit objectives  
14
- Audit scope of work  
15
- Audit basic procedures  
15
Audit program 15
Fieldwork 16
Informal communications 16
Working papers 16
Draft audit report 17
Exit conference 17
Final draft audit report 17
Management response 18
Final audit report 18
Client satisfaction survey 19
Audit follow-up review 19
Audit follow-up report 19
INTRODUCTION

Internal Audit provides independent and objective assurance and consulting services to management. It helps improve operations by bringing systematic disciplined approaches to evaluate and improve College governance, risk management, and internal control processes.

- Governance includes evaluating management philosophy and operating style, ethical environment, policy structure, human resources policies, organizing and developing people, communication and information, compliance, and resources allocation.
- Risk management involves identifying, assessing, and managing strategic and operational risks across the College. This control tool prepares managers at all levels to respond to risks and uncertainties.
- Internal control is a managerial action that management develops and implements to ensure that risk across the College is contained within the College risk appetite.

Internal Audit is a managerial control that functions by measuring and evaluating the effectiveness of other controls. Internal Audit evaluates the

- Reliability and integrity of information and the means used to identify, measure, classify, and report such information.
- Systems established to ensure compliance with applicable laws and regulations and College’s relevant policies and procedures.
- Means of safeguarding college assets and verifying that they exist.

Internal Audit assists investigating alleged or suspected illegal activities of fraud, misappropriation of College assets, and noncompliance.

The audit charter promulgates the Internal Audit purpose, organization, authority, responsibilities, and scope of work.

The Institute of Internal Auditors (IIA) and the Government Auditing standards govern the Internal Audit professional practice.
STRATEGIC AIM

In an effort to meet its stakeholders’ expectations in the wake of the College growth and increasing demands, Internal Audit identified the following strategies to guide its practice.

Enhancing Excellence

• Connect strategies to core processes.
• Launch new initiatives to promote excellence and influence a culture change through partnerships and collaborative structures.
• Draw attention to areas of interest, and gain commitment to react to sector and market changes, trends, and best practices.
• Stimulate and sustain new sources and methods of participation to influence knowledge and skills and improve overall efficiency and effectiveness.
• Influence management commitment and buy-in.
• Operate within a culture nurtured by its organizational structure.

Sustainability

• Sustain a high quality Internal Audit activity that is widely recognized and constantly adapting to its stakeholders developing needs.
• Demonstrate a well-led, managed and governed Internal Audit activity, and sustain intellectual, economic, social and environmental development.
• Reliance on accountability, self-evaluation, customer satisfaction, and collaborative and participative relationships.
• Maintain independence, objectivity, professionalism, integrity, and uphold professional and ethical standards.
CHAPTER 1 – TYPE OF AUDITS

Internal Audit provides the following audit engagements and consulting services:

**Financial Audits** - Financial audits address questions of accounting and reporting of financial transactions, including commitments, authorizations, and receipt and disbursement of funds.

The objectives of these engagements are to verify if there are adequate and effective processes and systems of internal controls over cash and cash-like assets, and the acquisition and use of College resources.

Recommendations often call for improvements in processes and controls intended to ensure accurate, reliable, timely, and adequately supported financial records and reports.

**Compliance Audits** – Compliance audits determine the degree of a unit’s adherence to applicable federal and state laws and regulations and to College policies and procedures.

Recommendations often call for improvements in processes and controls intended to ensure compliance with laws, regulations, and policies.

**Information Systems Audits** – Information systems audits address the internal control environment of automated information processing systems and how people use these systems.

These engagements typically evaluate system input, output, processing controls, backup and recovery plans, system security, and computer facility reviews. They can focus on existing systems as well as systems in their development stages. Internal audit may outsource or co-source specialized IS audits requiring specialized expertise.

Recommendations often call for improvements in managing confidential data, processing data, data security, and systems accessibility.

**Operational Audits** – Operational audits (a.k.a. Performance Audits) examine the use of a unit resources to evaluate whether those resources are being used in the most efficient and effective ways to fulfill the unit's mission and objectives.

These engagements focus on the departmental level activities that are components of the College's core business activities and processes (e.g., payroll, benefits, cash handling, inventory, grants, contracts, and financial reporting, etc.). An operational audit engagement includes elements of a compliance, financial, and an information system audit.

Recommendations often call for improvements in processes and controls intended to ensure accuracy and reliability of financial records; safeguards of assets; reliability of reports; personal information and data security; efficient and effective delegation of duties; security over systems
accessibility; compliance with laws, regulations and College policies; and ways to improve security and efficiency over the efficient use of College’s resources.

**Investigative audits** – Investigative audits (a.k.a. Administrative Reviews) are audit engagements requested by management based on specific emerging risks or needs.

These engagements typically focus on alleged illegal activities, misappropriation of College assets, and noncompliance with applicable federal and state laws and regulations.

These engagements also focus on potential violations of College policies and procedures that contemplates the possibility of a civil or criminal risk to the College.

**Consulting engagements** – Consulting Services are advisory services Internal Audit provides to management. Advisory services focus on adding value and improve college operations.

Consulting services include providing management with advice related to governance, risk management, and internal control processes; providing training; assisting with policy making; and participating in quality teams.
CHAPTER 2 – INTERNAL CONTROLS

Definition

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

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

The first category addresses the college basic business objectives, including performance and profitability goals and safeguarding of resources. The second category relates to the preparation of reliable published financial statements, including interim and condensed financial statements and selected financial data derived from such statements. The third category deals with complying those laws and regulations to which the College is subject.

Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved. Employee also play a key role in either strengthening or weakening the College’s systems of internal controls.

Internal Control Components

Internal Control consist of five interrelated components. All five components must be present and functioning correctly.

**Control Environment:** The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; and the way management assigns authority and responsibility, and organizes and develops its people.

**Risk Assessment:** Every entity faces a variety of risks from external and internal sources that must be assessed. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed.

**Control Activities:** Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as
approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

**Information and Communication:** Pertinent information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication must occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators and shareholders.

**Monitoring:** Internal control systems need to be monitored, a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties.

**Objectives of Internal Controls**

The primary objectives of evaluating controls is to provide reasonable assurance that

1. Financial and operating data and reports are accurate and reliable.
2. Compliance with policies, procedures, plans, laws and regulations actually occurs.
3. Assets exist and are protected against loss that could result from theft, fire, improper or illegal activities, or exposure to the elements.
4. Operations’ resources:
   a. Are used efficiently and economically.
   b. Operating standards have been established for measuring economy and efficiency.
   c. Standards are understood and being met.
   d. Deviations from operating standards are identified, analyzed and communicated to those responsible for corrective action.
   e. Adequate and effective corrective actions have been taken.
5. Operations and programs provide reasonable assurance that the operations and programs are being carried out as planned, and that the results of operations are consistent with established goals and objectives.

An internal audit could encompass all five audit objectives (full scope audit), or only one or a few of them (limited scope audit). Audit scope could be further limited by only assessing and evaluating the adequacy of controls (i.e., the degree to which the controls provide reasonable
assurance), or by only assessing and evaluating the effectiveness of the controls (i.e., the degree to which the controls actually function as management intended).

Levels of Controls

There are four levels of controls illustrated in the following figure.

<table>
<thead>
<tr>
<th>Level 4</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit</td>
<td>Execution</td>
<td>Supervisory</td>
<td>Oversight</td>
<td>Audit</td>
</tr>
<tr>
<td>Pre-operation</td>
<td>During</td>
<td>Immediately after</td>
<td>Shortly after</td>
<td>Post-operation</td>
</tr>
</tbody>
</table>

Type of Controls

Soft controls are the intangible expression of management values, culture and leadership strategies (e.g., tone at the top, ethical climate, open door policy, fairness, integrity, empowerment, competencies, equity, and diversity).

Hard controls are tangible organizational measures that management develops and implements to achieve specific goals that can be either measured or evaluated (e.g., policies, procedures, directives, flow charts, delegation of duties, and human resources policies)

Controls categories include but are not limited to:

1. **Primary Controls**
   a. **Preventive controls** deter the occurrence of unwanted events.
   b. **Detective controls** alert the proper people after an unwanted event. They are effective when detection occurs before material harm occurs.
   c. **Corrective controls** correct the adverse impact of unwanted events.
   d. **Directive controls** cause or encourage the occurrence of a desirable event. These include the following:
      i. Policies and procedures manuals.
      ii. Employee training.
      iii. Job descriptions.
2. **Secondary controls**
   a. *Compensatory controls* should be present when primary controls are ineffective. However, they do not, by themselves, reduce the risk to an acceptable level.
   b. *Complementary controls* work with other controls to reduce risk.
3. **Application controls** are performed by a particular system. They provide reasonable assurance that the recording, processing and reporting of data are properly performed.
   Application controls include:
   i. *Input controls* are the most economical point for correcting input errors in an application is at the time in which the data are entered into the system [e.g., batch, integration, and online input].
   ii. *Processing controls* ensure that data are complete and accurate during updating.
   iii. *Output controls* ensure that processing results are complete, accurate and properly distributed.
4. **Time-Based controls**
   a. *Feedback controls* report information about completed activities. These controls permit future improvement by learning from past mistakes.
   b. *Concurrent controls* adjust ongoing processes. Real time controls monitor activities in the present to prevent them from deviating too far from standards.
   c. *Feedforward controls* anticipate and prevent problems. These controls require long term perspective.
5. **Financial controls** should be based on relevant established accounting principles. Financial controls may include:
   a. Proper authorizations
   b. Appropriate recordkeeping
   c. Safeguarding of assets
   d. Compliance with laws, regulations, and contracts.
6. **Operating controls** apply to production and support activities. Because they may take established criteria or standards, they should be based on management principles and methods.
7. **People-Based controls** are dependent on the intervention of humans for their proper operation.
8. **System-Based controls** are executed whenever needed without human intervention.
9. **Segregation of Duties** – For any given transaction, the following three functions preferably should be performed by separate individuals in different part of the College:
   a. Authorization of the transaction
   b. Recording of the transaction
   c. Custody of the assets associated with the transaction
Control Tools

Controls include, but are not limited to

1. Ethical “tone at the top”, communicated in words and deeds.
2. Organizational structure that promotes the flow of information.
3. Clear definition of responsibilities.
4. Delegation of authority commensurate with responsibility.
5. Mechanisms to hold people accountable for results.
6. Reward mechanisms.
7. Qualified and well trained personnel, particularly in key positions.
8. Positive and motivating work environment.
9. Effective empowerment of employees.
10. An atmosphere of mutual trust.
11. Frequent interaction between senior and operating management.
12. Appropriate policies and procedures for hiring, training, promoting, and compensating employees.
13. Written policies and procedures.
15. Procedures for authorizing and processing transactions.
16. Reviews: budget to actual comparison, current to prior period comparison, performance indicators, project management reports, etc.
17. Reconciliations.
18. Security for assets and records.
19. Supervisor review.
20. Segregation of duties (e.g., separation of initiation, authorization, recording, and custody).
22. Former and current compliance programs including a designated compliance officer.
23. Forms controls (e.g., pre-numbered documents, maintaining integrity of numerical sequence, limited access to key forms).
24. Exception reports (e.g., receivable past due, overtime, duplicated payments, and discounts not taken).
25. Information systems controls:
   a. Environmental controls (e.g., heat, humidity, fire extinguishers).
   b. Data security systems.
   c. Backup and recovery policies and procedures.
   d. Disaster recovery and or business continuance plan (tested periodically).
   e. Input controls – authorization, validation, error notification and correction (e.g., blocked transactions, transaction limits, error listings, filed checks, self-checking digits, sequence checks, validity checks, and completeness checks).
   f. Processing controls (e.g., edit checks, control totals and other programmed steps within application software, audit trails).
g. Output controls (e.g., output review, exception reports, master file change reports).

h. Software license compliance controls.
What is an Audit Engagement?

An audit engagement is a specific internal audit assignment, task, or review activity, such as an internal audit, control self-assessment, review, fraud examination, or a consultancy. An audit engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives.

Planned engagements are those initially identified and assessed during the risk assessment process from which the internal audit plan derives. All planning, evidence gathering, and data evaluation begins with the audit objectives, and the audit ends when the auditor has enough competent and relevant evidence to write a report which satisfies the audit objectives.

Unplanned engagements are emerging consulting engagements, or engagements requested by management to address specific emerging risks.

The success of an audit engagement is based on sound planning, mutual trust, collaboration, constructive participation, and open communication between the client, client management, and Internal Audit.

The process works best when client, client management, and Internal Audit have a solid working relationship based on clear and continuing communication.

Many clients extend this relationship beyond a particular audit.

Audit Process

Although every audit engagement is unique in itself, the audit process is, however, similar for most engagements, and consists of planning, performing, communicating, and monitoring progress. Each phase serves different needs and provides different deliverables.

Entrance Conference

The client and client management receive the audit engagement letter that communicates the following information:
• An internal audit engagement is planned for a specific auditable area
• The engagement objectives
• The engagement start and end dates
• A request to schedule the audit entrance conference

During the entrance conference, the auditor meets with the client and client management to gather relevant information about the auditable area in order to obtain an understanding of its activities, governance, compliance, risks, controls, and reporting structure.

Preliminary Research

After the entrance conference, the auditor

• Reviews prior audit working papers and determines the status of deficiencies noted during previous audits, especially when corrective actions remain outstanding.
• Identifies significant changes.
• Reviews organisational charts and the nature of activities and processes.
• Reviews appropriate data and pertinent information (e.g., accounting information; contracts and agreements; established policies and procedures; human resources policies, applicable laws and regulations).
• Reviews processes structure and flowcharts, and evaluates their internal control systems.
• Performs an analytical review to determine significant variances (e.g., account balances; deviations form objectives; budget variations).

Risk Assessment

After completing the preliminary research, the auditor performs a preliminary risk assessment considering the reliability of management process to assess and address risk and control and management response when events exceed the auditable area’s risk tolerance. When assessing risk, the auditor considers among many others the risk and impact of fraud and misappropriation of assets.

There are three main attributes for assessing risk: Severity of impact (how significant the consequences might be); time of impact (when is it likely to happen); and controls (what actions management took to reduce the consequence or its probability to occur).

Audit Objectives

After the preliminary research and the risk assessment are complete, the auditor sets the objectives of the audit engagement. The engagement objectives are broad statements developed to explain why the auditable area is being audited and define what the auditor intend to achieve from the engagement.
The auditor determines the audit objectives with consideration for any concerns expressed by management, and based on the information gathered during the preliminary research phase.

For planned engagements, the objectives are consistent with those initially identified and assessed during the risk assessment process from which the internal audit plan derives. For unplanned engagements, the auditor establishes objectives to address the specific risks or needs that prompted the engagement.

**Audit Scope of Work**

The audit scope of work includes considerations of the activities the auditor wants to review, relevant systems, records, personnel, and physical properties, including those under the control of third parties.

The audit scope of work must be sufficient to achieve the audit objectives.

**Audit Basic Procedures**

Audit procedures are performed to obtain sufficient, reliable, relevant and useful information to the achievement of the engagement objectives. Audit basic procedures include:

- **Observing conditions:** Observation is effective to verify whether particular assets exist, and whether particular processes or procedures are performed appropriately at a specific moment in time.
- **Interviewing people:** Interviewing people (inquiry) is especially helpful to obtain an understanding of the client operations, because of the opportunity to ask questions to clarify preceding answers, and to pursue additional information.
- **Examining records:** Examining records (inspecting) is a broad term of the process of determining the validity, authenticity and reliability of information and support documentation.

**Audit Program**

The audit program outlines the fieldwork necessary to achieve the audit objectives. The program guides the auditor during the fieldwork to ensure that the audit coverage is adequate.
to provide sufficient and reliable evidence upon which the auditor concludes on the achievement of the audit objectives.

The auditor may use prior years’ audit programs and update them to ensure adequate coverage of current objectives.

**Fieldwork**

Audit fieldwork concentrates on transaction testing and informal communications. It is during this phase that the auditor examines the facts and related support documentation and determines whether the risk identified during the preliminary review are adequately mitigated. Also determined is whether the identified controls are operating properly and in the manner described by the client.

The extent of audit testing depends on the auditor’s professional judgment. Special consideration is given to the materiality of the amounts involved, the relative risk of errors or irregularities, the complexity of processes and operations, budget magnitude, and size of the auditable area.

The auditor documents the rationale for the sample size selection in the audit working papers.

**Informal Communications**

As the fieldwork progresses, the auditor discusses any significant observations with the client. The client can offer insight and work with the auditor to determine the best method of resolving the observation. These will be informal communications between the auditor and the client. However, written communications are an integral part of the audit working papers.

**Working papers**

Working papers serve as a means of communication between internal audit, client, and client management. Working papers include sufficient and reliable information to ensure that necessary procedures are performed.

The auditor takes the necessary steps to ensure that the information contained in the working papers is reliable and restricted to matters that are materially important and relevant to the audit objectives.
Draft Audit Report

At the conclusion of the fieldwork, the auditor prepares a draft audit report to use as the basis for subsequent discussions of the audit results with the client and client management. Depending on the observation in the draft audit report, the latter may not include the audit recommendations.

The auditor uses the draft audit report as the basis for discussion during the audit exit conference.

Exit Conference

The purpose of the exit conference is for the auditor to:

- Inform the client and client management about the preliminary audit observations and recommendations.
- Provide the client and client management the opportunity to correct any misstatements, factual errors, or misinterpretations.
- Obtain the client and client management views about the audit observations and recommendations.
- Discuss the practicality of the audit recommendations and timeframes for any remedial action.
- Reach an agreement on the draft audit report text, observations, and recommendations.

The auditor documents the exit conference in the audit working papers.

Final Draft Audit Report

Internal Audit is expected to make known the results of its work. Internal audit issues the final draft audit report promptly following the exit conference, taking into account any revisions resulting from the exit conference and other discussions.

The final draft audit report may vary by auditable area or by type of engagement. The final draft audit report includes observations that are relevant statements of fact necessary for understanding the audit conclusions and recommendations.

There are four attributes of observations and recommendations:

- The **criteria** are the standards, measures or expectations used in making an evaluation or verification (the correct state).
- The **condition** is the factual evidence the auditor finds during the examination (the current state).
- The **cause** is the reason of the difference between expected criteria and actual conditions.
• The **effect** is the risk or exposure the organization or other encounters because the condition is not consistent with the criteria.

This final draft audit report is primarily for internal use. Releasing any copies of this final draft audit report requires the written approval of the Senior Internal Auditor.

**Management Response**

Upon receiving the final draft audit report, the client and client management have 10 working days to respond in writing to the final draft audit report. Management response will only explain how the client and client management plan to address the audit observations including an implementation timetable.

In some cases, the client and client management may choose to respond with a decision not to implement the audit recommendations and to accept the risks associated with the respective audit observations. In a similar situation, the client and client management are required to provide an alternative corrective action plan to address the audit observations.

While management agreement is not always necessary, discussions will be held with the aim of reaching an agreement. The reasons for any disagreement will be included in the final audit report together with any Internal Audit response.

Internal Audit may issue the final audit report without the management response in the event of undue management delays in responding.

**Final Audit Report**

The final step in communicating engagement results is reporting the engagement outcomes. Promptly after receiving management response, Internal Audit issues a signed report to the client senior management, taking into consideration any revisions resulting from management response and other discussions.

The Senior Internal Auditor communicates and discusses the final audit report with the President and the Board of Trustees.

---

![Flowchart](chart.png)

**Planning**

- Client Satisfaction Survey

**Performing**

- Audit Follow-up Review

**Communicating**

**Monitoring**

- Audit Follow-up Report
Client Satisfaction Survey

Internal audit sends out a client satisfaction survey with the final audit report or shortly after, seeking the client and client management objective and constructive evaluation of its performance. Such feedback has proven to be very beneficial to Internal Audit.

The Senior Internal Auditor will follow-up on any feedback indicating possible shortcomings in Internal Audit performance.

Audit Follow-Up Review

The audit engagement does not end once the outcomes are communicated to the appropriate parties. Final steps include monitoring client management disposition of the reported outcomes and following up.

Internal Audit monitors and periodically seeks updates from client and client management regarding progress in implementing the audit recommendations or the client management alternative corrective actions.

Internal Audit performs a follow-up review to verify the resolution of the audit report observations that includes:

- Verifying the adequacy and effectiveness of the corrective actions taken by the client and client management
- Implementation of management response
- Implementation timeframe
- Following up

Internal Audit usually plans its follow-up reviews three or six month after issuing the final audit report.

Audit Follow-up Report

Promptly after completing the follow-up review, Internal Audit issues a signed report to the client management, including any unsatisfactory responses and any recommendations that remain outstanding.

The Senior Internal Auditor communicates and discusses the final audit follow-up reports with the President and the Board of Trustees.