APPENDIX A
THE IIA GLOSSARY

This appendix contains the Glossary appended to the *Standards*.

Activity-level controls – Controls that operate for the entire activity (area, process, or program). Examples are review of cost center reports, inventory counts, and the soft controls that influence the mini-control environment within the activity, which may or may not be consistent with that of the organization as a whole.

Add value – Value is provided by improving opportunities to achieve organizational objectives, identifying operational improvement, and/or reducing risk exposure thorough both assurance and consulting services.

Adequate control – Present if management has planned and organized (designed) in a manner that provides reasonable assurance that the organization’s risks have been managed effectively and that the organization’s goals and objectives will be achieved efficiently and economically.

Advisory services – Service activities provided by the internal audit function, the nature and scope of which are agreed with the recipients of the services, are intended to add value and improve an organization’s governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

Analytical procedures – The activities of comparing client information with expectations for that information obtained from an independent source, identifying variances, and investigating the cause of significant variances.

Application controls – Fully automated (i.e., performed automatically by the systems) IT controls designed to ensure effective business process enablement and the complete and accurate processing of data, from input through output.

Application systems – Sets of programs that are designed for end users such as payroll, accounts payable, and, in some cases, large applications such as enterprise resource planning (ERP) systems that provide many business functions.

Appropriate evidence – Any piece or collection of evidence gained during an engagement that provides relevant and reliable support for the judgments and conclusions reached during the engagement.

Asset misappropriation – Acts involving the theft or misuse of an organization’s assets (for example, skimming revenues, stealing inventory, or payroll fraud).

Assurance layering – A technique of coordinating multiple assurance activities designed to mitigate a known risk to a needed or desired level within an established risk tolerance.

Assurance map – A visual depiction of the different assurance activities and assurance functions within an organization. Such a depiction can help identify gaps or overlaps in assurance activities and help assess that risk is managed consistent with the board’s and management’s expectations.

Assurance services – An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.

Attribute sampling – A statistical sampling approach, based on binomial distribution theory, that enables the user to reach a conclusion about a population in terms of a rate of occurrence.

Audit committee – A committee of the board charged with recommending to the board the approval of auditors and financial reports.

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

Audit observation – Any identified and validated gap between the current and desired state arising from an assurance engagement.

Audit risk – The risk of reaching invalid audit conclusions and/or providing faulty advice based on the audit work conducted.

Audit sampling – The application of an audit procedure to less than 100 percent of the items in a population for the purpose of drawing an inference about the entire population.

Audit universe – A compilation of the subsidiaries, business units, departments, groups, processes, or other established subdivisions of an organization that exist to manage one or more business risks.

Auditee/audit client/audit customer – The subsidiary, business unit, department, group, or other established subdivision of an organization that is the subject of an assurance engagement.

Big data – A term used to refer to the large amount of constantly streaming digital information, massive increase in the capacity to store large amounts of data, and the amount of data processing power required to manage, interpret, and analyze the large volumes of digital information.

Blank confirmations – Confirmation that asks the third party to fill in a blank with the information requested. This provides stronger evidence than other confirmations.

Board – The highest level governing body (e.g., a board of directors, a supervisory board, or a board of governors or trustees) charged with the responsibility to direct and/or oversee the organization’s activities and hold senior management accountable. Although governance arrangements vary among jurisdictions and sectors, typically the board includes members who are not part of management. If a board does not exist, the word “board” in the *Standards* refers to a group or person charged with governance of the organization. Furthermore, “board” in the *Standards* may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee).

Bottom-up approach – To begin by looking at all processes directly at the activity level, and then aggregating the identified processes across the organization.

Bring your own device (BYOD) – A policy whereby organizations allow associates to access business email, calendars, and other data on their personal laptops, smartphones, tablets, or other devices.

Business acumen – Savviness and experience with regard to business management in general, and more specifically, with the way the organization and, in particular, specific business units operate.

Business process – The set of connected activities linked with each other for the purpose of achieving one or more business objectives.

Business process outsourcing (BPO) – The act of transferring some of an organization’s business processes to an outside provider to achieve cost reductions, operating effectiveness, or operating efficiency while improving service quality.

Capability maturity model – A tool used to measure today's capability and define the characteristics of higher levels of capability. Largely used in business to assess and develop operations and services.

Cause – The reason for the difference between the expected and actual conditions (why the difference exists).

Chief audit executive (CAE) – Chief audit executive describes the role of a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the mandatory elements of the International Professional Practices Framework. The chief audit executive or others reporting to the chief audit executive will have appropriate professional certifications and qualifications. The specific job title and/or responsibilities of the chief audit executive may vary across organizations.

Classical variables sampling – A statistical sampling approach based on normal distribution theory that is used to reach conclusions regarding monetary amounts.

Cloud computing – The use of various computer resources–both hardware and software–that are delivered through a network like the Internet. The cloud can be configured with various options of services along with configurations for the network. It allows for a great deal of flexibility in network, software, and hardware utilization. Cloud computing also provides options for remote storage of data and use of remote applications.

COBIT – An IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues, and business risks.

Code of Ethics – The Code of Ethics of The Institute of Internal Auditors (IIA) are principles relevant to the profession and practice of internal auditing and Rules of Conduct that describe behavior expected of internal auditors. The Code of Ethics applies to both parties and entities that provide internal audit services. The purpose of the Code of Ethics is to promote an ethical culture in the global profession of internal auditing.

Combined assurance – Aligning various assurance activities within an organization to ensure assurance gaps do not exist and assurance activities minimize duplication and overlap but still manage risk consistent with the board's and management's expectations.

Compensating control – An activity that, if key controls do not fully operate effectively, may help to reduce the related risk. Such controls also can back up or duplicate multiple controls and may operate across multiple processes and risks. A compensating control will not, by itself, reduce risk to an acceptable level.

Compliance – Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.

Computer-assisted audit techniques (CAATs) – Automated audit techniques, such as generalized audit software, utility software, test data, application software tracing and mapping, and audit expert systems, that help the internal auditor directly test controls built into computerized information systems and data contained in computer files.

Condition – The factual evidence that the internal auditor found in the course of the examination (what does exist).

Confirmations – Document sent to independent third parties asking them to verify the accuracy of client information in the course of audit testing.

Conflict of interest – Any relationship that is, or appears to be, not in the best interest of the organization. A conflict of interest would prejudice an individual's ability to perform his or her duties and responsibilities objectively.

Consulting services – Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

Continuous auditing – Using computerized techniques to perpetually audit the processing of business transactions.

Continuous monitoring – The automated review of business processes and controls by associates in the business unit. It helps an organization detect errors, fraud, abuse, and system inefficiencies.

Control – 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.

Control activities – Policies and procedures put in place to ensure that risk management actions are effectively carried out.

Control environment – The attitude and actions of the board and management regarding the importance 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
- Organizational structure
- Management's philosophy and operating style
- Assignment of authority and responsibility
- Human resource policies and practices
- Competence of personnel

Control processes – The policies, procedures (both manual and automated), and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organization is willing to accept.

Control risk – The potential that controls will fail to reduce controllable risk to an acceptable level.

Controllable risk – The portion of inherent risk that management can reduce through day-to-day operations and management activities.

Controls are adequately designed – Present if management has planned and organized (designed) the controls or the system of internal controls in a manner that provides reasonable assurance that the organization's entity-level and process-level risks can be managed to an acceptable level.

Controls are operating effectively – Present if management has executed (operated) the controls or the system of internal controls in a manner that provides reasonable assurance that the organization's entity-level and process-level risks have been managed effectively and that the organization's goals and objectives will be achieved efficiently and economically.

Core Principles for the Professional Practice of Internal Auditing – The Core Principles for the Professional Practice of Internal Auditing are the foundation for the International Professional Practices Framework (IPPF) and support internal audit effectiveness.

Corporate governance – The exercise of ethical and effective leadership by the board toward the achievement of ethical culture, good performance, effective control, and legitimacy.

Corporate social responsibility – The term commonly associated with the movement to define and articulate the responsibility of private enterprise for nonfinancial performance.

Corruption – Acts in which individuals wrongfully use their influence in a business transaction to procure some benefit for themselves or another person, contrary to their duty to their employer or the rights of another (for example, kickbacks, self-dealing, or conflicts of interest).

COSO – The Committee of Sponsoring Organizations of the Treadway Commission is a joint initiative of five private sector organizations dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control, and fraud deterrence.

Cosourcing – Activity of contracting with a third party to collaborate in the provision of assurance and consulting services.

Criteria – The standards, measures, or expectations used in making an evaluation and/or verification of an observation (what should exist).

Customer – The subsidiary, business unit, department, group, individual, or other established subdivision of an organization that is the subject of a consulting engagement.

Data analytics – A process of inspecting, cleaning, transforming, and modeling data with the goal of highlighting useful information, suggesting conclusions, and supporting decision-making.

Data visualization – Making complex data more understandable through visual depiction in terms of statistical graphics, plots, information graphics, tables, and charts.

Database – A large repository of data typically contained in many linked files and stored in a manner that allows it to be easily accessed, retrieved, and manipulated.

Descriptive analytics – The reporting of past events to characterize what has happened. It condenses large chunks of data into smaller, more meaningful bits of information.

Design evaluation – A detailed risk assessment of the activities within the audit scope, including identification of the controls and other risk management techniques over the major risks, and evaluation of the design of these controls and techniques.

Detective control – An activity that is designed to discover undesirable events that have already occurred. A detective control must occur on a timely basis (before the undesirable event has had a negative impact on the organization) to be considered effective.

Developmental objectives – Objectives that require enhancement or transformation to something new with a start and end date.

Diagnostic analytics – A process that provides insight into why certain trends or specific incidents occurred and helps analysts gain a better understanding of business performance, market dynamics, and how different inputs affect the outcome.

Directive control – A control that causes or encourages a desirable event to occur. Examples are guidelines, training programs, and incentive compensation plans. Also included in this category are soft controls like tone at the top.

Effect – The risk or exposure the organization and/or others encounter because the condition is not consistent with the criteria (the consequence of the difference).

Engagement – A specific internal audit assignment or project that includes multiple task or activities designed to accomplish a specific set of objectives. Also see Assurance Services and Consulting Services.

Engagement objectives – Broad statements developed by internal auditors that define intended engagement accomplishments.

Engagement opinion – The rating, conclusion, and/or other description of results of an individual internal audit engagement, relating to those aspects within the objectives and scope of the engagement.

Engagement work program – A document that lists the procedures to be followed during an engagement, designed to achieve the engagement plan.

Enterprise risk management (ERM) – Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Entity-level control – A control that operates across an entire entity and, as such, is not bound by, or associated with, individual processes.

External auditor – See Independent Outside Auditor.

External service provider – A person or firm outside of the organization that has special knowledge, skill, and experience in a particular discipline.

Framework – A body of guiding principles that form a template against which organizations can evaluate a multitude of business practices. These principles are comprised of various concepts, values, assumptions, and practices intended to provide a yardstick against which an organization can assess or evaluate a particular structure, process, or environment or a group of practices or procedures.

Fraud – Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

Fraudulent financial reporting – Acts that involve falsification of an organization's financial statements (for example, overstating revenues, or understating liabilities and expenses).

General information technology controls – Controls that operate across all IT systems and are in place to ensure the integrity, reliability, and accuracy of the application systems. Also represents a specific example of an "entity-level control."

Governance – The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

Haphazard sampling – A non-statistical sample selection technique used to select a sample without intentional bias to include or exclude a sample item that is expected to be representative of the population.

Hard controls – The tangible elements of governance controls, such as policies and procedures, accounting reconciliations, and management signoffs.

Illegal acts – Activities that violate laws and regulations of particular jurisdictions where a company is operating.

Impairment – Impairment to organizational independence and individual objectivity may include personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations (funding).

Impairment to independence or objectivity – The introduction of threats that may result in a substantial limitation, or the appearance of a substantial limitation, to the internal auditor's ability to perform an engagement without bias or interference.

Incremental objective – Improving the quality or efficiency of the existing operational outcome by enhancing one or more of the components (people, process, technology, or deliverable).

Independence – The freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner.

Independent outside auditor – A registered public accounting firm, hired by the organization's board or executive management, to perform a financial statement audit providing assurance for which the firm issues a written attestation report that expresses an opinion about whether the financial statements are fairly presented in accordance with applicable Generally Accepted Accounting Principles.

Information technology general controls – Controls that apply to all systems components, processes, and data present in an organization or systems environment. The objectives of these controls are to ensure the appropriate development and implementation of applications, as well as the integrity of program and data files and of computer operations.

Information technology governance – The leadership, structure, and oversight processes that ensure the organization's IT supports the objectives and strategies of the organization.

Information technology operations – The department or area in an organization (people, processes, and equipment) that performs the function of running the computer systems and various devices that support the business objectives and activities.

Inherent limitations of internal control – The confines that relate to the limits of human judgment, resource constraints and the need to consider the cost of controls in relation to expected benefits, the reality that breakdowns can occur, and the possibility of collusion or management override.

Inherent risk – The combination of internal and external risk factors in their pure, uncontrolled state, or, the gross risk that exists, assuming there are no internal controls in place.

Insight – An end product or result from the internal audit function's assurance and consulting work designed to provide valued input or information to an auditee or customer. Examples include identifying entity-level root causes of control deficiencies, emerging risks, and suggestions to improve the organization's governance process.

Internal audit activity – A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes.

Internal audit charter – The internal audit charter is a formal document that defines the internal audit activity's purpose, authority, and responsibility. The internal audit charter establishes the internal audit activity's position within the organization; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities.

Internal control – A process, effected 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.
- Compliance with applicable laws and regulations.

International Organization for Standardization (ISO) – A network of national standards institutes of 162 countries that issues globally accepted standards for industries, processes, and other activities.

International Professional Practices Framework (IPPF) – The conceptual framework that organizes the authoritative guidance promulgated by The IIA. Authoritative Guidance is composed of two categories - (1) mandatory and (2) strongly recommended.

Intrusion detection systems (IDS) – Network security appliances that monitor network or system activities and report the activities to management.

Intrusion prevention systems (IPS) – Network security appliances that monitor network or system activities and prevent malicious activities from happening on the network.

ISACA – Professional organization that provides practical guidance, benchmarks, and other effective tools for all enterprises that use information systems.

Judgmental sample – A nonrandom sample selected using the auditor's judgment in some way.

Key controls – Controls that must operate effectively to reduce a significant risk to an acceptable level.

Key performance indicator – A metric or other form of measuring whether a process or individual tasks are operating within prescribed tolerances.

Logical access – Tools used in computer systems for identification, authentication, authorization, and accountability.

Management action plan – What the audit customer, alone or in collaboration with others, intends to do to address the cause, correct the condition, and–if appropriate–recover from the condition.

Management control – Actions carried out by management to assure the accomplishment of their objectives, including the setting up of oversight for an objective and the alignment of people, processes, and technology to accomplish that objective.

Management trail – Processing history controls, often referred to as an audit trail, that enable management to identify the transactions and events they record by tracking transactions from their source to their output and by tracing backward.

Material observation – An individual observation, or a group of observations, is considered "material" if the control in question has a reasonable possibility of failing and the impact of its failure is not only significant, but also exceeds management's materiality threshold.

Monitoring – A process that assesses the presence and functioning of governance, risk management, and control over time.

Narrative – Free-form compositions used to describe processes. They have no inherent discipline like risk/control matrices and flowcharts, but they are useful for things that require an explanation too lengthy to fit within the confines of the disciplined tools.

Negative confirmations – Confirmations that ask for a response only if the information is not accurate.

Network – A configuration that enables computers and devices to communicate and be linked together to efficiently process data and share information.

Network firewall – A device or set of devices designed to permit or deny network transmissions based upon a set of rules. It is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass.

Nonsampling risk – The risk that occurs when an internal auditor fails to perform his or her work correctly (for example, performing inappropriate auditing procedures, misapplying an appropriate procedure, or misinterpreting sampling results).

Objectives – What an entity desires to achieve. When referring to what an organization wants to achieve, these are called business objectives, and may be classified as strategic, operations, reporting, and compliance. When referring to what an audit wants to achieve, these are called audit objectives or engagement objectives.

Objectivity – An unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others.

Observation – A finding, determination, or judgment derived from the internal auditor’s test results from an assurance or consulting engagement.

Observation (as an audit test) – An audit test that involves simply watching something being done.

Operating system – Software programs that run the computer and perform basic tasks, such as recognizing input from the keyboard, sending output to the printer, keeping track of files and directories on the hard drive, and controlling various computer peripheral devices.

Opinion – The auditor’s evaluations of the effects of the observations and recommendations on the activities reviewed; also called a micro opinion or conclusion. The opinion usually puts the observations and recommendations in perspective based on their overall implications.

Opportunity – The possibility that an event will occur and positively affect the achievement of objectives.

Organizational independence – The chief audit executive’s line of reporting within the organization that allows the internal audit function to fulfill its responsibilities free from interference. Also see Independence.

Other assurance providers – Other entities within the organization whose principal mission is to test compliance or assess business activities to confirm that risks are effectively evaluated and managed.

Outsourcing – Activity of contracting with an independent third party to provide assurance services.

Overall opinion – The rating, conclusion, and/or other description of results provided by the chief audit executive addressing, at a broad level, governance, risk management, and/or control processes of the organization. An overall opinion is the professional judgment of the chief audit executive based on the results of a number of individual engagements and other activities for a specific time interval.

Positive confirmations – Confirmations that ask for a response regarding whether the information is accurate or not.

Predictive analytics – Type of analytics that allows users to extract information from large volumes of existing data, apply certain assumptions, and draw correlations to predict future outcomes and trends.

Preventive control – An activity that is designed to deter unintended events from occurring.

Primary control – An activity designed to reduce risk associated with a critical business objective.

Principle – A fundamental proposition that serves as the foundation for a system of belief or a chain of reasoning.

Probability-proportional-to-size (PPS) sampling – A modified form of attribute sampling that is used to reach a conclusion regarding monetary amounts rather than rates of occurrence.

Process map (flowchart) – A tool that shows the process flow visually, which highlights the control points and therefore helps internal auditors to identify missing controls and assess whether existing controls are adequate.

Processing controls – Controls that provide an automated means to ensure processing is complete, accurate, and authorized.

Process-level control – An activity that operates within a specific process for the purpose of achieving process-level objectives.

Professional skepticism – The state of mind in which internal auditors take nothing for granted; they continuously question what they hear and see and critically assess audit evidence.

Random sample – A sample in which every item in the population has an equal chance of being selected.

Random sampling – A sampling technique in which each item in the defined population has an equal opportunity of being selected.

Rating – A component of an audit opinion or conclusion. Such a rating typically reflects the auditor's conclusion about residual risk.

Ratio analysis – Calculating financial or nonfinancial ratios. For example, the auditor could calculate the percent of products produced that were returned as defective, or the percent of sick days taken to the number of sick days allowed.

Reasonable assurance – A level of assurance that is supported by generally accepted auditing procedures and judgments. Reasonable assurance can apply to judgments surrounding the effectiveness of internal controls, the mitigation of risks, the achievement of objectives, or other engagement-related conclusions.

Reasonableness tests – The act of comparing information to the internal auditor's general knowledge of the organization or industry, rather than another specific piece of information.

Recommendation – The auditor's call for action to correct or improve operations. A recommendation may suggest approaches to correcting or enhancing performance as a guide for management in achieving desired results. The recommendation answers the question, "What is to be done?"

Regression analysis – Statistical technique used to establish the relationship of a dependent variable to one or more independent variables. For example, an internal auditor might estimate payroll expense based on the number of employees, average rate of pay, and the number of hours worked, and then compare the result to the recorded payroll expense.

Residual risk – The portion of inherent risk that remains after management executes its risk responses (sometimes referred to as net risk).

Risk – The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

Risk appetite – The level of risk that an organization is willing to accept.

Risk assessment – The identification and analysis (typically in terms of impact and likelihood) of relevant risks to the achievement of an organization's objectives, forming a basis for determining how the risks should be managed.

Risk capacity – The maximum risk a firm may bear and remain solvent.

Risk management – A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

Risk mitigation – An action, or set of actions, taken by management to reduce the impact and/or likelihood of a risk to a lower, more acceptable level.

Risk tolerance – The acceptable variation relative to performance to the achievement of objectives.

Risk treatment/risk response – An action, or set of actions, taken by management to achieve a desired risk management strategy. Risk responses can be categorized as risk avoidance, reduction, sharing, or acceptance. Exploiting opportunities that, in turn, enable the achievement of objectives, is also a risk response. ISO 31000 refers to this step in risk management as risk treatment.

Risk/control matrix – An audit tool that facilitates risk-based auditing. It usually consists of a series of columns, including columns for business objectives, risks to the objectives, controls or risk management techniques, and other columns that aid in the analysis.

Sampling risk – The risk that the internal auditor's conclusion based on sample testing may be different than the conclusion reached if the audit procedure was applied to all items in the population.

Secondary control – An activity designed to either reduce risk associated with business objectives that are not critical to the organization's survival or success or serve as a backup to a key control.

Significance – The relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors, such as magnitude, nature, effect, relevance, and impact. Professional judgment assists internal auditors when evaluating the significance of matters within the context of the relevant objectives.

Significant observation – An individual observation, or a group of observations, is considered "significant" if the control activity in question has a reasonable possibility of failing and the impact of its failure is significant.

Smart mobile devices – Intelligent mobile devices like smart phones and tablets.

Social media – Web-based and mobile technologies used to turn communication into interactive dialogue.

Social networks – The social network sites that are commonly used. Examples include Facebook, Google+, and Twitter.

Soft controls – The intangible, inherently subjective elements of governance control like tone at the top, integrity and ethical values, and management philosophy and operating style.

Standard – A professional pronouncement promulgated by the Internal Audit Standards Board that delineates the requirements for performing a broad range of internal audit activities and for evaluating internal audit performance.

Statistical sampling – A sampling technique that allows the auditor to define with precision how representative the sample will be. After applying the technique and testing the sample, the auditor can state the conclusion in terms of being “%” confident that the error rate in the population is less than or equal to “%.”

Strategic objectives – What an entity desires to achieve through the value creation choices management makes on behalf of the organization’s stakeholders.

Strategy – Refers to how management plans to achieve the organization’s objectives.

Sufficient evidence – A collection of evidence gained during an engagement that, in its totality, is enough to support the judgments and conclusions made in the engagement.

System of internal controls – Comprises the five components of internal control–the control environment, risk assessment, control activities, information and communication, and monitoring–that are in place to manage risks related to the financial reporting, compliance, and operational objectives of an organization. Also see Internal Control.

Third-party service provider – A person or firm, outside the organization, who provides assurance and/or consulting services to an organization.

Three Lines Model – A model of assurance that helps organizations identify structures and processes that best assist the achievement of objectives and facilitate strong governance and risk management. The model applies to all organizations and is optimized by:

- Adopting a principles-based approach and adapting the model to suit organizational objectives and circumstances.
- Focusing on the contribution risk management makes to achieving objectives and creating value, as well as to matters of “defense” and protecting value.
- Clearly understanding the roles and responsibilities represented in the model and the relationships among them.
- Implementing measures to ensure activities and objectives are aligned with the prioritized interests of stakeholders.

Tolerance – The boundaries of acceptable outcomes related to achieving business objectives.

Tone at the top – The entity-wide attitude of integrity and control consciousness, as exhibited by the most senior executives of an organization. Also see Control Environment.

Top-down approach – To begin at the entity level, with the organization’s objectives, and then identify the key processes critical to the success of each of the organization’s objectives.

Tracing – Taking information from one document, record, or asset forward to a document or record that was prepared later. For example, if auditors count inventory, they would trace their count forward to the client’s inventory records to verify the completeness of the records.

Transaction-level control – Controls that operate within a transaction-processing system. Examples are authorizations, segregation of duties, and exception reports.

Transformational objective – An objective that requires significantly altering operational components of people, processes, and/or technology to accomplish a new, higher objective or value-adding opportunity.

Transparency – Communicating in a manner that a prudent individual would consider to be fair and sufficiently clear and comprehensive to meet the needs of the recipient(s) of such communication.

Trend analysis – Comparing information from one period with the same information from the prior period.

Val IT – A governance framework and supporting publications addressing the governance of IT-enabled business investments.

Virtualization – When a physical IT component is partitioned into multiple “virtual” components; for example, when a physical server is logically partitioned into two virtual servers.

Vouching – The act of taking information from one document or record backward to an asset, document, or record that was prepared earlier. For example, auditors might vouch information on a computer report to the source documents from which the information was input to the system to verify the validity of the information.

Web content filtering – The technique whereby content is blocked or allowed based on analysis of its content, rather than its source or other criteria. It is most widely used on the Internet to filter email and web access.

APPENDIX B
THE IIA CIA EXAM SYLLABUS AND CROSS-REFERENCES

For your convenience, we have reproduced verbatim The IIA’s CIA Exam Syllabus for Part 2 of the CIA exam. Note that the “basic” cognitive level means the candidate must retrieve relevant knowledge from memory and/or demonstrate basic comprehension of concepts or processes. Those levels labeled “proficient” mean the candidate must apply concepts, processes, or procedures; analyze, evaluate, and make judgments based on criteria; and/or put elements or material together to formulate conclusions and recommendations.

We also have provided cross-references to the study units and subunits in this course that correspond to The IIA’s more detailed coverage. Please visit The IIA’s website for updates and more information about the exam. Rely on the Gleim materials to help you pass each part of the exam. We have researched and studied The IIA’s CIA Exam Syllabus as well as questions from prior exams to provide you with an excellent review program.

PART 2 – PRACTICE OF INTERNAL AUDITING

		Domain	Cognitive Level	Gleim Study Unit(s) or Subunit(s)
I	**Managing the Internal Audit Activity (20%)**			
	1. Internal Audit Operations			
	A	Describe policies and procedures for the planning, organizing, directing, and monitoring of internal audit operations	**Basic**	**1.1-1.4**
	B	Interpret administrative activities (budgeting, resourcing, recruiting, staffing, etc.) of the internal audit activity	**Basic**	**1.2, 1.4**
	2. Establishing a Risk-based Internal Audit Plan			
	A	Identify sources of potential engagements (audit universe, audit cycle requirements, management requests, regulatory mandates, relevant market and industry trends, emerging issues, etc.)	**Basic**	**4.1**
	B	Identify a risk management framework to assess risks and prioritize audit engagements based on the results of a risk assessment	**Basic**	**4.1-4.2**
	C	Interpret the types of assurance engagements (risk and control assessments, audits of third parties and contract compliance, security and privacy, performance and quality audits, key performance indicators, operational audits, financial and regulatory compliance audits)	**Proficient**	**2.1-2.8, 3.1-3.2**
	D	Interpret the types of consulting engagements (training, system design, system development, due diligence, privacy, benchmarking, internal control assessment, process mapping, etc.) designed to provide advice and insight	**Proficient**	**3.3-3.6**
	E	Describe coordination of internal audit efforts with the external auditor, regulatory oversight bodies, and other internal assurance functions, and potential reliance on other assurance providers	**Basic**	**1.5**
	3. Communicating and Reporting to Senior Management and the Board			
	A	Recognize that the chief audit executive communicates the annual audit plan to senior management and the board and seeks the board's approval	**Basic**	**4.3**
	B	Identify significant risk exposures and control and governance issues for the chief audit executive to report to the board	**Basic**	**4.3**
	C	Recognize that the chief audit executive reports on the overall effectiveness of the organization's internal control and risk management processes to senior management and the board	**Basic**	**4.3**
	D	Recognize internal audit key performance indicators that the chief audit executive communicates to senior management and the board periodically	**Basic**	**4.3**

		Domain	Cognitive Level	Gleim Study Unit(s) or Subunit(s)
II	**Planning the Engagement (20%)**			
	1. Engagement Planning			
	A	Determine engagement objectives, evaluation criteria, and the scope of the engagement	**Proficient**	**5.2**
	B	Plan the engagement to assure identification of key risks and controls	**Proficient**	**5.1**
	C	Complete a detailed risk assessment of each audit area, including evaluating and prioritizing risk and control factors	**Proficient**	**5.1**
	D	Determine engagement procedures and prepare the engagement work program	**Proficient**	**5.4-5.5**
	E	Determine the level of staff and resources needed for the engagement	**Proficient**	**5.3**
III	**Performing the Engagement (40%)**			
	1. Information Gathering			
	A	Gather and examine relevant information (review previous audit reports and data, conduct walk-throughs and interviews, perform observations, etc.) as part of a preliminary survey of the engagement area	**Proficient**	**5.1, 6.3-6.5, 8.2**
	B	Develop checklists and risk-and-control questionnaires as part of a preliminary survey of the engagement area	**Proficient**	**5.1, 6.3**
	C	Apply appropriate sampling (nonstatistical, judgmental, discovery, etc.) and statistical analysis techniques	**Proficient**	**SU 7**
	2. Analysis and Evaluation			
	A	Use computerized audit tools and techniques (data mining and extraction, continuous monitoring, automated workpapers, embedded audit modules, etc.)	**Proficient**	**8.1, 8.4**
	B	Evaluate the relevance, sufficiency, and reliability of potential sources of evidence	**Proficient**	**6.1-6.2**
	C	Apply appropriate analytical approaches and process mapping techniques (process identification, workflow analysis, process map generation and analysis, spaghetti maps, RACI diagrams, etc.)	**Proficient**	**8.2**
	D	Determine and apply analytical review techniques (ratio estimation, variance analysis, budget vs. actual, trend analysis, other reasonableness tests, benchmarking, etc.)	**Basic**	**3.6, 8.3**
	E	Prepare workpapers and documentation of relevant information to support conclusions and engagement results	**Proficient**	**8.4-8.5**
	F	Summarize and develop engagement conclusions, including assessment of risks and controls	**Proficient**	**8.6**
	3. Engagement Supervision			
	A	Identify key activities in supervising engagements (coordinate work assignments, review workpapers, evaluate auditors' performance, etc.)	**Basic**	**8.5, 8.7**

		Domain	Cognitive Level	Gleim Study Unit(s) or Subunit(s)
IV	**Communicating Engagement Results and Monitoring Progress (20%)**			
	1. Communicating Engagement Results and the Acceptance of Risk			
	A	Arrange preliminary communication with engagement clients	**Proficient**	**9.1**
	B	Demonstrate communication quality (accurate, objective, clear, concise, constructive, complete, and timely) and elements (objectives, scope, conclusions, recommendations, and action plan)	**Proficient**	**9.2-9.4**
	C	Prepare interim reporting on the engagement progress	**Proficient**	**9.1**
	D	Formulate recommendations to enhance and protect organizational value	**Proficient**	**9.2**
	E	Describe the audit engagement communication and reporting process, including holding the exit conference, developing the audit report (draft, review, approve, and distribute), and obtaining management's response	**Basic**	**9.3, 9.5-9.6**
	F	Describe the chief audit executive's responsibility for assessing residual risk	**Basic**	**9.7**
	G	Describe the process for communicating risk acceptance (when management has accepted a level of risk that may be unacceptable to the organization)	**Basic**	**4.3, 9.7**
	2. Monitoring Progress			
	A	Assess engagement outcomes, including the management action plan	**Proficient**	**9.7**
	B	Manage monitoring and follow-up of the disposition of audit engagement results communicated to management and the board	**Proficient**	**9.7**

APPENDIX C
THE IIA EXAMINATION BIBLIOGRAPHY

The Institute has prepared a listing of references for Part 2 of the revised version of the CIA exam. These publications have been chosen by the Professional Certifications Department as reasonably representative of the common body of knowledge for internal auditors. However, all of the information in these texts will not be tested. When possible, questions will be written based on the information contained in the suggested reference list. This bibliography is provided to give you an overview of the scope of the exam.

The IIA bibliography is for your information only. The texts you need to prepare for the CIA exam depend on many factors, including

1. Innate ability
2. Length of time out of school
3. Thoroughness of your undergraduate education
4. Familiarity with internal auditing due to relevant experience

CIA EXAM REFERENCES

Title/URL	Author
Internal Auditing: Assurance & Advisory Services *URL: https://bookstore.theiia.org/Internal-Auditing-Assurance-Advisory-Services-fourth-edition-2*	Urton L. Anderson, Michael J. Head, Sridhar Ramamoorti, Cris Riddle, Mark Salamasick, Paul J. Sobel
International Professional Practices Framework (IPPF), including ● Mission ● Definition of Internal Auditing ● Core Principles ● Code of Ethics ● *Standards* ● Implementation Guides ● Practice Guides ● Global Technology Audit Guides (GTAGs) *URL: http:bit.ly/1AilTOC*	The Institute of Internal Auditors, Inc.
Sawyer's Internal Auditing *URL: https://bookstore.theiia.org/sawyers-internal-auditing-enhancing-and-protecting-organizational-value-7th-edition*	L.B. Sawyer
Staffing Considerations for the Internal Audit Activity	The Institute of Internal Auditors, Inc.

AVAILABILITY OF PUBLICATIONS

The listing on the previous page presents only some of the current technical literature available, and The IIA does not carry all of the reference books. Quantity discounts are provided by The IIA. Visit bookstore.theiia.org or contact The IIA at bookstore@theiia.org or +1-407-937-1470.

Contact the publisher directly if you cannot obtain the desired texts from The IIA, online, or your local bookstore. Begin your study program with the Gleim CIA Review, which most candidates find sufficient. If you need additional reference material, borrow books mentioned in The IIA's bibliography from colleagues, professors, or a library.

APPENDIX D
ACCOUNTING CYCLES

On the following pages are five flowcharts and accompanying tables describing the steps in five basic accounting cycles and the controls in each step for an organization large enough to have an optimal segregation of duties.

NOTE: Except for manual checks and remittance advices, the flowcharts presented do not assume the use of either a paper-based or an electronic system. Each document symbol represents a business activity or control, whether manual or computerized.

NOTE: In the diagrams that follow, documents that originate outside the organization are separated by a thick border.

Sales-Receivables System Flowchart

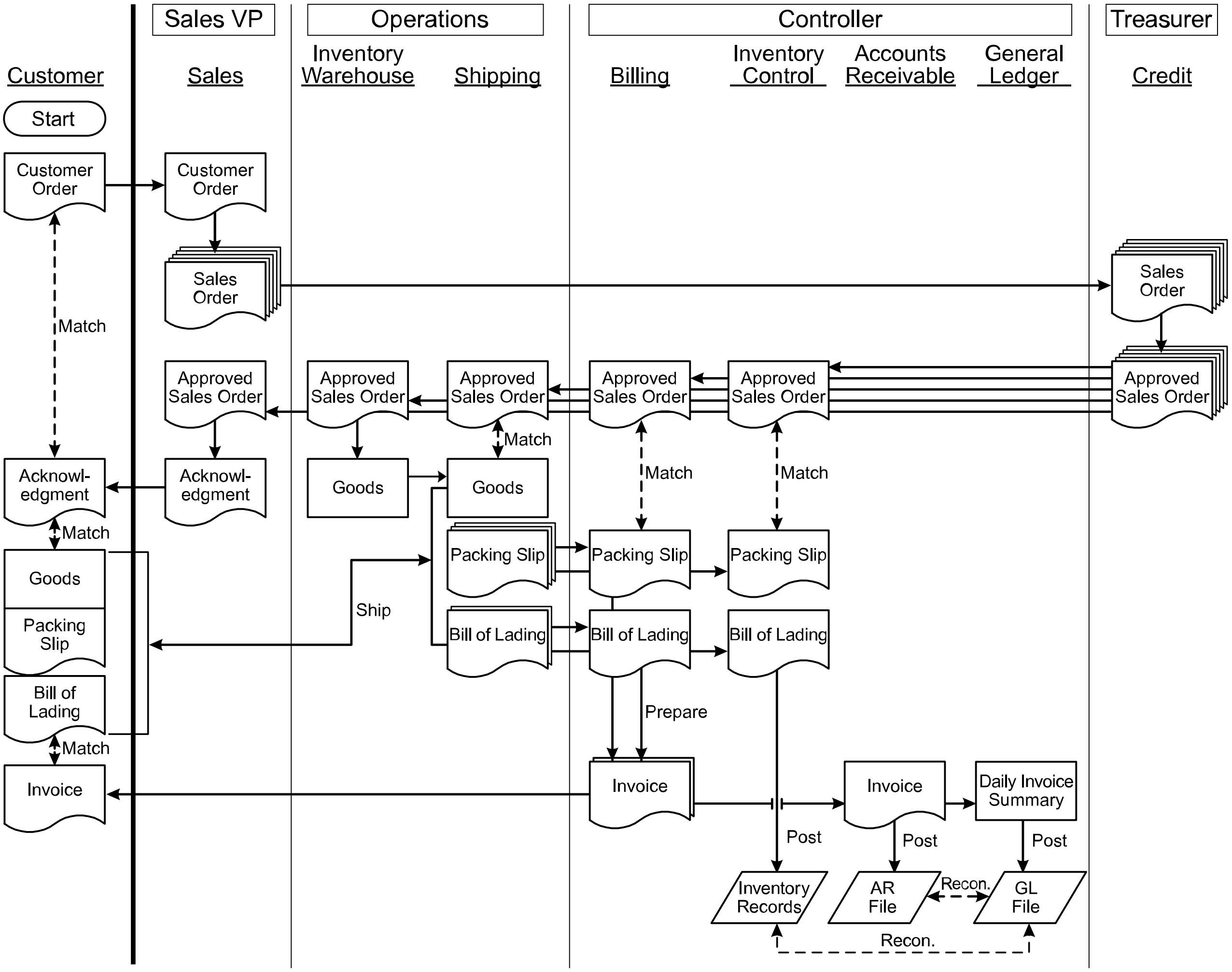


Figure D-1

Sales-Receivables System Flowchart Table

Function	Authorization			Custody		Recording			
Department	Customer	Sales	Credit	Shipping	Inventory Warehouse	Billing	Inventory Control	Accounts Receivable	General Ledger

Step	**Business Activity**	**Internal Control**
1	Sales receives a **customer order** and prepares a multi-part **sales order** then forwards it to Credit.	Reconciling sequentially numbered sales orders helps ensure that orders are legitimate.
2	Credit performs a credit check. If the customer is creditworthy, Credit approves the **sales order**.	Ensures that goods are shipped only to actual customers and that the account is unlikely to become delinquent.
3	Credit sends copies of the **approved sales order** to Sales, Inventory Warehouse, Shipping, Billing, and Inventory Control.	Notifies these departments that a legitimate sale has been made.
4	Upon receipt of the **approved sales order**, Sales sends an **acknowledgment** to the customer.	The customer's expectation of receiving goods reduces the chances of misrouting or misappropriation.
5	Upon receipt of the **approved sales order**, the Inventory Warehouse pulls the goods and forwards them to Shipping.	Ensures that goods are removed from the Inventory Warehouse only as part of a legitimate sale.
6	Shipping verifies that the goods received from Inventory Warehouse match the **approved sales order**, prepares a **packing slip** and a **bill of lading**, and ships the goods to the customer.	Ensures that the correct goods are shipped.
7	Shipping forwards a copy of the **packing slip** and **bill of lading** to Inventory Control and Billing.	Notifies these departments that the goods have been shipped.
8	Upon receipt of the **packing slip** and **bill of lading**, Inventory Control matches them with the **approved sales order** and updates the inventory records.	Ensures that inventory records are updated once the goods have been shipped.
9	Upon receipt of the **packing slip** and **bill of lading**, Billing matches them with the **approved sales order**, prepares a multi-part **invoice**, and sends a copy to the customer. Typically, a **remittance advice** is included for use in the cash receipts cycle.	Ensures that customers are billed for all goods, and only those goods, that were actually shipped. Reconciling sequentially numbered invoices helps prevent misappropriation of goods.
10	Accounts Receivable receives an **invoice** copy from Billing and posts a journal entry to the AR file.	Ensures that customer accounts are kept current.
11	Accounts Receivable prepares a **daily invoice summary** for the day and forwards it to General Ledger for posting to the GL file.	Separation of the Accounts Receivable, Billing, and General Ledger helps assure integrity of recording.
12	General Ledger receives a **daily invoice summary** from AR to post to the GL file.	Updating inventory, AR, and GL files separately provides an additional accounting control when they are periodically reconciled.

Cash Receipts System Flowchart

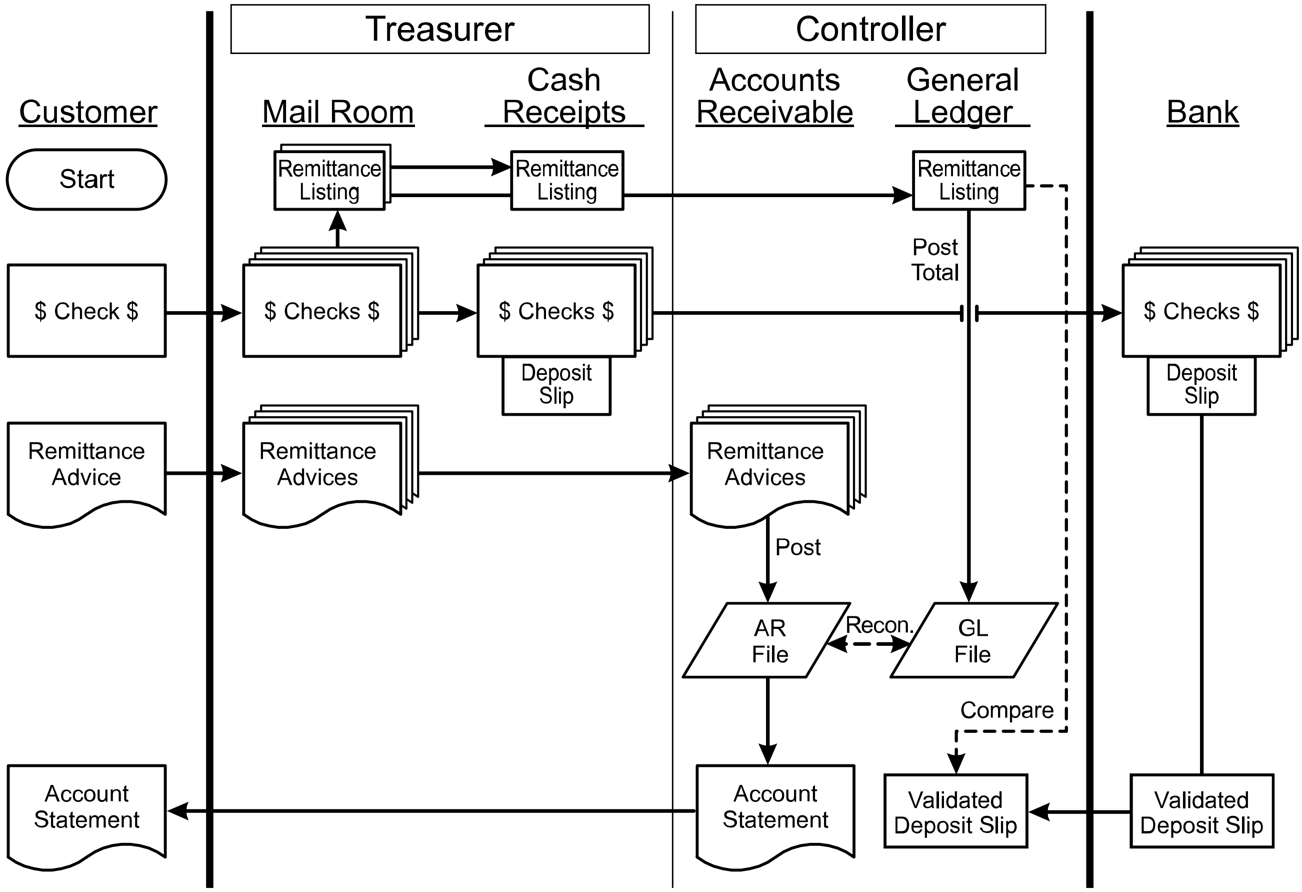


Figure D-2

Cash Receipts System Flowchart Table

Function	Authorization		Custody		Recording	
Department	Customer	Bank	Mail Room	Cash Receipts	Accounts Receivable	General Ledger

Step	**Business Activity**	**Internal Control**
1	Mail Room opens customer mail with two clerks always present. Customer **checks** are immediately endorsed “For Deposit Only into Account XXX.” **Remittance advices** are separated (one is prepared if not included in the payment).	Reduces risk of misappropriation by a single employee. Checks stamped “For Deposit Only into Account XXX” cannot be diverted.
2	Mail Room prepares a **remittance listing** of all **checks** received during the day and forwards it with the checks to Cash Receipts.	Remittance listing provides a control total for later reconciliation.
3	Cash Receipts prepares a **deposit slip** and deposits checks in Bank. Bank validates the **deposit slip**.	Bank provides independent evidence that the full amount was deposited.
4	Mail Room sends **remittance advices** to Accounts Receivable for updating of customer accounts in the AR file.	Ensures that customer accounts are kept current.
5	Mail Room also sends a copy of the **remittance listing** to General Ledger for posting of the total to the GL file.	Updating AR and GL files separately provides an additional accounting control when they are periodically reconciled.
6	**Validated deposit slip** is returned to General Ledger to compare with **remittance listing**.	Ensures that all cash listed on the remittance listing from the Mail Room was deposited.
7	Accounts Receivable periodically sends an **account statement** to customers showing all sales and payment activity.	Customers will complain about mistaken billings or missing payments.

Purchases-Payables System Flowchart

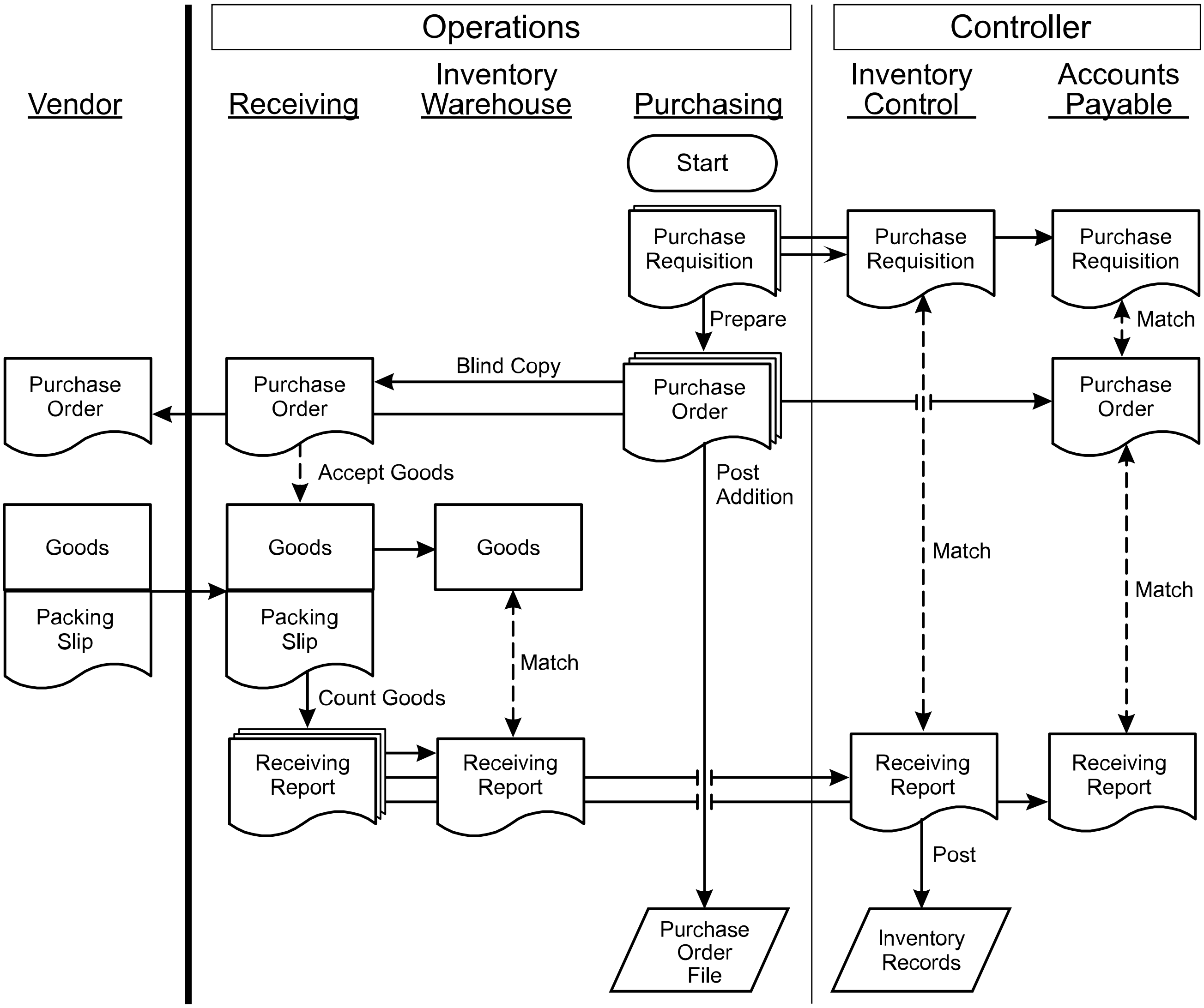


Figure D-3

Purchases-Payables System Flowchart Table

Function	Authorization		Custody			Recording	
Department	Inventory Control	Purchasing	Vendor	Receiving	Inventory Warehouse	Accounts Payable	General Ledger

Step	Business Activity	Internal Control
1	Inventory Control prepares a **purchase requisition** when inventory reaches the reorder point due to sales and sends it to Purchasing and Accounts Payable.	Predetermined inventory levels trigger authorization to initiate a purchase transaction.
2	Purchasing locates the authorized vendor in the vendor file, prepares a **purchase order**, and updates the purchase order file.	• Purchasing ensures that goods are bought only from vendors who have been preapproved for reliability. • Reconciling sequentially numbered purchase orders helps ensure that orders are legitimate.
3	Purchasing sends the **purchase order** to Vendor, Receiving, and Accounts Payable. Receiving's copy has blank quantities.	• Receiving is put on notice to expect shipment. • Accounts Payable is put on notice that liability to this vendor will increase when goods arrive.
4	When goods arrive, Receiving accepts goods based on the file copy of the **purchase order**, prepares a **receiving report**, and forwards the **receiving report** with the goods to the Inventory Warehouse.	Because quantities are blank on Receiving's copy of the purchase order, employees must count items to prepare the receiving report.
5	The Inventory Warehouse verifies that goods received match those listed on the **receiving report**.	Detects any loss or damage between Receiving and the Inventory Warehouse. Inventory Warehouse accepts responsibility for safeguarding receipted goods.
6	Receiving sends the **receiving report** to Inventory Control for matching with the **purchase requisition** and updating of inventory records.	Ensures that inventory records are current.
7	Receiving also sends a copy of the **receiving report** to Accounts Payable for matching with the **purchase order** and **purchase requisition**.	Accounts Payable ensures that all documents reconcile and will await the arrival of the vendor invoice to record the payable transaction (as shown in the Cash Disbursements System Flowchart on the next page).

Cash Disbursements System Flowchart

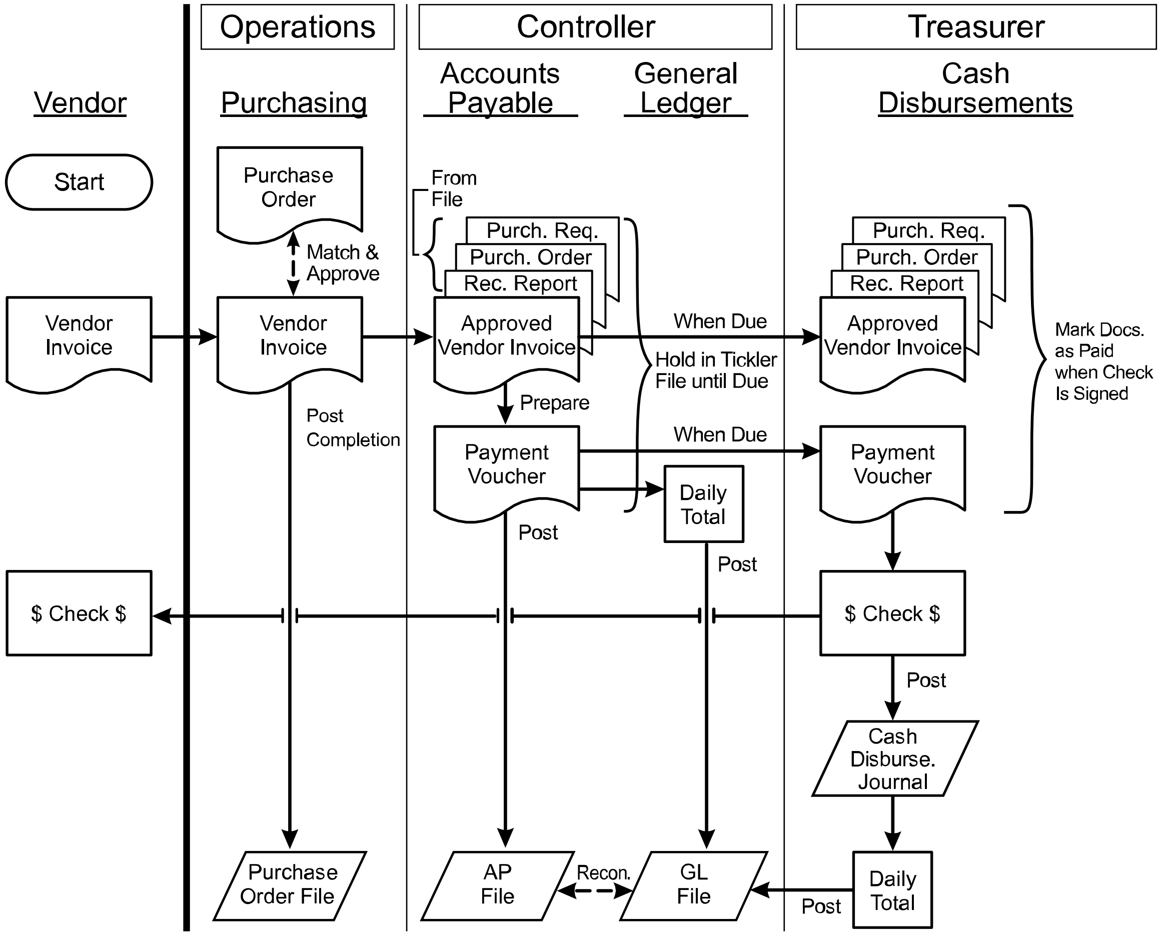


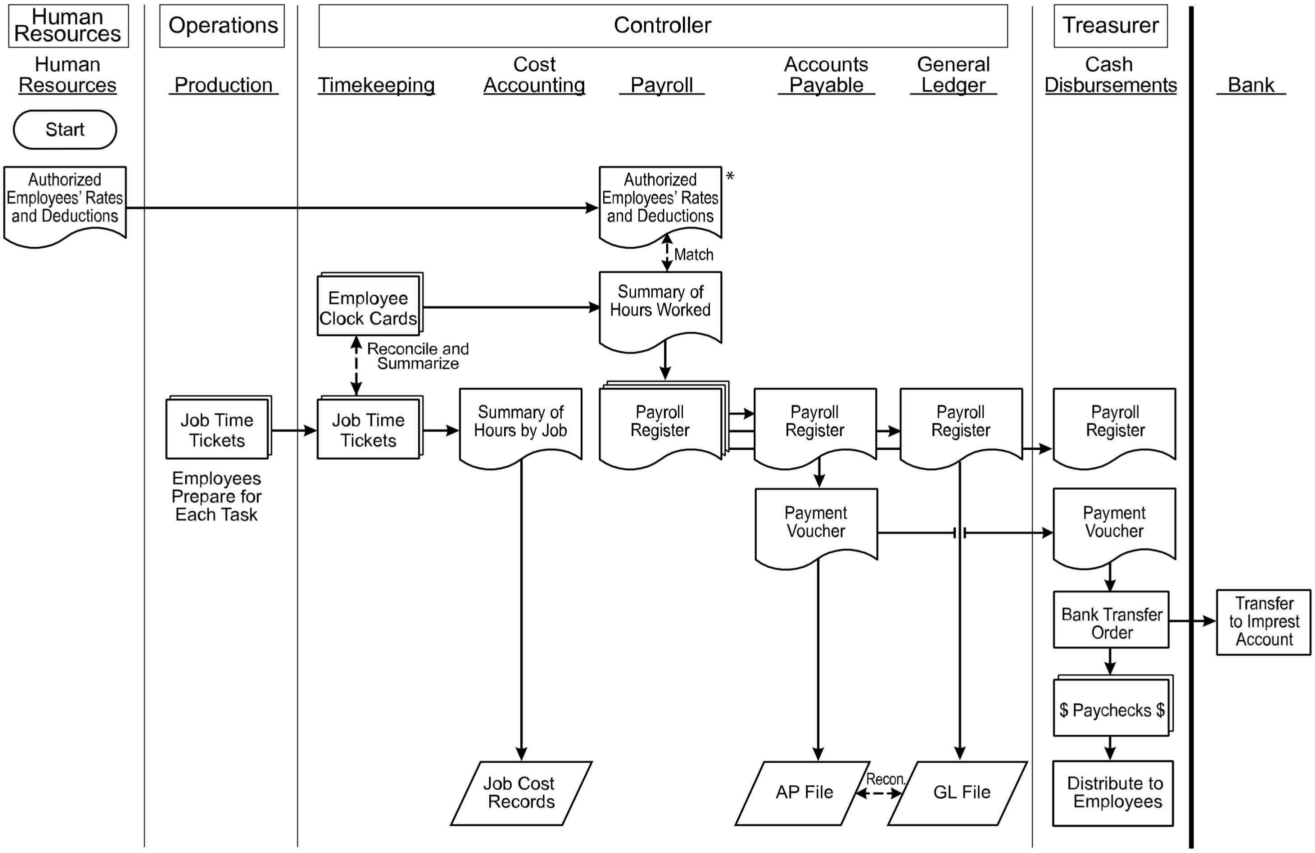
Figure D-4

Cash Disbursements System Flowchart Table

Function	Authorization		Custody	Recording	
Department	Vendor	Purchasing	Cash Disbursements	Accounts Payable	General Ledger

Step	Business Activity	Internal Control
1	Purchasing receives a **vendor invoice**. The **vendor invoice** is matched with the **purchase order** and approved for payment. The **purchase order** is marked as closed in the purchase order file if completed, and the **approved vendor invoice** is forwarded to Accounts Payable.	• Purchasing ensures the vendor invoiced for the proper amount and the terms are as agreed. • Purchasing can follow up on partially filled orders.
2	Accounts Payable matches the **approved vendor invoice** with the file copies of the **purchase requisition, purchase order**, and **receiving report** and prepares a **payment voucher**. The **payment voucher** is recorded in the accounts payable file.	• Matching all documents provides assurance that only goods that were appropriately ordered, received, and invoiced are recorded as a liability. • Periodic reconciliation with the payment vouchers in the tickler file (maintained by due date) with the accounts payable file (maintained by vendor) ensures proper recording.
3	The **payment voucher**, with the attached documents, is filed in a tickler file by due date. The **daily total** of all payment vouchers is sent to the General Ledger to record the purchase (inventory) and liability (accounts payable).	Filing by due date ensures that payment will be made on a timely basis (e.g., to obtain discounts or avoid default).
4	On the due date, the **payment voucher** and attached documents are removed from the tickler file sent to Cash Disbursements for **check** preparation, signing, and mailing. The **check** is recorded in the cash disbursements journal.	• Cash Disbursements cannot issue a check without an approved payment voucher. • Large payments may require two signatures on the check to provide additional oversight.
5	The **payment voucher** and attached documents are stamped "Paid," and the **check** is mailed to the vendor.	Stamping the documents "Paid" prevents them from supporting a second, illicit payment voucher.
6	The **daily total** of all checks written and mailed for the day is sent to General Ledger to record the reduction in accounts payable and cash.	Periodic reconciliation of the accounts payable and general ledger ensures proper recording.

Payroll System Flowchart



*Payroll receives only a list of authorized employees' rates and deductions and does not have authority to change those rates.

Figure D-5

Payroll System Flowchart Table

Function	Authorization		Custody		Recording				
Department	Human Resources	Production	Cash Disbursements	Bank	Timekeeping	Cost Accounting	Payroll	Accounts Payable	General Ledger

Step	Business Activity	Internal Control
1	Human Resources sends an **authorized employees’ rates and deductions** list to Payroll.	Ensures that only actual employees are included on the payroll and that rates of pay and withholding amounts are accurate.
2	Employees record the start and end times of their workdays on **employee clock cards** held in Timekeeping.	The recording process mechanically or electronically captures employee work hours.
3	Production employees record time worked on various tasks on **job time tickets**.	Allows accumulation of labor costs by job as well as tracking of direct and indirect labor.
4	At the end of each day, a production supervisor approves the **job time tickets** and forwards them to Timekeeping, where they are reconciled with the **employee clock cards**.	Ensures that employees worked only authorized hours. Reconciles the time allocated to direct and indirect labor with total time worked.
5	Timekeeping prepares a **summary of hours worked** by employee and forwards it to Payroll. Payroll matches it with the **authorized employees’ rates and deductions** list and prepares a **payroll register**.	Ensures that employees are paid the proper amount.
6	Timekeeping prepares a **summary of hours worked by job** and forwards it to Cost Accounting for updating of the job cost records.	Ensures that direct labor costs are appropriately assigned to jobs.
7	Accounts Payable receives the **payroll register** from Payroll, prepares a **payment voucher**, and forwards it along with the **payroll register** to Cash Disbursements.	Ensures that a payable is accrued. Authorizes the transfer of cash to the payroll imprest account.
8	Payroll also forwards the **payroll register** to General Ledger for posting of the total to the GL file.	Updating AP and GL files separately provides an additional accounting control when they are periodically reconciled.
9	Cash Disbursements compares the **payment voucher** with the **payroll register** total and initiates the bank transfer to the payroll imprest fund.	Ensures that the correct amount is transferred to the payroll imprest account (and governmental authorities).
10	**Paychecks** are distributed to employees by the Treasurer function.	Treasurer has custody responsibility but no recording or authorization responsibility. This ensures that Payroll or supervisory personnel cannot perpetrate fraud by creating fictitious employees.

APPENDIX E
GLOSSARY OF ACCOUNTING TERMS
U.S. TO BRITISH VS. BRITISH TO U.S.

U.S. TO BRITISH

Accounts payable	Trade creditors
Accounts receivable	Trade debtors
Accrual	Provision (for liability or charge)
Accumulated depreciation	Aggregate depreciation
Additional paid-in capital	Share premium account
Allowance	Provision (for diminution in value)
Allowance for credit losses	Provision for bad debt
Annual Stockholders' Meeting	Annual General Meeting
Authorized capital stock	Authorized share capital
Bellweather stock	Barometer stock
Bond	Loan finance
Business combination	Merger accounting
Bylaws	Articles of Association
Certificate of Incorporation	Memorandum of Association
Checking account	Current account
Common stock	Ordinary shares
Consumer price index	Retail price index
Corporation	Company
Cost of goods sold	Cost of sales
Credit Memorandum	Credit note
Equity	Reserves
Equity interest	Ownership interest
Financial statements	Accounts
Income statement	Profit and loss account
Income taxes	Taxation
Inventories	Stocks
Investment bank	Merchant bank
Labor union	Trade union
Land	Freehold
Lease not for a short term	Long leasehold
Liabilities	Creditors
Listed company	Quoted company
Long-term investments	Fixed asset investments
Merchandise trade	Visible trade
Mutual funds	Unit trusts
Net income	Net profit
Note payable	Bill payable
Note receivable	Bill receivable
Paid-in surplus	Share premium
Par value	Nominal value
Preferred stock	Preference share
Prime rate	Base rate
Property, plant, and equipment	Tangible fixed assets
Provision for credit losses	Charge
Purchase method	Acquisition accounting
Purchase on account	Purchase on credit
Retained earnings	Profit and loss account
Real estate	Property
Revenue	Income
Reversal of accrual	Release of provision
Sales on account	Sales on credit
Sales/revenue	Turnover
Savings and loan association	Building society
Shareholders' equity	Shareholders' funds
Stock	Inventory
Stock dividend	Bonus share
Stockholder	Shareholder
Stockholders' equity	Share capital and reserves or Shareholders' funds
Taxable income	Taxable profit
Treasury bonds	Gilt-edged stock (gilts)

BRITISH TO U.S.

Accounts	Financial statements
Acquisition accounting	Purchase method
Aggregate depreciation	Accumulated depreciation
Annual General Meeting	Annual Stockholders’ Meeting
Articles of Association	Bylaws
Authorized share capital	Authorized capital stock
Barometer stock	Bellweather stock
Base rate	Prime rate
Bill payable	Note payable
Bill receivable	Note receivable
Bonus share	Stock dividend
Building society	Savings and loan association
Charge	Provision for credit losses
Company	Corporation
Cost of sales	Cost of goods sold
Credit note	Credit Memorandum
Creditors	Liabilities
Current account	Checking account
Fixed asset investments	Long-term investments
Freehold	Land
Gilt-edged stock (gilts)	Treasury bonds
Income	Revenue
Inventory	Stock
Loan finance	Bond
Long leasehold	Lease not for a short term
Memorandum of Association	Certificate of Incorporation
Merchant bank	Investment bank
Merger accounting	Business combination
Net profit	Net income
Nominal value	Par value
Ordinary shares	Common stock
Ownership interest	Equity interest
Preference share	Preferred stock
Profit and loss account	Income statement
Profit and loss account	Retained earnings
Property	Real estate
Provision for bad debt	Allowance for credit losses
Provision (for diminution in value)	Allowance
Provision (for liability or charge)	Accrual
Purchase on credit	Purchase on account
Quoted company	Listed company
Release of provision	Reversal of accrual
Reserves	Equity
Retail price index	Consumer price index
Sales on credit	Sales on account
Share capital and reserves or Shareholders’ funds	Stockholders’ equity
Shareholder	Stockholder
Shareholders’ funds	Shareholders’ equity
Share premium	Paid-in surplus
Share premium account	Additional paid-in capital
Stocks	Inventories
Tangible fixed assets	Property, plant, and equipment
Taxable profit	Taxable income
Taxation	Income taxes
Trade creditors	Accounts payable
Trade debtors	Accounts receivable
Trade union	Labor union
Turnover	Sales/revenue
Unit trusts	Mutual funds
Visible trade	Merchandise trade

STUDY UNIT ONE

INTERNAL AUDIT OPERATIONS

This study unit is the first of four covering **Domain I: Managing the Internal Audit Activity** from The IIA's CIA Exam Syllabus. This domain makes up 20% of Part 2 of the CIA exam and is tested at the **basic** and **proficient** cognitive levels. Refer to the complete syllabus located in Appendix B to view the relevant sections covered in Study Unit 1.

1.1 INTRODUCTION TO INTERNAL AUDITING

Performance Standard 2100
Nature of Work

The internal audit activity must evaluate and contribute to the improvement of the organization's governance, risk management, and control processes using a systematic, disciplined, and risk-based approach. Internal audit credibility and value are enhanced when auditors are proactive and their evaluations offer new insights and consider future impact.

1. **Nature of Work**

   a. According to The IIA's Definition of Internal Auditing, the internal audit activity "helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes."

      1) These processes are closely related. The IIA Glossary (in Appendix A) defines them as follows:

         a) **Governance** – "The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives."

         b) **Risk management** – "A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives."

         c) **Control** – "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."

            i) **Control processes** – "The policies, procedures (both manual and automated), and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organization is willing to accept."

   b. According to IG 2100, *Nature of Work*, an understanding of the processes above is necessary. The chief audit executive (CAE) then interviews the board and senior management about the responsibilities of each stakeholder for these processes.

      1) Ordinarily, the board is responsible for guiding governance processes, and senior management is responsible for leading risk management and control processes.

   c. An understanding of the business also is necessary, and established frameworks may be used in the auditors' evaluations.

      1) To acquire this understanding, the CAE will ordinarily review the organization's mission, strategic plan, key objectives, related risks and controls, and the minutes of the board.

   d. After discussions with the board and senior management, the CAE may document in the internal audit charter the roles and responsibilities of the board, senior management, and the internal audit activity.

   e. When determining the strategy for assessing governance, risk management, and control, the CAE typically considers (1) the maturity of these processes, (2) the seniority of the persons responsible, and (3) the organizational culture.

   f. Internal auditors may use their knowledge, experience, and best practices to provide (1) observations of weaknesses and (2) recommendations.

      1) **Compliance** is defined in The IIA Glossary as "adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements."

         a) The internal audit activity must evaluate the risks involved in governance, operations, and information systems that relate to compliance with laws, regulations, policies, procedures, and contracts. The internal audit activity also must evaluate the controls regarding compliance.

2. **Reasonable Assurance**

   a. Governance, risk management, and control processes are **adequate** if management has planned and designed them to provide reasonable assurance of achieving the organization’s objectives efficiently and economically.

      1) **Efficient** performance accomplishes objectives in an accurate, timely, and economical fashion. **Economical** performance accomplishes objectives with minimal use of resources (i.e., cost) proportionate to the risk exposure.

      2) **Reasonable assurance** is provided if the most cost-effective measures are taken in the design and implementation of controls to reduce risks and restrict expected deviations to a tolerable level.

3. **Basic Types of Internal Audit Engagements**

   a. The essential strategic function of the internal audit activity is to provide assurance services and consulting services. Thus, the Definition of Internal Auditing describes internal auditing as “an independent, objective assurance and consulting activity.”

   b. Separate **Implementation Standards** have been issued for assurance services and consulting services. These services are defined in The IIA Glossary as follows:

      1) **Assurance services** – “An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.”

      2) **Consulting services** – “Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization’s governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.”

4. **Reporting**

   a. Reporting to senior management and the board provides assurance about

      1) Governance,
      2) Risk management, and
      3) Control.

   b. Periodic reports also are made on the internal audit’s purpose, authority, responsibility, and performance.

   c. Reporting to senior management and the board is covered in more detail in Study Unit 4, Subunit 3.

1.2 INTERNAL AUDIT ADMINISTRATIVE ACTIVITIES

1. Overview

a. The chief audit executive (CAE) is responsible for management of internal audit activity resources in a manner that ensures fulfillment of its responsibilities. Like any well-managed department, the internal audit activity should operate effectively and efficiently. This can be accomplished through proper planning, which includes budgeting and human resources management.

Performance Standard 2000
Managing the Internal Audit Activity

The chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization.

Interpretation of Standard 2000

The internal audit activity is effectively managed when:

- It achieves the purpose and responsibility included in the internal audit charter.
- It conforms with the *Standards*.
- Its individual members conform with the Code of Ethics and the *Standards*.
- It considers trends and emerging issues that could impact the organization.

The internal audit activity adds value to the organization and its stakeholders when it considers strategies, objectives, and risks; strives to offer ways to enhance governance, risk management, and control processes; and objectively provides relevant assurance.

b. Management oversees the day-to-day operations of the internal audit activity, including the following administrative activities:

1) Budgeting and management accounting
2) Human resource administration, including personnel evaluations and compensation
3) Internal communications and information flows
4) Administration of the internal audit activity's policies and procedures

Performance Standard 2040
Policies and Procedures

The chief audit executive must establish policies and procedures to guide the internal audit activity.

2. Form, Content, and Review

Interpretation of Standard 2040

The form and content of policies and procedures are dependent upon the size and structure of the internal audit activity and the complexity of its work.

a. Further guidance is provided in IG 2040, *Policies and Procedures.*

1) A large, **mature** internal audit activity may include policies and procedures in a formal operations **manual**. If the activity is smaller or less mature, policies and procedures may reside in separate documents or an audit management software program.

2) The following **content** generally is included in an operations manual or other separate documents:

a) Policies on

i) Purposes and responsibilities of the internal audit activity

ii) Compliance with mandatory guidance

iii) Independence of the internal audit activity and objectivity of internal auditors

iv) Ethics requirements

v) Maintaining the confidentiality of information

vi) Retention of internal audit records

b) Procedures for

i) Drafting the audit plan based on the risk assessment
ii) Drafting plans and work programs for specific engagements
iii) Performance and documentation of engagements
iv) Communicating results of engagements
v) Monitoring and follow-up

c) Guidance on the quality assurance and improvement programs

d) Management of the internal audit activity related to

i) Professional training and certification
ii) Continuing professional education
iii) Evaluations of auditors

3) "Internal audit policies and procedures should be **reviewed** periodically, either by the CAE or an internal audit manager assigned to monitor internal audit processes and emerging issues."

3. **Budgeting**

   a. The CAE is responsible for creating the operating and financial budget. Generally, the CAE, audit managers, and the internal audit activity work together to develop the budget annually. The budget is then submitted to management and the board for their review and approval.

4. **Human Resources**

   a. The skill set and knowledge of the internal audit activity are essential to its ability to help the organization achieve its objectives. According to *Internal Auditing: Assurance & Consulting Services* (Redding, et al), “The CAE is responsible for hiring associates to fill the organizational structure of the internal audit function in a way that maximizes efficiency, effectively provides the necessary skill base, and makes good use of the financial budget.”

   b. Internal auditors should be qualified and competent. Because the selection of a superior staff is dependent on the ability to evaluate applicants, selection criteria must be well-developed.

      1) Appropriate questions and forms should be prepared in advance to evaluate, among other things, the applicant’s (a) technical qualifications, (b) educational background, (c) personal appearance, (d) ability to communicate, (e) maturity, (f) persuasiveness, (g) self-confidence, (h) intelligence, (i) motivation, and (j) potential to contribute to the organization.

   c. Internal auditors need a diverse set of skills to perform their jobs effectively. These skills are not always apparent in a standard resumé. Developing effective interviewing techniques will ensure that the internal audit function acquires the proper set of skills, capabilities, and technical knowledge needed to accomplish its goals.

   d. Effective interviewing methods are structured interviews and behavioral interviews.

      1) **Structured interviews** are designed to eliminate individual bias. These interviews use a set of job-related questions with standardized answers, which then are scored by a committee of three to six members. According to *Management* (Kreitner & Cassidy, 12th edition), interviewers can use four general types of questions:

         a) Situational – “What would you do if you saw two people arguing loudly in the work area?”

         b) Job knowledge – “Do you know how to do an Internet search?”

         c) Job sample simulation – “Can you show us how to compose and send an e-mail message?”

         d) Worker requirements – “Are you able to spend 25 percent of your time on the road?”

      2) **Behavioral interviews** determine how candidates handled past situations. Past performance is generally indicative of future performance.

1.3 STAKEHOLDER RELATIONSHIPS

1. **Stakeholder Relationships**

   a. For internal auditors to be effective, *Sawyer's Guide for Internal Auditors*, 6th edition, states that they must build and maintain strong constructive relationships with managers and other stakeholders within the organization.

   b. These relationships require conscious ongoing focus to ensure that risks are appropriately identified and evaluated to best meet the needs of the organization.

   c. Internal auditors have a responsibility to work together with external auditors and other stakeholders to facilitate work efforts and compliance with regulators.

   d. Key stakeholders include the board of directors, audit committees, management, external auditors, and regulators.

2. **The Board and the Audit Committee**

   a. For the internal audit activity to achieve organizational independence, the chief audit executive (CAE) must have direct and unrestricted access to senior management and the board. Accordingly, the CAE should report administratively to senior management and functionally to the board.

      1) The IIA defines a **board**, in part, as "[t]he highest level governing body . . . charged with the responsibility to direct and/or oversee the organization's activities and hold senior management accountable."

   b. The **audit committee** is a subunit of the board of directors. However, not every member of the board is necessarily qualified to serve on the audit committee.

      1) Some statutes have imposed the following significant restrictions on the membership of the audit committee:

         a) No member may be an employee of the organization except in his or her capacity as a board member.

         b) At least one member must be a financial expert.

      2) Many stock exchanges require that all listed organizations have an audit committee.

   c. To avoid creating conflict between the CEO and the audit committee, the CAE should request board establishment of policies covering the internal audit activity's relationships with the audit committee.

3. **Role of the Audit Committee**
   a. The most important function of the audit committee is to promote the independence of the internal and external auditors by protecting them from management's influence.
   b. The following are other functions of the audit committee regarding the internal audit activity:
      1) Selecting or removing the CAE and setting his or her compensation
      2) Approving the internal audit charter
      3) Reviewing and approving the internal audit activity's work plan
      4) Ensuring that the internal audit activity is allocated sufficient resources
      5) Resolving disputes between the internal audit activity and management
      6) Communicating with the CAE, who attends all audit committee meetings
      7) Reviewing the internal audit activity's work product (e.g., interim and final engagement communications)
      8) Ensuring that engagement results are given due consideration
      9) Overseeing appropriate corrective action for deficiencies noted by the internal audit activity
      10) Making appropriate inquiries of management and the CAE to determine whether audit scope or budgetary limitations impede the ability of the internal audit activity to meet its responsibilities
   c. The following are other functions of the audit committee regarding the external auditor:
      1) Selecting the external auditing firm and negotiating its fee
      2) Overseeing and reviewing the work of the external auditor
      3) Resolving disputes between the external auditor and management
      4) Reviewing the external auditor's internal control and audit reports

4. **Relationships with Management**
   a. According to *Sawyer's Guide for Internal Auditors*, 6th edition, internal auditors are responsible for performing their mission, maintaining their objectivity, and ensuring the internal audit activity's independence. They also should develop and maintain good working relationships with management.
   b. Good relationships are developed by communicating effectively, resolving conflicts constructively, and using participative auditing methods.
      1) **Participative auditing** is a collaboration between the internal auditor and management during the auditing process. The objective is to minimize conflict and build a shared interest in the engagement. People are more likely to accept changes if they have participated in the decisions and in the methods used to implement changes.
      2) However, internal auditors are ultimately responsible for guiding and directing the audit because the responsibility for the final audit opinion is theirs.

1.4 INTERNAL AUDIT RESOURCE REQUIREMENTS

Performance Standard 2030
Resource Management

The chief audit executive must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

Interpretation of Standard 2030

Appropriate refers to the mix of knowledge, skills, and other competencies needed to perform the plan. Sufficient refers to the quantity of resources needed to accomplish the plan. Resources are effectively deployed when they are used in a way that optimizes the achievement of the approved plan.

1. **Managing Internal Audit Resources**
   a. The CAE is primarily responsible for the sufficiency and management of resources, including communication of needs and status to senior management and the board. These parties ultimately must ensure the adequacy of resources.
      1) **Resources** may include employees, service providers, financial support, and IT-based audit methods. To determine the sufficiency of resource allocation, the CAE considers relevant factors, including
         a) Communications received from management and the board;
         b) Information about ongoing and new engagements;
         c) Consequences of not completing an engagement on time; and
         d) Knowledge, skills, and competencies of the internal audit staff.
   b. The **competencies** of the internal audit staff should be appropriate for the planned activities. The CAE may conduct a documented **skills assessment** based on the needs identified in the risk assessment and audit plan.
      1) A job description summarizes the duties and qualifications required for a job. Properly formulated job descriptions provide a basis for identifying job qualifications, such as training and experience. They also facilitate recruiting the appropriate internal audit staff with the necessary attributes for the planned activities.
   c. Resources need to be sufficient for audit activities to be performed in accordance with the expectations of senior management and the board. **Resource planning** considers
      1) The audit universe,
      2) Relevant risk levels,
      3) The internal audit plan,
      4) Coverage expectations, and
      5) An estimate of unanticipated activities.
   d. Resources must be effectively **deployed** by assigning qualified auditors and developing an appropriate resourcing approach and organizational structure.

e. Some organizations maintain field offices to improve the internal audit function's efficiency and effectiveness.

1) The advantages of field offices compared with sending internal auditors from the home office include

a) Reduced travel time and expense,
b) Improved service in the operating locations served by the field offices,
c) Better morale of internal auditors as a result of increased authority, and
d) The possibility of employing persons who do not wish to travel.

f. The CAE considers succession planning, staff evaluation and development, and other human resource disciplines.

1) The CAE also addresses **resourcing needs**, including whether those skills are present.

2) Other ways to meet needs include external service providers, specialized consultants, or other employees of the organization.

g. The CAE's ongoing communications with senior management and the board include periodic summaries of resource status and adequacy, e.g., the effect of temporary vacancies and comparison of resources with the audit plan.

h. When selecting the appropriate audit staff, the CAE must consider the following factors:

1) Complexity of the engagement
2) Experience levels of the auditors
3) Training needs of the auditors
4) Available resources

2. **Outsourcing the Internal Audit Activity**

a. An organization's governing body may decide that an external service provider is the most effective means of obtaining internal audit services.

1) In such cases, the following Performance Standard requires those performing internal audit services to remind the organization of the ultimate responsibility for maintaining an effective internal audit activity.

Performance Standard 2070
External Service Provider and Organizational Responsibility for Internal Auditing

When an external service provider serves as the internal audit activity, the provider must make the organization aware that the organization has the responsibility for maintaining an effective internal audit activity.

2) Accordingly, oversight of and responsibility for the internal audit activity must not be outsourced.

Interpretation of Standard 2070

This responsibility is demonstrated through the quality assurance and improvement program which assesses conformance with the Code of Ethics and the *Standards*.

1.5 COORDINATION

1. **The IIA's Three Lines Model** is based on six principles.
   a. **Principle 1: Governance.** Appropriate structures and processes should enable
      1) Accountability by a governing body (generally the board) to stakeholders for organizational oversight. Stakeholders are those whose interests are served or affected.
      2) Managerial actions (including risk management) to achieve objectives through risk-based decisions.
      3) Assurance and advice by a competent, objective, and independent internal audit function that provides confidence and clarity and facilitates continuous improvement.

   b. **Principle 2: Governing body roles.** They include
      1) Ensuring structures and processes exist for effective governance.
      2) Ensuring objectives and activities align with stakeholder interests.
      3) Giving management the responsibility and resources to achieve objectives and compliance with laws, regulations, and ethics.
      4) Establishing and overseeing the internal audit function.

   c. **Principle 3: Management – First and second line roles.**
      1) **First line roles** most directly relate to delivery of products or services to clients. They include support functions (e.g., human resources). They are directly responsible for risk management.
      2) **Second line roles** (some of which may be assigned to specialists) assist with risk management (a first line role) by providing expertise, support, monitoring, and challenge. Specific objectives may relate to compliance, sustainability, ethics, internal control, IT, quality, or ERM.

   d. **Principle 4: Third line roles.**
      1) Internal audit (a) provides assurance and advice on the adequacy and effectiveness of governance, risk management, and compliance, and (b) reports to management and the governing body on objective achievement and continuous improvement. It may consider assurance from other internal or external providers when performing these responsibilities.

   e. **Principle 5: Third line independence.**
      1) Internal audit independence is achieved through (a) accountability to the governing body; (b) unaffected access to people, resources, and data; and (c) freedom from bias and interference.

   f. **Principle 6: Creating and protecting value.**
      1) Alignment of the activities of roles (communication, cooperation, and collaboration) collectively create and protect value. It ensures the reliability, coherence, and transparency of risk-based decisions.

2. Coordinating the Work of the Internal Audit Activity with Other Providers

Performance Standard 2050
Coordination and Reliance

The chief audit executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts.

Interpretation of Standard 2050

In coordinating activities, the chief audit executive may rely on the work of other assurance and consulting service providers. A consistent process for the basis of reliance should be established, and the chief audit executive should consider the competency, objectivity, and due professional care of the assurance and consulting service providers. The chief audit executive should also have a clear understanding of the scope, objectives, and results of the work performed by other providers of assurance and consulting services. Where reliance is placed on the work of others, the chief audit executive is still accountable and responsible for ensuring adequate support for conclusions and opinions reached by the internal audit activity.

a. Further guidance is provided in IG 2050, *Coordination and Reliance*:

1) The CAE should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting providers to ensure proper coverage and minimize duplication of efforts (Perf. Std. 2050).

a) Whether reporting administratively to the quality audit function or to senior management, the CAE should identify appropriate liaison activities with the quality audit function to ensure coordination of audit schedules and overall audit responsibilities.

i) The quality audit standards proposed by the quality audit manager should comply with the applicable standards for internal auditing (i.e., the *Standards*).

ii) The internal audit activity as a whole, not each auditor individually, must be proficient in all necessary competencies (Attr. Std. 1210).

2) Internal vs. External

a) **Internal** providers may report to senior management or be part of senior management. Their activities may address such functions as “environmental, financial control, health and safety, IT security, legal, risk management, compliance, or quality assurance. These are often considered ‘second line of defense’ activities, according to The IIA’s Three Lines of Defense model.”

b) **External** providers may report to senior management, external parties, or the CAE.

3) Subject to the organization's confidentiality constraints, "the parties share the objectives, scope, and timing of upcoming reviews, assessments, and audits; the results of prior audits; and the possibility of relying on one another's work."

4) Process and Methods of Coordinating Assurance Activities

    a) The **process** varies by organization. Smaller entities may have informal coordination. Large or regulated entities may have formal and complex coordination.

    b) **Methods** of Coordinating Assurance Coverage

        i) **Assurance mapping** (a) connects significant risk categories and sources of assurance and (b) assesses each category. The CAE then can determine whether assurance services sharing the results with other providers facilitates agreement on coordinating services to avoid duplication and maximize efficiency and effectiveness of coverage.

        ii) In the **combined assurance model**, the internal audit activity coordinates activities with second line of defense activities, e.g., compliance, to minimize "the nature, frequency and redundancy of internal audit engagements."

5) **Coordinating activities** include the following:

    a) Simultaneity of the nature, extent, and timing of scheduled work

    b) Mutual understanding of methods and vocabulary

    c) The parties' access to each other's programs, workpapers, and communications of results

    d) Reliance on others' work to avoid overlap

    e) Meeting to adjust the timing of scheduled work given results to date

6) Reliance on another service provider does not excuse the CAE from final responsibility for conclusions and opinions.

7) **Criteria** the CAE may consider in determining whether to rely on the work of another service provider include the following:

    a) The objectivity, independence, competency, and due professional care of the provider relating to the relevant assurance or consulting service

    b) The scope, objectives, and results of the service provider's work to evaluate the degree of reliance

    c) Assessing the service provider's findings to determine whether they are reasonable and meet the information criteria in the *Standards*

    d) The incremental effort required to obtain sufficient, reliable, relevant, and useful information as a basis for the degree of planned reliance

3. **Coordinating with Regulatory Oversight Bodies**

   a. Businesses and not-for-profit organizations are subject to governmental regulation in many countries. Below is a sample of typical subjects of regulation:

      1) Labor relations
      2) Occupational safety and health
      3) Environmental protection
      4) Consumer product safety
      5) Business mergers and acquisitions
      6) Securities issuance and trading
      7) Trading of commodities

      NOTE: Local and regional governments may have their own regulatory bodies.

   b. Particularly in larger organizations, entire departments or functions are established to monitor compliance with the regulations issued by these governmental bodies.

      1) For example, broker-dealers in securities establish compliance departments to ensure that trades are executed according to the requirements of securities laws. Moreover, manufacturers have departments to monitor wage-and-hour compliance, workplace safety issues, and discharge of toxic wastes.

   c. Among the responsibilities of the internal audit activity is the evaluation of the organization’s compliance with applicable laws and regulations.

      1) The internal audit activity coordinates its work with that of inspectors and other personnel from the appropriate governmental bodies and with personnel from internal assurance functions.

STUDY UNIT TWO

ASSURANCE AND COMPLIANCE ENGAGEMENTS

This study unit is the second of four covering **Domain I: Managing the Internal Audit Activity** from The IIA's CIA Exam Syllabus. This domain makes up 20% of Part 2 of the CIA exam and is tested at the **basic** and **proficient** cognitive levels. Refer to the complete syllabus located in Appendix B to view the relevant sections covered in Study Unit 2.

2.1 ASSURANCE ENGAGEMENTS

SUCCESS TIP

The professional standards for internal auditors and external auditors differ significantly in the scope of their treatment of consulting services. For example, the AICPA's standards for financial statement auditing in the United States are extremely detailed, but its standards for consulting are limited. However, The IIA recognizes that consulting is a way for internal auditors to add significant value to the organization. Candidates for the CIA exam must be able to distinguish the requirements for consulting engagements from those for assurance engagements.

1. **Financial, Compliance, Operational, and IT Auditing**

   a. According to the Introduction to the *Standards*, "Assurance services involve the internal auditor's objective assessment of evidence to provide opinions or conclusions regarding an entity, operation, function, process, system, or other subject matters."

   b. **Assurance services** are "[a]n objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization.

      1) Examples may include financial, performance, compliance, system security, and due diligence engagements" (The IIA Glossary).

      2) The nature and scope of the assurance engagement are determined by the internal auditor.

c. The following overview of assurance services is based on various publications of The IIA:

1) **Financial** assurance provides analysis of the economic activity of an entity as measured and reported by accounting methods.

a) **Financial auditing** looks at the past to determine whether financial information was properly recorded and adequately supported. It also assesses the safeguarding of assets, as well as whether the financial statement assertions about past performance are fair, accurate, and reliable.

2) **Compliance** assurance is the review of financial and operating controls to assess conformance with established laws, standards, regulations, policies, plans, procedures, contracts, and other requirements.

a) **Compliance auditing** looks at the past and examines the present to ask such questions as the following:

i) Have we adhered to laws and regulations?

ii) Are we currently complying with legal and regulatory requirements?

iii) What are our organization’s corporate standards of business conduct?

iv) Do all members of our staff and management team consistently comply with internal policies and procedures?

3) **Operational** assurance is the review of a function or process to appraise the efficiency and economy of operations and the effectiveness with which those functions achieve their objectives.

a) **Operational auditing** focuses on the present and future. It is closely aligned with the organization’s mission, vision, and objectives.

i) It also evaluates the effectiveness (ensuring the right things are done), efficiency (ensuring things are done the right way), and economy (ensuring cost-effectiveness) of operations.

ii) This mindset includes such areas as (a) product quality, (b) customer service, (c) revenue maximization, (d) expense minimization, (e) fraud prevention, (f) asset safeguarding, (g) corporate social responsibility and citizenship, (h) streamlined workflows, (i) safety, and (j) planning.

iii) It concentrates on what is working and what is not, as well as the opportunities for future improvement.

4) **IT** assurance is the review and testing of IT (for example, computers, technology infrastructure, IT governance, mobile devices, and cloud computing) to assure the integrity of information. Traditionally, IT auditing has been done in separate projects by IT audit specialists, but increasingly it is being integrated into all audits.

d. The three distinct categories of assurance services (financial, compliance, and operational) correspond to the categories of objectives defined in the control framework adopted by the Committee of Sponsoring Organizations (COSO).

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

a) **Operations** objectives relate to the effectiveness and efficiency of operations, e.g., achievement of operational and financial performance goals, and the safeguarding of assets against loss.

b) **Reporting** objectives relate to internal and external financial and nonfinancial reporting and may include the reliability, timeliness, and transparency of such reporting.

c) **Compliance** objectives relate to adherence to applicable laws and regulations.

Assurance Services

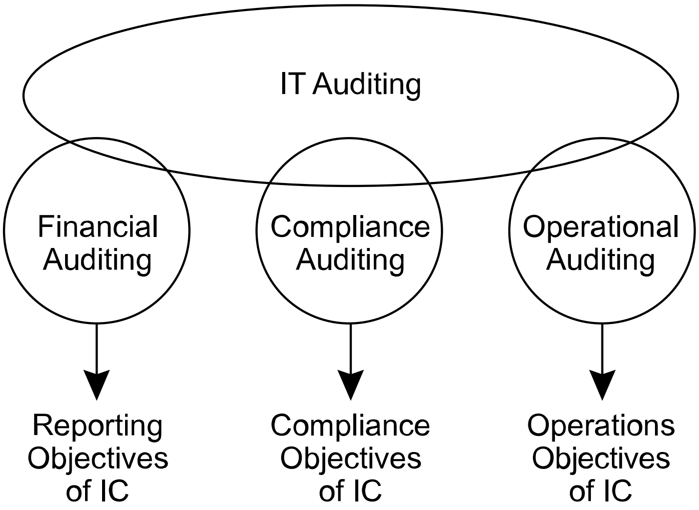

IT Auditing
Financial Auditing
Compliance Auditing
Operational Auditing
Reporting Objectives of IC
Compliance Objectives of IC
Operations Objectives of IC

Figure 2-1

e. The services described also may be performed by external auditors, for example, in outsourcing or cosourcing engagements. Nevertheless, the traditional focus of external auditors is on the fair presentation of general purpose financial information.

1) By contrast, the traditional focus of internal auditors is on supporting management and governance authorities in performing their functions.

2. **Assurance Mapping**

   a. An assurance map is a visual representation of an organization’s risks and assurance activities. An assurance map may include the following:

      1) Identity of the assurance providers
      2) Risk
      3) Level of assurance
      4) Urgency or importance of the issue
      5) Action to be taken

   b. Assurance providers are internal and external stakeholders that are responsible for implementing or maintaining assurance services.

      1) Management provides assurance through compliance with laws and regulations, quality assurance, and self-assessments.
      2) The board of directors provides assurance through the internal audit function.
      3) External stakeholders provide assurance through the independent external auditor, government regulators, and trade associations such as ISO.

   c. Risk is determined by judging the inherent risk of the activity, the risk that internal controls may not prevent or detect noncompliance, and the potential consequences of noncompliance.

   d. The level of assurance is determined by considering the quality, extent, and costs of internal controls.

   e. The higher the risk or assurance, the more urgent or important an issue likely is.

   f. The actions to be taken depend on the specific issue and the urgency or importance of that issue.

      1) In general, users of an assurance map have the option to increase or decrease assurance.
      2) If a low-risk area has a high level of assurance, the entity may want to consider shifting those assurance resources to a high-risk area.

EXAMPLE 2-1 Assurance Map

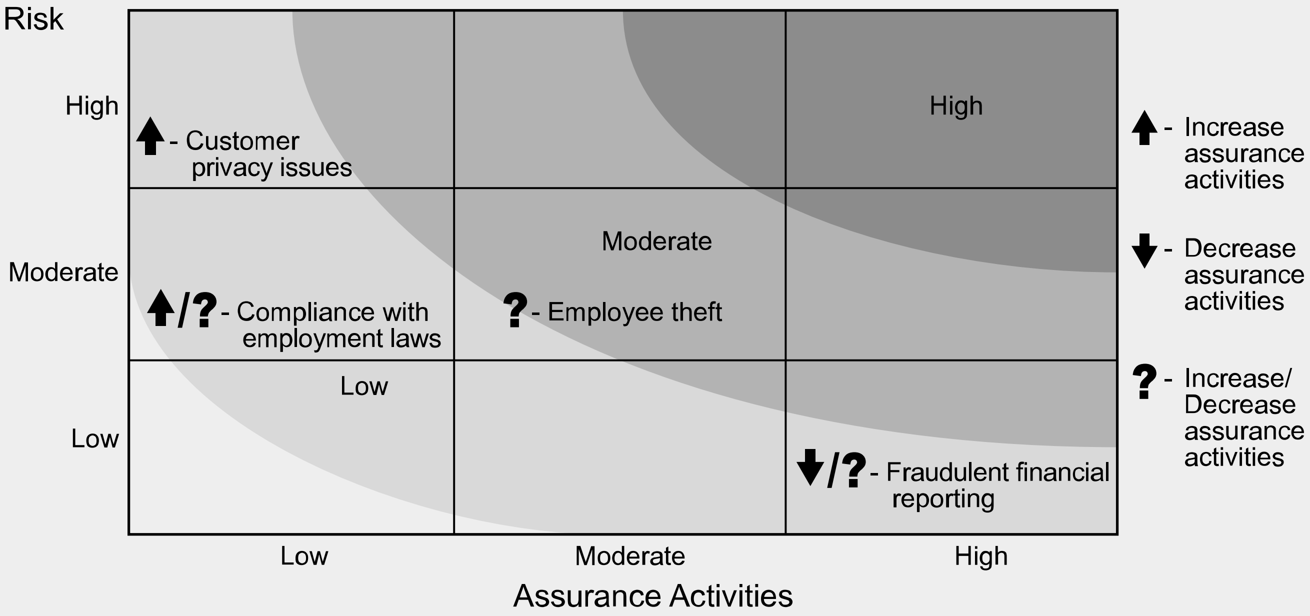


Figure 2-2

Notes:

- As customer privacy concerns have become more important, the entity has determined that its assurance activities related to customer privacy need to be increased.
- Compliance with employment law has not previously been an issue. However, due to recent changes in the law, the entity is considering increasing assurance activities.
- Due to the balance between risk and assurance activities, the entity does not know whether it should increase or decrease assurance activities.
- The level of assurance activities for fraudulent financial reporting is high. The entity therefore is considering using some resources for those assurance activities elsewhere.

2.2 RISK AND CONTROL SELF-ASSESSMENT

1. **Control Self-Assessment (CSA)**
   a. Managers and auditors have an interest in using methods that (1) improve the assessment of risk management and control processes and (2) identify ways to improve their effectiveness.
   b. CSA increases awareness of risk and control throughout the organization.
      1) Risk assessment, business processes, and internal controls are not treated as exclusive concerns of senior management and the internal audit activity. Instead, CSA involves client personnel, asks for their input, and gives them a sense of participation.
   c. CSA's **basic philosophy** is that control is the responsibility of everyone in the organization. The people who work within the process, i.e., the employees and managers, are asked for their assessments of risks and controls in their process.
   d. CIA candidates should understand (1) the objectives of CSA, (2) its advantages to an organization, and (3) its limitations.
2. **Elements of CSA**
   a. A typical CSA process has the following elements:
      1) Front-end planning and preliminary audit work.
      2) An in-person meeting, typically involving a facilitation seating arrangement (U-shaped table) and a meeting facilitator. The participants are process owners, i.e., management and staff who
         a) Are involved with the particular issues under examination,
         b) Know them best, and
         c) Are critical to the implementation of appropriate process controls.
      3) A structured agenda used by the facilitator to lead the group through an examination of the process's risks and controls. Frequently, the agenda is based on a well-defined framework or model so that participants can be sure to address all necessary issues. A model may focus on controls, risks, or a framework developed for that project.
      4) An option is the presence of a scribe to take an online transcription of the session and electronic voting technology to enable participants to state their perceptions of the issues anonymously.
      5) Reporting and the development of action plans.
   b. Accordingly, CSA typically employs a **workshop-facilitation approach** to self-assessment that is structured, documented, and repetitive. Thus, it should be contrasted with an approach that merely surveys employees regarding risks and controls.
3. **Responsibilities**
   a. **Senior management** should oversee the establishment, administration, and evaluation of the processes of risk management and control.
   b. **Operating managers**' responsibilities include assessment of the risks and controls in their units.
   c. **Internal and external auditors** provide varying degrees of assurance about the state of effectiveness of the risk management and control processes of the organization.

4. **How Internal Auditors Use CSA**

   a. Internal auditing's investment in CSA programs may be significant. It may

      1) Sponsor, design, implement, and own the process;
      2) Conduct the training;
      3) Supply the facilitators, scribes, and reporters; and
      4) Coordinate the participation of management and work teams.

   b. But in other organizations, internal auditing may serve only as an interested party and consultant for the whole process and as the ultimate verifier of the evaluations produced by the teams.

      1) In most programs, the investment in the organization's CSA efforts is somewhere between the two extremes described above. As the level of involvement in the CSA program and individual workshop deliberations increases, the chief audit executive (CAE)

         a) Monitors the objectivity of the internal audit staff,
         b) Takes steps to manage that objectivity (if necessary), and
         c) Augments internal audit testing to ensure that bias or partiality does not affect the final judgments of the staff.

   c. A CSA program augments the traditional role of the internal audit activity by assisting management in fulfilling its responsibilities to establish and maintain risk management and control processes and by evaluating the adequacy of that system.

      1) Through a CSA program, the internal audit activity and the business units and functions **collaborate** to produce better information about how well the control processes are working and how significant the residual risks are.

   d. Although it provides staff support for the CSA program as facilitator and specialist, the internal audit activity often finds that it may reduce the effort spent in gathering information about control procedures and eliminate some testing.

      1) A CSA program

         a) Increases the coverage of assessments of control processes across the organization,
         b) Improves the quality of corrective actions made by the process owners, and
         c) Focuses the internal audit activity's work on reviewing high-risk processes and unusual situations.

      2) A CSA also can focus on

         a) Validating the evaluation conclusions produced by the CSA process,
         b) Synthesizing the information gathered from the components of the organization, and
         c) Expressing its overall judgment about the effectiveness of controls to senior management and the board.

5. **Key Features**

   a. CSA includes **self-assessment surveys** and **facilitated workshops**. It is a useful and efficient approach for managers and internal auditors to collaborate in assessing and evaluating control procedures. In its purest form, CSA integrates business objectives and risks with control processes.

      1) CSA also is called control/risk self-assessment.

   b. Although CSA practitioners use different methods and formats, most implemented programs share some key features and goals. An organization that uses self-assessment will have a formal, documented process that allows management and work teams who are directly involved in a business unit, function, or process to participate in a structured manner for the purpose of

      1) Identifying risks and exposures,
      2) Assessing the control processes that mitigate or manage those risks,
      3) Developing action plans to reduce risks to acceptable levels, and
      4) Determining the likelihood of achieving the business objectives.

6. **Outcomes**

   a. People in the business units become trained and experienced in assessing risks and associating control processes with managing those risks and improving the chances of achieving business objectives.

   b. Informal, soft controls are more easily identified and evaluated.

   c. People are motivated to take ownership of the control processes in their units, and corrective actions taken by the work teams are often more effective and timely.

   d. The entire objectives-risks-controls infrastructure of an organization is subject to greater monitoring and continuous improvement.

   e. Internal auditors become involved in and knowledgeable about the self-assessment process by serving as facilitators, scribes, and reporters for the work teams and as trainers in risk and control concepts supporting the CSA program.

   f. The internal audit activity acquires more information about the control processes within the organization and can leverage that additional information in allocating its scarce resources.

      1) The result is greater effort devoted to investigating and performing tests of business units or functions that have significant control weaknesses or high residual risks.

   g. Management’s responsibility for the risk management and control processes of the organization is reinforced, and managers will be less tempted to abdicate those activities to specialists, such as auditors.

   h. The primary role of the internal audit activity will continue to include validation of the evaluation process by the performance of tests and the expression of its professional judgment about the adequacy and effectiveness of the whole risk management and control system.

7. **Approaches**

   a. The three primary approaches of CSA programs are (1) facilitation, (2) survey (questionnaire), and (3) self-certification. Organizations often combine approaches.

   b. The variety of approaches used for CSA processes in organizations reflects the differences in industry, geography, structure, organizational culture, degree of employee empowerment, dominant management style, and the manner of formulating strategies and policies. Thus, the success of a particular type of CSA program in one organization might not be replicated in another.

      1) The CSA process should be customized to fit the unique characteristics of each organization. Also, a CSA approach needs to be dynamic and change with the continual development of the organization.

8. **Facilitation Approach**

   a. The facilitation approach has four possible formats:

      1) The **objective-based format** focuses on the best way to accomplish a business objective. The workshop begins by identifying the controls presently in place to support the objective and then determines the residual risks remaining.

         a) The aim of the workshop is to decide whether the control procedures are working effectively and are resulting in residual risks within an acceptable level.

      2) The **risk-based format** focuses on listing the risks to achieving an objective. The workshop begins by listing all possible barriers, obstacles, threats, and exposures that might prevent achieving an objective and then examines the control procedures to determine whether they are sufficient to manage the key risks.

         a) The workshop's aim is to determine significant residual risks. This format takes the work team through the entire objective-risks-controls formula.

      3) The **control-based format** focuses on how well the controls in place are working. This format is different from the objective-based and risk-based formats because the facilitator identifies the key risks and controls before the beginning of the workshop. During the workshop, the work team assesses how well the controls mitigate risks and promote the achievement of objectives.

         a) The aim of the workshop is to produce an analysis of the gap between how controls are working and how well management expects those controls to work.

      4) The **process-based format** focuses on selected activities that are elements of a chain of processes. The processes are usually a series of related activities that go from some beginning point to an end, such as the various steps in purchasing, product development, or revenue generation. This type of workshop usually covers the identification of the objectives of the whole process and the various intermediate steps.

         a) The workshop's aim is to evaluate, update, validate, improve, and even streamline the whole process and its component activities.

         b) This workshop format may have a greater breadth of analysis than a control-based approach by covering multiple objectives within the process and by supporting concurrent management efforts, such as reengineering, quality improvement, and continuous improvement initiatives.

9. **Survey Approach**

    a. The survey form of CSA uses a questionnaire that tends to ask mostly simple “yes/no” or “have/have not” questions that are carefully written to be understood by the target recipients.

        1) Surveys often are used if the desired respondents are too numerous or widely dispersed to participate in a workshop. They also are preferred if the culture in the organization may limit open, candid discussions in workshop settings or if management desires to minimize the time spent and costs incurred in gathering the information.

10. **Self-Certification Approach**

    a. This form of self-assessment is based on management-produced analyses to produce information about selected business processes, risk management activities, and control procedures. The analysis is often intended to reach an informed and timely judgment about specific characteristics of control procedures and is commonly prepared by a team in a staff or support role.

        1) The internal auditor may synthesize this analysis with other information to enhance the understanding about controls and to share the knowledge with managers in business or functional units as part of the organization’s CSA program.

11. **Understanding of Risk and Control**

    a. All self-assessment programs assume that managers and members of the work teams understand risk and control concepts and use them in communications.

        1) For training sessions, to facilitate the orderly flow of workshop discussions, and as a check on the completeness of the overall process, organizations often use a control framework, such as the COSO (Committee of Sponsoring Organizations) model.

12. **Workshop Reports**

    a. In the typical CSA facilitated workshop, a report is substantially created during the deliberations. A consensus is recorded for the various segments of the discussions, and the group reviews the proposed final report before the end of the final session.

        1) Some programs use anonymous voting to ensure the free flow of information and opinions during the workshops and to aid in negotiating differences between interest groups.

13. **Limitations**

    a. The internal auditor may not effectively use the selected CSA approach(es), or the persons performing the self-assessment may not be skilled in risk management and control. The relevant risks and controls then may not be identified or, if identified, not properly assessed.

2.3 AUDITS OF THIRD PARTIES AND CONTRACT AUDITING

1. **External Business Relationships**
    a. Organizations have multiple external (extended) business relationships (EBRs). The IIA's Practice Guide, *Auditing External Business Relationships*, contains extensive guidance.
        1) Each EBR has risks, and management is responsible for managing and monitoring the risks and achieving the benefits.
        2) Internal auditing assists management and validates its efforts.
    b. EBRs may involve the following:
        1) Service providers (e.g., for providing internal audit services, processing of payroll, sharing of services, or use of IT services)
        2) Supply-side partners (e.g., outsourcing of production or R&D)
        3) Demand-side partners (e.g., licensees or distributors)
        4) Strategic alliances and joint ventures (e.g., cost-, revenue-, and profit-sharing in media production and development)
        5) Intellectual property (IP) partners (e.g., licensing of software)
    c. Among other things, EBR partners may offer lower costs, better operational efficiency, special expertise, new technology, a known brand, or economies of scale.
    d. The internal audit activity helps management and the board identify, assess, and manage risks, including reputation risks as well as economic risks. The following are examples of significant risks of EBRs:
        1) They may not be identified and therefore may not be
            a) Managed in accordance with relevant policies,
            b) Assessed, or
            c) Monitored.
        2) EBRs may adversely affect the organization's reputation, e.g., by violating laws, committing fraud, or not complying with contracts.
        3) EBRs may have inadequate insurance coverage.
        4) Service levels or products may be unsatisfactory, e.g., because of inadequate definition in the contract.
        5) Conflicts of interest may arise, e.g., when the work is affected by the EBR's contractual obligations to others.
        6) Licensing of intellectual property may result in misuse, theft, or loss of revenue.
        7) The organization may be overcharged for services.
        8) The EBR partner may become insolvent.
        9) The organization's confidential information (e.g., personally identifiable information) may be lost.

2. **Auditing EBRs**

   a. Before auditing an EBR, the internal auditors first must determine whether the EBR partner has agreed to the audit.

      1) This right ordinarily is granted in an audit clause in the contract creating the EBR.

   b. Internal auditors need to understand all elements of an EBR:

      1) Initiating the EBR
      2) Contracting for and defining the EBR
      3) Procurement
      4) Managing and monitoring the EBR (including control environment considerations of objectivity and independence of managers)
      5) Discontinuing the EBR

   c. The internal auditors need to understand the expectations of the parties and the processes for managing and monitoring the EBR.

      1) They then develop an appropriate audit program with relevant objectives.

         a) Internal audit procedures may include evaluating compliance with the contract to determine whether monetary and nonmonetary obligations are met.
         b) Audit procedures may discover missed revenue or cost savings, improve reporting, and add value to the EBR through the following:

            i) Limiting fraud
            ii) Increasing trust
            iii) Fostering feedback
            iv) Improving relationships
            v) Helping management improve internal and external controls

   d. The CAE decides whether to audit (1) each EBR separately, (2) certain EBRs, or (3) the total EBR process. The following is the cycle for an EBR audit:

      1) **Understanding the organization, its environment, its processes, and the nature of each EBR**

         a) The internal auditors need to understand

            i) The reasons for, and the importance of, EBRs;
            ii) Whether they have been identified; and
            iii) The risks of noncompliance by EBR partners.

      2) **Assessing risks and controls**

         a) The internal auditors need to

            i) Understand the EBR’s inherent risks and the design of relevant controls;
            ii) Determine the key controls; and
            iii) Understand the EBR partner’s environment, processes, and controls (including the work done by its auditors).

3) **Performing the audit**

   a) The internal auditors need to determine whether to

      i) Do on-site work at the EBR,

      ii) Evaluate results,

      iii) Identify findings and their application (to one EBR, certain EBRs, or the total EBR process), and

      iv) Reach conclusions.

4) **Reporting**

   a) The internal auditors need to determine the frequency and content of reports to the board and senior management.

5) **Monitoring progress**

   a) The internal auditors may determine whether findings (especially deficiencies) have been addressed. They also may assist in determining whether EBRs are well managed.

3. **Third-Party Audits**

   a. The organization may be audited. This is routine for organizations that issue general-use financial statements and for many EBRs.

      1) For example, if the organization is a service provider, the external and internal auditors of the organization's clients must obtain assurance about the security of the organization's operations and the fulfillment of contractual obligations. Such audits are also common for joint ventures.

      2) Another typical third-party audit is the audit performed by a qualified registrar as part of the ISO 9000 certification process.

   b. In these cases, the internal auditors should coordinate their activities with those of the third-party auditor to share information and to prevent duplication of effort.

4. **Contract Auditing**

   a. Internal auditors often perform engagements to monitor and evaluate significant construction contracts and operating contracts that involve the provision of services. The usual types of arrangements for such contracts are lump-sum (fixed-price), cost-plus, and unit-price.

   b. **Lump-sum contracts.** The internal auditor may have little to evaluate when the work is performed in accordance with the contract. However, reviewing such an agreement may call for consideration of the following:

      1) Progress payments

      2) Incentives (e.g., for early completion)

      3) An escalator clause (e.g., one causing the entire price to be due in the event of some breach of the contract)

      4) Adjustments for labor costs (e.g., premiums paid to obtain necessary labor)

      5) Change orders

c. **Cost-plus contracts** are ways to cope with uncertainties about costs by setting a price equal to (1) cost plus a fixed amount or (2) cost plus a fixed percentage of cost. A problem is that the contractor may have little incentive for economy and efficiency, a reason for careful review by the internal auditors. These contracts may have provisions for

   1) Maximum costs, with any savings shared by the parties, or
   2) Incentives for early completion.

d. **Unit-price contracts** are often used when a convenient measure of work is available, such as acres of land cleared, cubic yards of earth moved, or square footage patrolled by a security service.

   1) The key issue is the accurate measurement of the work performed.

e. To protect the organization, internal auditors should be involved throughout the contracting process, not merely in the performance phase. They should review the terms of the contract and the following:

   1) Procedures for bidding (e.g., competitive bidding)
   2) Procedures for cost estimation and control
   3) Budgets and financial forecasts
   4) The contractor's information and control systems
   5) The contractor's financial position
   6) Funding and tax matters
   7) Progress of the project and costs incurred

f. When reviewing a contract for the purchase of a business application system, the internal auditor should recommend that the contract contain a **source code escrow clause**.

   1) A source code escrow clause requires the application source code to be held in escrow by a trusted third party.

      a) The third party releases the source code to the purchaser, or licensee, on the occurrence of an event, or events, specified in the clause.

2.4 QUALITY AUDITING

1. **Quality Auditing**

   a. The internal audit activity’s role is to provide assurance that the approved quality structures are in place and quality processes are functioning as intended.

2. **Traditional vs. Modern Views of Quality**

   a. The traditional view of quality emphasized the detection of products that do not meet standards.

      1) This view involved the rejection or reworking of defective goods.

   b. The modern view is that quality is a value-added activity performed throughout all processes, from product design to raw materials acquisition and final inspection.

      1) It also extends to all of the organization’s business processes, not just to the production of goods.

      2) This view of quality is the basis for total quality management (TQM).

3. **Total Quality Management (TQM)**

   a. TQM can increase revenues and decrease costs significantly. Thus, the internal audit activity’s services with respect to the quality function may add substantial value. Indeed, the improvement of operations is part of the definition of internal auditing.

   b. Quality is best viewed from multiple perspectives:

      1) Attributes of the product (performance, serviceability, durability, etc.),
      2) Customer satisfaction,
      3) Conformity with manufacturing specifications, and
      4) Value (relation of quality and price).

   c. TQM is a comprehensive approach. It treats the pursuit of quality as a basic organizational function that is as important as production or marketing. It is also a strategic weapon because its cumulative effects cannot be easily duplicated by competitors.

      1) TQM is the **continuous pursuit of quality** in every aspect of organizational activities through

         a) A philosophy of doing it right the first time,
         b) Employee training and empowerment,
         c) Promotion of teamwork,
         d) Improvement of processes, and
         e) Attention to satisfaction of internal and external customers.

   d. TQM emphasizes the supplier’s relationship with the customer and identifies customer needs. It also recognizes that everyone in a process is at some time a customer or supplier of someone else, either within or outside the organization.

      1) Thus, TQM begins with external customer requirements, identifies internal customer-supplier relationships and requirements, and establishes requirements for external suppliers.

e. The management of quality is not limited to quality management staff, engineers, production personnel, etc.

   1) Given the organization-wide scope of TQM and of the internal audit activity, the role of the internal auditors is to evaluate the entire quality function.

      a) The internal audit activity is well qualified to perform risk assessments and promote continuous improvement of controls.

         i) The personnel involved in the technical improvements of processes may be unqualified with regard to risk management and control issues.

      b) The internal audit activity performs procedures to provide assurance that the basic objectives of TQM are reached: customer satisfaction, continuous improvement, and promotion of teamwork.

      c) TQM concepts also apply to the operations of the internal audit activity itself. For example, periodic internal assessments of those operations may include benchmarking its practices and performance metrics against relevant best practices of the profession.

2.5 SECURITY AND PRIVACY AUDITS

NOTE: Physical security, such as safeguards against environmental risks and wrongful access to computers, must be audited even if software provides most of the protection for information.

1. **Information Security Auditing**

   a. Information security auditing is an expansion of the assurance services performed by auditors. The creation of organization-wide computer networks with the potential for access by numerous outside parties has greatly increased risk. Thus, risk management and control processes may be inadequate.

   b. The role of the internal audit activity in these circumstances is to assess risks, monitor the implementation of corrective action, and evaluate controls.

      1) The internal audit activity also may act in a consulting capacity by identifying security issues and by working with users of information systems and with systems security personnel to devise and implement controls.

      2) The internal audit activity works closely with senior management and the board to assist in the performance of the governance function with respect to information security.

Implementation Standard 2130.A1

The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to the risks within the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives;
- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programs;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, procedures, and contracts.

c. **Information Reliability and Integrity**

1) Information reliability and integrity includes accuracy, completeness, and security. The internal audit activity determines whether senior management and the board clearly understand that it is a management responsibility for all critical information regardless of its form.

2) The CAE determines whether the internal audit activity has competent audit resources for evaluating internal and external risks to information reliability and integrity.

3) The CAE determines whether senior management, the board, and the internal audit activity will be promptly notified about breaches and conditions that might represent a threat.

4) Internal auditors assess the effectiveness of preventive, detective, and mitigative measures against past and future attacks. They also determine whether the board has been appropriately informed.

5) Internal auditors periodically assess reliability and integrity practices and recommend new or improved controls. Such assessments can be made as separate engagements or as multiple engagements integrated with other elements of the audit plan.

d. Internal auditors also evaluate compliance with privacy laws and regulations. Thus, they assess the adequacy of the identification of risks and the controls that reduce those risks.

2. **Security Auditing**

a. The most common use of the term **security** in an organizational setting is in connection with information technology (IT).

1) However, the organization must take a more comprehensive view of security.

2) One example is the protection of employees and visitors from workplace violence. Thus, security is an appropriate governance and risk management issue even in the absence of IT.

b. The internal audit activity evaluates the adequacy and effectiveness of controls designed and implemented by management in all areas of security.

3. **Privacy Auditing**

   a. The amount of personal information stored on computers has greatly increased. The security risks involved also have increased because of the interconnections among computers permitted by the Internet.

   b. **Evaluation of a Privacy Framework**

      1) Protection of personal information prevents such negative organizational consequences as legal liability and loss of reputation.

      2) The following are various definitions of privacy:

         a) Personal privacy (physical and psychological)
         b) Privacy of space (freedom from surveillance)
         c) Privacy of communication (freedom from monitoring)
         d) Privacy of information (collection, use, and disclosure of personal information by others)

      3) Personal information is any information that can be associated with a specific individual or that might be combined with other information to do so. The following are examples:

         a) Name, address, identification numbers, family relationships
         b) Employee files, evaluations, comments, social status, or disciplinary actions
         c) Credit records, income, financial status
         d) Medical status

      4) **The board** is ultimately accountable for identifying principal risks, implementing controls, and managing privacy risk, e.g., by establishing and monitoring a privacy framework.

      5) **The internal audit activity** assesses the adequacy of (a) management's risk identification and (b) the controls that reduce those risks.

         a) Moreover, the internal audit activity evaluates the privacy framework, identifies significant risks, and makes recommendations. The internal audit activity also considers

            i) Laws, regulations, and practices in relevant jurisdictions;
            ii) The advice of legal counsel; and
            iii) The security efforts of IT specialists.

      6) The internal audit activity's role depends on the level or maturity of the organization's privacy practices.

         a) Accordingly, the internal auditors may

            i) Facilitate the development and implementation of the privacy program,
            ii) Evaluate management's privacy risk assessment, or
            iii) Perform an assurance service regarding the effectiveness of the privacy framework.

         b) However, assumption of responsibility may impair independence.

7) The internal auditor identifies

   a) Personal information gathered,

   b) Collection methods, and

   c) Whether use of the information is in accordance with its intended use and applicable law.

8) Given the difficulty of the technical and legal issues, the internal audit activity needs the knowledge and competence to assess the risks and controls of the privacy framework.

c. **Use of Personal Information in Performing Engagements**

1) Advances in IT and communications present privacy risks and threats. Thus, internal auditors need to consider the protection of personally identifiable information gathered during audits. Privacy controls are legal requirements in many jurisdictions.

2) Many jurisdictions require organizations to identify the purposes for which personal information is collected at or before collection. These laws also prohibit using and disclosing personal information for purposes other than those for which it was collected except with the individual’s consent or as required by law.

3) Internal auditors must understand and comply with all laws regarding the use of personal information.

4) It may be inappropriate or illegal to access, retrieve, review, manipulate, or use personal information in conducting certain engagements. If the internal auditor accesses personal information, procedures may be necessary to safeguard this information. For example, the internal auditor may not record personal information in engagement records in some situations.

5) The internal auditor may seek advice from legal counsel before beginning audit work if questions arise about access to personal information.

d. Privacy engagements address the security of personal information, especially information stored in computer systems. An example is healthcare information in the files of insurers and providers.

1) The organization must comply with governmental statutory and regulatory mandates. Internal auditors consult the organization’s legal counsel and then communicate the requirements to those responsible for designing and implementing the required safeguards.

   a) Internal auditors determine that the requirements are incorporated into the information system and that compliance is achieved in its operation.

2) Personal information needs to be protected from both unauthorized intrusion and misuse by those who have authorized access.

3) Privacy is balanced with the need to allow appropriate and prompt availability of personal information to legitimate users.

4) The organization documents compliance with privacy and other legal requirements.

5) Benefits of the security arrangements should exceed the costs. For example, encryption is an expensive way to address threats to the security of private information. Other methods, such as access controls, may be more appropriate relative to the assessed risk.

e. The IIA's Code of Ethics requires internal auditors to maintain the confidentiality of private information.

   1) "Internal auditors shall be prudent in the use and protection of information acquired in the course of their duties" (Rule of Conduct 3.1).

   2) "Internal auditors shall not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organization" (Rule of Conduct 3.2).

2.6 PERFORMANCE AUDITING

1. Performance Auditing

a. A performance audit may provide assurance about the organization's **key performance indicators**.

   1) A consulting engagement may be performed to design a performance measurement system.

b. Internal auditors assess an organization's ability to measure its performance, recognize deficiencies, and take corrective actions.

   1) Effective management control requires performance measurement and feedback. This process affects allocation of resources to organizational subunits. It also affects decisions about managers' compensation, advancement, and future assignments.

   2) Furthermore, evaluating their performance serves to motivate managers to optimize the measures in the performance evaluation model. However, that model may be inconsistent with the organization's model for managerial decision making.

      a) To achieve consistency, the models should be synchronized. For example, if senior management wishes to maximize results over the long term, subordinates should be evaluated over the long term.

c. A **balanced scorecard** is useful for performance measurement. It is a report that connects critical success factors determined in a strategic analysis with financial and nonfinancial measures of the elements of performance.

   1) An organization identifies its critical success factors by means of an analysis that addresses internal factors (strengths and weaknesses) and external factors (opportunities and threats). This process is **SWOT analysis**.

      a) The organization's greatest strengths are its core competencies. These are the basis for its ability to compete successfully and its strategy.

      b) **Strengths** and **weaknesses** are internal resources or a lack of resources. For example, strengths include technologically advanced products, a broad product mix, capable management, leadership in R&D, modern production facilities, and a strong marketing organization. Weaknesses result from the lack of such advantages.

c) **Opportunities** and **threats** arise from factors external to the organization, such as government regulations, advances in technology, and demographic changes. They may be reflected in certain competitive conditions, including the following:

i) The number and strength of competitors in the industry

ii) Changes in the intensity of rivalry within the industry, for example, because of excessive production capacity

iii) The relative availability of substitutes for the organization’s products or services

iv) Bargaining power of customers

v) Bargaining power of suppliers

d) The SWOT analysis facilitates development of a strategy by emphasizing the basic factors of cost, quality, and the speed of product development and delivery.

2) Specific, reliable measures must be determined for each factor relevant to organizational success.

3) Measures should be **nonfinancial** as well as financial, **long-term** as well as short-term, and **internal** as well as external. The balanced scorecard de-emphasizes short-term financial results and focuses attention on factors vital to future success.

4) The development and implementation of a comprehensive balanced scorecard requires active participation by senior management.

a) The scorecard should contain detailed measures to permit everyone to understand how his or her efforts affect results.

b) The scorecard and the strategy it represents must be communicated to all managers and used as a basis for compensation decisions.

c) The scorecard should permit a determination of whether certain objectives are being achieved at the expense of others. For example, reduced spending on customer service may improve short-term financial results but cause a decline in customer satisfaction.

5) A typical balanced scorecard includes measures in four categories:

a) **Financial** measures are ultimate results provided to owners, e.g., sales, fair value of the organization’s stock, profits, and liquidity.

b) **Customer** measures reflect customer needs and satisfaction, e.g., customer retention rate, dealer and distributor relationships, marketing and selling performance, prompt delivery, quality, and market share.

c) **Internal** measures of key processes drive the business, e.g., quality, productivity (an input-output relationship), flexibility of response to changing conditions, operating readiness, and safety.

d) **Learning, growth, and innovation** measures are the basis for future success (people and infrastructure). Examples are development of new products, promptness of their introduction, human resource development, morale, and competence of the work force.

2.7 OPERATIONAL AUDITING

1. **Operational Audit Engagements**
   a. An operational audit assesses the efficiency and effectiveness of an organization's operations. The following are typical operational audit engagements:
      1) **Process (functional) engagements** are operational audit engagements that follow process-crossing organizational lines, service units, and geographical locations.
         a) The focus is on operations and how effectively and efficiently the organizational units affected will cooperate.
         b) These engagements tend to be challenging because of their scope and the need to deal with organizational units that may have conflicting objectives.
         c) Typical processes or functions are
            i) Purchasing and receiving
            ii) Distribution of services, materials, and supplies to users in the organization
            iii) Modification of products
            iv) Safety practices
            v) Scrap handling and disposal
            vi) Development of budgets
            vii) Marketing
            viii) Management of depreciable assets
      2) **Program-results engagements** are intended to obtain information about the costs, outputs, benefits, and effects of a program. They attempt to measure the accomplishment and relative success of the undertaking.
         a) Because benefits often cannot be quantified in financial terms, a special concern is the ability to measure effectiveness. Thus, clear definitions of objectives and standards should be provided at the outset of the program.
         b) A program is a funded activity not part of the normal, continuing operations of the organization, such as an expansion or a new information system.
   b. Measures used to assess effectiveness and efficiency include the following:
      1) The productivity ratio measures output relative to input.
      2) The productivity index measures production potential.
      3) The resource usage rate measures resource use relative to available resources.
      4) The operating ratio measures the operational efficiency of an organization.

2.8 COMPLIANCE AUDITING

SUCCESS TIP

An internal audit activity can add value to its organization by performing many types of engagements. CIA candidates must know not only the requirements of these engagements but also when and where to perform each kind of engagement.

1. **Compliance**
   a. The IIA Glossary defines compliance as follows:

      Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.

   b. Internal auditors assess compliance in specific areas as part of their role in organizational governance. They also follow-up and report on management’s response to regulatory body reviews. Given the scope of governmental regulation, these duties of internal auditors have great importance.

      Caution: Internal auditors are encouraged to consult legal counsel in all matters involving legal issues. Requirements may vary significantly in different jurisdictions.

   c. The internal audit activity’s responsibilities with regard to compliance are addressed in two Implementation Standards.
      1) The internal audit activity must evaluate risk exposures relating to governance, operations, and information systems with regard to
         a) Compliance (Implementation Standard 2120.A1) and
         b) The adequacy and effectiveness of controls responding to these risks (Implementation Standard 2130.A1).

2. **Programs**
   a. Compliance programs assist organizations in preventing unintended employee violations, detecting illegal acts, and discouraging intentional employee violations. They also help (1) prove insurance claims, (2) determine director and officer liability, (3) create or enhance corporate identity, and (4) decide the appropriateness of punitive damages.
      1) Internal auditors need to evaluate an organization’s regulatory compliance programs.
      2) The CAE should meet with regulators to provide relevant information or receive advice on necessary compliance.

3. **Organizational Standards and Procedures**
   a. The organization establishes compliance standards and procedures that are reasonably capable of reducing the probability of criminal conduct by its employees and other agents. They include the following:
      1) A clearly written, straightforward, and fair business code of conduct that provides guidance to employees on relevant issues and is user-friendly
      2) An organizational chart identifying personnel responsible for compliance programs
      3) Financial incentives that do not reward misconduct
      4) For an international organization, a compliance program on a global basis that reflects local conditions and laws
4. **Responsibility**
   a. Specific high-level personnel who are properly empowered and supplied with necessary resources should be responsible for the compliance program.
      1) Senior management also should be involved.
      2) High-level personnel should have substantial control of the organization or a substantial role in making policy.
      3) Compliance personnel should have adequate access to senior management, and the chief compliance officer should report directly to the CEO.
5. **Applicant Screening**
   a. Due care should be used to avoid delegating authority to those with a tendency to engage in illegal activities.
      1) Applications should inquire about criminal convictions or discipline by licensing boards.
      2) All applicants should be screened in a lawful manner that does not infringe upon privacy rights. The purpose is to detect evidence of past wrongdoing, especially that within the organization’s industry.

6. **Communication**
   a. Standards and procedures, including readily available ethics-related documents, should be communicated effectively, preferably in an interactive format and on multiple occasions.
      1) Training programs and publications are typical methods. The best training allows employees to practice new techniques and use new information.
      2) Compliance information should be conveyed through a variety of media. Moreover, it should be targeted to the areas important to each functional employee group and its job requirements.
         a) For example, environmental compliance information should be directed to subunits, such as manufacturing, that are more likely to violate (or detect violations of) such laws and regulations.
      3) New employees should receive basic compliance training as part of their orientation, and agents of the organization should be given a presentation specifically for them.
         a) Agents should understand the organization’s core values and that their actions will be monitored.
      4) Organizations also should require employees to certify periodically that they have read, understood, and complied with the code of conduct. This information is relayed annually to senior management and the board.
7. **Monitoring and Reporting**
   a. Monitoring and auditing systems for detecting illegal or unethical behavior and employee hotlines should be used. The best approach is to coordinate multiple monitoring and auditing systems.
      1) For example, the internal audit plan should be given appropriate resources and applied to all of the organization’s businesses. Also, it should include a review of the compliance program.
      2) The compliance review considers (a) effectiveness of written materials, (b) employee receipt of communications, (c) handling of violations, (d) fairness of discipline, (e) observance of any protections given to informants, and (f) fulfillment of compliance unit responsibilities.
   b. Attorney-client and attorney work-product privileges protect certain information disclosed to (or produced by) an attorney from being used by an adverse party in a legal proceeding. An attorney monitoring the hotline is best able to protect the privileges.
      1) Employees may have little confidence in such hotlines or in write-in reports or an off-site person assigned to hear complaints. But they may have confidence in hotlines answered by an in-house representative and backed by a nonretaliation policy.
         a) However, a hotline cannot ensure anonymity.

c. An on-site official may be assigned to receive and investigate complaints. This individual (an **ombudsperson**) is more effective if (s)he (1) reports directly to the chief compliance officer or the board, (2) keeps the names of informants secret, (3) provides guidance to informants, and (4) undertakes follow-up to ensure that retaliation has not occurred.

d. An ethics questionnaire should be sent to each employee asking whether the employee is aware of kickbacks, bribes, or other wrongdoing.

e. Organizational compliance standards should be consistently enforced by adequate, fair, case-specific discipline.

   1) Punishment should be appropriate to the offense, such as a warning, loss of pay, suspension, transfer, or termination.

   2) The program should provide for the discipline of managers and other responsible persons who knew or should have known of misconduct and did not report it. Failure to do so indicates a lack of due diligence.

      a) As a result, a court may rule that (1) the program is not effective and (2) the organization is therefore legally liable for giving authority to persons with a tendency to commit crimes.

f. Termination or other discipline of employees may be limited by

   1) Whistleblower laws;

   2) Statutory exceptions to the employee-at-will doctrine (the right of an employer to fire an employee for any reason);

   3) Employee or union contracts; and

   4) Employer responsibilities with regard to discrimination, wrongful discharge, and requirements to act in good faith.

g. Employee discipline should be thoroughly documented so that the organization will be able to prove that it made its best effort to collect information and took appropriate action.

h. After detection, the response should be appropriate and designed to prevent other similar offenses.

   1) In some circumstances, an appropriate response may require self-reporting of violations to the government, cooperation with investigations, and the acceptance of responsibility.

      a) An effective compliance program and appropriate responses may result in more lenient punishment for committing the offense.

i. Failure to detect or prevent a serious violation may indicate that the compliance program needs to be restructured. One change that may be required is the replacement or transfer of compliance personnel.

STUDY UNIT THREE

FINANCIAL, ENVIRONMENTAL, AND CONSULTING ENGAGEMENTS

This study unit is the third of four covering **Domain I: Managing the Internal Audit Activity** from The IIA's CIA Exam Syllabus. This domain makes up 20% of Part 2 of the CIA exam and is tested at the **basic** and **proficient** cognitive levels. Refer to the complete syllabus located in Appendix B to view the relevant sections covered in Study Unit 3.

3.1 FINANCIAL ENGAGEMENTS

1. **Financial Statements and Corporate Governance**
   a. The financial reporting process encompasses the steps to create information and prepare financial statements, related notes, and other accompanying disclosures in the organization's financial reports.
   b. Internal auditors provide assurance regarding financial reporting to management and the board. For example, in many countries, laws require that management certify that the general-purpose financial statements are fairly stated in all material respects.

Performance Standard 2120
Risk Management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

Interpretation of Standard 2120

Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

- Organizational objectives support and align with the organization's mission.
- Significant risks are identified and assessed.
- Appropriate risk responses are selected that align risks with the organization's risk appetite.
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness.

Risk management processes are monitored through ongoing management activities, separate evaluations, or both.

Implementation Standard 2120.A1

The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

Implementation Standard 2120.A2

The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

2. **Management's Assertions**

   a. Management implicitly or explicitly makes assertions about the measurement, presentation, and disclosure of information in financial statements.

      1) Part of any engagement may involve testing these assertions to determine whether they are supported by the evidence.
      2) Determining whether these assertions are supported by the evidence also can help the auditor to determine whether controls are working as designed.
      3) For example, the assertions relevant to financial engagements in the AICPA's guidance are covered in Study Unit 5, Subunit 4.

3. **Key Risks**

   a. Key risks affecting the reliability and integrity of financial information include the following:

      1) Overstating revenues (e.g., improper timing of revenue recognition)
      2) Understating expenses (e.g., improperly capitalizing expenditures that should be recorded as an expense in the current period)
      3) Applying unreasonable accounting estimates (e.g., accounting estimates are neither consistent with past results nor reasonable in light of expected future events)
      4) Applying accounting principles that are no longer in effect

4. **Accounting Cycles**

   a. An audit of financial information may follow the cycle approach to internal accounting control (a cycle is a functional grouping of transactions).

   b. **Sales, Receivables, and Cash Receipts Cycle**

      1) Processing customer orders
      2) Customer acceptance and granting credit
      3) Shipping goods
      4) Recording sales and receivables (including observing a proper cutoff)
      5) Billing customers
      6) Receiving, processing, and recording cash receipts
      7) Providing for, and writing off, bad debts
      8) Receiving, processing, and recording sales returns
      9) Providing for adjustments, allowances, warranties, and other credits

c. **Purchases, Payables, and Cash Disbursements Cycle**

1) Processing purchase requests
2) Issuing purchase orders
3) Receiving goods and services
4) Processing vendor invoices, receiving reports, and purchase orders
5) Disbursing cash
6) Accounting for and documenting receipts, liabilities, cash disbursements, and accrued expenses

d. **Production or Conversion Cycle**

1) Inventory planning
2) Receipt and storage of goods
3) Production or conversion of goods or provision of services
4) Accounting for costs, deferred costs, and property
5) Storage of produced or converted goods
6) Shipment

e. **Financial Capital and Payment Cycle**

1) Issuing long-term debt and stock
2) Paying interest and dividends
3) Repurchase of equity and debt securities and payment at maturity
4) Maintaining detailed records for payment of interest, dividends, and taxes
5) Purchases and sales of investments
6) Recording receipts of interest and dividends
7) Recording stock options and treasury stock
8) Accounting for investing and financing transactions

f. **Personnel and Payroll Cycle**

1) Personnel department’s hiring of employees
2) Personnel department’s authorization of payroll rates, deductions, etc.
3) Timekeeping
4) Payroll preparation and payment
5) Filing payroll tax returns and paying the taxes

g. **External Financial Reporting Cycle**

1) Preparation of financial statements
2) Disclosure of related information
3) Controls over financial reporting
4) Selection of accounting principles
5) Unusual or nonrecurring items
6) Contingencies

SUCCESS TIP

The IIA has consistently tested candidates on the aspects of internal control in different accounting cycles. Appendix D is dedicated to reviewing the most significant accounting cycles. This review is needed for an understanding of basic internal controls. Other accounting cycles and controls may be tested.

Thus, the subject of a control question on the exam may not be covered. However, an understanding of (1) basic control principles, (2) accounting cycles, and (3) how the controls help prevent or detect fraud or error should enable candidates to handle any other cycles and controls that are tested.

For example, authorizations required by a health insurer before a claim is paid are not significantly different from those required for a debtor's payment of interest on a note payable. Both require the auditor to trace the payment to documentation about authorization as well as supporting documentation.

Furthermore, candidates should not necessarily be concerned about memorizing every control in every cycle. Rather, they should understand control concepts.

h. In Appendix D are five flowcharts and accompanying tables describing the steps in five basic accounting cycles and the controls in each step for an organization large enough to have an optimal segregation of duties.

   1) In small- and medium-sized organizations, some duties must be combined. The internal auditor must assess whether organizational segregation of duties is adequate.

5. **Fraud Risk**

   a. The auditor plans and performs the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by fraud or error.

      1) The auditor's initial responsibility regarding errors discovered during a financial statement audit is to assess the risk of misrepresentation.

   b. The types of fraud relevant to the financial statement auditor include misstatements arising from

      1) Fraudulent financial reporting. These are intentional misstatements or omissions to deceive users, such as altering accounting records or documents, misrepresenting or omitting significant information, and misapplying accounting principles.

      2) Misappropriation of assets. These result from theft, embezzlement, or an action that causes payment for items not received.

6. Assessment of Internal Control

a. Many countries require management to provide an assessment of the organization's internal control over financial reporting. Internal auditors assist management in meeting these responsibilities.

b. Control is 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 (The IIA Glossary).

Performance Standard 2130
Control

The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

Implementation Standard 2130.A1

The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

c. Performance Standard 2130 and Implementation Standard 2130.A1 emphasize the internal audit activity's responsibility regarding internal controls.

1) Thus, an internal auditor must not simply assume that controls are adequate and effective.

a) Nondiscovery is most likely to suggest a violation of The IIA's International Professional Practices Framework.

d. Further guidance on the internal audit activity's responsibilities for controls is provided in IG 2130, *Control*:

1) Controls **mitigate risks** at the entity, activity, and transaction levels.

2) The roles and responsibilities are as follows:

a) **Senior management** oversees the establishment, administration, and assessment of the system of controls.

b) **Managers** assess controls within their responsibilities.

c) The **internal auditors** provide assurance about the effectiveness of existing controls.

3) In fulfilling their responsibilities, internal auditors should
   a) Clearly understand control and typical control processes
   b) Consider risk appetite, risk tolerance, and risk culture
   c) Understand (1) the critical risks that could prevent reaching objectives and (2) the controls that mitigate risks
   d) Understand the control framework(s) used
   e) Have a process for planning, auditing, and reporting control problems
4) Evaluating the **effectiveness** of controls
   a) Controls should be assessed relative to risks at each level. A **risk and control matrix** may be useful to
      i) Identify objectives and related risks.
      ii) Determine the significance of risks (impact and likelihood).
      iii) Determine responses to the significant risks (for example, accept, pursue, transfer, mitigate, or avoid).
      iv) Determine key management controls.
      v) Evaluate the adequacy of control design.
      vi) Test adequately designed controls to ascertain whether they have been implemented and are operating effectively.
5) Evaluating the **efficiency** of controls
   a) The internal auditors consider whether management monitors the **costs and benefits** of control. The issue is whether
      i) Resources used exceed the benefits and
      ii) Controls create significant issues (for example, error, delay, or duplication of effort).
   b) The level of a control should be appropriate to the relevant risk.
6) Promoting **continuous improvement**
   a) The chief audit executive (CAE) may recommend a **control framework** if none exists. The internal audit activity also may recommend improvements in the **control environment** (for example, the tone at the top should promote an ethical culture and not tolerate noncompliance).
   b) Continuous improvement of controls involves
      i) Training and ongoing self-monitoring
      ii) Control (or risk and control) assessment meetings with managers
      iii) A logical structure for documentation, analysis, and assessment of design and operation
      iv) Identification, evaluation, and correction of control weaknesses
      v) Informing managers about new issues, laws, and regulations
      vi) Monitoring relevant technical developments

7. **Internal Audit Plan**

    a. The CAE should develop a flexible internal audit plan to provide sufficient evidence to evaluate control. It should permit adjustments during the year. The plan

    1) Covers all major operations, functions, and controls

    2) Gives special consideration to operations most affected by recent or unexpected changes

    3) Considers relevant work performed by others, including management’s assessments of risk management, control, and quality processes and the work completed by external auditors

    b. The CAE evaluates the plan’s coverage.

    1) If the scope of the plan is insufficient to permit expression of an opinion about risk management and control, the CAE informs senior management and the board about gaps in audit coverage.

8. **A Framework for Internal Control**

    a. The assessment of internal control uses a broad definition of control. One source of effective internal control guidance is *Internal Control – Integrated Framework*, published by the Committee of Sponsoring Organizations (COSO).

    1) The COSO model is widely accepted, but it may be appropriate to use some other model recognized worldwide. Also, regulatory or legal requirements may specify a particular model or control design.

    b. In the COSO framework, control has five interrelated components:

    1) **Control activities** are the policies and procedures applied to ensure that management directives are executed and actions are taken to address risks affecting achievement of objectives. Whether automated or manual, they have various objectives and are applied at all levels and functions of the organization. They include

    a) Performance reviews by top managers,

    b) Performance reviews at the functional or activity level,

    c) Analysis of performance indicators,

    d) Controls over information processing (e.g., application controls and general controls),

    e) Physical controls, and

    f) Segregation of duties (separation of the functions of authorization, recordkeeping, and asset custody).

    2) **Risk assessment** is based on a set of complementary operational, financial reporting, and compliance objectives linked across all levels of the organization.

    a) Risk assessment identifies and analyzes external or internal risks affecting achievement of the objectives at the activity level and the entity level.

    3) **Information and communication.** Relevant internal and external information should be identified, captured, and communicated in a timely manner and in appropriate forms.

4) **Monitoring** assesses the quality of a system’s performance over time.

5) The **control environment** reflects the attitude and actions of the board and management regarding the significance of control within the organization.

NOTE: A common memory aid is **CRIME**.

c. The following conclusions by the COSO are relevant:

1) Internal control is defined broadly. It is not limited to accounting controls or financial reporting.

2) Accounting and financial reports are important. However, other matters also are important, such as (a) resource protection; (b) operational efficiency and effectiveness; and (c) compliance with rules, regulations, and organization policies.

a) These factors affect financial reporting.

3) Internal control is management’s responsibility. The participation of all persons within an organization is required if it is to be effective.

4) The control framework should relate to business objectives and be adaptable.

9. Reporting on the Effectiveness of Internal Control

a. The CAE’s report on control processes is usually presented annually to senior management and the board. It describes

1) The role of control processes,
2) The work performed, and
3) Any reliance on other assurance providers.

b. The CAE provides the board an assessment of the effectiveness of the organization’s controls, including the adequacy of the control model or design. The board must rely on management to maintain adequate and effective internal control. It reinforces this reliance with independent oversight.

1) Controls are **effective** if management directs processes to provide reasonable assurance that objectives are achieved.

2) Controls are **adequate** if management has designed them to provide reasonable assurance that (a) risks are managed effectively and (b) objectives are achieved effectively (The IIA Glossary).

c. However, even effective internal controls cannot ensure success. Bad decisions, poor managers, or environmental factors can negate controls. Also, dishonest management may override controls and discourage, ignore, or conceal communications from subordinates.

1) An active and independent board needs open and truthful communications from all components of management. Moreover, the board needs to be assisted by capable financial, legal, and internal audit functions.

a) In these circumstances, the board can identify problems and provide effective oversight.

d. The board or other governance body should request evaluations of internal controls as part of its oversight function. Those evaluations by the internal audit activity depend on answers to the following questions:

1) Is the **ethical environment and culture** strong?

   a) Do board members and senior executives set examples of high integrity?

   b) Are performance and incentive targets realistic, or do they create excessive pressure for short-term results?

   c) Is the organization’s code of conduct reinforced with training and top-down communication? Does the message reach the employees in the field?

   d) Are the organization’s communication channels open? Do all levels of management get the information they need?

   e) Does the organization have zero tolerance for fraudulent financial reporting at any level?

2) How does the organization **identify and manage risks**?

   a) Does the organization have a risk management process, and is it effective?
   b) Is risk managed throughout the organization?
   c) Are major risks candidly discussed with the board?

3) Is the **control system** effective?

   a) Are the organization’s controls over the financial reporting process comprehensive, including preparation of financial statements, related notes, and the other required and discretionary disclosures that are an integral part of the financial reports?

   b) Do senior and line management demonstrate that they accept control responsibility?

   c) Is the frequency of surprises increasing at the senior management, board, or public levels from the organization’s reported financial results or in the accompanying financial disclosures?

   d) Is communication and reporting good throughout the organization?

   e) Are controls seen as enhancing the achievement of objectives or as a necessary evil?

   f) Are qualified people hired promptly, and do they receive adequate training?

   g) Are problems fixed quickly and completely?

4) Is **monitoring** strong?

   a) Is the board independent of management, free of conflicts of interest, well informed, and inquisitive?

   b) Does internal auditing have the support of senior management and the board?

   c) Do the internal and external auditors have and use open lines of communication and private access to all members of senior management and the board?

   d) Is line management monitoring the control process?

   e) Does the organization have a program to monitor outsourced processes?

10. **Roles for the Internal Auditor**

    a. Adequate internal audit resources need to be committed to helping senior management, the board, and the external auditor with their responsibilities relating to financial reporting. Furthermore, the CAE needs to review internal audit's risk assessment and audit plans for the year.

    b. The CAE's allocation of the internal audit activity's resources to the financial reporting, governance, and control processes is consistent with the organization's risk assessment.

        1) The CAE performs procedures that provide a level of assurance to senior management and the board that controls over the processes supporting the development of financial reports are adequately designed and effectively executed.

        2) Controls need to be adequate to ensure the prevention and detection of (a) significant errors; (b) fraud; (c) incorrect assumptions and estimates; and (d) other events that could result in inaccurate or misleading financial statements, related notes, or other disclosures.

    c. The following are lists of suggested topics that the CAE considers in supporting the organization's governance process and the oversight responsibilities of the board:

        1) **Financial Reporting**

            a) Providing information relevant to the appointment of the independent accountants.

            b) Coordinating audit plans, coverage, and scheduling with the external auditors.

            c) Sharing audit results with the external auditors.

            d) Communicating pertinent observations to the external auditors and board about

                i) Accounting policies and policy decisions (including accounting decisions for discretionary items and off-balance-sheet transactions),

                ii) Specific components of the financial reporting process, and

                iii) Unusual or complex financial transactions and events (e.g., related party transactions, mergers and acquisitions, joint ventures, and partnership transactions).

            e) Participating in the financial reports and disclosures review process with the board, external auditors, and senior management.

            f) Evaluating the quality of financial reports, including those filed with regulatory agencies.

            g) Assessing the adequacy and effectiveness of the organization's internal controls, specifically those controls over the financial reporting process.

                i) This assessment considers the organization's susceptibility to fraud and the effectiveness of programs and controls to mitigate or eliminate those exposures.

            h) Monitoring management's compliance with the organization's code of conduct and ensuring that ethical policies and other procedures promoting ethical behavior are being followed.

                i) An important factor in establishing an effective ethical culture in the organization is that members of senior management set a good example of ethical behavior and provide open and truthful communications to employees, the board, and outside stakeholders.

2) **Governance**

   a) Reviewing the organization’s policies relating to

      i) Compliance with laws and regulations,

      ii) Ethics,

      iii) Conflicts of interest, and

      iv) The timely and thorough investigation of misconduct and fraud allegations.

   b) Reviewing pending litigation or regulatory proceedings bearing upon organizational risk and governance.

   c) Providing information on employee conflicts of interest, misconduct, fraud, and other outcomes of the organization’s ethical procedures and reporting mechanisms.

3) **Corporate Control**

   a) Reviewing the reliability and integrity of the operating and financial information compiled and reported by the organization.

   b) Performing an analysis of the controls over critical accounting policies and comparing them with preferred practices.

      i) For example, transactions that raise questions about revenue recognition or off-balance-sheet accounting treatment are reviewed for compliance with appropriate standards, such as International Financial Reporting Standards.

   c) Evaluating the reasonableness of estimates and assumptions used in preparing operating and financial reports.

   d) Ensuring that estimates and assumptions included in disclosures or comments are consistent with underlying organizational information and practices and with similar items reported by other organizations, if appropriate.

   e) Evaluating the process of preparing, reviewing, approving, and posting journal entries.

   f) Evaluating the adequacy of controls in the accounting function.

3.2 ENVIRONMENTAL ENGAGEMENTS

1. **Environmental Risks**
   a. The chief audit executive (CAE) includes **environmental, health, and safety (EHS)** risks in any organization-wide risk management assessment. These activities are assessed in a balanced manner relative to other types of risk associated with an organization's operations. Among the **risk exposures** to be evaluated are the following:
      1) Organizational reporting structures
      2) Likelihood of causing environmental harm, fines, and penalties
      3) Expenditures mandated by governmental agencies
      4) History of injuries and deaths
      5) History of losing customers
      6) Episodes of negative publicity and loss of public image and reputation
2. **Environmental Audit Function**
   a. If the CAE finds that the management of these risks largely depends on an environmental audit function, the CAE needs to consider the implications of that structure and its effects on operations and reporting.
      1) If the CAE finds that the exposures are not adequately managed and residual risks exist, changes in the internal audit activity's plan of engagements and further investigations are normal results.
      2) The typical environmental audit function reports to the organization's environmental component or general counsel. The common models for environmental auditing are the following:
         a) The CAE and environmental audit executive are in separate functional units and have little contact.
         b) The CAE and environmental audit executive are in separate functional units and coordinate their activities.
         c) The CAE has responsibility for auditing environmental issues.

3. **Research Findings**

   a. A research study of EHS auditing found the following risk and independence issues:

      1) The EHS audit function is **isolated** from other auditing activities.

         a) It is (1) organized separately from internal auditing, (2) only tangentially related to external audits of financial statements, and (3) reports to an EHS executive, not to the board or senior management.

         b) This structure suggests that management believes EHS auditing to be a technical field that is best placed within the EHS function. In this position, auditors could be unable to maintain their independence.

      2) EHS audit managers usually report administratively to the executives who are responsible for the physical facilities being audited.

         a) Because poor EHS performance reflects badly on the facilities management team, these executives have an incentive to influence

            i) Audit findings,
            ii) How audits are conducted, or
            iii) What is included in the audit plan.

         b) This potential subordination of the auditors' professional judgment, even when only apparent, violates auditor independence and objectivity.

      3) It is also common for written audit reports to be distributed no higher in the organization than to senior environmental executives.

         a) Those executives may have a potential conflict of interest, and they may prevent or limit further distribution of EHS audit results to senior management and the board.

      4) Audit information is often classified as either (a) subject to the attorney-client privilege or attorney work-product doctrine (if available in the relevant jurisdiction); (b) secret and confidential; or (c) if not confidential, then closely held.

         a) The effect is severely restricted access to EHS audit information.

4. **Role of the CAE**
   a. The CAE fosters a close working relationship with the chief environmental officer and coordinates activities with the plan for environmental auditing.
      1) When the environmental audit function reports to someone other than the CAE, the CAE offers to review the audit plan and the performance of engagements.
      2) Periodically, the CAE schedules a quality assurance review of the environmental audit function if it is organizationally independent of the internal audit activity. That review determines whether environmental risks are being adequately addressed.
      3) An EHS audit program may be
         a) **Compliance-focused** (verifying compliance with laws, regulations, and the organization’s own EHS policies, procedures, and performance objectives),
         b) **Management systems-focused** (providing assessments of management systems intended to ensure compliance with legal and internal requirements and the mitigation of risks), or
         c) A **combination** of both approaches.
   b. The CAE evaluates whether the environmental auditors, who are not part of the CAE’s organization, are conforming with recognized professional auditing standards and a recognized code of ethics.
   c. The CAE evaluates the organizational placement and independence of the environmental audit function to ensure that significant matters resulting from serious risks to the organization are reported up the chain of command to the board.
      1) The CAE also facilitates the reporting of significant EHS risk and control issues to the board.

      NOTE: The internal audit activity has an established place in the organization and normally has a broad scope of work permitting ready assimilation of the new function. Thus, it is an advantage to conduct environmental audits under the direction of the internal audit activity because of its position within the organization.

5. **Environmental Auditing**
   a. An organization subject to environmental laws and regulations having a significant effect on its operations should establish an environmental management system.
      1) One feature of this system is environmental auditing, which includes reviewing the adequacy and effectiveness of the controls over hazardous waste. It also extends to review of the reasonableness of contingent liabilities accrued for environmental remediation.
   b. According to a research report prepared for The IIA Research Foundation,

      *An **environmental management system** is an organization’s structure of responsibilities and policies, practices, procedures, processes, and resources for protecting the environment and managing environmental issues. Environmental auditing is an integral part of an environmental management system whereby management determines whether the organization’s environmental control systems are adequate to ensure compliance with regulatory requirements and internal policies.*

c. The report describes seven types of environmental audits:

1) **Compliance audits** are the most common form for industrial organizations. Their extent depends on the degree of risk of noncompliance.

   a) They are detailed, site-specific audits of current operations, past practices, and planned future operations.

   b) They usually involve a review of all environmental media the site may contaminate, including air, water, land, and wastewater. Moreover, they have quantitative and qualitative aspects and should be repeated periodically.

   c) Compliance audits range from preliminary assessments to

      i) Performance of detailed tests,
      ii) Installation of groundwater monitoring wells, and
      iii) Laboratory analyses.

2) **Environmental management systems audits** determine whether systems are in place and operating properly to manage future environmental risks.

   a) Environmental issues may arise from practices that were legal when they were undertaken.

3) **Transactional audits** assess the environmental risks and liabilities of land or facilities prior to a property sale or purchase. Current landowners may be responsible for contamination whether or not they caused it.

   a) Transactional audits require due diligence (a reasonable level of research) from the auditor. What constitutes due diligence for each phase of a transactional audit and the definitions of the phases are questions for debate. These phases are often characterized as follows:

      i) Phase I – qualitative site assessments involving a review of records and site reconnaissance

      ii) Phase II – sampling for potential contamination

      iii) Phase III – confirming the rate and extent of contaminant migration and the cost of remediation

   b) A transactional audit addresses all media exposures and all hazardous substances, e.g., radon, asbestos, PCBs, operating materials, and wastes.

4) **Treatment, storage, and disposal facility (TSDF) audits.** The law may require that hazardous materials be tracked from their acquisition or creation to disposal by means of a document (a manifest). All owners in the chain of title may be liable.

   a) For example, if an organization contracts with a transporter to dispose of hazardous waste in a licensed landfill and the landfill owner contaminates the environment, all the organizations and their officers may be financially liable for cleanup.

   b) TSDF audits are conducted on facilities the organization owns, leases, or manages, or on externally owned facilities where the organization's waste is treated, stored, or disposed. Thus, when an outside vendor is used for these purposes, the audit should consist of such procedures as

      i) Reviewing the vendor's documentation on hazardous material,

      ii) Reviewing the financial solvency of the vendors,

      iii) Reviewing the vendor's emergency response planning,

      iv) Determining that the vendor is approved by the governmental organization that is responsible for environmental protection,

      v) Obtaining the vendor's permit number, and

      vi) Inspecting the vendor's facilities.

5) A **pollution prevention audit** determines how waste can be minimized and pollution can be eliminated at the source. The following is a **pollution prevention hierarchy** from most desirable (recovery) to least (release without treatment):

   a) Recovery as a usable product
   b) Elimination at the source
   c) Recycling and reuse
   d) Energy conservation
   e) Treatment
   f) Disposal
   g) Release without treatment

6) **Environmental liability accrual audits.** Recognizing, quantifying, and reporting liability accruals may require redefinition of what is probable, measurable, and estimable. When an environmental issue becomes a liability is also unclear.

   a) The internal auditors may be responsible for assessing the reasonableness of cost estimates for environmental remediation. Due diligence may require assistance from independent experts, such as engineers.

7) **Product audits** determine whether products are environmentally friendly and whether product and chemical restrictions are being met. This process may result in the development of

   a) Fully recyclable products,
   b) Changes in the use and recovery of packaging materials, and
   c) The phaseout of some chemicals.

3.3 CONSULTING ENGAGEMENTS -- OVERVIEW

1. **Definition**

   a. **Consulting services** are "advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training" (The IIA Glossary).

> **Implementation Standard 1000.C1**
>
> The nature of consulting services must be defined in the internal audit charter.

      1) The nature and scope of the consulting engagement are subject to agreement with the engagement client.

      2) The IIA's Consulting Implementation Standards describe the requirements of consulting engagements. The related outlines are based on IIA publications.

2. **Principles Applied to Internal Auditors' Consulting Activities**

   a. **Value Proposition** – The value proposition of the internal audit activity is realized within every organization that employs internal auditors in a manner that suits the culture and resources of that organization.

      1) That value proposition is captured in the definition of internal auditing and includes assurance and consulting activities designed to add value to the organization by bringing a systematic, disciplined approach to the areas of governance, risk, and control.

   b. **Consistency with Internal Audit Definition** – A disciplined, systematic evaluation methodology is incorporated in each internal audit activity.

      1) The list of services can generally be incorporated into the broad categories of assurance and consulting. However, the services also may include evolving forms of value-adding services that are consistent with the broad definition of internal auditing.

   c. **Audit Activities beyond Assurance and Consulting** – Assurance and consulting are not mutually exclusive and do not preclude other internal audit services, such as investigations and nonaudit roles.

      1) Many audit services will have both an assurance and consultative (advising) role.

   d. **Interrelationship between Assurance and Consulting** – Internal audit consulting enriches value-adding internal auditing.

      1) While consulting is often the direct result of assurance services, assurance also could result from consulting engagements.

e. **Empower Consulting through the Internal Audit Charter** – Internal auditors have traditionally performed many types of consulting services, including the analysis of controls built into developing systems, analysis of security products, serving on task forces to analyze operations and make recommendations, and so forth.

   1) The board empowers the internal audit activity to perform additional services if they do not represent a conflict of interest or detract from its obligations to the board. That empowerment is reflected in the internal audit charter.

f. **Objectivity** – Consulting services may enhance the auditor’s understanding of business processes or issues related to an assurance engagement and do not necessarily impair the auditor’s or the internal audit activity’s objectivity.

   1) Internal auditing is not a management decision-making function. Decisions to adopt or implement recommendations made as a result of an internal audit advisory service are made by management.

   2) Therefore, internal audit objectivity is not impaired by the decisions made by management.

g. **Internal Audit Foundation for Consulting Services** – Much of consulting is a natural extension of assurance and investigative services and may represent informal or formal advice, analysis, or assessments.

   1) The internal audit activity is uniquely positioned to perform this type of consulting work based on (a) its adherence to the highest standards of objectivity and (b) its breadth of knowledge about organizational processes, risk, and strategies.

h. **Communication of Fundamental Information** – A primary internal audit value is to provide **assurance** to senior management and the board.

   1) Consulting engagements cannot be performed in a manner that masks information that, in the judgment of the chief audit executive (CAE), should be presented to senior executives and board members. All consulting is to be understood in that context.

i. **Principles of Consulting Understood by the Organization** – Organizations must have ground rules for the performance of consulting services that are understood by all members of an organization.

   1) These rules are codified in the audit charter approved by the board and issued within the organization.

j. **Formal Consulting Engagements** – Management often engages external consultants for formal consulting engagements that last a significant period of time. However, an organization may find that the internal audit activity is uniquely qualified for some formal consulting tasks.

   1) If an internal audit activity undertakes to perform a formal consulting engagement, the internal audit group brings a systematic, disciplined approach to the conduct of the engagement.

k. **CAE Responsibilities** – Consulting services permit the CAE to enter into dialogue with management to address specific managerial issues. In this dialogue, the breadth of the engagement and time frames are made responsive to management needs.

1) However, the CAE retains the prerogative of setting the audit techniques and the right of reporting to senior executives and the board when the nature and materiality of results pose significant risks to the organization.

l. **Criteria for Resolving Conflicts or Evolving Issues** – An internal auditor is first and foremost an internal auditor.

1) Thus, in the performance of all services, the internal auditor is guided by The IIA Code of Ethics and the Attribute and Performance Standards of the *International Standards for the Professional Practice of Internal Auditing*.

2) The resolution of any unforeseen conflicts of activities needs to be consistent with the Code of Ethics and the *Standards*.

3. **Classification of Engagements**

Implementation Standard 2010.C1

The chief audit executive should consider accepting proposed consulting engagements based on the engagement’s potential to improve management of risks, add value, and improve the organization’s operations. Accepted engagements must be included in the plan.

Implementation Standard 2120.C1

During consulting engagements, internal auditors must address risk consistent with the engagement’s objectives and be alert to the existence of other significant risks.

Implementation Standard 2120.C2

Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization’s risk management processes.

Implementation Standard 2120.C3

When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

Implementation Standard 2130.C1

Internal auditors must incorporate knowledge of controls gained from consulting engagements into evaluation of the organization’s control processes.

a. The chief audit executive determines the methodology to use for classifying engagements within the organization.

   1) In some circumstances, it may be appropriate to conduct a blended engagement that incorporates elements of both consulting and assurance activities into one consolidated approach.

   2) In other cases, it may be appropriate to distinguish between the assurance and consulting components of the engagement.

b. Internal auditors may conduct consulting services as part of their normal or routine activities as well as in response to requests by management. Each organization considers the type of consulting activities to be offered and determines whether specific policies or procedures need to be developed for each type of activity. Possible categories include the following:

   1) **Formal consulting** engagements are planned and subject to written agreement.

   2) **Informal consulting** engagements involve routine activities, such as (a) participation on standing committees, (b) limited-life projects, (c) ad-hoc meetings, and (d) routine information exchange.

   3) **Special consulting** engagements include participation on a merger and acquisition team or system conversion team.

   4) **Emergency consulting** engagements include participation on a team (a) established for recovery or maintenance of operations after a disaster or other extraordinary business event or (b) assembled to supply temporary help to meet a special request or unusual deadline.

c. Auditors generally should not agree to conduct a consulting engagement simply to circumvent, or to allow others to circumvent, requirements that would normally apply to an assurance engagement if the service in question is more appropriately conducted as an assurance engagement. This does not preclude adjusting methods if services once conducted as assurance engagements are deemed more suitable to being performed as a consulting engagement.

3.4 CONSULTING ENGAGEMENTS -- INTERNAL AUDITOR

1. Independence and Objectivity

Implementation Standard 1130.C1

Internal auditors may provide consulting services relating to operations for which they had previous responsibilities.

Implementation Standard 1130.C2

If internal auditors have potential impairments to independence or objectivity relating to proposed consulting services, disclosure must be made to the engagement client prior to accepting the engagement.

a. Internal auditors are sometimes requested to provide consulting services relating to operations for which they had previous responsibilities or had conducted assurance services.

   1) Prior to offering consulting services, the chief audit executive (CAE) confirms that the board understands and approves the concept of providing consulting services.

   2) Once approved, the internal audit charter is amended to include authority and responsibilities for consulting activities, and the internal audit activity develops appropriate policies and procedures for conducting such engagements.

b. Internal auditors maintain their objectivity when drawing conclusions and offering advice to management.

   1) If impairments to independence or objectivity exist prior to commencement of the consulting engagement, or subsequently develop during the engagement, disclosure is made immediately to management.

c. Independence and objectivity may be impaired if assurance services are provided within 1 year after a formal consulting engagement. Steps can be taken to minimize the effects of impairment by

   1) Assigning different auditors to perform each of the services,

   2) Establishing independent management and supervision,

   3) Defining separate accountability for the results of the projects, and

   4) Disclosing the presumed impairment. Management is responsible for accepting and implementing recommendations.

d. Care is taken, particularly involving consulting engagements that are ongoing or continuous in nature, so that internal auditors do not inappropriately or unintentionally assume management responsibilities that were not intended in the original objectives and scope of the engagement.

2. Due Professional Care

Implementation Standard 1210.C1

The chief audit executive must decline the consulting engagement or obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

Implementation Standard 1220.C1

Internal auditors must exercise due professional care during a consulting engagement by considering the:

- Needs and expectations of clients, including the nature, timing, and communication of engagement results;
- Relative complexity and extent of work needed to achieve the engagement's objectives; and
- Cost of the consulting engagement in relation to potential benefits.

a. The internal auditor exercises due professional care in conducting a formal consulting engagement by understanding the following:

  1) Needs of management officials, including the nature, timing, and communication of engagement results
  2) Possible motivations and reasons of those requesting the service
  3) Extent of work needed to achieve the engagement's objectives
  4) Skills and resources needed to conduct the engagement
  5) Effect on the scope of the audit plan previously approved by the audit committee
  6) Potential impact on future audit assignments and engagements
  7) Potential organizational benefits to be derived from the engagement

b. In addition to the independence and objectivity evaluation and due professional care considerations, the internal auditor

  1) Conducts appropriate meetings and gathers necessary information to assess the nature and extent of the service to be provided.
  2) Confirms that those receiving the service understand and agree with (a) the relevant guidance contained in the internal audit charter, (b) internal audit activity's policies and procedures, and (c) other related guidance for consulting engagements.

    a) The internal auditor declines to perform consulting engagements that

      i) Are prohibited by the charter,
      ii) Conflict with the policies and procedures of the internal audit activity, or
      iii) Do not add value and promote the best interests of the organization.

  3) Evaluates the consulting engagement for compatibility with the internal audit activity's overall plan of engagements. The risk-based plan of engagements may incorporate and rely on consulting engagements, to the extent deemed appropriate, to provide necessary audit coverage.
  4) Documents general terms, understandings, deliverables, and other key factors of the formal consulting engagement in a written agreement or plan. It is essential that the internal auditor and those receiving the consulting engagement understand and agree with the reporting and communication requirements.

3. Scope of Work

Implementation Standard 2201.C1

Internal auditors must establish an understanding with consulting engagement clients about objectives, scope, respective responsibilities, and other client expectations. For significant engagements, this understanding must be documented.

Implementation Standard 2210.C1

Consulting engagement objectives must address governance, risk management, and control processes to the extent agreed upon with the client.

Implementation Standard 2210.C2

Consulting engagement objectives must be consistent with the organization's values, strategies, and objectives.

Implementation Standard 2220.C1

In performing consulting engagements, internal auditors must ensure that the scope of the engagement is sufficient to address the agreed-upon objectives. If internal auditors develop reservations about the scope during the engagement, these reservations must be discussed with the client to determine whether to continue with the engagement.

a. Internal auditors design the scope of work to ensure that the professionalism, integrity, credibility, and reputation of the internal audit activity will be maintained.

b. In planning formal consulting engagements, internal auditors design objectives to meet the appropriate needs of management officials receiving these services. If management makes special requests and the internal auditor believes the objectives that need to be pursued go beyond those requested by management, the internal auditor may consider

   1) Persuading management to include the additional objectives in the consulting engagement or

   2) Documenting the failure to pursue the objectives, disclosing that observation in the final communication of consulting engagement results, and including the objectives in a separate and subsequent assurance engagement.

Implementation Standard 2240.C1

Work programs for consulting engagements may vary in form and content depending upon the nature of the engagement.

c. **Work programs** for formal consulting engagements document the objectives and scope of the engagement and the methods to be used in satisfying the objectives.

   1) In establishing the scope of the engagement, internal auditors may expand or limit the scope to satisfy management. However, the internal auditor needs to be satisfied that the projected scope of work will be adequate to meet the objectives of the engagement.

   2) The objectives, scope, and terms of the engagement are periodically reassessed and adjusted during the course of the work.

Implementation Standard 2220.C2

During consulting engagements, internal auditors must address controls consistent with the engagement's objectives and be alert to significant control issues.

d. Internal auditors are observant of the effectiveness of risk management and control processes during formal consulting engagements. Substantial risk exposures or material control weaknesses are reported to management.

1) In some situations, the auditor's concerns also are communicated to senior management or the board. (According to The IIA Glossary, the board includes any "designated body of the organization, including the audit committee.")

2) Auditors determine

a) The significance of exposures or weaknesses and the actions taken or contemplated to mitigate or correct and

b) The expectations of senior management and the board about reporting.

4. **Communicating Results**

Implementation Standard 2410.C1

Communication of the progress and results of consulting engagements will vary in form and content depending upon the nature of the engagement and the needs of the client.

Implementation Standard 2440.C1

The chief audit executive is responsible for communicating the final results of consulting engagements to clients.

Implementation Standard 2440.C2

During consulting engagements, governance, risk management, and control issues may be identified. Whenever these issues are significant to the organization, they must be communicated to senior management and the board.

a. Reporting requirements are generally determined by those requesting the consulting service and meet the objectives as determined and agreed to with management.

1) However, the format for communicating the results clearly describes the nature of the engagement and any limitations, restrictions, or other factors about which users of the information need to be made aware.

b. In some circumstances, the internal auditor may communicate results beyond those who received or requested the service. In such cases, the internal auditor expands the reporting so that results are communicated to the appropriate parties. The auditor therefore takes the following steps until satisfied with the resolution of the matter:

   1) Determine what direction is provided in the agreement concerning the consulting engagement and related communications.

   2) Attempt to persuade those receiving or requesting the service to expand the communication to the appropriate parties.

   3) Determine what guidance is provided in the internal audit charter or the internal audit activity's policies and procedures concerning consulting communications.

   4) Determine what guidance is provided in the organization's code of conduct, code of ethics, and other related policies, administrative directives, or procedures.

   5) Determine what guidance is provided by The IIA's *Standards* and Code of Ethics, other standards or codes applicable to the auditor, and any legal or regulatory requirements that relate to the matter under consideration.

c. Internal auditors disclose to management, the board, or other governing body of the organization the nature, extent, and overall results of formal consulting engagements along with other reports of internal audit activities. Internal auditors keep management and the board informed about how audit resources are being deployed.

   1) Neither detail reports of these consulting engagements nor the specific results and recommendations are required to be communicated.

      a) But an appropriate description of these types of engagements and their significant recommendations are communicated.

      b) This communication is essential in satisfying the CAE's responsibility to comply with Performance Standard 2060, *Reporting to Senior Management and the Board*.

5. **Documentation**

> **Implementation Standard 2330.C1**
>
> The chief audit executive must develop policies governing the custody and retention of consulting engagement records, as well as their release to internal and external parties. These policies must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

a. Documentation requirements for assurance engagements do not necessarily apply to consulting engagements.

b. In formal consulting engagements, auditors adopt appropriate record retention policies and address such related issues as ownership of the engagement records.

   1) Legal, regulatory, tax, and accounting matters may require special treatment in the records.

6. **Monitoring**

> **Implementation Standard 2500.C1**
>
> The internal audit activity must monitor the disposition of results of consulting engagements to the extent agreed upon with the client.

a. Varying types of monitoring may be appropriate for differing types of consulting engagements.

b. The monitoring effort may depend on various factors, such as management's explicit interest in the engagement or the internal auditor's assessment of the project's risks or value to the organization.

3.5 CONSULTING ENGAGEMENTS -- BENCHMARKING

1. **Benchmarking**

a. Benchmarking is one of the primary tools used in total quality management (TQM). It is a means of helping organizations with productivity management and business process review. It is therefore a source of consulting engagements for internal auditors.

b. Benchmarking is a continuous evaluation of the practices of the best organizations in their class and the adaptation of processes to reflect the best of these practices.

1) It involves

a) Analyzing and measuring key outputs against those of the best organizations and

b) Identifying the underlying key actions and causes that contribute to the performance difference.

2) **Best practices** are recognized by authorities in the field and by customers for generating outstanding results. They are generally innovative technically or in their management of human resources.

3) Benchmarking is an ongoing process that involves quantitative and qualitative measurement of the difference between the organization's performance of an activity and the performance by the benchmark organization.

c. The following are kinds of benchmarking:

1) **Competitive** benchmarking studies an organization in the same industry.

2) **Process (function)** benchmarking studies operations of organizations with similar processes regardless of industry. Thus, the benchmark need not be a competitor or even a similar organization.

   a) This method may introduce new ideas that provide a significant competitive advantage.

3) **Strategic** benchmarking is a search for successful competitive strategies.

4) **Internal** benchmarking is the application of best practices in one part of the organization to its other parts.

5) **Generic** benchmarking observes a process in one operation and compares it with a process having similar characteristics but in a different industry.

d. The first phase in the benchmarking process is to select and prioritize benchmarking projects.

1) An organization must understand its critical success factors and business environment to identify key business processes and drivers and to develop parameters defining what processes to benchmark.

2) The criteria for selecting what to benchmark are based mostly on satisfaction of customer needs.

e. The next phase is to organize benchmarking teams. A team organization is appropriate because it permits a fair division of labor, participation by those responsible for implementing changes, and inclusion of a variety of functional expertise and work experience.

1) The benchmarking team must thoroughly investigate and document the organization’s internal processes.

   a) The team must develop a family of measures that are true indicators of process performance.

   b) The development of key indicators for performance measurement in a benchmarking context is an extension of the basic evaluative function of internal auditors.

f. Researching and identifying best-in-class performance is often the most difficult phase. The critical steps are

1) Setting up databases,

2) Choosing information-gathering methods (internal sources, external public domain sources, and original research),

3) Formatting questionnaires (lists of questions prepared in advance), and

4) Selecting benchmarking partners.

g. Data analysis involves identifying performance gaps, understanding the reasons, and prioritizing the key activities that will facilitate the behavioral and process changes needed to implement recommendations.

h. Leadership is most important in the implementation phase because the team must justify its recommendations. Moreover, the process improvement teams must manage the implementation of approved changes.

3.6 CONSULTING ENGAGEMENTS -- OTHER TYPES

1. **Internal Control Training**

   a. Internal auditors may perform consulting engagements to provide internal control training to the employees of the organization.

      1) Such training may involve instruction about the organization's objectives, policies, standards, procedures, performance measurements, and feedback methods.

      2) In addition to providing courses for client personnel, the internal audit activity may offer internships to some new managers. Among other things, these managers gain experience in assessing controls.

   b. As part of their coordination with external auditors, the internal auditors may provide opportunities for joint control training and other matters.

   c. Internal auditors also should undergo internal control training, for example, with regard to control frameworks, specific controls and control objectives, standards, technological developments, and new professional literature.

   d. Control self-assessment provides training for people in business units. Participants gain experience in assessing risks and associating control processes with managing those risks and improving the chances of achieving business objectives.

   e. The ethical culture of an organization is linked to the governance process and is the most important soft control.

      1) Internal auditors have many roles in supporting the ethical culture, including those of ethics counselor and ethics expert.

2. **Due Diligence Auditing**

   a. The term "due diligence" is applied to a service in which internal auditors and others (external auditors, tax experts, finance professionals, attorneys, etc.) determine the business justification for a major transaction (business combination, joint venture, divestiture, etc.) and whether that justification is valid.

      1) Internal auditors might, for example, review operations (purchasing, shipping and receiving, inventory management, etc.), internal control over information systems, the compatibility of the organizational cultures, and finance and accounting issues.

      2) The term "due diligence" also may be used for other engagements, for example, certain environmental audits.

   b. The due diligence process establishes whether the expected benefits of the transaction (wider markets, more skilled employees, access to intellectual property, operating synergies, etc.) are likely to be realized.

      1) It also may facilitate the realization of those benefits by improving the effectiveness and efficiency of the implementation of the transaction.

   c. One of the keys to the effectiveness and efficiency of the engagement is coordination among the groups involved. For example, the same software should be used for preparation of electronic workpapers to facilitate sharing of information.

   d. The final report should be factual, not subjective, with supporting information indexed and backed up on computer disks.

      1) The report should contain an executive summary with key points highlighted.

      2) The cycle approach used by the acquiring organization to organize its business is a desirable means of structuring the report.

3. **Business Process Mapping**

   a. One approach to business process mapping (review) is **reengineering** (also called business process reengineering). It involves process innovation and core process redesign. Instead of improving existing procedures, it finds new ways of doing things.

      1) The emphasis is on simplification and elimination of nonvalue-adding activities. Thus, reengineering is not continuous improvement, it is not simply downsizing or modifying an existing system, and it should be reserved for the most important processes.

      2) An organization may need to adapt quickly and radically to change. Thus, reengineering is usually a cross-departmental process of innovation requiring substantial investment in information technology and retraining.

         a) Successful reengineering may bring dramatic improvements in customer service and the speed with which new products are introduced.

   b. One well-known tool useful in reengineering is **work measurement**, a process that involves analysis of activities. The nature and extent of a task, the procedures needed for its execution, and the efficiency with which it is carried out are determined by work measurement.

      1) This technique is appropriate when management takes an engineered-cost approach to control. Such an approach is indicated when the workload is divisible into control-factor units, for example, accounting entries made, lines of text word processed, or number of packages shipped. The cost of a control-factor unit is treated as a variable cost for budgeting purposes.

      2) One method used for work measurement is micromotion study, which requires videotaping the performance of a job, e.g., assembly-line activities.

      3) Another method is work sampling, making many random observations of an activity to determine what steps it normally requires.

   c. Reengineering and total quality management (TQM) techniques (TQM is discussed in Study Unit 2, Subunit 4) eliminate many traditional controls. They exploit modern technology to improve productivity and decrease the number of clerical workers. Thus, the emphasis is on developing controls that are automated and self-correcting and that require minimal human intervention.

      1) The emphasis shifts to monitoring internal control so management can determine when an operation may be out of control and corrective action is needed.

         a) Most reengineering and TQM techniques also assume that humans will be motivated to work actively in improving operations when they are full participants in the process.

      2) Monitoring assesses the quality of internal control over time. Management considers whether internal control is properly designed and operating as intended and modifies it to reflect changing conditions. Monitoring may be in the form of separate, periodic evaluations or of ongoing monitoring.

         a) Ongoing monitoring occurs as part of routine operations. It includes management and supervisory review, comparisons, reconciliations, and other actions by personnel as part of their regular activities.

d. Internal auditors may perform the functions of determining whether the reengineering process has senior management's support, recommending areas for consideration, and developing audit plans for the new system. However, they should not become directly involved in the implementation of the process. This involvement would impair their independence and objectivity.

4. **System Development Reviews**

   a. Internal auditor involvement throughout the systems development life cycle can ensure that the appropriate internal controls and audit trails are included in the application. According to The IIA's *GTAG Auditing IT Projects*, "Internal auditing can bring the value of their experience and methodology to review projects in the early stages to also help increase the likelihood of success." Benefits of internal audit involvement may include

      1) Providing independent, ongoing advice throughout the project and

      2) Identifying key risks or issues early, which enables project teams to operate proactively to mitigate risks.

   b. The section for systems development and acquisition controls in *GTAG Information Technology Risks and Controls* is useful for understanding the role of the internal auditor.

      1) It states that "the IT auditor should assess whether the organization uses a controlled method to develop or acquire application systems and whether it delivers effective controls over and within the applications and data they process. By examining application development procedures, the auditor can gain assurance that application controls are adequate. Some basic control issues should be addressed in all systems development and acquisition work. For example,

         a) User requirements should be documented, and their achievement should be measured.

         b) Systems design should follow a formal process to ensure that user requirements and controls are designed into the system.

         c) Systems development should be conducted in a structured manner to ensure that requirements and approved design features are incorporated into the finished product.

         d) Testing should ensure that individual system elements work as required, system interfaces operate as expected, and that the system owner has confirmed that the intended functionality has been provided.

         e) Application maintenance processes should ensure that changes in application systems follow a consistent pattern of control. Change management should be subject to structured assurance validation processes."

   c. If "systems development is outsourced, the outsourcer or provider contracts should require similar controls. Project management techniques and controls should be part of the development process—whether developments are performed in-house or are outsourced. Management should know whether projects are on time and within budget and that resources are used efficiently. Reporting processes should ensure that management understands the current status of development projects and does not receive any surprises when the end product is delivered."

5. **Design of Performance Measurement Systems**

   a. As an assurance engagement, internal auditors conduct performance audits to measure how well an organization is achieving its targets for its key performance indicators.

   b. As a consulting engagement, internal auditors work with clients to improve the performance measured by the key performance indicators.

STUDY UNIT FOUR

THE INTERNAL AUDIT PLAN

This study unit is the fourth of four covering **Domain I: Managing the Internal Audit Activity** from The IIA's CIA Exam Syllabus. This domain makes up 20% of Part 2 of the CIA exam and is tested at the **basic** and **proficient** cognitive levels. Refer to the complete syllabus located in Appendix B to view the relevant sections covered in Study Unit 4.

4.1 RISK-BASED AUDIT PLAN

1. **Risk**
    a. According to The IIA Glossary, risk is the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.
2. **Priorities Based on the Risk Assessment**
    a. The large, complex, interconnected organizations in the modern economy require sophisticated assessment of many diverse risks. Thus, the audit plan of any internal audit activity must reflect the organization's assessment of these risks.
        1) The knowledge, skills, and other competencies of the internal auditors affect what engagements can be performed without using external service providers.
        2) However, the knowledge, skills, and other competencies of the internal auditors do not affect the risk assessment.
    b. The audit plan must be logically related to identified risks of the organization. These risks relate to the organization's strategic and operational goals. Making this connection between identified risks and how they relate to strategic and operational goals is a requirement of risk-based audit planning. This requirement is stated in the following standard:

Performance Standard 2010
Planning

The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.

    c. The purpose of establishing an internal audit plan is to ensure adequate coverage of areas with greatest exposure to risks.
        1) Accordingly, the priorities of the internal audit activity are based on the results of risk assessments. The chief audit executive (CAE) should generally assign engagement priorities to activities with higher risks.
        2) The internal audit activity must prioritize to make decisions for applying resources.

d. The importance of basing the audit work plan on a systematic assessment of risk is emphasized in the following Interpretation and Implementation Standards:

Interpretation of Standard 2010

To develop the risk-based plan, the chief audit executive consults with senior management and the board and obtains an understanding of the organization's strategies, key business objectives, associated risks, and risk management processes. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.

Implementation Standard 2010.A1

The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.

e. In developing the risk-based plan, the internal audit activity ordinarily reviews and corroborates the results of risk assessments performed by senior management.

    1) The key input in the evaluation of risk is the internal auditor's judgment.

f. Planning also involves considering what services stakeholders want.

Implementation Standard 2010.A2

The chief audit executive must identify and consider the expectations of senior management, the board, and other stakeholders for internal audit opinions and other conclusions.

g. Planning for consulting services involves considering what benefits these engagements may offer.

Implementation Standard 2010.C1

The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Accepted engagements must be included in the plan.

h. The goals of the internal audit activity should be capable of accomplishment within given operating plans and budgets and should be measurable to the extent possible.

    1) They should be accompanied by measurement criteria and targeted dates of accomplishment.

3. **The Risk-Based Audit Plan**

   a. Developing the internal audit activity's audit plan often follows developing or updating the audit universe.

      1) The **audit universe** (all auditable risk areas) may include the organization's strategic plan. Thus, it may reflect

         a) Overall business objectives,
         b) The attitude toward risk,
         c) The difficulty of reaching objectives,
         d) The results of risk management, and
         e) The operating environment.

      2) The audit universe includes all business units, processes, or operations that can be evaluated and defined. They include accounts, divisions, functions, procedures, products, services, programs, systems, controls, and many other possibilities.

         a) Thus, the audit plan includes audits requested by management or required by regulators, e.g., as a condition of receiving government contracts.

         b) Moreover, many entity operations or functions are audited cyclically. Accordingly, the priority of an audit may depend on how recently a specific operation or function has been audited.

      3) The audit universe should be assessed **at least annually** to reflect the most current strategies and direction of the organization.

         a) But more frequent updating of audit plans may be needed to respond to changes in circumstances.

   b. The internal audit activity's **audit plan** is based on

      1) The audit universe,
      2) Input from senior management and the board, and
      3) Assessed risks.

   c. An internal audit plan usually is prepared for an annual period. But it might be for a rolling 12-month cycle or two or more years with annual evaluation. The plan most often includes

      1) A set of proposed assurance and consulting engagements.

      2) The basis for inclusion of each engagement (e.g., risk or time elapsed from the most recent audit).

      3) The objective and scope of each proposed engagement.

      4) Projects derived from the internal audit activity's strategy.

   d. Key audit objectives are to provide assurance and information to senior management and the board.

      1) Assurance includes an assessment of **risk management activities**.

e. **Work schedules** are based on, among other factors, an assessment of risk and exposure.

1) Most **risk models** address internal and external risks using risk factors to prioritize engagements.

a) Internal risk factors include quality of and adherence to controls, degree of change, timing and results of last engagement, impact, likelihood, materiality, asset liquidity, and management competence.

b) External risk factors include competitor actions, suppliers, industry issues, and employee and government relations.

c) An unexpected, significant change in an account that cannot be explained raises the assessed risk for that account.

4. **Risk Management Process**

a. The plan of engagements must consider the organization’s risk management process.

1) The IIA Glossary defines risk management as a process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization’s objectives.

2) **Risk management (RM)** is critical to sound governance of all organizational activities. Consistent RM should be fully integrated into management at all levels.

a) Management typically uses a framework (e.g., COSO, ERM, ISO 31000) to conduct the risk assessment and document the results.

b) The chief audit executive takes into account the organization’s risk management framework. If a framework does not exist, the chief audit executive uses his or her own judgment of risks after consultation with senior management and the board.

3) Effective RM assists in identifying key controls related to significant inherent risks.

a) Control is often used to manage risk within the risk appetite. Internal auditors audit key controls and provide assurance on the management of significant risks.

4) Inherent risk and residual risk (also known as current risk) are fundamental risk concepts.

a) Financial (external) auditors define **inherent risk** as the susceptibility of information or data to a material misstatement given no related mitigating controls.

b) Current risk is the risk managed within existing controls or control systems.

5) Key controls reduce an otherwise unacceptable risk to a tolerable level. Controls are processes that address risks.

a) Effective RM identifies key controls based on the difference between inherent and residual risk across all affected systems. Key controls are relied upon to reduce the rating of significant risks.

b) When identifying key controls (and if RM is mature and reliable), the internal auditor looks for

i) Individual risk factors when the reduction from inherent to residual risk is significant (particularly if inherent risk was very high).

ii) Controls that mitigate a large number of risks.

6) Audit planning uses the organizational RM process if one exists. The internal auditor considers the significant risks of the activity and the means by which management mitigates the risks.
   a) Risk assessment methods are used to develop the audit plan and to determine priorities for allocating audit resources.
   b) Risk assessment examines auditable units and selects areas for review that have the greatest risk exposure.
7) The following factors affect the internal audit plan:
   a) Inherent and residual risks should be identified and assessed.
   b) Mitigating controls, contingency plans, and monitoring activities should be linked to events or risks.
   c) Risk registers should be systematic, complete, and accurate.
      i) A **risk register** (risk log) identifies and analyzes risks. The register (a) describes each risk, its impact and likelihood, and the risk score (Impact × Likelihood) and (b) records planned responses if the event occurs, preventive measures, and a risk ranking.
      ii) Risk registers may document risks below the strategic level. They address (a) significant risks, (b) inherent and residual risk ratings, (c) key controls, and (d) mitigating factors.
         - The auditors then can identify more direct links between (1) risk categories and aspects described in the risk registers and, (2) if applicable, the items already in the audit universe.
   d) Risks and activities should be documented.
8) The internal auditor also coordinates with other assurance providers and considers planned reliance on their work.
9) The internal audit activity needs to identify high inherent and residual risks and key control systems, and management needs to be notified about unacceptable residual risk.
   a) Strategic audit planning identifies the following activities to include in the plan:
      i) Control reviews to provide assurance
      ii) Inquiry activities to gain a better understanding of the residual risk
      iii) Consulting activities to give advice on controls to mitigate unacceptable risks
   b) Internal auditors also identify controls with costs exceeding benefits.
10) Lower-risk audits need to be included in the audit plan to give them coverage and confirm that their risks have not changed.
   a) Also, priorities should be set for outstanding risks not yet subject to audit.
11) An internal audit plan normally focuses on the following:
   a) Unacceptable current risks requiring management action
   b) Control systems on which the organization is most reliant
   c) Areas where the difference between inherent risk and residual risk is great
   d) Areas where inherent risk is very high
12) When planning individual audits, the internal auditor identifies and assesses risks relevant to the area under review.

13) Due professional care requires work assignments to be proportional to the complexities of the engagement and must ensure that the technical proficiency and educational background of the personnel assigned are appropriate.

a) A risk and skill analysis of tasks to be performed is therefore necessary.

i) Among the many considerations for judging an item’s risk are the ease with which it can be converted to cash, its accessibility, and its monetary value.

4.2 RISK MODELING

1. **Rank and Validate Risk Priorities**

a. Risk modeling is an effective method used to rank and validate risk priorities when prioritizing engagements in the audit plan.

b. Risk factors (e.g., impact and likelihood) may be weighted based on professional judgments to determine their relative significance, but the weights need not be quantified.

1) This simple model and the resulting risk assessment process can be depicted as in Example 4-1 below.

EXAMPLE 4-1 Risk Map

A chief audit executive is reviewing the following enterprise-wide **risk map**:

IMPACT		LIKELIHOOD		
		Remote	**Possible**	**Likely**
	Critical	Risk A	Risk C	Risk D
	Major		Risk B	
	Minor			

In establishing the appropriate priorities for the deployment of limited internal audit resources, the CAE undertakes the following analysis:

- Risk D clearly takes precedence over Risk C because D has a higher likelihood.
- Risk C also clearly has a higher priority than Risk A because C has a higher likelihood and the same impact.

Choosing the higher priority between Risk B and Risk A is a matter of professional judgment based on the organizational risk assessment and the stated priorities of senior management and the board.

- If the more likely threat is considered the greater risk, Risk B will rank higher in the internal audit work plan.
- Likewise, if the threat with the greater possible impact causes senior management and the board more concern, the internal audit activity will place a higher priority on Risk A.

c. Risk modeling in a consulting service can be accomplished by ranking the engagement’s potential to improve management of risks, add value, and improve the organization’s operations as identified in Implementation Standard 2010.C1.

1) Senior management assigns different weights to each of these items based on organizational objectives.

2) The engagements with the appropriate weighted value would be included in the annual audit plan.

2. AICPA Audit Risk Model

a. Overview

1) Internal auditors must establish a framework for assessing risk.

2) The American Institute of Certified Public Accountants (AICPA) is the private sector body that establishes standards for external audits of financial statements in the United States.

   a) The following is the audit risk model used by the AICPA:

   Audit risk = Risk of material misstatement × Detection risk

   Audit risk = (Inherent risk × Control risk) × Detection risk

3) This model is used by an independent auditor engaged to report on whether financial statements are fairly presented, in all material respects, in accordance with the applicable financial reporting framework.

   a) The IIA does not officially define audit risk or its components. However, internal auditors can adapt the model to other audit and assurance engagements.

b. Audit Risk and Its Components

1) **Audit risk** is the risk that an auditor expresses an inappropriate opinion on materially misstated financial statements.

   a) In an internal audit context, audit risk is the risk that the auditor will provide senior management and the board with flawed or incomplete information about governance, risk management, and control.

2) **Inherent risk** is the susceptibility of an assertion about a transaction class, balance, or disclosure to a material misstatement before considering relevant controls.

   a) In an internal audit context, inherent risk is the risk arising from the nature of the account or activity under review. For example, a uranium mine is inherently riskier than an accounts payable function.

3) **Control risk** is the risk that internal control will not timely prevent, or detect and correct, a material misstatement of an assertion.

   a) In an internal audit context, control risk is the risk that the system of internal control designed and implemented by management will fail to achieve management’s goals and objectives for the account or activity under review.

4) **Detection risk** is the risk that the audit procedures intended to reduce audit risk to an acceptably low level will not detect a material misstatement.

   a) In an internal audit context, detection risk is the risk that the auditor will fail to discover conditions relevant to the established audit objectives for the account or activity under review.

c. **Auditor Response to Assessed Risk**

1) Of the three components, only detection risk is under the auditor’s direct control.

2) The internal auditor must first determine the levels of inherent and control risk for the account or activity under review. Detection risk is then adjusted to achieve an overall acceptable level of audit risk.

a) If inherent risk, control risk, or both are determined to be high, detection risk must be set at a low level to compensate, and the nature, timing, and extent of engagement procedures are changed.

EXAMPLE 4-2 Response to Assessed Control Risk

After gathering evidence during an audit, the auditor decides to increase the assessed control risk from the level originally planned. To achieve the same overall audit risk as originally planned, the auditor should decrease the assessed detection risk.

Audit risk is a function of inherent risk, control risk, and detection risk. The only risk the auditor directly controls is detection risk. Detection risk has an inverse relationship with control risk. Accordingly, if the auditor chooses to increase the assessed control risk, the assessed detection risk should be decreased to maintain the same overall audit risk.

3) All three components may be assessed in quantitative (e.g., scale of 1% to 100%, with 100% being maximum risk) or nonquantitative (e.g., high, medium, low) terms.

4.3 COMMUNICATING AND REPORTING TO SENIOR MANAGEMENT AND THE BOARD

1. Communication and Approval

Performance Standard 2020
Communication and Approval

The chief audit executive must communicate the internal audit activity’s plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations.

a. Further guidance is provided in IG 2020, *Communication and Approval*.

1) The **proposed internal audit plan** and the risk assessment are discussed with the board to communicate (a) the risks addressed by the plan and (b) those that cannot be because of resource limits.

2) The proposed plan of engagement includes the following:

a) The proposed assurance and consulting engagements

b) The reason for selecting each engagement (e.g., risk or time elapsed since the last audit)

c) Objectives and scope of each engagement

d) Projects indicated by the internal audit strategy but not necessarily related to audit engagements

3) The plan should be flexible enough to respond to changes in circumstances.

   a) Significant changes in the plan, its basis, or its effects must be approved by the board and senior management.

   b) Review of, and changes in, the plan may occur at quarterly or semiannual board meetings.

Performance Standard 2060
Reporting to Senior Management and the Board

The chief audit executive must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan and on its conformance with the Code of Ethics and the *Standards*. Reporting must also include significant risk and control issues, including fraud risks, governance issues, and other matters that require the attention of senior management and/or the board.

2. The following excerpt from the Interpretation of Standard 2060 addresses the frequency and content of reporting:

   The frequency and content of reporting are determined collaboratively by the chief audit executive, senior management, and the board. The frequency and content of reporting depends on the importance of the information to be communicated and the urgency of the related actions to be taken by senior management and/or the board.

3. **The CAE's Duty to Report**

   a. Further guidance is provided in IG 2060, *Reporting to Senior Management and the Board*. The *Standards* require the CAE to communicate information to senior management and the board about the following:

      1) The internal audit charter

         a) The CAE periodically reviews the charter and presents it for approval.

      2) Organizational independence of the internal audit activity

         a) The CAE annually confirms organizational independence to the board.
         b) Impairments of independence must be disclosed to the board.

3) Internal audit plans, resource requirements, and performance

   a) Performance reporting should relate to the most recently approved plan.

   b) "To quantify the level of performance, many CAEs use key performance indicators such as the percentage of the audit plan completed, percentage of audit recommendations that have been accepted or implemented, status of management's corrective actions, or average time taken to issue reports."

4) Results of audit engagements

5) Results of the quality assurance and improvement program

   a) Included is a conclusion on whether the internal audit activity conforms with the Code of Ethics and *Standards*.

6) Significant risk and control issues and management's acceptance of risk

   a) Significant risk exposures and control issues may result in unacceptable exposure to internal and external risks, including control weaknesses, fraud, illegal acts, errors, inefficiency, waste, ineffectiveness, conflicts of interest, and financial viability.

   b) Senior management and the board determine the responses to significant issues.

      i) They may assume the risk of not correcting the reported condition because of cost or other considerations.

      ii) Senior management should inform the board of decisions about all significant issues raised by internal auditing.

   c) When the CAE believes that senior management has accepted an unacceptable risk, the CAE must discuss the matter with senior management. The CAE should

      i) Understand management's basis for the decision,
      ii) Identify the cause of any disagreement,
      iii) Determine whether management has the authority to accept the risk, and
      iv) Preferably resolve the disagreement.

   d) If the CAE and senior management cannot agree, the CAE must inform the board.

      i) If possible, the CAE and management should jointly present their positions.

      ii) The CAE should consider timely discussion of financial reporting issues with the external auditors.

b. The CAE may share and discuss the contents of the report with senior management before presenting it to the board.

c. The CAE reports on the overall effectiveness of the organization's internal control and risk management processes to senior management and the board.

STUDY UNIT FIVE

ENGAGEMENT PLANNING

This study unit covers **Domain II: Planning the Engagement** from The IIA’s CIA Exam Syllabus. This domain makes up 20% of Part 2 of the CIA exam and is tested at the **proficient** cognitive level. This study unit also is the first of four covering **Domain III: Performing the Engagement**. This domain makes up 40% of Part 2 of the CIA exam and is tested at the **basic** and **proficient** cognitive levels. Refer to the complete syllabus located in Appendix B to view the relevant sections covered in Study Unit 5.

An engagement consists of planning, performing procedures, communicating results, and monitoring progress. The internal auditor’s responsibility is to plan and perform the engagement, subject to review and approval by supervisors. This study unit applies to the planning phase of the engagement.

5.1 ENGAGEMENT PLANNING AND RISK ASSESSMENT

1. **Engagements**
    a. An **engagement** is a “specific internal audit assignment, task, or review activity, such as an internal audit, control self-assessment review, fraud examination, or consultancy. An engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives” (The IIA Glossary).

Performance Standard 2200
Engagement Planning

Internal auditors must develop and document a plan for each engagement, including the engagement’s objectives, scope, timing, and resource allocations. The plan must consider the organization’s strategies, objectives, and risks relevant to the engagement.

b. Internal auditors may develop a **planning memo** to document the engagement objectives, scope, risk assessment, prioritized areas for testing, and the approved audit work program.

Performance Standard 2201
Planning Considerations

In planning the engagement, internal auditors must consider:

- The strategies and objectives of the activity being reviewed and the means by which the activity controls its performance.
- The significant risks to the activity's objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level.
- The adequacy and effectiveness of the activity's governance, risk management, and control processes compared to a relevant framework or model.
- The opportunities for making significant improvements to the activity's governance, risk management, and control processes.

2. **Engagement Planning**

a. Further guidance is provided in IG 2200, *Engagement Planning*.

1) Planning requires internal auditors to understand the internal audit plan of engagements.

a) Internal auditors should be aware of the planning and discussions that preceded development of the plan.

b) Internal auditors should understand any significant organizational changes since the engagement was included in the annual plan.

c) Internal auditors need to understand how the entity's strategies, objectives, and risks affect the engagement.

2) Setting engagement objectives is crucial to planning. Accordingly, internal auditors should consider the following matters to the extent they are relevant to the areas reviewed:

a) Management's current risk assessment
b) The risk assessment made for the plan of engagements
c) Prior engagement-level risk assessments
d) Prior audit reports

3) Setting risk-based objectives permits definition of the scope of the engagement.

4) The following are other considerations during the engagement planning stage:

   a) Resources required and their most effective and efficient use.

   b) Retention of documents and decisions about requirements and formats.

   c) Beginning preparation of the engagement program, with attention to budgets, forms of final communications, and logistical concerns.

b. The CAE determines how, when, and to whom results are communicated. If appropriate, these documented determinations are communicated to management during planning.

   1) Subsequent changes that affect the timing or reporting of engagement results also are communicated.

3. **Preliminary Survey**

a. The internal auditors may perform a survey to (1) become familiar with activities, risks, and controls for the purpose of identifying areas for engagement emphasis and (2) invite comments and suggestions from stakeholders. The components of a survey include the following:

   1) Input from stakeholders
   2) Analytical procedures
   3) Questionnaires (covered in Subunit 5.4 and Study Unit 6, Subunit 3)
   4) Interviews (covered in Subunit 5.4 and Study Unit 6, Subunit 4)
   5) Observations (covered in Subunit 5.4 and Study Unit 6, Subunit 5)
   6) Prior audit reports and other relevant documentation
   7) Process mapping (covered in Study Unit 8, Subunit 2)
   8) Checklists

b. Input from Stakeholders

   1) Auditee management and other stakeholders may be sources of information for the formulation of engagement objectives.

   2) Onsite observations and interviews with users of the activity's output and other stakeholders may be part of the survey.

c. Prior Audit Reports and Other Relevant Documentation

   1) Prior audit reports and workpapers may be other sources of information. The issues and the process by which they were resolved may provide insights into the client's particular circumstances.

      a) The auditor must use such documentation for informational purposes only, not as a basis for objectives or conclusions.

d. Checklists

1) During the preliminary survey and throughout the engagement, checklists (reminder lists) ensure that the auditor has completed necessary tasks. For example, they include receipt of requested documentation and updates of the continuing audit file.

Sample Checklist	
Add to permanent audit file:	
□	Amortization schedule for new bond issues
□	Plan for disposal of assets of discontinued operation
□	Most recent forms filed with regulators
□	Most recent client-prepared process control maps

2) Checklists increase the uniformity of data acquisition. They ensure that a standard approach is taken and minimize the possibility of omitting factors that can be anticipated.

3) Disadvantages of checklists include the following:

a) Providing a false sense of security that all relevant factors are addressed

b) Inappropriately implying that equal weight is given to each item

c) The difficulty of translating the observation represented by each item

d) Treating a checklist as a rote exercise rather than part of a thoughtful understanding of the unique aspects of the audit

4) Checklists may be used to control administrative details involved in performing the engagement, to prepare for opening and closing conferences, etc.

e. Documentation and Communication of Results

1) The results of the survey are documented and, if appropriate, communicated to management in an oral presentation.

2) A **summary** of results is prepared that includes

a) Significant issues;

b) Engagement objectives and procedures;

c) Critical control points, deficiencies, or excess controls;

d) Methods, such as those that are technology-based; and

e) Reasons for modifying objectives (e.g., to expand or decrease audit work) or not continuing the engagement.

4. **Risk Identification**

   a. During planning, internal auditors must identify key business risks and controls, especially the client's inherent risks.

      1) In the context of an engagement, **risk** is an event that may impact the business objectives of the area or process under review.
      2) **Controls** are actions taken to mitigate risks.
      3) **Inherent risk** is the risk in the absence of controls.
      4) A key risk or control is determined by its significance, which is measured as a combination of risk factors (e.g., magnitude, nature, effect, relevance, impact, and likelihood).

   b. **Brainstorming.** Internal auditors may conduct brainstorming sessions to identify key risks and controls. During such sessions, internal auditors may ask the following questions to identify relevant risks:

      1) What would prevent the activity from achieving its business objectives?
      2) How would the activity be affected if no controls existed?

   c. **Risk and control matrix.** Internal auditors also may create a risk and control matrix to identify key risks and controls. The risk and control matrix below is an excerpt from a relevant IIA publication.

Risk and Control Matrix for Accounts Payable

Business Objectives	Inherent Risk	Impact (L, M, H)*	Likelihood (L, M, H)*	Control
A. Personnel expenses are appropriate and authorized.	A.1 Corporate cards are issued inappropriately, resulting in fraudulent expenses.	M	M	Duties are segregated.
	A.2 Personnel are not provided guidance on corporate card usage and expense policies, resulting in inappropriate expenses.	L	M	Expense policy is communicated to personnel authorized to incur organizational expenses.
	A.3 Expense reports are not submitted/reviewed timely, resulting in inappropriate expenses.	H	H	No control is in place.
	A.4 Expense reports with receipts are not reviewed and approved by appropriate personnel, resulting in inappropriate expenses.	H	M	Approvals are based on management hierarchy. Expense reports cannot be submitted until a manager approves them. Expense team conducts monthly reviews.

*Impact and likelihood are commonly described as low (L), medium (M), or high (H).

5. Risk Assessment

Implementation Standard 2210.A1

Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

a. After identifying risks and controls, the internal auditors perform a preliminary risk assessment.

1) Internal auditors consider

a) Management’s **assessment of risks**;

b) Its reliability;

c) The process for addressing risk and control matters;

d) The reporting about, and the responses to, events exceeding the **risk appetite**; and

e) Risks in related activities.

b. Two factors of significance commonly used to assess risks are impact and likelihood.

1) Internal auditors may use a **heat map** to visually display assessed risks and prioritize risks according to significance. The heat map below is excerpted from the aforementioned IIA publication.

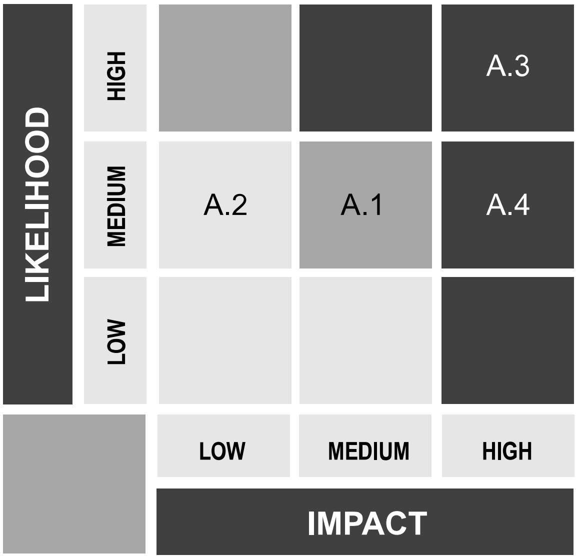


Figure 5-1

2) Accordingly, the risks ranked from most (highest) to least (lowest) significant (priority) are A.3, A.4, A.1, and A.2.

5.2 ENGAGEMENT OBJECTIVES, SCOPE, AND CRITERIA

1. Engagement Objectives

a. After the preliminary survey and risk assessment are complete, internal auditors establish objectives. The objectives should explain the reasons the activity is being audited, the scope of the engagement, and the assurances to be provided.

Performance Standard 2210
Engagement Objectives

Objectives must be established for each engagement.

b. **Engagement objectives** are "broad statements developed by internal auditors that define intended engagement accomplishments" (The IIA Glossary).

c. Objectives for **assurance engagements** must reflect the results of the preliminary assessment of risks relevant to the activity under review. In contrast, objectives for **consulting engagements** must address governance, risk management, and control processes to the extent agreed upon with the client (Implementation Standard 2210.C1).

d. Further guidance is provided in IG 2210, *Engagement Objectives*:

1) Objectives assist in determining the **procedures** to perform and the priorities for testing risks and controls.

2) Objectives ordinarily are based on identified **key risks** relevant to the area or process under review.

3) **Preliminary objectives** of engagements may be based on (a) the plan of engagements, (b) prior results, (c) stakeholder feedback, and (d) the auditee's mission, vision, and objectives. **Risk assessment exercises** should be performed related to the auditee's governance, risk management, and controls.

Implementation Standard 2210.A2

Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

2. **Engagement Scope**

   a. After establishing risk-based objectives, internal auditors establish the engagement scope.

> **Performance Standard 2220**
> **Engagement Scope**
>
> The established scope must be sufficient to achieve the objectives of the engagement.

   b. According to IG 2200, *Engagement Planning*, scope sets the boundaries within which the internal auditors will work.

   c. Further guidance is provided in IG 2220, *Engagement Scope*:

      1) Scope defines "what will and will not be included in the engagement."

      2) Internal auditors **generally consider** the following factors, among others, when establishing the engagement scope:

         a) The boundaries, subprocesses, and components of the area or process under review.

         b) In-scope versus out-of-scope locations.

         c) Time frame.

   d. The Implementation Standard below provides factors internal auditors **must consider** when establishing the engagement scope.

> **Implementation Standard 2220.A1**
>
> The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.

3. **Engagement Criteria**

   a. Criteria are needed to evaluate the area or process under review.

> **Implementation Standard 2210.A3**
>
> Adequate criteria are needed to evaluate governance, risk management, and controls. Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must identify appropriate evaluation criteria through discussion with management and/or the board.

      1) Acceptable industry standards, standards developed by professions or associations, standards in law and government regulations, and other sound business practices are usually deemed to be appropriate criteria.

5.3 ENGAGEMENT STAFF AND RESOURCES

Performance Standard 2230
Engagement Resource Allocation

Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.

Interpretation of Standard 2230

Appropriate refers to the mix of knowledge, skills, and other competencies needed to perform the engagement. Sufficient refers to the quantity of resources needed to accomplish the engagement with due professional care.

1. **Resources at the Engagement Level**
   a. The standard above imposes a responsibility on **internal auditors**, not on the CAE. Standards that impose responsibilities on the CAE address management of the internal audit activity, organizational independence, and certain other matters.
   b. Engagement resource allocation is based on evaluation of
      1) The number and experience of staff;
      2) The knowledge, skills, and competencies of the staff;
      3) Training needs; and
      4) Whether external resources are required.
   c. If available staff do not have the requisite skills to perform the engagement, internal auditors should consider using external resources to supplement the needed knowledge, skills, and other competencies.
2. **Audit Staff Schedules**
   a. Audit staff schedules should be prepared to achieve effective use of time.
      1) Audit teams are selected based on their knowledge, skills, and other competencies to meet engagement objectives efficiently and effectively. Any training opportunities also should be considered.
      2) All engagements should be under budgetary control. Project budgets and schedules should be developed for each engagement.
         a) Budgets are derived by carefully analyzing the time spent in the prior year on the same or a comparable engagement.
         b) Because no projects are precisely the same (even those covering the same activity), budgets are reevaluated after the preliminary survey.
            i) The CAE reduces excessive budgets, increases insufficient budgets, or changes the scope of the engagements.
            ii) Adjustments and the reasons for them are documented.
         c) Time budgets for engagements are usually prepared in employee-hours or employee-days. Time estimates are given to each internal auditor to help with time management.

3) Budget adjustments need to be justified and approved at a level higher than the engagement supervisor. Requests for adjustment should include the following:

   a) The operational activities to be reviewed,
   b) The activities actually being performed, and
   c) The employee-days or hours attributable to the difference.

4) Monitoring time budgets and schedules allows the CAE to control projects and avoid overruns.

   a) Staff auditors submit periodic time sheets that indicate time spent and the status of the job.

5.4 ENGAGEMENT PROCEDURES

1. Engagement Procedures

> **SUCCESS TIP**
>
> Many questions on the CIA exam require the selection of engagement procedures. Few such questions are answerable based on memorization of lists. Moreover, it is not feasible or practical to try to provide such an exhaustive list. Thus, candidates must be able to apply knowledge of auditing concepts to unfamiliar situations when choosing procedures. The best way to prepare yourself for these questions is to answer as many practice questions as possible.

a. Procedures are performed to obtain sufficient, reliable, relevant, and useful information to achieve the engagement objectives.

   1) An auditor’s **physical examination** provides the most persuasive form of evidence.
   2) Direct **observation** by the auditor, e.g., of performance of work by client personnel, is the next most persuasive.
   3) Information originating from a **third party** is less persuasive than information gathered directly by the auditor but more persuasive than information originating from the client.
   4) Information originating with the **client** can be somewhat persuasive in documentary form, especially if it is subject to effective internal control. But client oral testimony is the least persuasive of all.
   5) Original documents are more persuasive than copies, which can be altered.

b. Management implicitly or explicitly makes assertions about the recognition, measurement, presentation, and disclosure of information in the financial statements. Engagement objectives typically require internal auditors to perform procedures that test the validity of these assertions and assess the risks of material misstatement.

   1) According to the AICPA, assertions used by the auditor to consider the types of potential misstatements may be classified as follows:

      a) **Assertions** about classes of **transactions and events** for the period (the income statement and statement of cash flows)

         i) **Occurrence** -- Recorded transactions and events actually occurred.

         ii) **Completeness** -- All transactions and events that should have been recorded were recorded.

         iii) **Accuracy** -- Amounts and other data were recorded appropriately.

         iv) **Cutoff** -- Transactions and events were recorded in the proper period.

         v) **Classification** -- Transactions and events were recorded in the proper accounts.

      b) **Assertions** about **account balances** at period end (the balance sheet)

         i) **Existence** -- Assets, liabilities, and equity interests exist.

         ii) **Rights and obligations** -- The entity holds or controls the rights to assets, and liabilities are its obligations.

         iii) **Completeness** -- All assets, liabilities, and equity interests that should have been recorded were recorded.

         iv) **Valuation and allocation** -- Assets, liabilities, and equity interests are included at appropriate amounts, and any valuation or allocation adjustments are appropriately recorded.

      c) **Assertions** about **presentation and disclosure** (notes to the financial statements)

         i) **Occurrence and rights and obligations** -- Disclosed transactions, events, and other matters have occurred and pertain to the entity.

         ii) **Completeness** -- All disclosures that should have been included were included.

         iii) **Classification and understandability** -- Financial information is appropriately presented and described, and disclosures are clearly expressed.

         iv) **Accuracy and valuation** -- Information is disclosed fairly and at appropriate amounts.

c. **Sampling** procedures are frequently performed to test a population. (Sampling is covered in detail in Study Unit 7.)

d. Internal auditors should use available information technology (IT), such as generalized audit software (GAS), computer-assisted auditing techniques (CAAT), or an integrated test facility (ITF), to assist in performing audit work (computerized audit tools are covered in Study Unit 8, Subunit 1). The benefits of using IT include

   1) Reduced audit risk
   2) Increased productivity, resulting in more timely audit engagements
   3) Increased audit opportunities

2. **Audit Procedures**

   a. **Risk assessment procedures** are performed to obtain an understanding of the entity and its environment, including internal control.

   b. **Further audit procedures** include tests of controls and substantive procedures.

      1) **Tests of controls** test the operating effectiveness of controls in preventing, or detecting and correcting, instances of noncompliance, whether they take the form of a material misstatement in the financial statements, failure to comply with a law or regulation, or some other undesired outcome. They are required when

         a) The auditor's risk assessment is based on an expectation of the operating effectiveness of controls or

         b) Substantive procedures alone do not provide sufficient appropriate evidence.

      2) **Substantive procedures** are used to detect material misstatements at the relevant assertion level. They include (a) tests of details and (b) substantive analytical procedures.

         a) They should be performed for **all** relevant assertions about each material (1) transaction class, (2) account balance, and (3) disclosure.

3. **Selection of Engagement Procedures**

SUCCESS TIP

A necessary problem-solving skill on Part 2 of the CIA exam is the ability to determine which audit engagement procedure is appropriate in a given situation. Few such questions are answerable based on memorization of lists. Moreover, it is not feasible or practical to try to provide such an exhaustive list. Thus, candidates must be able to apply knowledge of auditing concepts to unfamiliar situations when choosing procedures. The best way to prepare yourself for these questions is to answer as many practice questions as possible.

   a. **Basic Procedures**

      1) Three basic procedures performed by internal auditors to gather information are (a) observing conditions, (b) interviewing people, and (c) examining records.

      2) **Observation** is effective for verifying whether (a) particular assets, such as inventory or equipment, exist or (b) a certain process or procedure is being performed appropriately at a moment in time. (Observation is covered in more detail in Study Unit 6, Subunit 5.)

         a) However, observation provides less persuasive information about the assertions of completeness, rights, valuation, and presentation and disclosure. For example, merely observing inventory does not determine whether the engagement client has rights in it.

3) **Interviewing** (inquiring) is especially helpful in obtaining an understanding of client operations because of the opportunity to ask questions to clarify preceding answers or to pursue additional information. (Interviewing is covered in more detail in Study Unit 6, Subunit 4.)

    a) A supplement to interviewing is the use of an **internal control questionnaire**. It consists of a series of questions about the controls designed to prevent or detect errors or fraud. (Questionnaires are covered in more detail in Study Unit 6, Subunit 3.)

        i) Answers to the questions help the internal auditor to identify specific policies and procedures relevant to specific assertions. They also help in the design of tests of controls to evaluate their effectiveness.

        ii) The questionnaire provides a means for ensuring that specific concerns are not overlooked, but it is not sufficient for an understanding of the entire system. Thus, the evidence obtained is indirect and requires corroboration by means of observation, interviews, flowcharting, examination of documents, etc.

    b) Evidence obtained by interviews should be corroborated by gathering objective data.

4) **Examining** (inspecting) records is used in many audit activities. The methods predominantly used are discussed below.

    a) **Inspection of records or documents** is the examination of records or documents, whether internal or external, in paper, electronic, or other media.

    b) **Inspection of tangible assets** is the physical examination of assets to test existence. For example, it is combined with observation of inventory counts.

    c) **Verification** is a broad term for the process of determining the validity of information.

b. Other specific procedures that are variations of the basic procedure of examining records include the following:

1) **Confirmations** obtain audit evidence as a direct, written response to the auditor from a third party.

    a) Confirmations are commonly used to verify the amounts of accounts receivable, goods on consignment, and liabilities.

    b) **Positive** confirmations are used when the amounts being confirmed are material. The recipient is asked to sign and return the letter with a positive assertion that the amount is either correct or incorrect.

        i) Because the amounts involved are material, unanswered positive confirmations require follow-up. They are thus more time-consuming than negative confirmations.

    c) **Negative** confirmations are used when the amounts being confirmed are immaterial or when controls are deemed to be functioning extremely well.

        i) The use of negative confirmations assumes that the recipients will complain only if they have a dispute with the amount. Thus, if a negative confirmation is unanswered, the auditor concludes that the amount has been confirmed.

2) **Tracing and Vouching**

   a) **Tracing** follows a transaction forward from the triggering event to a resulting event, ensuring that the transaction was accounted for properly.

      i) Tracing is used to gain assurance regarding the completeness assertion, for example, that a liability was properly accrued for all goods received.

   b) **Vouching** tracks a result backward to the originating event, ensuring that a recorded amount is properly supported.

      i) Vouching is used to gain assurance regarding the existence assertion, for example, that a receivable claimed on the statement of financial position is supported by a sale to a customer.

NOTE: The direction of testing is important in evaluating certain assertions.

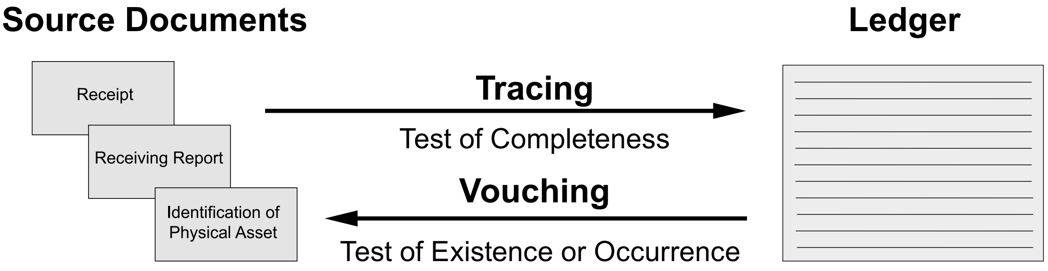


Figure 5-2

SUCCESS TIP

The terms “tracing” and “vouching” are defined above using classic auditing definitions. However, the CIA exam may use the word “tracing” to mean either process. Be extremely careful when encountering questions on this topic and focus on which process is relevant, not which term is used.

3) **Reperformance** (Recalculation)

   a) Reperformance consists of duplicating the client’s work and comparing the results. This is most useful for checking arithmetic accuracy and the correct posting of amounts from source documents to journals to ledgers.

4) **Analytical Procedures**

   a) Analytical procedures are evaluations of financial information made by an analysis of relationships among financial and nonfinancial data. The basic premise is that plausible relationships among data may reasonably be expected to exist and continue in the absence of known conditions to the contrary.

   b) During the planning phase, analytical procedures are used by the internal auditor to determine the nature, extent, and timing of auditing procedures. The objective is to identify such things as the existence of unusual transactions and events and amounts, ratios, and trends that might indicate matters which require further investigation.

   c) Common analytical procedures performed by the internal auditor include (1) analysis of common-size financial statements, (2) ratio analysis, (3) trend analysis, (4) analysis of future-oriented information, and (5) internal and external benchmarking.

d) **Scanning** is a use of professional judgment to review accounting data to identify significant or unusual items to test. For example, an internal auditor might scan the warehouse for damaged or obsolete inventory.

e) Analytical procedures are covered in more detail in Study Unit 8, Subunit 3.

c. The best descriptive assertion is illustrated for each audit procedure included in the charts below and on the following pages. Depending on the procedure performed, more than one assertion could be addressed. Thus, the same procedure may be applied to different assertions. Accordingly, the following chart is not exhaustive:

<table>
<tr><th colspan="3">Sales and Receivables</th></tr>
<tr><th>Objective</th><th>Assertion</th><th>Procedure(s)</th></tr>
<tr><td>Determine whether accounts receivable represent valid sales.</td><td>Occurrence
→</td><td>Vouch a sample of accounts receivable debit entries from subsidiary ledgers and/or sales journal to customer invoices and related shipping documents
<i>or</i></td></tr>
<tr><td></td><td>Existence
→</td><td>Send requests for external confirmation of accounts receivable.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
Generally, confirming receivables is performed after analytical procedures that identified the possibility of fictitious sales. An auditor wants to detect fictitious sales and ensure that each claimed sale is properly supported. This objective is accomplished by vouching amounts recorded in the ledger to the source documents. Confirmations are more likely to be effective for determining the existence of receivables and less likely to be effective for assessing the collectibility of receivables.</td></tr>
<tr><td>Determine whether debits to accounts receivable represent valid transactions.</td><td>Existence
→</td><td>Vouch entries from the accounts receivable ledger to sales documentation.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
An auditor wants to verify that recorded amounts are properly supported by originating events. This objective is accomplished through vouching. Only the two choices that involve tracking ledger entries back to a journal or source document describe a vouching procedure. A debit to accounts receivable is properly supported by a credit sale to a customer.</td></tr>
<tr><td>Ensure that shipments are billed to customers.</td><td>Completeness
→</td><td>Trace shipping documents (i.e., bills of lading) to sales records, such as the accounts receivable subsidiary ledger and/or invoices.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
The completeness assertion relates to whether all transactions that should be presented are included. An auditor traces from the shipment of goods (the triggering event) to the invoicing of the same goods (the resulting event). The auditor verifies that everything shipped was subsequently billed to the appropriate customers.

-- Continued on next page --</td></tr>
</table>

<table>
<tr><th colspan="3">Sales and Receivables (Continued)</th></tr>
<tr><th>Objective</th><th>Assertion</th><th>Procedure(s)</th></tr>
<tr><td rowspan="3">Determine whether all credit sales are recorded in accounts receivable.</td><td>Completeness
→</td><td>Trace from a sample of shipping documents to related sales invoices and subsidiary ledgers</td></tr>
<tr><td></td><td>*or*</td></tr>
<tr><td>Completeness
→</td><td>Account for the numerical sequence of sales orders, shipping documents, invoices, etc.</td></tr>
<tr><td colspan="3">**WHY?**</td></tr>
<tr><td colspan="3">To determine that all credit sales are recorded, the proper direction of testing is from the shipping records (such as the bills of lading) to the sales invoices and the accounts receivable subsidiary ledger. Tracing supports the completeness assertion.</td></tr>
<tr><td rowspan="5">Measure accounts receivable appropriately and ascertain the collectibility of receivables.</td><td>Valuation and Allocation
→</td><td>Examine cash receipts records to determine promptness of interest and principal payments,</td></tr>
<tr><td></td><td>*or*</td></tr>
<tr><td>Valuation and Allocation
→</td><td>Review delinquent customers’ credit ratings,</td></tr>
<tr><td></td><td>*or*</td></tr>
<tr><td>Valuation and Allocation
→</td><td>Classify receivables by age and compare collection rates within classifications with those of prior years (also called aging the accounts receivable).</td></tr>
<tr><td colspan="3">**WHY?**</td></tr>
<tr><td colspan="3">The best information about the collectibility of notes receivable is actual cash collection. Nonpayment or late payment reduces the probability of collection. An effective credit-granting function will generally be evidenced by minimal write-offs of receivables.
The probability of collection is inversely proportional to the age of the receivables. Thus, aging the receivables provides information that is highly relevant. Current economic conditions also are relevant because collectibility varies with changes in the economic cycle.</td></tr>
</table>

<table>
<tr><th colspan="3">Cash and Short-Term Investments</th></tr>
<tr><th>Objective</th><th>Assertion</th><th>Procedure(s)</th></tr>
<tr><td>Determine that cash transactions actually occurred.</td><td>Occurrence
→</td><td>Vouch a sample of recorded cash receipts to accounts receivable and customer orders
<i>or</i></td></tr>
<tr><td></td><td>Occurrence
→</td><td>Vouch a sample of recorded cash disbursements to approved vouchers.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
An auditor should verify that recorded amounts are properly supported by originating events.</td></tr>
<tr><td>Determine that cash reported actually exists.</td><td>Existence
→</td><td>Count cash on hand,
<i>or</i></td></tr>
<tr><td></td><td>Existence
→</td><td>Send bank confirmations,
<i>or</i></td></tr>
<tr><td></td><td>Existence
→</td><td>Prepare bank reconciliations and then compare bank and book cash balances.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
Counting cash provides direct information to support the reported cash amount.
Bank confirmations and reconciliations provide direct, externally generated information to support the reported cash amount. Additionally, interbank transfers that have cleared within a reasonable time after year end assert that cash exists in the appropriate bank account and is not double counted.</td></tr>
<tr><td>Determine that investments in short-term marketable equity securities are recorded at appropriate amounts.</td><td>Valuation
→</td><td>Compare cost data, such as par value and shares amount, with current market quotations
<i>or</i></td></tr>
<tr><td></td><td>Rights and Obligations
→</td><td>Send confirmations.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
Market quotations generally are based on sufficient market activity. Accordingly, they provide sufficient competent evidence regarding valuation. Confirmations concerning securities in the client’s name are directly related to the rights and obligations assertion and indirectly to the valuation or allocation assertions.</td></tr>
</table>

<table>
<tr><th colspan="3">Inventory</th></tr>
<tr><th>Objective</th><th>Assertion</th><th>Procedure(s)</th></tr>
<tr><td>Determine whether unused inventory associated with capital projects is appropriately allocated to inventory.</td><td>Accuracy
→</td><td>Review all inventory adjustment journal entries transferring costs from capital projects to inventory.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
Some transfers from capital accounts to inventory may be legitimate, for example, because materials previously transferred from inventory were unused. However, the transfer of costs actually incurred for capital projects back to inventory misstates both accounts and undermines the budget process.</td></tr>
<tr><td>Determine whether purchase orders generated by an automated inventory control system are approved by authorized personnel.</td><td>Existence
→</td><td>Review the listing of personnel authorized to approve purchase orders to ensure that only authorized persons can change purchase order parameters in the automated inventory control system.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
An auditor should determine whether computer-generated purchase orders are appropriately authorized.</td></tr>
<tr><td>Determine whether inventory transactions actually occurred.</td><td>Occurrence
→</td><td>Vouch a sample of recorded purchases to documentation
<i>or</i></td></tr>
<tr><td></td><td>Occurrence
→</td><td>Vouch a sample of recorded cost of sales to documentation.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
An auditor should verify that recorded amounts are properly supported by originating events.</td></tr>
<tr><td>Determine whether inventory actually exists.</td><td>Existence
→</td><td>Observe inventory and make test counts.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
Observing inventory provides direct information to support the reported inventory amount. A physical inventory is a time-consuming but effective procedure. Physical inventory counts and reconciling discrepancies are strong procedures when controls over inventory are weak or when fraud is suspected as a result of inventory shrinkage. One way to overstate gross margin and profit is to overstate ending inventory.</td></tr>
</table>

-- Continued on next page --

<table>
<tr><th colspan="3">Inventory (Continued)</th></tr>
<tr><th>Objective</th><th>Assertion</th><th>Procedure(s)</th></tr>
<tr><td>Determine whether all inventory usage is recorded.</td><td>Completeness
→</td><td>Match prenumbered inventory disbursement forms to inventory system records.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
Physical information is best obtained through direct observation or inspection. Disbursement forms can be matched to inventory system activity (i.e., usage) to test the completeness of disbursement records.</td></tr>
<tr><td>Determine whether inventory is obsolete.</td><td>Valuation
→</td><td>Scan inventory for old items with no activity and recompute the value of the inventory.</td></tr>
<tr><td>Determine whether inventory amounts are measured appropriately.</td><td>Valuation
→</td><td>Ensure that manufactured goods are tested for reasonableness.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
Performing analytical reviews to identify obsolete inventory and recomputing the value of obsolete items is necessary to establish current inventory carrying amounts.</td></tr>
<tr><td>Determine whether the purchaser owns inventory at year end.</td><td>Rights and Obligations
→</td><td>Examine paid vendor invoices.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
Mere possession of inventory does not signify that another party does not have a claim to it. For example, the inventory may be held on consignment. Payment of vendor invoices is the culmination of the purchases-payables cycle. The paid invoice evidences the purchaser’s ownership of the inventory.</td></tr>
</table>

Property, Plant, and Equipment

Objective	Assertion	Procedure(s)
Determine whether transactions affecting property, plant, and equipment are properly recorded.	Existence →	Vouch a sample of recorded purchases to documentation.
Determine whether depreciation expense is calculated and recorded correctly.	Classification and Understandability →	Recompute depreciation expense and applicable financial statements *or*
	Valuation →	Examine repair and maintenance records of depreciable assets.

WHY?

An auditor should verify that recorded amounts are properly supported by originating events and properly presented, described, and disclosed. Repair and maintenance records evidence that the assets exist and were placed in service.

Accounts Payable		
Objective	**Assertion**	**Procedure(s)**
Determine whether purchases occurred.	Occurrence →	Vouch a sample of recorded payables to documentation, e.g., requisitions, purchase orders, receiving reports, and approved invoices.
WHY? An auditor should verify that recorded amounts are properly supported by originating events.		
Determine whether accounts payable are all accounted for.	Completeness →	Trace subsequent payments to recorded payables;
		or
	Completeness →	Collect supporting documentation and search for unmatched documents to determine whether relevant documents have been lost, misplaced, or misfiled;
		or
	Completeness →	Send confirmation to vendors.
WHY? The completeness assertion is that all legitimate accounts payable have been recorded. Thus, the auditor's procedures must address whether all accounts payable that should have been recorded were recorded.		
Determine whether payments were made to fictitious vendors.	Existence →	Use generalized audit software to match all vendor information and sort by common names, addresses, phone numbers, etc., and then compare the vendor information to the master vendor list for verification
		or
	Existence →	Examine paid invoices from vendors deemed questionable (e.g., post office box number on file instead of an actual address) and compare to receiving documentation.
WHY? Sampling is inappropriate when fraud is suspected. Generalized audit software enables analysis of an entire population of information to assist with identification of fictitious vendors. Examining paid invoices to vendors deemed questionable and searching for indications that goods or services were actually received could reveal fraudulent invoices.		

Other Liabilities

Objective	Assertion	Procedure(s)
Determine whether contingency estimates are recorded appropriately.	Accuracy →	Contact the external organizational counsel regarding contingency estimates, including any threatened or pending litigation, claims, and assessments.

WHY?

An auditor should verify that recorded amounts are properly supported by originating events.

Purchases

Objective	Assertion	Procedure(s)
Determine whether items purchased are used for business purposes and not for individual use.	Occurrence →	Perform a comparison of items received (e.g., computer monitors) to usage (e.g., IT service records) to determine whether quantity received is reasonable or excessive. If deemed excessive, additional investigation generally will be required.
Determine whether blanket purchase orders used for routine purchases are closely monitored.	Occurrence →	Perform trend analysis [e.g., compare same month or period to same month or period in prior year(s)] to determine whether increase or decrease is reasonable. If deemed unreasonable, additional investigation generally will be required.

WHY?

A basic premise underlying the application of analytical procedures is that plausible relationships among data may reasonably be expected to exist and continue in the absence of known conditions to the contrary. Thus, an analysis of purchases received and actual business usage may raise a red flag, such as an unexplained increase in materials used, that abuse may be occurring.

	Payroll	
Objective	**Assertion**	**Procedure(s)**
Determine whether payroll costs have been accurately distributed to work-in-process accounts.	Accuracy →	Trace the individual time tickets to the payroll cost distribution, then trace that total to the various work-in-process accounts and compare to the budget.
WHY? An auditor traces from triggering events (individual time tickets) to test the recorded amounts.		
Determine whether payroll payments are received by nonexistent employees.	Existence →	Verify payees actually worked (e.g., reconcile time cards to employees),
		or
	Existence →	Examine direct deposit bank confirmations or canceled checks and compare to personnel documentation,
		or
	Existence →	Determine whether payroll payments and hiring functions are performed by different people.
WHY? The personnel department should authorize hiring and termination of employees and changes in wage rates but should have no authority over payment of wages.		

<table>
<tr><th colspan="3">General</th></tr>
<tr><th>Objective</th><th>Assertion</th><th>Procedure(s)</th></tr>
<tr><td>Determine whether transactions and events were recorded in the proper period.</td><td>Cutoff
→</td><td>Trace documents (e.g., sales invoices, shipping documents) to the accounting records for several days prior to and after the balance sheet date.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
Documents are traced to the accounting records for several days prior to and after the balance sheet date by the auditor to detect recording of the transaction(s) in a period other than that in which title passed.</td></tr>
<tr><td>Determine whether amounts are appropriately described and disclosures are fairly and clearly expressed.</td><td>Presentation and Disclosure
→</td><td>Inspect financial statements,
<i>or</i></td></tr>
<tr><td></td><td>Presentation and Disclosure
→</td><td>Evaluate note disclosures,
<i>or</i></td></tr>
<tr><td></td><td>Presentation and Disclosure
→</td><td>Inspect any other relevant documentation.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
An auditor should determine whether financial statements and disclosures are properly classified and disclosed.</td></tr>
<tr><td>Determine the existence of credit lines and collateral arrangements.</td><td>Existence
→</td><td>Send bank confirmations.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
Confirmation has the advantage of obtaining information from sources external to the entity. Information from external sources provides greater assurances of reliability than information from sources within the entity.</td></tr>
</table>

4. **Maturity Models**

a. Audit procedures may require the internal auditor to assess the maturity of a business process (i.e., where the process currently lies on a predefined maturity scale) and compare results with management’s expectations for that process. Thus, the internal auditor may use a maturity model to perform this procedure.

b. “Maturity models establish a systematic basis of measurement for describing the ‘as is’ state of a process.” Thus, they provide the criteria for assessing the **current state** of a business process.

c. An example maturity model is the capability maturity model (CMM). This model consists of the following maturity levels:

1) **Initial** level. The process is defined.
2) **Repeatable** level. The process is established.
3) **Defined** level. Standards that govern the process are developed.
4) **Managed** level. Performance measures are defined.
5) **Optimizing** level. All expectations are met and continuous improvement is enabled.

d. The **Capability Maturity Model Integration (CMMI) Development V2.0** (2018) focuses on organizational performance at each maturity level. A maturity level is the extent of process improvement in multiple process areas. This model consists of the following levels, presented in order of maturity:

Level 0	**Incomplete:** whether work can be completed is not known.
Level 1	**Initial:** work can be completed, but not on time or within the budget.
Level 2	**Managed:** projects are planned, implemented, managed, and monitored.
Level 3	**Defined:** standards for projects are defined throughout the organization.
Level 4	**Quantitatively managed:** the organization quantifies performance improvement goals to meet stakeholder needs.
Level 5	**Optimizing:** the organization pursues continuous improvement, responds to change, and innovates.

e. The following are three steps for creating a maturity model:

1) Determine the model’s purpose and components.

   a) Considerations include

      i) What management wants to assess

      ii) The business processes involved

      iii) How the expected outcome can be stated in terms of a metric or qualitative statement

   b) Components are the categories of attributes related to the process.

      i) For example, if a maturity model is used to assess an organization’s ethics program, a component could include the organization’s code of ethics.

2) Determine the model’s scale (the number of levels).

3) Develop expectations for each component level.

5.5 ENGAGEMENT WORK PROGRAM

Performance Standard 2240
Engagement Work Program

Internal auditors must develop and document work programs that achieve the engagement objectives.

Implementation Standard 2240.A1

Work programs must include the procedures for identifying, analyzing, evaluating, and documenting information during the engagement. The work program must be approved prior to its implementation, and any adjustments approved promptly.

1. The internal auditor plans and performs the engagement, with supervisory review and approval. A primary result of engagement planning is the preparation of the work program. The **engagement work program** is a “document that lists the procedures (also referred to as methods) to be followed during an engagement, designed to achieve the engagement plan” (The IIA Glossary).
   a. The essentials of the engagement work plan are expected to be understood by the internal audit activity and are not a required part of its risk-based plan of engagements.
2. Further guidance is provided in IG 2240, *Engagement Work Program*:
   a. Matters to be considered prior to preparing the work program include
      1) Engagement scope
      2) Management’s operating goals and objectives
      3) Means of achieving objectives
      4) A risk and control matrix
      5) Availability of essential resources
      6) Sample sizes
      7) Conclusions and judgments during planning
      8) Prior engagement communications
   b. Work programs reflect choices of procedures needed to assess risks and test related controls in the areas reviewed. They also reflect the **nature, extent, and timing** of procedures needed to achieve objectives.
      1) Each procedure should test a specific control over risk.
      2) Work programs should be documented so that all team members know what remains to be done.

c. Work programs are **approved** by management of the internal audit activity prior to the beginning of the work.

1) The program is amended as necessary during the engagement to respond to findings. Amendments also should be approved by internal audit activity management.

2) IG 2340, *Engagement Supervision*, states that the **engagement supervisor** should approve the work program. The primary concern is that the work program is an efficient way to achieve objectives.

a) The work program should provide not only procedures for obtaining information but also for analysis, evaluation, and documentation of that information.

d. Work programs typically include a time budget used to control and evaluate the progress of the engagement.

3. An unplanned engagement is an **impromptu** audit. The first procedure therefore is to develop the work program. Once the work program is completed, the auditor performs surveys and establishes initial engagement objectives.

a. For example, if an internal audit supervisor suspects that an auditable issue exists in Department X, a staff auditor should be instructed to follow up promptly. In this case, the first procedure performed by the staff auditor is to develop the work program. Next, the auditor should document the initial engagement objectives.

4. If certain balances (e.g., cash) are subject to a greater risk of fraud, more effective engagement procedures may need to be performed.

a. Materiality relates to the qualitative (e.g., quality assurance programs) or quantitative (i.e., monetary) significance of an item. Thus, in planning the engagement, internal auditors consider, among other things, material risks and opportunities for material improvements.

5. If internal auditors discover that an area was omitted from the engagement work program, they must evaluate whether completion of the engagement as planned will be adequate to achieve the engagement objectives. They should

a. Document the discrepancies and communicate recommendations to management.
b. Modify the engagement work program to adjust for differences noted.

6. **Use of a Pro Forma Work Program**

a. A pro forma or standardized work program is used for repeated engagements related to similar operations. For example, when auditing a specific fast-food location, the pro forma work program can be repeated for multiple locations.

1) It is ordinarily modified over a period of years in response to problems encountered.

a) The pro forma work program ensures at least minimum coverage; provides comparability; and saves resources when operations at different locations have similar activities, risks, and controls.

b) However, a pro forma work program is not appropriate for a complex or changing operating environment. The engagement objectives and related procedures may no longer be relevant.

STUDY UNIT SIX

INFORMATION GATHERING

This study unit is the second of four covering **Domain III: Performing the Engagement** from The IIA's CIA Exam Syllabus. This domain makes up 40% of Part 2 of the CIA exam and is tested at the **basic** and **proficient** cognitive levels. Refer to the complete syllabus located in Appendix B to view the relevant sections covered in Study Unit 6.

6.1 THE FOUR QUALITIES OF INFORMATION

SUCCESS TIP

The practice of internal auditing is governed by professional standards. Thus, how an internal auditor performs an engagement is as important as the final product. Part 2 of the CIA exam contains numerous questions regarding (1) the procedures to be applied in a given situation and (2) the proper documentation. Workpapers must be formatted and cross-referenced so that a reviewer can understand how the engagement was conducted and whether the evidence gathered supports the results reported.

Performance Standard 2310
Identifying Information

Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.

Interpretation of Standard 2310

- **Sufficient** information is factual, adequate, and convincing so that a prudent, informed person would reach the same conclusions as the auditor.
- **Reliable** information is the best attainable information through the use of appropriate engagement techniques.
- **Relevant** information supports engagement observations and recommendations and is consistent with the objectives for the engagement.
- **Useful** information helps the organization meet its goals.

1. Determining whether information is adequate for the internal auditor's purposes is a matter of professional judgment that depends on
   a. The particular situation and
   b. The internal auditor's training, experience, and other personal traits.

2. **Sufficient Information**
   a. The sufficiency criterion applies an objective standard. The conclusions reached should be those of a prudent, informed person.
      1) Sufficiency is enhanced when samples are chosen using standard statistical methods.
   b. The basic issue is whether the information has the degree of persuasiveness needed.
      1) For example, persuasiveness must be greater in a fraud investigation of a senior manager than in an engagement involving petty cash. The difference in risk determines the quality and quantity of information.
3. **Reliable Information**
   a. Information is reliable when it is obtained and documented so that a prudent, informed individual can produce the same results and draw the same conclusions. Thus, the internal auditor's results should be verifiable by others. Verifiability is facilitated by systematic documentation.
      1) Reliable information is valid. It accurately represents the observed facts and is free from error and bias.
      2) A synonym for "reliable" is "competent."
   b. Information should consist of what may be collected using reasonable efforts subject to such inherent limitations as the cost-benefit constraint.
      1) Accordingly, internal auditors use different methods, e.g., statistical sampling and analytical auditing procedures.
   c. Information is more reliable if it is
      1) Obtained from sources independent of the engagement client, such as confirmations of receivables or expert appraisals that are timely and made by a source with no connection to the auditee
      2) Corroborated by other information
      3) Direct, such as the internal auditor's personal observation, rather than indirect, such as hearsay
      4) An original document, not a copy
4. **Relevant Information**
   a. The definition of relevance emphasizes the need for work to be restricted to achieving objectives. However, information also should be gathered on all matters within the engagement's scope.
   b. Relevant information has a logical relationship to what it is offered to prove.
      1) For example, vouching journal entries to the original documents does not support the completeness assertion about reported transactions. Instead, tracing transactions to the accounting records provides relevant information.

5. **Useful Information**

   a. Information is useful when it helps the organization meet its objectives.

   b. The organization’s ultimate objective is to create value for its owners, other stakeholders, customers, and clients. Accordingly, this characteristic of information is consistent with the definition of internal auditing. It should add value, improve operations, and help an organization achieve its objectives.

   The following is a useful memory aid for the four qualities of information:

Should	**S**ufficient
Rick	**R**eliable
Record	**R**elevant
Uniformly	**U**seful

6.2 SOURCES AND NATURE OF INFORMATION

1. **Sources of Information**

   a. **Internal information** originates and remains with the engagement client.

      1) Payroll records are an example. They are initially generated by the client and then are subsequently processed and retained by the client.

      2) Lack of involvement of external parties reduces the persuasiveness of information.

         a) The reliability of information is greater when it comes from sources that are independent of the client.

   b. **Internal-external information** originates with the client but also is processed by an external party.

      1) Examples are canceled checks. These documents are created by the client but circulate through the banking system. A bank’s acceptance of a check is some confirmation of its validity.

      2) Internal-external information is deemed to be more reliable than purely internal information.

   c. **External-internal information** is created by an external party but subsequently processed by the client.

      1) Such information has greater validity than information initiated by the client, but its value is impaired because of the client’s opportunity to alter or destroy it.

         a) Suppliers’ invoices are typical examples of external-internal information. Others include the canceled checks included in a cutoff bank statement received by the auditor directly from the bank.

   d. **External information** is created by an independent party and transmitted directly to the internal auditor. External information is ordinarily regarded as the most reliable because it has not been exposed to possible alteration or destruction by the client.

      1) Common examples are confirmations of receivables sent in response to the internal auditor’s requests.

   e. **Outsourcing services**, such as clerical, accounting, and internal audit services, may result in information difficult to classify in this framework.

2. **Nature of Information**
   a. The following are forms of **legal evidence**:
      1) **Direct evidence** establishes a particular fact or conclusion without having to make any assumptions.
         a) Testimony by a witness to an event is a form of direct evidence.
      2) **Circumstantial evidence** establishes a fact or conclusion that can then lead by inference to another fact.
         a) The existence of a flat tire can lead to the conclusion that the tire was sabotaged. Obviously, such evidence must be used very carefully because the tire might have been damaged accidentally.
      3) **Conclusive evidence** is absolute proof, by itself.
         a) The classic example is that of a watch in the desert. The mere fact of finding the watch proves that someone put it there. It did not assemble itself spontaneously out of sand.
      4) **Corroborative evidence** serves to confirm a fact or conclusion that can be inferred from other evidence.
         a) An example is an employee who claims to have been working late on a certain night. A member of the building custodial staff can provide corroborating evidence that this employee was seen in the office.
   b. The following are forms of **audit evidence**:
      1) **Physical information** consists of the internal auditor’s direct observation and inspection of people, property, or activities, e.g., of the counting of inventory.
         a) Photographs, maps, graphs, and charts may provide compelling physical information.
         b) When physical observation is the only information about a significant condition, at least two internal auditors should view it.
      2) **Testimonial information** consists of written or spoken statements of client personnel and others in response to inquiries or interview questions.
         a) Such information may give important indications about the direction of engagement work.
         b) Testimonial information may not be conclusive and should be supported by other forms of information when possible.
      3) **Documentary information** exists in some permanent form, such as checks, invoices, shipping records, receiving reports, and purchase orders.
         a) Thus, it is the most common type gathered by internal auditors.
         b) Documentary information may be internal or external.
            i) Examples of external information are replies to confirmation requests, invoices from suppliers, and public information held by a governmental body, such as real estate records.
            ii) Examples of internal information include accounting records, receiving reports, purchase orders, depreciation schedules, and maintenance records.

4) **Analytical information** is drawn from the consideration of the interrelationships among data or, in the case of internal control, the particular policies and procedures of which it is composed.

   a) Analysis produces circumstantial information in the form of inferences or conclusions based on examining the components as a whole for consistencies, inconsistencies, cause-and-effect relationships, relevant and irrelevant items, etc.

3. **Levels of Persuasiveness of Evidence**

   a. An auditor's **physical examination** provides the most persuasive form of evidence.

   b. Direct **observation** by the auditor is the next most persuasive. The lack of precise measurement is a weakness. (Observation is covered in Subunit 6.5.)

   c. Information originating from a **third party** is less persuasive than information gathered by the auditor but more persuasive than information originating from the client.

   d. Information originating with the **client** can be somewhat persuasive in documentary form, especially if it is subject to effective internal control. But client oral testimony is the least persuasive of all.

4. **Incomplete Information**

   a. If the client provides the internal auditor with incomplete information that is used to conclude on the effectiveness of a function or process, the internal auditor should

      1) Perform the analysis,
      2) Assess the effects of the incomplete information, and
      3) Disclaim any assertion regarding the information's reliability.

5. **Other Issues**

   a. Engagement client feedback is valuable in the internal auditor's determination of whether the information supports observations, conclusions, and recommendations.

   b. If engagement observations are negative, the client has a reason to find flaws in the internal auditor's information and reasoning. Constructive feedback of this kind helps the internal auditor strengthen the evidential base of engagement communications.

      1) The client's tendency to be critical of negative observations means that agreement lends substantial credibility to the internal auditor's position.

      2) However, agreement with positive observations may represent client self-interest rather than useful feedback.

6.3 QUESTIONNAIRES

1. **Internal Control Questionnaires**
   a. One use of questionnaires is to obtain an understanding of the client's controls. An internal control questionnaire is often very structured and detailed and is drafted in a yes/no or short-answer format.
   b. Appropriate uses of an internal control questionnaire include
      1) Filling out the questionnaire while interviewing the person who has responsibility for the function or subunit being reviewed,
      2) Drafting the questionnaire so that a "no" response requires attention, and
      3) Supplementing the completed questionnaire with a narrative description or flowchart.
   c. Disadvantages of these questionnaires are that
      1) They are difficult to prepare.
      2) They are time-consuming to administer.
      3) Engagement clients may anticipate the preferred responses and therefore may lie or give insufficient consideration to the task.
      4) Not all circumstances can be addressed.
      5) They are less effective than interviewing.
2. **Pre-Interview Questionnaires**
   a. Questionnaires are also an efficient way of preparing for an interview if they are properly designed and transmitted in advance. A formal questionnaire
      1) Involves the engagement client's supervisors and employees in the engagement and minimizes their anxiety.
      2) Provides an opportunity for engagement client self-evaluation.
      3) May result in a more economical engagement because the information it generates is prepared by those most familiar with it.
         a) The internal auditor must still ask clarifying questions and verify responses. However, only those answers that appear inappropriate should be pursued by asking for clarification or explanation.
         b) In this way, problems may be isolated and either compensating controls identified or extensions to the engagement procedures planned.
3. **Sequence and Format**
   a. The sequence and format of questions have many known effects on responses.
      1) For example, questions should be in a logical order, and personal questions should be asked last because of possible emotional responses.
   b. One method of reducing these effects is to use questionnaire variations that cause these biases to average out across the sample.
      1) Many types of questions may be used, e.g., multiple-choice, checklists, fill-in-the-blank, essay, or options indicating levels of agreement or disagreement.
      2) Questions must be reliably worded so that they measure what was intended to be measured.
      3) The questionnaire should be short to increase the response rate.

6.4 INTERVIEWING

1. **Use**

   a. Interviewing and other data-gathering activities are usually performed during the preliminary survey phase of an audit engagement.

      1) Interviews obtain testimonial evidence from engagement clients, other members of the organization who have contact with them, and independent parties.

   b. An interview allows auditors to ask questions clarifying initial testimony. Thus, auditors may deepen their understanding of operations and seek reasons for unexpected results and unusual events and circumstances.

      1) An interview is a secure and personal form of communication compared with, for example, email or paper-based documents.

      2) People tend to be less careful in their responses if the interview is one-to-one.

   c. The main purpose of interviews is to gather facts related to the audit engagement.

2. **Dislike of Evaluation**

   a. One fundamental problem faced by the internal auditor-interviewer is that people dislike being evaluated.

      1) Engagement clients may resent even the most constructive criticism and fear the possible adverse consequences of an audit report.

   b. Consequently, the internal auditor must gain the confidence of clients by demonstrating self-assurance, persuasiveness, fairness, empathy, and competence.

      1) The internal auditor may gain clients’ willing cooperation by explaining how the engagement may be helpful and by emphasizing that all parties are members of a team with the same objectives.

      2) Moreover, the internal auditor must avoid over-criticism.

         a) An internal auditor who finds no major problems may be insecure about the result. (S)he may therefore resort to excessive criticism of minor matters, an approach that may alienate engagement clients and management and not be cost beneficial.

3. **Four Types of Interviews**
   a. A **preliminary** interview is used to
      1) Promote the value of internal auditing,
      2) Understand the interviewee,
      3) Gather general information, and
      4) Serve as a basis for planning future interview strategies.

   b. A **fact-gathering** interview is oriented to the specific details that can be provided by a particular interviewee.
      1) Additional information can be sought in a nondirective manner, i.e., by asking open-ended questions.

   c. A **follow-up** interview is intended to answer questions raised during the analysis of the fact-gathering interview. It also tests the interviewee's acceptance of new ideas generated by the auditor.

   d. An **exit** interview helps to ensure the accuracy of conclusions, findings, and recommendations in the final engagement communication by discussing them with the interviewee.

4. **Planning an Interview**
   a. The auditor should prepare by reading operations manuals, organizational charts, prior engagement communications, results of questionnaires, etc.
      1) The auditor should understand not only the engagement client's functions, procedures, and terminology but also the psychological traits of auditee managers.

   b. The auditor should design basic questions.
      1) An auditor may use a directive approach emphasizing narrowly focused questions.
      2) An alternative is a nondirective approach using broad questions that are more likely to provide clarification and to result in unexpected observations.
      3) A combination of these approaches is often recommended.

5. **Scheduling Issues**
   a. Except when surprise is needed (e.g., in a review of cash or a fraud engagement), an appointment should be made well in advance for a specific time and place.
   b. The meeting should be in the engagement client's office, if feasible.
   c. The interview's duration should be set in advance.
   d. People tend to respond more freely if the interview is one-to-one.
   e. Except in fraud engagements, the purpose should be explained to the client.
   f. If possible, interviews should not be scheduled very late in the day, just before or after a vacation, or just before or after a meal.

6. **Opening the Interview**

   a. The auditor should be on time, and prompt notice should be given if delay is unavoidable.
   b. Engaging in initial, brief pleasantries may put the engagement client at ease.
   c. The purpose of the interview should be explained.
   d. The auditor should be polite, helpful, and nonthreatening.
   e. Confidentiality should be assured if feasible.

7. **Conducting the Interview**

   a. Interviewing requires an understanding of basic communications theory.

      1) A sender transmits an idea through a message.
      2) This message is encoded in a writing, in an oral statement, or in body language.
      3) The encoded message is transmitted through a channel or medium to a receiver.
         a) Barriers in the channel may interrupt or distort the message.
      4) The receiver decodes the message and interprets the message in accordance with his or her experience and knowledge.
         a) Technical jargon should be avoided so as to increase the chance that the message will be accurately decoded.
      5) The receiver may then undertake **action** or respond to the message.
      6) The words or actions of the receiver provide feedback to the sender.
         a) Feedback is vital because it tells the sender whether the message has been understood and acted upon.
      7) Nonverbal communication (body language) consists of facial expressions, vocal intonations, posture, gestures, appearance, and physical distance. Thus, by its nature, nonverbal communication is much less precise than verbal communication. However, in some cases, it may convey more information than verbal communication. But it is not necessarily more truthful.
         a) Nonverbal communication is heavily influenced by culture. For example, a nod of the head may have opposite meanings in different cultures.

   b. The interviewer should be tactful, objective, reasonable, and interested.

      1) (S)he also must avoid an accusatory tone and avoid statements not yet supported by evidence.
      2) The interviewer should not react negatively if the interviewee is uncooperative. (S)he should carefully explain the situation and provide an opportunity for the interviewee to calm down and continue the interview.
      3) The interviewee should not feel pressured or coerced during the interview.

   c. The interview should follow the agenda developed in the planning phase.

      1) Nevertheless, the interviewer should be flexible. Unexpected but worthwhile lines of inquiry may open up during the interview.

d. Active (effective) listening includes observing interviewee behavior (body language, such as eye contact), reserving judgment about what is said, asking clarifying questions, and allowing for periods of silence.

  1) An effective listener also enhances the communication process by sending appropriate nonverbal signals to the speaker.

    a) Thus, a listener who wishes to convey a positive and encouraging message should stop other activities and focus complete attention on the speaker.

  2) Reflecting what is said, that is, summarizing or rephrasing an answer, is a means of stimulating additional comments.

  3) Furthermore, the interviewee should be encouraged to ask relevant questions.

    a) These questions should be respectfully heard and duly included in the record of the interview.

  4) Empathy is a sensitive awareness of the speaker's feelings, thoughts, and experience. An empathic listener understands what the speaker wants to communicate rather than what the listener wants to understand.

  5) Listening with intensity involves concentrating on the speaker's message and disregarding distractions.

  6) Attentiveness is promoted by use of active listening techniques.

    a) For example, changing the wording of the questions and the sequence in which they are asked may eliminate some of the boredom associated with a series of interviews.

      i) The interviewer also may be able to refine the technique during the process.

e. Anticipation is one approach the interviewer can use to maintain focus during a far-ranging discussion. It assumes that the interviewer has done some preparation and is ready to listen intelligently.

  1) Active listening permits anticipation because the mind can process information more rapidly than most people speak. Thus, the listener has time to analyze the information and determine what is most important.

f. Leading questions (questions suggesting the answer) should be avoided.

g. Loaded questions (questions with self-incriminating answers) also should be avoided.

h. Questions requiring an explanatory response are usually preferable to those with binary (yes or no) responses.

i. An interviewer should be suspicious of answers that (1) are too smoothly stated, (2) fit too neatly with the interviewer's own preconceptions, (3) consist of generalizations, or (4) contain unfamiliar technical terminology.

  1) Thus, the interviewer must ask for greater specificity or other clarifications.

j. Care should be taken to differentiate statements of fact from statements of opinion.

k. The interviewer should understand what the interviewee regards as important.

l. Debate and disagreement with the interviewee should be avoided.

8. **Documentation**
   a. Good note taking during the interview is essential.
      1) Notes should be sufficiently readable and thorough to permit a full reconstruction of the information gathered. This write-up step should occur as soon as possible after the interview.
      2) The interviewee should be informed about the need for note taking.
      3) Notes should be properly dated and labeled, and the names and positions of interviewees should be included.
      4) The amount of time spent not looking at the interviewee should be minimized, and questions should not be asked while jotting notes.
      5) Interviews may be recorded only with the permission of the client.
   b. The notes and the memorandum prepared with their help are part of the workpapers and therefore the documentation of the engagement used to prepare communications.
      1) The memorandum should include significant events during the interview, such as interruptions or emotional outbursts.
      2) The internal auditor must be careful to use information in its proper context.
9. **Evaluation**
   a. This step is especially important if a follow-up interview is considered, but it is useful as a means of internal auditor self-improvement.
   b. The internal auditor should consider whether objectives were appropriate, whether they were attained, and, if not, why not.
   c. The internal auditor also should consider whether the planning was efficient, the interviewee was cooperative, and the interviewer made errors.

6.5 OTHER INFORMATION-GATHERING METHODS

1. **Observation**
   a. Observation is looking at a process or procedure being performed.
   b. By watching the physical activities of employees to see how they perform their duties, the auditor can determine whether written policies have been implemented.
      1) Moreover, observing a phenomenon in its natural setting eliminates some experimental bias.
   c. Observation is limited because employees who know they are being observed may behave differently while being observed. Accordingly, unobtrusive measures may be preferable.
      1) The possibility of observing unexpected or unusual behavior makes such measures useful for exploratory investigations.
   d. Observation is most persuasive for the existence or occurrence assertion (whether assets or liabilities exist and whether transactions have occurred).
      1) It is less persuasive for the completeness assertion (whether all transactions that should be reported are reported).
   e. Lack of experimental control and measurement precision are other limitations of observational research.
      1) Another is that some things, such as private behavior, attitudes, feelings, and motives, cannot be observed.
2. **Internal Surveys**
   a. Mail questionnaires are relatively cheap, eliminate interviewer bias, and gather large amounts of data. However, they tend to be inflexible, have a slow response time, and have nonresponse bias.
      1) The sample will not be truly random if respondents as a group differ from nonrespondents. Thus, people may choose not to respond for reasons related to the purpose of the questionnaire.
   b. Telephone interviews are a flexible means of obtaining data rapidly and controlling the sample. However, they introduce interviewer bias, are more costly, and gather less data than mail surveys.
   c. Rating scales are used to allow people to rate such things as service. The scale represents a continuum of responses.

EXAMPLE 6-1 Rating Scale

Rate the service you received on a scale of 1 to 10, 10 being the best. Circle the appropriate number.

1 2 3 4 5 6 7 8 9 10

STUDY UNIT SEVEN

SAMPLING AND STATISTICAL QUALITY CONTROL

This study unit is the third of four covering **Domain III: Performing the Engagement** from The IIA's CIA Exam Syllabus. This domain makes up 40% of Part 2 of the CIA exam and is tested at the **basic** and **proficient** cognitive levels. Refer to the complete syllabus located in Appendix B to view the relevant sections covered in Study Unit 7.

7.1 STATISTICAL CONCEPTS

1. Populations and Samples

a. A population is an entire group of items.

b. Sampling involves selecting representative items from a population, examining those selected items, and drawing a conclusion about the population based on the results derived from the examination of the selected items. Other data collection methods include the following:

1) A **case study** is a data collection method that identifies hypotheses that can be tested on a larger scale.

2) An **evaluation synthesis** is a systematic procedure that organizes observations and results from separate engagements and combines them into a single evaluation for all of the included engagements.

3) **Modeling** is a data collection method that simulates an existing fact, occurrence, or circumstance for further study.

c. Auditors must draw conclusions about populations (invoices, accounts receivable, etc.) that are too numerous for every item to be tested.

1) By applying the principles of statistics, auditors can test relatively small samples that allow them to draw conclusions about a population with measurable reliability.

2) The main issue in sampling is choosing a sample that is representative of the population. Valid conclusions then may be stated about the population.

2. **Population Distributions**

   a. For audit purposes, each item in a population is associated with a variable of interest to the auditor.

      1) **Discrete variables**, such as the yes/no decision whether to authorize payments of invoices, are tested using **attribute sampling** (discussed in further detail in Subunit 7.3).

      2) **Continuous variables**, such as the monetary amounts of accounts receivable, are tested using **variables sampling** (discussed in further detail in Subunit 7.4).

   b. An important characteristic of a population is the distribution of the values of the variable of interest.

      1) Of the many types of distributions, the most important is the **normal distribution** (the bell curve), depicted in Figure 7-1 on the next page. Its values form a symmetrical, bell-shaped curve centered around the mean.

3. **Measures of Central Tendency**

   a. The shape, height, and width of a population's distribution curve are quantified through its measures of central tendency.

      1) The **mean** is the arithmetic average of a set of numbers.

      2) The **median** is the middle value if data are arranged in numerical order. Thus, half the values are smaller than the median, and half are larger. It is the 50th percentile.

      3) The **mode** is the most frequently occurring value. If all values are unique, no mode exists.

EXAMPLE 7-1 Mean, Median, and Mode

An investor has eight investments and calculates the measures of central tendency for returns on the portfolio.

Mean = Arithmetic average of population values
= (US $43,500 + $52,100 + $19,800 + $41,600 + $52,100 + $66,700 + $33,900 + $54,900) ÷ 8
= US $364,600 ÷ 8
= US $45,575

Median = Midpoint between two central-most population values
Values ranked: US $19,800; $33,900; $41,600; $43,500; $52,100; $52,100; $54,900; $66,700
= (US $43,500 + $52,100) ÷ 2
= US $95,600 ÷ 2
= US $47,800

Mode = Most frequent value in population
= US $52,100

b. In a **normal distribution**, the mean, median, and mode are the same, and the tails are identical. (Shown in Figure 7-1.)

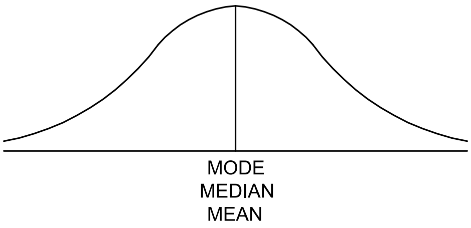


Figure 7-1

c. In some asymmetrical frequency distributions, the **mean is greater than the mode**. The right tail is longer, and the distribution is positively skewed (to the right).

1) Accounting distributions tend to be skewed to the right. For instance, accounts receivable generally include many medium- and low-value items and a few high-value items. (Shown in Figure 7-2.)

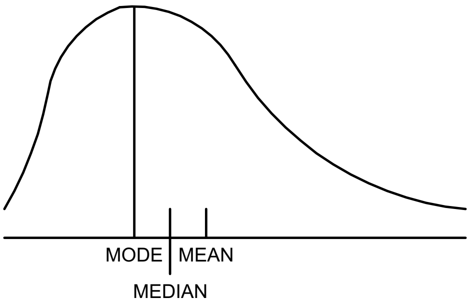


Figure 7-2

d. In some asymmetrical frequency distributions, the **median is greater than the mean**. The left tail is longer, and the distribution is negatively skewed (to the left). (Shown in Figure 7-3.)

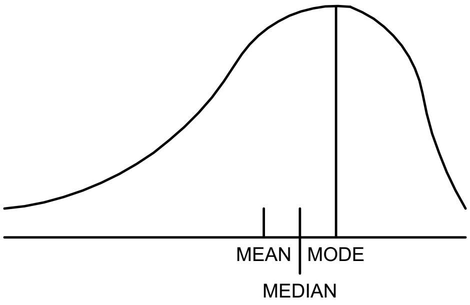


Figure 7-3

e. The median is the best estimate of central tendency for many asymmetrical distributions because the median is not biased by extremes.

4. Standard Deviation and Confidence Level for Normal Distributions

a. A population’s variability is the extent to which the values of items are spread about the mean (dispersion). It is measured by the **standard deviation**.

1) The standard deviation is a measure of the dispersion of a set of data from its mean.

a) When the items have little dispersion, the standard deviation is small.

b) When the items are highly dispersed, the bell curve is relatively flat and the standard deviation is large.

2) Normal distributions may have the following fixed relationships between the area under the curve and the distance from the mean.

Distance (±) in Standard Deviations (Confidence Coefficient)	Area under the Curve (Confidence Level)
1.0	68%
1.64	90%
1.96	95%
2.0	95.5%
2.57	99%
3.0	99.7%

3) For example, 68% of the items are within one standard deviation of the mean in either direction.

a) Approximately 95% of the items are within 2 standard deviations of the mean.

EXAMPLE 7-2 Normal Distribution

A certain species of pine tree has an average adult height of 20 feet, with each standard deviation representing 1 foot. The conclusion from the distribution below is that 68% of all trees of this species will reach a height between 19 and 21 feet (1 standard deviation), 95.5% will be between 18 and 22 feet (2 standard deviations), and 99.7% will be between 17 and 23 feet (3 standard deviations).

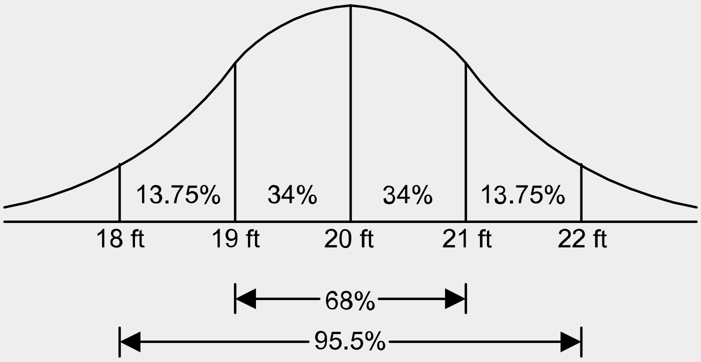


Figure 7-4

5. **Confidence Level and Confidence Interval**

   a. The area under the curve is the confidence level.

      1) The **confidence level** is the percentage of times that a sample is expected to be representative of the population; i.e., a confidence level of 95% should result in representative samples 95% of the time.

      2) A person selecting an item at random from a normally distributed population can be, for example, 95% confident that the value of the item is within 1.96 standard deviations of the mean and 99% confident that it will fall within 2.57 standard deviations of the mean.

   b. A **confidence interval** for a given confidence level is the range around a sample value that is expected to contain the true population value. It is constructed using the confidence coefficient for the number of standard deviations (based on the normal distribution) for the confidence level chosen.

      1) If repeated random samples are drawn from a normally distributed population and the auditor specifies a 95% confidence level, the probability is that 95% of the confidence intervals constructed around the sample results will contain the population value.

EXAMPLE 7-3 Confidence Level and Confidence Interval

An auditor took a random sample of sales authorizations. Based on the sample, the sales department authorized a sale after checking the credit score of the customer 88% of the time.

- If the confidence interval (or precision) is 6%, the auditor can be confident that between 82% (88% – 6%) and 94% (88% + 6%) of all the company’s sales were authorized after checking credit scores.
- The confidence level is the auditor’s desired reliability of the sample. If the specified confidence level is 95% and the precision is 6%, the auditor can be 95% confident that the percentage of all the company’s sales that were authorized after checking credit scores is between 82% and 94%.

      2) For a given confidence level, the size of the confidence interval depends on the sample size.

         a) The larger the sample size, the smaller the confidence interval can be.

         b) A smaller confidence interval means that the true population value is expected to be in the narrower range around the sample value.

      3) After the sample is drawn, the confidence interval may be widened or narrowed based on a change in the confidence level.

         a) If the confidence level is increased, then the confidence interval will be widened.

         b) If the confidence level is decreased, then the confidence interval will be narrowed.

6. **Pilot Sampling and Standard Error**

   a. The auditor can estimate the standard deviation of a population using a pilot sample.

   b. The **standard error of the mean** is the standard deviation of the distribution of sample means. The standard error is used to compute precision (the confidence interval). The larger the standard error, the wider the interval.

   c. The **coefficient of variability** measures the relative variability within the data and is calculated by dividing the standard deviation of the sample by the mean.

7.2 SAMPLING CONCEPTS

1. **Nonstatistical (Judgmental) Sampling**
    a. Judgmental sampling uses the auditor's **subjective** judgment to determine the sample size (number of items examined) and sample selection (which items to examine).
        1) This subjectivity is not always a weakness. The auditor, based on his or her experience, is able to select and test only the items (s)he considers to be the most important.
    b. The following are the advantages of judgmental sampling:
        1) The process can be less expensive and less time consuming. No special knowledge of statistics and no special statistics software are required.
        2) The auditor has greater discretion to use his or her judgment and expertise. Thus, if the auditor has substantial experience, no time is wasted on testing immaterial items.
    c. The following are the disadvantages of judgmental sampling:
        1) It does not provide a quantitative measure of sampling risk.
        2) It does not provide a quantitative expression of sample results.
        3) If the auditor is not proficient, the sample may not be effective.
2. **Statistical Sampling**
    a. Statistical sampling provides an objective method of determining sample size and selecting the items to be examined.
        1) Unlike judgmental sampling, it also provides a means of **quantitatively** assessing **precision** (how closely the sample represents the population) and **confidence level** (the percentage of time the sample will adequately represent the population).
    b. Statistical sampling helps the auditor design an efficient sample, measure the sufficiency of evidence obtained, and evaluate the sample results based on quantified data.
    c. The following are the advantages of statistical sampling:
        1) It provides a quantitative measure of sampling risk, confidence level, and precision.
        2) It provides a quantitative expression of sample results.
        3) It helps the auditor to design an efficient sample.
    d. The following are the disadvantages of statistical sampling:
        1) It can be more expensive and time consuming than nonstatistical sampling.
        2) It requires special statistical knowledge and training.
        3) It requires statistical software.
    e. In some instances, internal auditors may need to evaluate whether the use of historical data or drawing a new sample is optimal.
3. **Nonsampling vs. Sampling Risk**
    a. **Nonsampling risk** is audit risk not related to sampling. A common audit risk is the auditor's failure to detect an error in a sample.
        1) Nondetection of an error in a sample can be caused by auditor inattention or fatigue. It also can be caused by application of an inappropriate audit procedure, such as looking for the wrong approvals in a sample of documents.

b. **Sampling risk** is the risk that a sample is not representative of the population. An unrepresentative sample may result in an incorrect conclusion.

   1) Statistical sampling allows the auditor to quantify sampling risk. An auditor should never attempt to quantify the sampling risk of a nonstatistically drawn sample.

   2) Sampling risk is **inversely related** to sample size. As the sample increases, sampling risk decreases.

4. **Selecting the Sampling Approach**

a. In a **random sample**, every item in the population has an equal and nonzero chance of being selected.

   1) If enough large random samples are drawn, the mean of their means will approximate the population mean closely enough that they are considered to be representative of the population.

   2) For very large populations, the absolute size of the sample affects the precision of its results more than its size relative to the population. Thus, above a certain population size, the sample size generally does not increase.

   3) The traditional means of ensuring randomness is to assign a random number to each item in the population. Random number tables are often used for this purpose.

      a) Random number tables contain collections of digits grouped randomly into columns and clusters. After assigning numbers to the members of the population, the tables can be used to select the sample items.

b. An **interval (systematic) sampling** plan assumes that items are arranged randomly in the population. If they are not, a random selection method should be used.

   1) Interval sampling divides the population by the sample size and selects every *n*th item after a random start in the first interval. For example, if the population has 1,000 items and the sample size is 35, every 28th item (1,000 ÷ 35 = 28.57) is selected.

      a) Interval sampling is appropriate when, for instance, an auditor wants to test whether controls were operating throughout an entire year. (A random sample might result in all items being selected from a single month.)

      b) Because interval sampling requires only counting in the population, no correspondence between random numbers and the items in the population is necessary as in random number sampling.

EXAMPLE 7-4 Interval (Systematic) Sampling

If the population contains 8,200 items and a sample of 50 is required, every 164th item is selected (8,200 ÷ 50). After a random start in the first interval (1 to 164), every additional 164th item is selected. For example, if the 35th item is the first selected randomly, the next is the 199th (35 + 164). The third item is the 363rd (199 + 164). The process is continued until the 50 items are identified.

c. **Block (cluster) sampling** randomly selects groups of items as the sampling units rather than individual items. An example is the inclusion in the sample of all cash payments for May and September.

   1) One possible disadvantage is that the variability of items within the clusters may not be representative of the variability within the population.

5. **Basic Steps in a Statistical Plan**

   a. **Determine the objectives of the plan.**

      1) For a test of controls, an example is to conclude that control is reasonably effective.

      2) For a test of details, an example is to conclude that a balance is not misstated by more than an immaterial amount.

   b. **Define the population.** This step includes defining the sampling unit (an individual item in the population) and considering the completeness of the population.

      1) For tests of controls, the period covered is defined.
      2) For tests of details, individually significant items may be defined.

   c. **Determine acceptable levels of sampling risk** (e.g., 5% or 10%).

   d. **Calculate the sample size** using tables or sample-size formulas.

      1) In some cases, it is efficient to divide the population into subpopulations or strata. The primary objective of **stratification** is to minimize variability.

      2) Stratification also allows the auditor to apply more audit effort to larger elements or more risky parts of the population.

      3) For example, when auditing sales revenue, an auditor could divide the population into strata of dollar increments. The auditor could test transactions under US $500, between US $501 and US $2,000, and US $2,001 and above.

   e. **Select the sampling approach**, e.g., random, interval, or block.

   f. **Take the sample.** The auditor selects the items to be evaluated.

   g. **Evaluate the sample results.** The auditor draws conclusions about the population.

   h. **Document the sampling procedures.** The auditor prepares appropriate workpapers.

7.3 ATTRIBUTE SAMPLING

1. **Uses**

   a. In attribute sampling, each item in the population has an attribute of interest to the auditor, e.g., evidence of proper authorization. Thus, attribute sampling is appropriate for **discrete variables**.

      1) Attribute sampling is used for tests of controls, i.e., when two outcomes are possible (compliance or noncompliance).

2. **Sample Size**

   a. The sample size for an attribute test depends on the following four factors:

      1) The **confidence level** is the percentage of times that a sample is expected to be representative of the population. The **greater** the desired confidence level, the **larger** the sample size should be.

         a) For a test of the controls, the confidence level is the complement of the allowable risk of **overreliance** on the control. For example, if this risk is 5%, the confidence level is 95% (100% – 5%).

      2) The **population size** is the sum of the items to be considered for testing. The larger the population size, the larger the sample size should be.

         a) However, for a very large population, the population size has a small effect on the sample size. Above a certain population size, the sample size generally does not increase.

      3) The **expected deviation rate** (expected rate of occurrence) is an estimate of the deviation rate in the current population.

         a) The **greater** the population deviation (variability in the population), the **larger** the sample size should be.

      4) The **tolerable deviation rate** (desired precision) is the highest allowable percentage of the population that can be in error (noncompliance rate) and still allow the auditor to rely on the tested control.

         a) The **lower** the tolerable deviation rate, the **larger** the sample size should be.

Factors Affecting Attribute Sample Size			
As the confidence level	*increases,*	*the sample size must*	*increase.*
As the expected deviation rate	*increases,*	*the sample size must*	*increase.*
As the tolerable deviation rate	*increases,*	*the sample size can*	*decrease.*
As the confidence level	*decreases,*	*the sample size must*	*decrease.*
As the expected deviation rate	*decreases,*	*the sample size must*	*decrease.*
As the tolerable deviation rate	*decreases,*	*the sample size can*	*increase.*

3. **Evaluation of Sample Results**

   a. The evaluation includes calculating the sample deviation rate and the achieved upper deviation limit.

   b. The **sample deviation rate** is the number of deviations observed in a sample divided by the sample size.

      1) This rate is the best estimate of the population deviation rate.

   c. The **achieved upper deviation limit (UDL)** is based on the sample size and the number of deviations discovered. Auditors use standard tables to calculate the UDL. In Table 1 below (adapted from an Audit Practice Release of the AICPA), the intersection of the sample size and the number of deviations indicates the achieved upper deviation limit.

   d. The **allowance for sampling risk** (achieved precision) is the difference between the achieved UDL determined from a standard table and the sample deviation rate.

      1) When the sample deviation rate exceeds the expected population deviation rate, the achieved UDL exceeds the tolerable rate at the given risk of overreliance. In that case, the sample does not support the planned reliance on the control.

      2) When the sample deviation rate does not exceed the expected population deviation rate, the achieved UDL does not exceed the tolerable rate at the given risk level. Thus, the sample supports the planned reliance on the control.

EXAMPLE 7-5 Evaluation of Sample Results

Assume the risk of overreliance is 5%, the tolerable rate is 6%, the expected population deviation rate is 2.5%, and the population size is over 5,000. Given these data, the sample size is 150.

During the engagement, the auditor discovered 3 deviations in the sample of 150. Using Table 1, the auditor can state at a 95% confidence level (the complement of a 5% risk of overreliance) that the true error occurrence rate is not greater than 5.1%.

The sample deviation rate equals 2% (3 deviations ÷ 150 sample size). Thus, the allowance for sampling risk equals 3.1% (5.1% – 2%).

The sample deviation rate (2%) does not exceed the expected population deviation rate (2.5%), and the sample supports the planned reliance on the control.

Table 1 -- Results Evaluation for Tests of Controls -- Upper % Limits at 5% Risk of Overreliance

Sample Size	Actual Number of Deviations Found										
	0	1	2	3	4	5	6	7	8	9	10
100	3.0	4.7	6.2	7.6	9.0	10.3	11.5	12.8	14.0	15.2	16.4
125	2.4	3.8	5.0	6.1	7.2	8.3	9.3	10.3	11.3	12.3	13.2
150	2.0	3.2	4.2	5.1	6.0	6.9	7.8	8.6	9.5	10.3	11.1
200	1.5	2.4	3.2	3.9	4.6	5.2	5.9	6.5	7.2	7.8	8.4

e. Each deviation should be analyzed to determine its nature, importance, and probable cause. Obviously, some are much more significant than others. Sampling provides a means of forming a conclusion about the overall population but should not be used as a substitute for good judgment.

1) The table below is based on a method for testing sampling concepts related to tests of controls. It is used to explain how to analyze the information. Many questions can be answered based on the analysis. The table depicts the possible combinations of the sample results and the true state of the population.

Auditor's Estimate Based on Sample Results	**True State of Population**	
	Deviation rate is less than tolerable rate.	Deviation rate exceeds tolerable rate.
Deviation rate is less than tolerable rate.	I. Correct	III. Incorrect
Deviation rate exceeds tolerable rate.	II. Incorrect	IV. Correct

a) Cell II represents potential underreliance on internal control. It affects the efficiency but not the effectiveness of the audit.

b) Cell III represents potential overreliance on internal control. It may result in audit failure.

4. **Other Attribute Sampling Methods**

a. **Discovery sampling** is appropriate when even a single deviation (noncompliance) is critical.

1) The occurrence rate is assumed to be at or near 0%, and the method cannot be used to evaluate results statistically if deviations are found in the sample.

2) The sample size is calculated so that it will include **at least one** instance of a deviation if deviations occur in the population at a given rate.

b. The objective of **stop-or-go sampling**, also called sequential sampling, is to reduce the sample size when the auditor believes the deviation rate in the population is low.

1) The auditor examines only enough sample items to be able to state that the deviation rate is below a specified rate at a specified level of confidence. If the auditor needs to expand the sample to obtain the desired level of confidence, (s)he can do so in stages.

2) Because the sample size is not fixed, the internal auditor can achieve the desired result, even if deviations are found, by enlarging the sample sufficiently. In contrast, discovery sampling uses a fixed sample size.

7.4 VARIABLES SAMPLING

1. **Uses**

   a. Variables sampling is used for **continuous variables**, such as weights or monetary amounts. Variables sampling provides information about whether a stated amount (e.g., the balance of accounts receivable) is materially misstated.

      1) Thus, variables sampling is useful for substantive tests. The auditor can determine, at a specified confidence level, a range that includes the true value.

   b. In variables sampling, both the upper and lower limits are relevant (a balance, such as accounts receivable, can be either under- or overstated).

   c. Auditors may employ the following variables sampling techniques:

      1) Unstratified mean-per-unit
      2) Stratified mean-per-unit
      3) Difference estimation
      4) Ratio estimation
      5) Monetary unit sampling

      NOTE: Each method is covered in this subunit, following a discussion of sample selection and interpretation.

2. **Sample Size**

   a. The sample size for a variables test depends on the following four factors:

      1) **Confidence level.** The **greater** the desired confidence level, the **greater** the sample size should be.

         a) For a variables sampling application, the confidence level is the complement of the allowable risk, also commonly referred to as acceptable risk, of **incorrect rejection**. For example, if this risk is 5%, the confidence level is 95% (100% – 5%).

         b) If the auditor needs a more precise estimate of the tested amount, (s)he must increase the confidence level and the sample size.

            i) A more precise estimate requires a narrower precision (confidence interval).

         c) The confidence coefficient serves the same function as in attribute sampling. But, in variables sampling, it corresponds to a range around the calculated amount rather than an estimate of the maximum error rate.

      2) **Population size.** Generally, the **larger** the population, the **larger** the sample.

         a) However, for a very large population, the population size has a small effect on sample size. Above a certain population size, the sample size generally does not increase.

            i) Increasing the confidence level results in a wider precision (confidence interval) if the standard error is constant.

            ii) Decreasing the allowable risk of incorrect rejection (the complement of the confidence level) increases the confidence level and results in a wider interval if the standard error is constant.

3) **Tolerable misstatement** (precision) is an interval around the sample statistic that is expected to include the true balance of the population at the specific confidence level.

   a) For example, an auditor has tested a variables sample with precision of ±4% and a confidence level of 90%. The conclusion is that the true balance of the account is US $1,000,000.

      i) The precision of ±4% gives the boundaries of the computed range.

      ii) Thus, 4% of US $1,000,000 equals US $40,000, resulting in a range of US $960,000 to US $1,040,000.

      iii) The auditor can conclude that the probability is only 10% that the true balance lies outside this range.

   b) The **narrower** the precision, the **larger** the sample should be.

4) **Standard deviation** (variability) of the population is a measure of the variability of the amounts in the population.

   a) An **increase** in the estimated standard deviation **increases** the sample size.
   b) The estimate can be based on pilot sample.

Factors Affecting Variables Sample Size			
As the confidence level	*increases,*	*the sample size must*	*increase.*
As the estimated standard deviation	*increases,*	*the sample size must*	*increase.*
As the population size	*increases,*	*generally, the sample size must*	*increase.*
As the tolerable misstatement	*increases,*	*the sample size can*	*decrease.*
As the confidence level	*decreases,*	*the sample size must*	*decrease.*
As the estimated standard deviation	*decreases,*	*the sample size must*	*decrease.*
As the population size	*decreases,*	*the sample size must*	*decrease.*
As the tolerable misstatement	*decreases,*	*the sample size can*	*increase.*

b. Important determinants of sample size include the following:

1) The greater the variability, the greater the required sample size.

2) The more sensitive the decision is to estimation errors, the greater the appropriate sample size.

3) In accordance with the cost-benefit principle, the greater the cost per observation, the smaller the appropriate sample size.

3. **Primary Methods of Variables Sampling**

   a. **Mean-per-unit (MPU) estimation** (also called unstratified MPU) averages the audited amounts of the sample items. It multiplies the average by the number of items in the population to estimate the population amount. An achieved precision at the desired level of confidence is then calculated.

      1) **Stratified** MPU is a means of increasing audit efficiency by separating the population into logical groups, usually by various ranges of the tested amounts. By creating multiple populations, the variability within each is reduced, allowing for a smaller overall sample size.

   b. **Difference estimation** estimates the misstatement of an amount by calculating the difference between the observed and recorded amounts for items in the sample. This method is appropriate only when per-item recorded amounts and their total are known. Difference estimation

      1) Determines differences between the audited and recorded amounts of items in the sample,
      2) Adds the differences,
      3) Calculates the mean difference,
      4) Multiplies the mean by the number of items in the population, and
      5) Calculates an achieved precision at the desired level of confidence.

   c. **Ratio estimation** is similar to difference estimation. However, it estimates the population misstatement by multiplying the recorded amount of the population by the ratio of the total audited amount of the sample items to their total recorded amount.

      1) Ratio estimation is preferable to MPU estimation when the standard deviation of the sample item amounts is greater than the standard deviation of the distribution of the ratios of the audited amounts of sample items compared with their recorded amounts.

      2) Ratio estimation is preferable to difference estimation when differences between the audited amounts of sample items and their recorded amounts are expected to vary in proportion to the size of the sample items.

         a) For example, a sample of two items consists of an account with a US $1,000 recorded balance and a misstatement of US $100 and an account with a recorded balance of US $100 and a misstatement of US $10.

            i) The misstatements of US $900 and US $90 are quite different but vary in proportion to the size of the account since each misstatement is 10% of the account value.

            ii) In situations like this, ratio estimation is preferable to difference estimation.

EXAMPLE 7-6 Comparison of Variables Sampling Methods

An auditor examines a sample of 150 accounts receivable with a total recorded amount of US $172,500. The total population of 3,400 accounts receivable has a total recorded amount of US $3,500,000. Based on the audit, the total amount of the 150 sampled accounts is US $168,000.

MPU Estimation

- The average amount per sampled item is US $1,120 ($168,000 ÷ 150).
- The estimated correct balance of the population (accounts receivable) is **US $3,808,000** ($1,120 mean per unit value × 3,400 number of items in the population).
- The projected understatement is US $308,000.

Difference Estimation

- The difference between the audited and recorded amounts of items in the sample is US $4,500 ($172,500 – $168,000).
- The mean difference is US $30 ($4,500 ÷ 150 number sample items).
- The estimated total population error is determined by multiplying the mean by the number of items in the population. It equals US $102,000 (3,400 × $30).
- The estimated correct balance of the population (accounts receivable) is **US $3,398,000** ($3,500,000 recorded amount of the population – $102,000 estimated error).
- The projected overstatement is US $102,000.

Ratio Estimation

- The ratio of the total audited amount of the sample items to their total recorded amount is 0.974 (US $168,000 audited amount ÷ $172,500 recorded amount).
- The estimated correct balance of the population (accounts receivable) is **US $3,409,000** ($3,500,000 recorded amount of the population × 0.974 ratio).
- The projected overstatement is US $91,000.

NOTE: An achieved precision at the desired level of confidence is then calculated. For example, assume the sample of 150 accounts with a total amount of US $168,000 was based on precision of ±3% and a confidence level of 95%. Using ratio estimation, the precision interval equals ±US $102,270 ($3,409,000 × 3%). The auditor can conclude that the probability is only 5% that the true balance lies outside the range of US $3,306,730 to US $3,511,270.

d. **Monetary-unit sampling (MUS)**, also known as probability-proportional-to-size (PPS) sampling, uses a monetary unit as the sampling unit. It applies **attribute sampling** methods to reach a conclusion about the probability of overstating monetary amounts.

1) Under MUS, the sampling unit is a unit of money rather than, for example, an invoice or an account balance. The item (invoice, account, etc.) containing the sampled monetary unit is selected for testing.

2) MUS is appropriate for testing account balances for overstatement when some items may be far larger than others in the population. In effect, it stratifies the population because the larger account balances have a greater chance of being selected.

3) MUS is most useful if few misstatements are expected.

4) MUS does not require the use of a measure of variability (e.g., standard deviation) to determine the sample size or interpret the results.

5) Thus, in Example 7-6 above, the objective of MUS may be to determine that the total recorded amount of accounts receivable (US $3,500,000) is not overstated by more than 3%, with a confidence level of 95%.

Characteristics of Variables and Attribute Sampling Methods

Unstratified Mean-Per-Unit

- Less efficient than ratio estimation when a high error rate is expected.
- Inappropriate when many small balance account errors exist.

Stratified Mean-Per-Unit

- Less efficient than ratio estimation when a high error rate is expected.
- Inappropriate when many small balance account errors exist.
- Greater emphasis on larger or more important items.
- Increases audit efficiency by separating the population into logical groups (subpopulations).
- Variability within a stratum is reduced. Thus, sample size is reduced.

Difference Estimation

- Used when sampling for monetary values.
- Individual carrying amounts must be known to use difference estimation.
- Sufficient misstatements must exist to generate a reliable sample.
- Reliable and efficient when small errors predominate and the errors are not skewed.
- If the number of errors is small, a very large sample is required to provide a representative difference between audit and recorded amounts.

Ratio Estimation

- More efficient than mean-per-unit when a high error rate is expected.
- Reliable and efficient when small errors predominate and the errors are not skewed.
- Audit amounts should be proportional to carrying amounts.
- Appropriate for proportional differences.
- If the number of errors is small, a very large sample is required to provide a representative difference between audit and recorded amounts.
- A minimum number of differences must be present to use ratio estimation.
- Proportional relationships and differences support the use of ratio estimation.

Monetary-Unit Sampling

- Less accurate when many errors are expected.
- Estimates monetary amounts of errors when the expected error frequency is low.
- Because the sampling unit is the monetary unit, this method increases the likelihood of selecting large items.
- A measure of variability is not needed.

Attribute Sampling

- Not used to estimate a monetary amount.
- Used for applications involving binary (yes/no or right/wrong) propositions.
- Turnover volume is a characteristic of interest in attribute sampling.

7.5 STATISTICAL QUALITY CONTROL

1. **Uses**
   a. Statistical quality control determines whether a shipment or production run of units lies within acceptable limits. Items are either good or bad, i.e., inside or outside of control limits. It is also used to determine whether production processes are out of control.

2. **Acceptance Sampling**
   a. This method determines the probability that the rate of defective items in a batch is less than a specified level.

EXAMPLE 7-7 Acceptance Sampling

Assume a sample is taken from a population of 500. According to standard acceptance sampling tables, if the sample consists of 25 items and not one is defective, the probability is 93% that the population deviation rate is less than 10%. If 60 items are examined and no defects are found, the probability is 99% that the deviation rate is less than 10%. If two defects in 60 units are observed, the probability is 96% that the deviation rate is less than 10%.

3. **Statistical Control Charts**
   a. Statistical control charts are graphic aids for monitoring the status of any process subject to acceptable or unacceptable variations during repeated operations.
      1) They also have applications of direct interest to auditors and accountants, for example,
         a) Unit cost of production,
         b) Direct labor hours used,
         c) Ratio of actual expenses to budgeted expenses,
         d) Number of calls by sales personnel, or
         e) Total accounts receivable.
   b. A control chart consists of three lines plotted on a horizontal time scale.
      1) The center line represents the overall mean or average range for the process being controlled. The other two lines are the upper control limit (UCL) and the lower control limit (LCL).
      2) The processes are measured periodically, and the values (X) are plotted on the chart.
         a) If the value falls within the control limits, no action is taken.
         b) If the value falls outside the limits, the result is abnormal, the process is considered out of control, and an investigation is made for possible corrective action.

c. Another advantage of the chart is that it makes trends and cycles visible.

1) A disadvantage of the chart is that it does not indicate the cause of the variation.

EXAMPLE 7-8 Statistical Control Chart

The chart below depicts 2 weeks of production by a manufacturer who produces a single precision part each day. To be salable, the part can vary from the standard by no more than ± 0.1 millimeter.

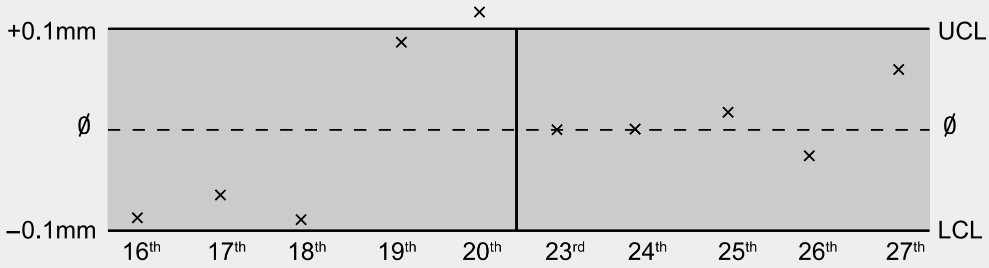


Figure 7-5

The part produced on the 20th had to be scrapped, and changes were made to the equipment to return the process to the controlled state for the following week's production.

d. Other chart types

1) P charts show the percentage of defects in a sample. They are based on an attribute (acceptable/not acceptable) rather than a measure of a variable.

2) C charts also are attribute control charts. They show defects per item.

3) An R chart shows the range of dispersion of a variable, such as size or weight. The center line is the overall mean.

4) An X-bar chart shows the sample mean for a variable. The center line is the average range.

4. **Variations**

a. Variations in a process parameter may have several causes.

1) Random variations occur by chance. Present in virtually all processes, they are not correctable because they will not repeat themselves in the same manner.

a) Excessively narrow control limits will result in many investigations of what are simply random fluctuations.

2) Implementation deviations occur because of human or mechanical failure to achieve target results.

3) Measurement variations result from errors in the measurements of actual results.

4) Model fluctuations can be caused by errors in the formulation of a decision model.

5) Prediction variances result from errors in forecasting data used in a decision model.

5. **Benchmarks**

a. Establishing control limits based on benchmarks is a common method. A more objective method is to use the concept of expected value. The limits are important because they are the decision criteria for determining whether a deviation will be investigated.

6. **Cost-Benefit Analysis**

   a. An analysis using expected value provides a more objective basis for setting control limits. The limits of controls should be set so that the cost of an investigation is less than or equal to the benefits derived.

      1) The expected costs include investigation cost and the cost of corrective action.

	(Probability of being out of control × Cost of corrective action)
+	(Probability of being in control × Investigation cost)
	Total expected cost

   b. The benefit of an investigation is the avoidance of the costs of continuing to operate an out-of-control process. The expected value of benefits is the probability of being out of control multiplied by the cost of not being corrected.

7. **Pareto Diagrams**

   a. A Pareto diagram is a bar chart that assists managers in what is commonly called 80:20 analysis.

      1) The 80:20 rule states that 80% of all effects are the result of only 20% of all causes. In the context of quality control, managers optimize their time by focusing their effort on the sources of most problems.

   b. The independent variable, plotted on the x-axis, is the factor selected by the manager as the area of interest: department, time period, geographical location, etc. The frequency of occurrence of the defect (dependent variable) is plotted on the y-axis.

      1) The occurrences of the independent variable are ranked from highest to lowest, allowing the manager to see at a glance which areas are of most concern.

EXAMPLE 7-9 Pareto Diagram

A chief administrative officer uses a Pareto diagram to view which departments are generating the most travel vouchers that have been rejected because of incomplete documentation.

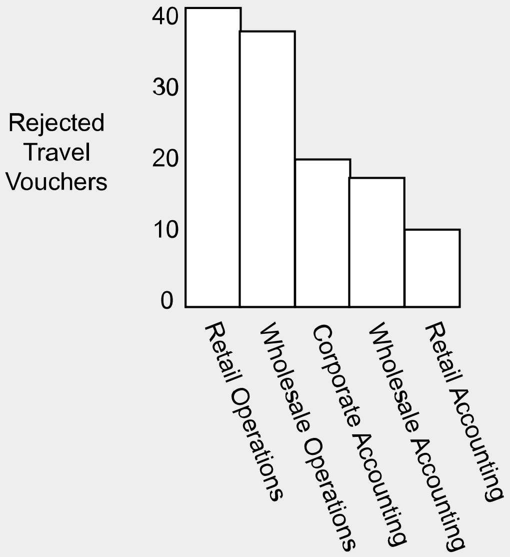


Figure 7-6

8. **Histograms**

    a. A histogram displays a continuous frequency distribution of the independent variable.

EXAMPLE 7-10 Histogram

This histogram shows the CAO the amount of travel reimbursement delayed by a typical returned travel voucher.

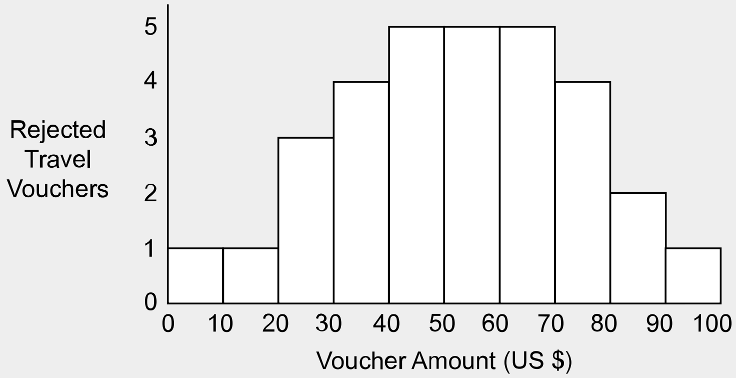


Figure 7-7

9. **Fishbone Diagrams**

    a. A fishbone (Ishikawa) diagram (also called a cause-and-effect diagram) is a total quality management process improvement technique.

        1) Fishbone diagrams are useful in studying causation (why the actual and desired situations differ).

    b. This format organizes the analysis of causation and helps to identify possible interactions among causes.

        1) The head of the skeleton contains the statement of the problem.

        2) The principal classifications of causes are represented by lines (bones) drawn diagonally from the heavy horizontal line (the spine).

        3) Smaller horizontal lines are added in their order of probability in each classification.

c. Below is a generic fishbone diagram.

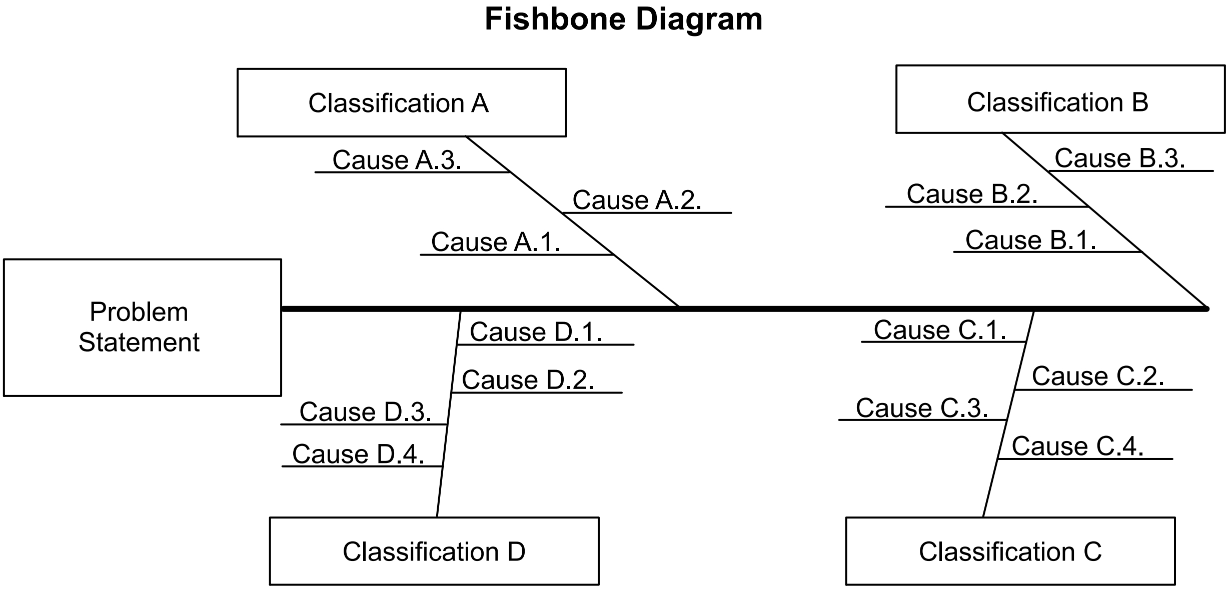


Figure 7-8

STUDY UNIT EIGHT

ANALYSIS, EVALUATION, DOCUMENTATION, AND SUPERVISION

This study unit is the fourth of four covering **Domain III: Performing the Engagement** from The IIA's CIA Exam Syllabus. This domain makes up 40% of Part 2 of the CIA exam and is tested at the **basic** and **proficient** cognitive levels. Refer to the complete syllabus located in Appendix B to view the relevant sections covered in Study Unit 8.

8.1 COMPUTERIZED AUDIT TOOLS

1. **Overview**
   a. Internal auditors should use available information technology (IT) to assist in performing audit work. The benefits of using IT include
      1) Reduced audit risk
      2) Increased productivity, resulting in more timely audit engagements
      3) Increased audit opportunities
2. Computer-assisted audit techniques (CAATs) may be systems- or transaction-based or may provide automated methods for extracting and analyzing large amounts of data.
3. **Generalized Audit Software (GAS)**
   a. Using GAS, the auditor loads a copy of the client's production data onto the auditor's own computer to perform various analytical procedures.
      1) For example, the auditor can search for duplicate records, gaps in numerically sequenced records, high-monetary-amount transactions, and suspect vendor numbers. Also, control totals can be calculated, and balances can be stratified for receivables testing.
      2) A limitation of GAS is that it can only be used on hardware with compatible operating systems. An advantage of using GAS is that a complete understanding of the client's hardware and software features or programming language is not required.
      3) Two GAS packages are ACL (Audit Command Language) and IDEA (Interactive Data Extraction and Analysis).

4. **Test Data**

   a. Test data allow the auditor to assess the controls embedded in an application by observing (1) whether the good data are correctly processed and (2) how well the system handles bad data.

      1) Test data, sometimes called a test deck, consist of a set of dummy inputs containing both good and bad data elements. This approach subjects auditor-created data to the client's programs.

      2) Test data must never be mingled with real data, and test data must not be allowed to interfere with production processing. Monitoring by IT personnel is crucial when the auditor uses test data.

5. **Parallel Simulation**

   a. Parallel simulation allows an auditor to determine whether the data are subjected to the processes that the client claims the application performs.

      1) Parallel simulation subjects client data to auditor-created programs.

      2) Parallel simulation requires the auditor to have considerable technical knowledge. The auditor also must have extensive communications with client personnel to learn the designed functions of the application being imitated.

6. **Data Mining and Extraction**

   a. The oldest form of data extraction is the manual copying of client records. Until the widespread use of photocopy machines, it was the only method.

      1) With the easy availability of computing, especially networking technology, data extraction can be performed quickly in very large volumes.

      2) The issue is ensuring that the data extracted are those required for the audit procedure being performed. Control totals and other methods are used for this purpose.

7. **Integrated Test Facility (ITF)**

   a. In this approach, the auditor creates a fictitious entity (a department, vendor, employee, or product) on the client's live production system.

      1) All transactions associated with the dummy entity are processed by the live system, and the auditor can observe the results.

   b. Use of an ITF requires great care to ensure that no transactions associated with the dummy entity are included in production reports and output files.

8. **Embedded Audit Module**

   a. An embedded audit module is an integral part of an application system. It is designed to identify and report actual transactions and other information that meet criteria having audit significance.

      1) An advantage is that it permits **continuous monitoring** of online, real-time systems.

      2) A disadvantage is that audit hooks must be programmed into the operating system and application programs to permit insertion of audit modules.

   b. Continuous monitoring is a management process that monitors whether internal controls are operating effectively on an ongoing basis.

9. **Application Tracing and System Mapping**

   a. Application tracing uses a feature of the programming language in which the application was written.

      1) Tracing aids computer programmers in following the step-by-step operation of a computer program's source code. It can be used by auditors for the same purpose.

   b. System mapping is similar to application tracing. But mapping is performed by another computer program instead of by the auditor.

10. **Spreadsheet Analysis**

    a. Electronic spreadsheets, such as Microsoft Excel, organize information into intersecting rows and columns. This organization permits easy analysis of large amounts of client data.

    b. Internal auditors can use spreadsheets to

       1) Evaluate "what if" scenarios,
       2) Create graphs,
       3) Analyze variances between actual and budgeted amounts, and
       4) Perform other analytical procedures.

11. **Internet**

    a. The Internet is a useful audit tool for gathering and disseminating audit-related information.

    b. The major use of the Internet by internal auditors is electronic communication.

    c. Users transmitting sensitive information across the Internet must understand the threats that arise that could compromise the confidentiality of the data.

       1) Security measures, such as encryption technology, need to be taken to ensure that the information is viewed only by those authorized to view it.

8.2 ANALYTICAL APPROACHES AND PROCESS MAPPING

1. Uses of Flowcharts

a. Flowcharts are graphical representations of the step-by-step progression of information through preparation, authorization, flow, storage, etc. The system depicted may be manual, computerized, or a combination of the two.

1) Flowcharting allows the internal auditor to analyze a system and to identify the strengths and weaknesses of internal controls and the appropriate areas of audit emphasis.

b. Flowcharting is typically used during the **preliminary survey** to gain an understanding of the client’s processes and controls.

2. Flowchart Symbols

a. Commonly used document flowchart symbols include the following:

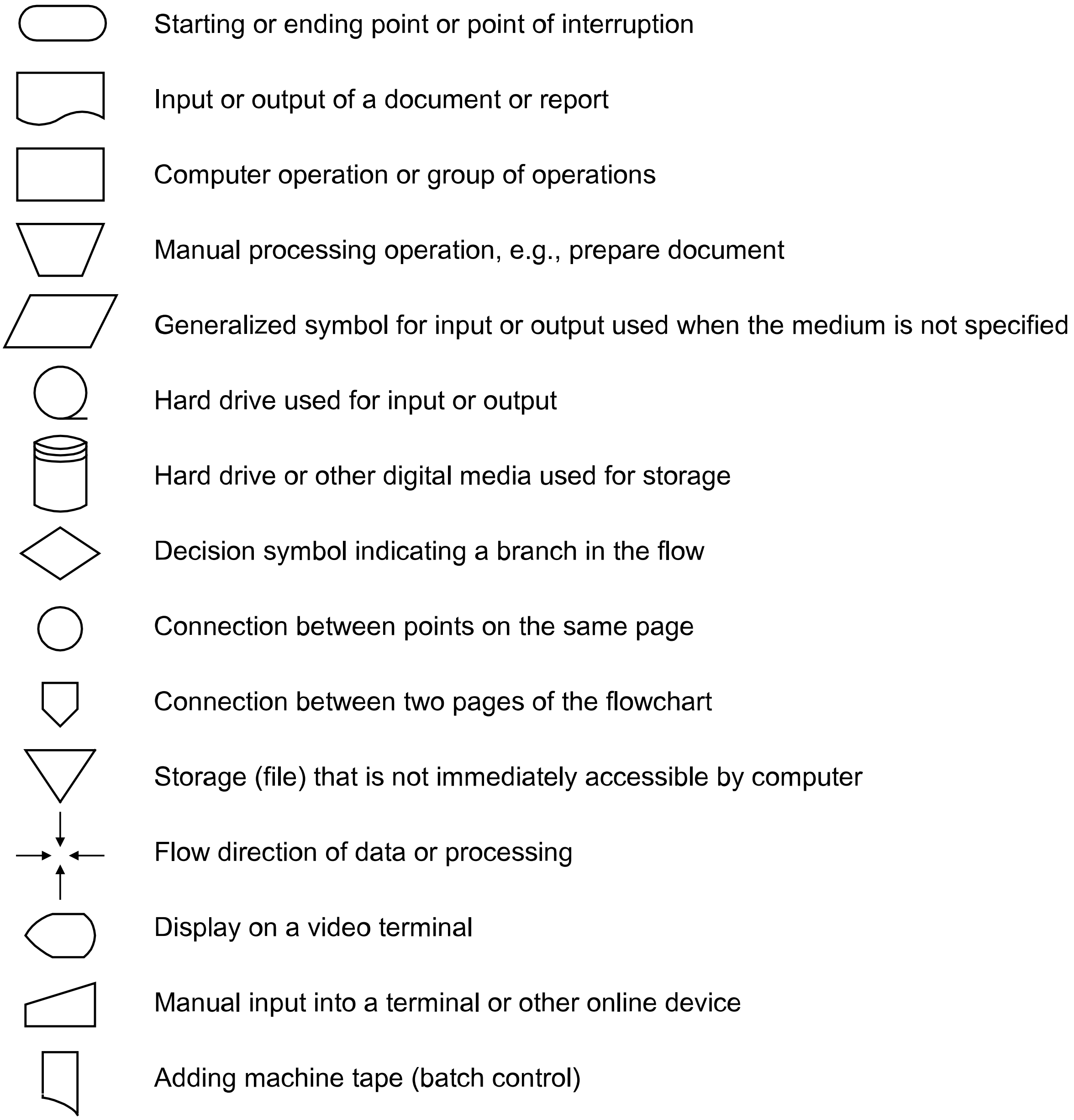

Starting or ending point or point of interruption
Input or output of a document or report
Computer operation or group of operations
Manual processing operation, e.g., prepare document
Generalized symbol for input or output used when the medium is not specified
Hard drive used for input or output
Hard drive or other digital media used for storage
Decision symbol indicating a branch in the flow
Connection between points on the same page
Connection between two pages of the flowchart
Storage (file) that is not immediately accessible by computer
Flow direction of data or processing
Display on a video terminal
Manual input into a terminal or other online device
Adding machine tape (batch control)

Figure 8-1

3. Horizontal Flowcharts

a. Horizontal flowcharts (sometimes called **system flowcharts**) depict areas of responsibility (departments or functions) arranged horizontally across the page in vertical columns.

1) Accordingly, activities, controls, and document flows that are the responsibility of a given department or function are shown in the same column.

a) **PO** is a purchase order and **AP** is accounts payable.

2) The following is an example:

Horizontal (System) Flowchart

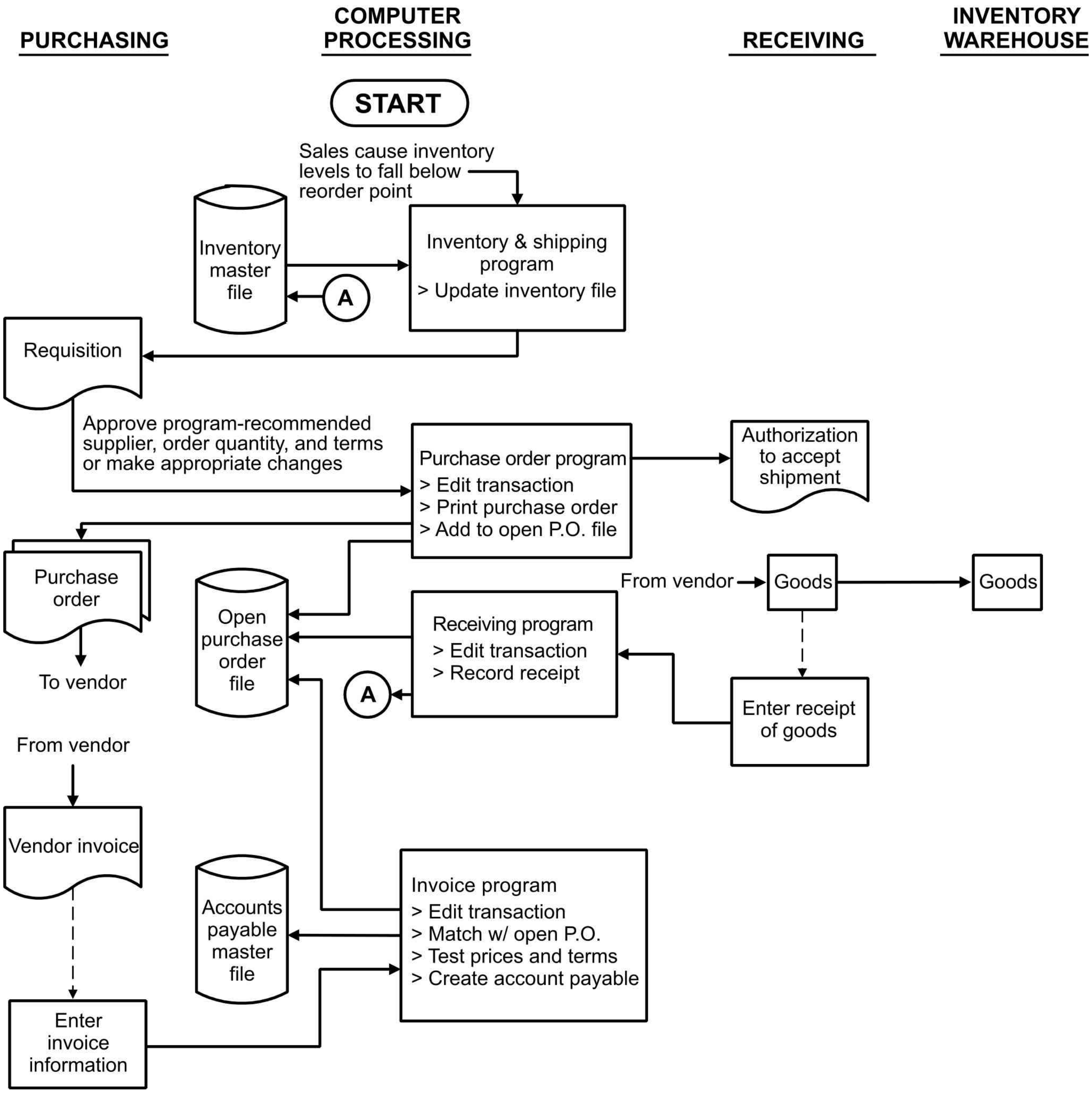


Figure 8-2

4. **Vertical Flowcharts**

   a. Vertical flowcharts, sometimes called **program flowcharts**, present successive steps in a top-to-bottom format.

      1) Their principal use is in the depiction of the specific actions carried out by a computer program.

Vertical (Program) Flowchart

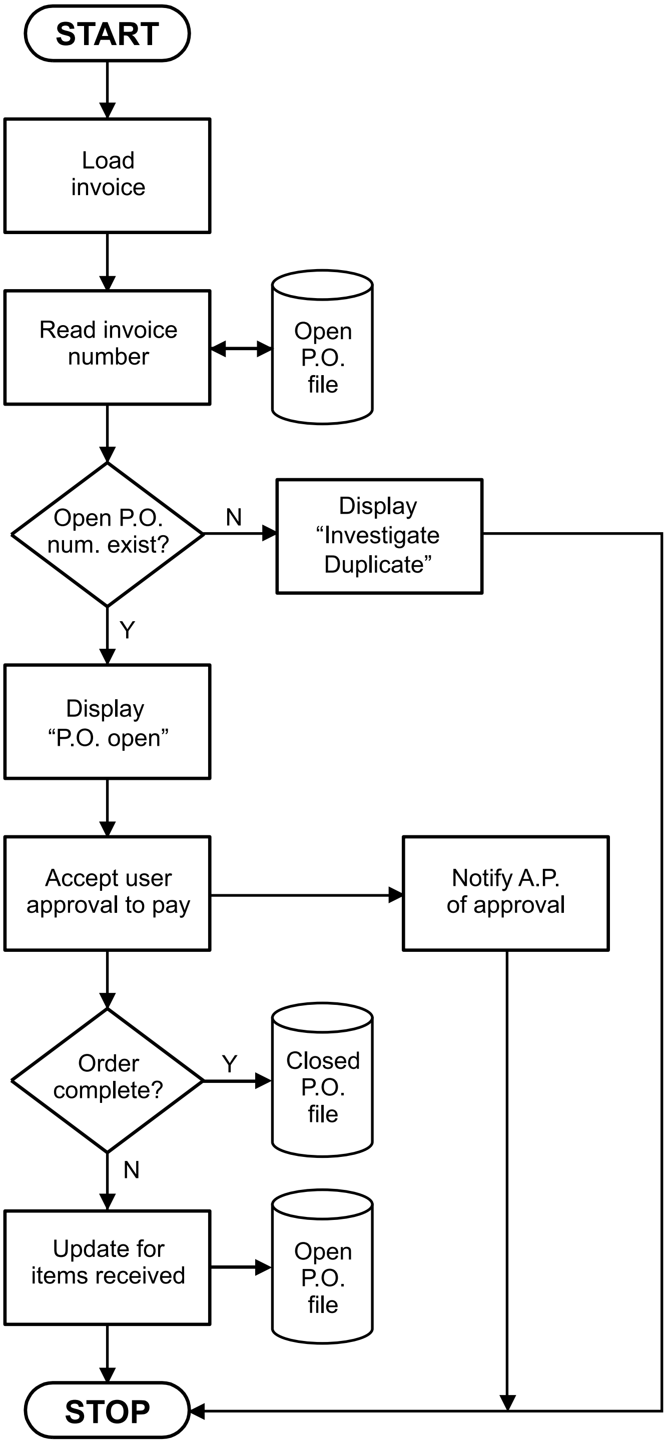


Figure 8-3

5. **Data Flow Diagrams**

   a. Data flow diagrams show how data flow to, from, and within an information system and the processes that manipulate the data. A data flow diagram can be used to depict lower-level details as well as higher-level processes.

      1) A system can be divided into subsystems, and each subsystem can be further subdivided at levels of increasing detail. Thus, any process can be expanded as many times as necessary to show the required level of detail.

      2) The symbols used in data flow diagrams are presented below:

Data Flow Diagram Symbols

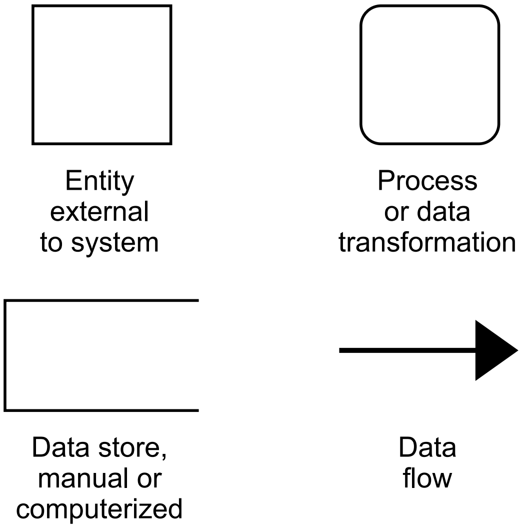

Entity external to system
Process or data transformation
Data store, manual or computerized
Data flow

Figure 8-4

         a) No symbol is needed for documents or other output because data flow diagrams depict only the flow of data. For the same reason, no distinction is made between manual and online storage.

6. **Process Mapping**

   a. A process map is the pictorial representation or narrative description of a client process. During the **preliminary survey**, reviewing the process map aids the internal auditor in assessing the efficiency of processes and controls.

      1) Narratives should be used only for simple processes.

   b. Pictorial process mapping uses the three most common flowcharting symbols:

Process Mapping Symbols

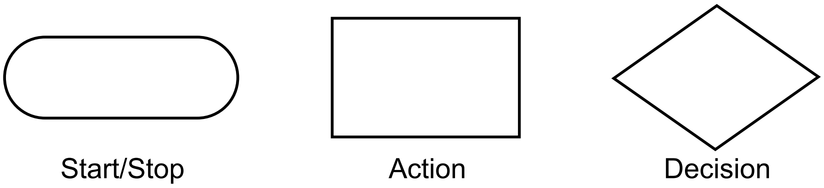


Figure 8-5

c. Below is an example of a process map prepared by the client or auditor for processing an invoice against a purchase order (PO). Approved invoices ultimately are forwarded to accounts payable (AP).

Process Map for Invoice Processing in Purchasing Department

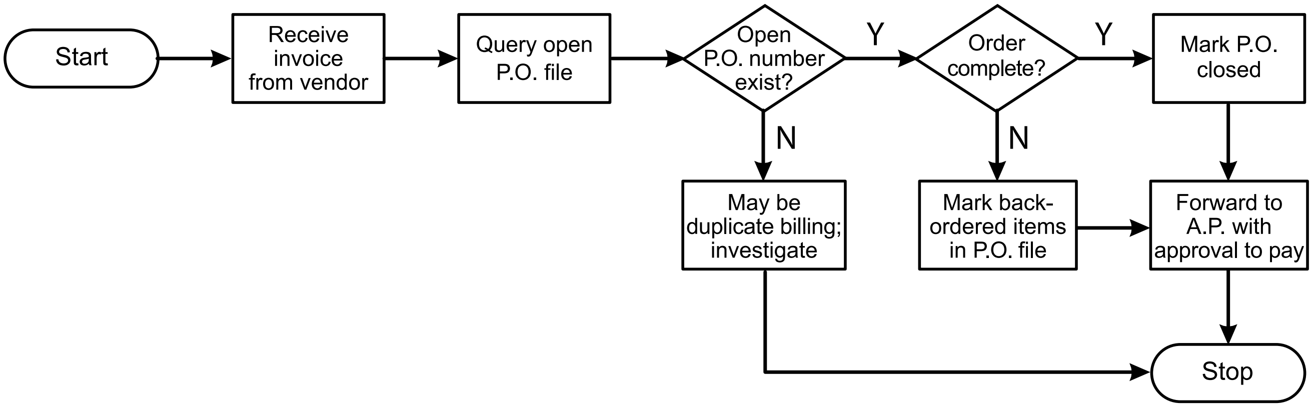

Start
Receive invoice from vendor
Query open P.O. file
Open P.O. number exist?
Y
Order complete?
Y
Mark P.O. closed
N
N
May be duplicate billing; investigate
Mark back-ordered items in P.O. file
Forward to A.P. with approval to pay
Stop

Figure 8-6

d. The auditor verifies the map by observing the process (a functional **walk-through**).

7. **Spaghetti Map**

a. A spaghetti map depicts the flow of people, material, and information from the first to last steps of a process. It highlights the number of key steps and spatial relationships of a particular process by tracing each step of the process. The resulting traces resemble “spaghetti.”

b. The goal is to identify the inefficiencies in a process, eliminate the superfluous steps, and create more streamlined process paths.

8. **RACI Diagram**

a. A RACI diagram is used to clarify decision-making assignments in cross-functional or departmental projects and processes.

1) **R – Responsible.** A person who is responsible for performing the particular task.

2) **A – Accountable.** A person who is the final decision maker and is ultimately accountable for the task.

3) **C – Consulted.** A person who must be consulted before completing the task or making a decision.

4) **I – Informed.** A person who is informed after a decision is made or when the task is completed.

8.3 ANALYTICAL REVIEW TECHNIQUES

Performance Standard 2320
Analysis and Evaluation

Internal auditors must base conclusions and engagement results on appropriate analyses and evaluations.

1. Analysis and evaluation are required to some extent in (a) notating engagements, (b) planning the engagement, (c) developing the work program, and (d) performing procedures. Planning may involve obtaining information by performing procedures, e.g., a risk-and-control matrix and evaluation of control design.
    a. The work program and workpapers are linked. Examples of workpapers are
        1) A planning memo
        2) Flowcharts or narratives
        3) A process-risk map
        4) A risk-and-control matrix connecting risks, controls, evidence, and conclusions
2. **Analytical Procedures**
    a. Specific guidance is in Implementation Guide 2320, *Analysis and Evaluation*.
        1) Use of analytical procedures as a planning tool or to perform the engagement requires developing expectations against which specified information can be compared. The information used to form an expectation should be reliable (e.g., independent of the source of the information tested).
            a) The premise of analytical procedures is that certain relationships among different kinds of information, such as direct correlations, are reasonably expected to continue unless invalidated by known conditions.
            b) Analytical procedures are useful in identifying (1) unexpected differences, (2) the absence of differences when they are expected, (3) potential errors, (4) potential fraud or illegal acts, or (5) other unusual or nonrecurring transactions or events.
        2) “Examples of analytical procedures include:
            a) Ratio, trend, and regression analysis.
            b) Reasonableness tests.
            c) Period-to-period comparisons.
            d) Forecasts.
            e) Benchmarking information against similar industries or organizational units.”
        3) Any significant variances from auditor-developed expectations should be investigated (including validating management responses).
            a) Matters that cannot be explained may require follow-up and possible communication to senior management and the board.

b. When determining the extent to which analytical procedures should be used, internal auditors consider the

1) Significance of the area being examined,
2) Assessment of risk management in the audited area,
3) Adequacy of the internal control system,
4) Availability and reliability of financial and nonfinancial information,
5) Precision with which the results of analytical audit procedures can be predicted,
6) Availability and comparability of information regarding the industry in which the organization operates, and
7) Extent to which other procedures provide evidence.

c. The following chart describes some of the possible analytical procedures and the information they provide.

<table>
<tr><th colspan="3">General</th></tr>
<tr><th>Objective</th><th>Assertion</th><th>Procedure(s)</th></tr>
<tr><td>Assess whether expectations are reasonable or realistic.</td><td>Occurrence
→</td><td>Compare information with expectations and determine whether actual results meet, exceed, or do not meet expectations. If they do not meet expectations, determine whether expectations need to be refined. For example, samples must be stratified to consider data resulting from significant changes in what is sampled.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
Analytical procedures often provide the internal auditor with an efficient and effective means of obtaining evidence.</td></tr>
<tr><td>Assess whether expectations are reasonable or realistic.</td><td>Occurrence
→</td><td>Determine whether the difference from expectations could be a result of fraud, error, or a change in conditions. Corroborate management’s explanation for the reasons for the difference.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
If discrepancies are found, the appropriate authorities within the organization should be consulted.</td></tr>
</table>

<table>
<tr><th colspan="3">Inventory</th></tr>
<tr><th>Objective</th><th>Assertion</th><th>Procedure(s)</th></tr>
<tr><td>Identify possible materials lost outside the normal course of everyday operations, such as by misappropriation of inventory.</td><td>Occurrence
→</td><td>Obtain inventory data (e.g., transaction codes, part numbers), analyze materials issued, and trace to projects to confirm materials issued are used only for approved projects. Document any discrepancies and determine the reason for the issuance of materials not used on approved projects.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
An analysis of materials used and materials issued may reveal a discrepancy.</td></tr>
<tr><td>Identify possible materials lost outside the normal course of everyday operations, such as by misappropriation of inventory.</td><td>Occurrence
→</td><td>Select a representative sample of inventory issuance transactions from a sample of summary reports and determine whether transactions were appropriately approved electronically.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
An analysis of materials used and materials issued may reveal a discrepancy.</td></tr>
</table>

<table>
<tr><th colspan="3">High-Risk Loans Marketing Focus</th></tr>
<tr><th>Objective</th><th>Assertion</th><th>Procedure(s)</th></tr>
<tr><td>Assess whether the current business focus involves high-risk investments to achieve faster returns.</td><td>Classification and Understandability →</td><td>Perform an analytical review of interest income as a percentage of the investment portfolio in comparison with a group of peer financial institutions.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
Higher-risk investments should generate higher short-term interest income compared with that earned by comparable institutions. Higher-risk investments have higher yields.</td></tr>
<tr><td>Assess whether the current business focus involves high-risk investments to achieve faster returns.</td><td>Classification and Understandability →</td><td>Take a random sample of investments made during the period and compare the risk of the investments with that of a random sample of investments made in prior periods.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
Identify whether a trend has formed indicating high-risk investments are the current focus of the entity.</td></tr>
<tr><td>Assess whether the current business focus has changed from low-risk, lower yielding investments to high-risk, higher yielding investments.</td><td>Classification and Understandability →</td><td>Develop a multiple-regression time-series analysis of income over the past 5 years including such factors as interest rates, size of the investment portfolio, and dollar amounts of new investments each year.</td></tr>
<tr><td colspan="3"><b>WHY?</b>
Multiple regression explains the change in a dependent variable (interest income) attributable to two or more independent variables. Thus, it allows the internal auditor to estimate how much of the change might be due to a change in the risk of the investments.</td></tr>
</table>

3. Ratio Analysis

a. One of the most common analytical procedures is ratio analysis, the comparison of one financial statement element with another. Ratios are used frequently to assess an organization’s liquidity and profitability. The following balance sheet and income statement provide inputs for the examples throughout this subunit.

EXAMPLE 8-1 Balance Sheet

RESOURCES

CURRENT ASSETS:	**Current Year End**	**Prior Year End**
Cash and equivalents	US $ 325,000	US $ 275,000
Available-for-sale debt securities	165,000	145,000
Accounts receivable (net)	120,000	115,000
Notes receivable	55,000	40,000
Inventories	85,000	55,000
Prepaid expenses	10,000	5,000
Total current assets	**US $ 760,000**	**US $ 635,000**
NONCURRENT ASSETS:		
Equity-method investments	US $ 120,000	US $ 115,000
Property, plant, and equip.	1,000,000	900,000
Minus: Accum. depreciation	(85,000)	(55,000)
Goodwill	5,000	5,000
Total noncurrent assets	**US $1,040,000**	**US $ 965,000**
Total assets	**US $1,800,000**	**US $1,600,000**

FINANCING

CURRENT LIABILITIES:	**Current Year End**	**Prior Year End**
Accounts payable	US $ 150,000	US $ 75,000
Notes payable	50,000	50,000
Accrued interest on note	5,000	5,000
Current maturities of L.T. debt	100,000	100,000
Accrued salaries and wages	15,000	10,000
Income taxes payable	70,000	35,000
Total current liabilities	**US $ 390,000**	**US $ 275,000**
NONCURRENT LIABILITIES:		
Bonds payable	US $ 500,000	US $ 600,000
Long-term notes payable	90,000	60,000
Employee-related obligations	15,000	10,000
Deferred income taxes	5,000	5,000
Total noncurrent liabilities	**US $ 610,000**	**US $ 675,000**
Total liabilities	**US $1,000,000**	**US $ 950,000**
SHAREHOLDERS’ EQUITY:		
Preferred stock, US $50 par	US $ 120,000	US $ 0
Common stock, US $1 par	500,000	500,000
Additional paid-in capital	110,000	100,000
Retained earnings	70,000	50,000
Total shareholders’ equity	**US $ 800,000**	**US $ 650,000**
Total liabilities and shareholders’ equity	**US $1,800,000**	**US $1,600,000**

EXAMPLE 8-2 Income Statement

	Current Year	**Prior Year**
Net sales	US $1,800,000	US $1,400,000
Cost of goods sold	(1,450,000)	(1,170,000)
Gross profit	US $ 350,000	US $ 230,000
SG&A expenses	(160,000)	(80,000)
Operating income	US $ 190,000	US $ 150,000
Other revenues and losses	(40,000)	(25,000)
Earnings before interest and taxes	US $ 150,000	US $ 125,000
Interest expense	(15,000)	(10,000)
Earnings before taxes	US $ 135,000	US $ 115,000
Income taxes (40%)	(54,000)	(46,000)
Net income	US $ 81,000	US $ 69,000

b. **Liquidity** is the ability to meet current obligations as they come due and continue operating in the short run. The following ratios are measures of an organization's relative liquidity (the higher the ratio, the higher the liquidity) based on balance sheet amounts:

1) The **current ratio** equals current assets divided by current liabilities.

$$\frac{\text{Current assets}}{\text{Current liabilities}}$$

EXAMPLE 8-3 Current Ratio

Current Year:	US $760,000 ÷ $390,000 = 1.949
Prior Year:	US $635,000 ÷ $275,000 = 2.309

a) A low ratio indicates a possible solvency problem.

i) A firm with a low current ratio may become insolvent. High credit risk may prevent lenders from extending credit to a firm with a low ratio.

b) An overly high ratio indicates that management may not be investing idle assets productively.

c) The quality of accounts receivable and merchandise inventory should be considered before evaluating the current ratio.

i) Obsolete or overvalued inventory or receivables can artificially inflate the current ratio.

d) The general principle is that the current ratio should be proportional to the operating cycle. Thus, a shorter cycle may justify a lower ratio.

i) For example, a grocery store has a short operating cycle and can survive with a lower current ratio more easily than a gold mining company with a much longer operating cycle.

2) The **accounts receivable turnover ratio** measures the number of times the organization's average balance in receivables is converted to cash during a fiscal year (or financial statement cycle).

$$\frac{\text{Net credit sales}}{\text{Average accounts receivable}}$$

a) Average accounts receivable equals beginning accounts receivable plus ending accounts receivable, divided by 2.

i) If a business is seasonal, a simple average of beginning and ending balances is inadequate. The monthly balances should be averaged instead.

EXAMPLE 8-4 Accounts Receivable Turnover

All of the company's sales are on credit. Accounts receivable at the beginning of the prior year were US $105,000.

Current Year:	US $1,800,000 ÷ [($120,000 + $115,000) ÷ 2] = 15.3 times
Prior Year:	US $1,400,000 ÷ [($115,000 + $105,000) ÷ 2] = 12.7 times

The company turned over its accounts receivable balance 2.6 more times during the current year, even as receivables were growing in absolute terms. Thus, the company's effectiveness at collecting accounts receivable has improved.

b) A higher turnover implies customers may be paying their accounts promptly.

i) Because sales are the numerator, higher sales without an increase in receivables results in a higher turnover. Encouraging customers to pay quickly (thereby lowering the denominator) also results in a higher turnover ratio.

c) A lower turnover implies that customers are taking longer to pay.

i) If the discount period is extended, customers can wait longer to pay while still getting the discount.

3) The **inventory turnover ratio** measures the number of times the organization's average balance in inventory is converted to cash during a year (or financial statement cycle).

$$\frac{\text{Cost of goods sold}}{\text{Average inventory}}$$

a) Average inventory equals beginning inventory plus ending inventory, divided by 2.

i) If a business is seasonal, a simple average of beginning and ending balances is inadequate. The monthly balances should be averaged instead.

EXAMPLE 8-5 Inventory Turnover

The balance in inventories at the beginning of the prior year was US $45,000.

Current Year: US $1,450,000 ÷ [($85,000 + $55,000) ÷ 2] = 20.7 times
Prior Year: US $1,170,000 ÷ [($55,000 + $45,000) ÷ 2] = 23.4 times

The company did not turn over its inventories as many times during the current year. This result is expected when sales and inventories are increasing.

b) A higher turnover implies strong sales or that the firm may be carrying low levels of inventory.

c) A lower turnover implies that the firm may be carrying excess levels of inventory or inventory that is obsolete.

i) Because cost of goods sold is the numerator, higher sales without an increase in inventory balances result in a higher turnover. Reducing the denominator also results in a higher turnover ratio.

d) The ideal level for inventory turnover is industry specific, with the nature of the inventory items determining the ideal ratio. For example, spoilable items such as meat require a higher turnover ratio than natural resources, such as gold, silver, and coal. Thus, a grocery store should have a much higher inventory turnover ratio than a uranium mine or a jewelry store.

c. **Total asset turnover** measures net sales generated relative to total assets.

$$\frac{\text{Net sales}}{\text{Average total assets}}$$

1) Average total assets equals beginning total assets plus ending total assets, divided by 2.

EXAMPLE 8-6 Total Assets Turnover Ratio

Total assets 2 years ago were US $1,520,000.

Current Year: US $1,800,000 ÷ [($1,800,000 + $1,600,000) ÷ 2] = 1.06 times
Prior Year: US $1,400,000 ÷ [($1,600,000 + $1,520,000) ÷ 2] = .897 times

2) A higher turnover implies effective use of net assets to generate sales.

3) Certain assets, for example, investments, do not relate to net sales. Their inclusion decreases the ratio.

4) If net sales increase and all other factors remain the same, the asset turnover ratio improves because more sales are being generated by the same amount of assets.

d. **Profitability** is measured by three common percentages based on income statement amounts:

1) **Gross profit margin** is the percentage of gross sales that is retained after paying for merchandise. The key issue is the relationship of gross profit to the increase or decrease in sales.

$$\frac{\text{Gross profit}}{\text{Sales}}$$

2) **Operating profit margin** is the percentage that remains after selling, general, and administrative expenses have been paid.

$$\frac{\text{Operating profit}}{\text{Sales}}$$

3) **Net profit margin** is the ratio of net profit to sales. This percentage is particularly important because it measures the proportion of the organization’s revenues that it can pass on to its owners.

$$\frac{\text{Net profit}}{\text{Sales}}$$

EXAMPLE 8-7 Net Profit Margin

	Dollars	**Percent**	
Net sales	US $1,800,000	100.0%	
Cost of goods sold	(1,450,000)	(80.6%)	
Gross margin	**US $ 350,000**	**19.4%**	**(Gross profit margin)**
SG&A expenses	(160,000)	(8.9%)	
Operating income	**US $ 190,000**	**10.6%**	**(Operating profit margin)**
Other income and loss	(40,000)	(2.2%)	
EBIT	US $ 150,000	8.3%	
Interest expense	(15,000)	(0.8%)	
Earnings before taxes	US $ 135,000	7.5%	
Income taxes (40%)	(54,000)	(3.0%)	
Net income	**US $ 81,000**	**4.5%**	**(Net profit margin)**

a) The numerator also may be stated in terms of the net income available to common shareholders.

b) Another form of the ratio excludes nonrecurring items from the numerator, e.g., unusual or infrequent items, discontinued operations, and effects of accounting changes. The result is the net profit margin. This adjustment may be made for any ratio that includes net income.

i) Still other numerator refinements are to exclude equity-based earnings and items in the other income and other expense categories.

e. Sometimes ratio analysis is used to relate a financial statement item to nonfinancial data. An example is average sales per retail location.

4. **Ratio Comparisons**

a. Ratios by themselves reveal little about the organization.

1) **Trend** analysis tracks the changes in a ratio over time, e.g., the last 3 fiscal years. It helps assess the effects of changes in the overall economy or the relative success of a marketing campaign.

2) **Period-to-period** analysis compares performance for similar time periods, e.g., the third quarter of the current year and the third quarter of the prior year. This approach is especially informative in seasonal industries, such as retailing and agriculture.

3) **Industry** analysis compares the organization’s ratios with those of competitors or with the published averages for the entire industry. These must be used with caution because different organizations in the same industry may have different cost structures.

5. **Other Analytical Procedures**

a. **Regression analysis** determines the degree of relationship, if any, between two variables, such as that between actual sales and actual cost of goods sold. The degree of relationship can be used as a benchmark to test for reasonableness.

b. **Variance analysis** studies the difference (favorable or unfavorable) between an amount based on an actual result and the corresponding budgeted amount. It is a method of planning and control that focuses attention on the causes of significant deviations from expectations.

1) Variance analysis is a form of **reasonableness test** used in accounting applications.

c. **Benchmarking** compares some aspect of an organization’s performance with best-in-class performance. (Benchmarking is covered in detail in Study Unit 3, Subunit 5.)

d. **Benford's law** (or First-Digit Law) states that leading digits in a data set are disproportionately more likely to be lower numbers (e.g., 1, 2, or 3).

1) Consequently, internal auditor analyses that reveal a contrary state could be indicative of fraud and may result in expanded procedures.

EXAMPLE 8-8 Response to Less-Restrictive Credit Standards

An internal auditor reviews the accounts receivables system and determines that credit requirements for new customers have been loosened. The result is an increase in sales and accounts receivable. To determine (1) whether further investigation is justified and (2) what should be investigated, the auditor should review the reasonableness of the accounts receivables balance and the effects of the new credit requirements on the accounts receivable turnover ratio. Amounts can be compared with those for prior periods and for similar organizations in the same industry.

Internal auditors have many resources for analyzing and interpreting data. Analytical procedures often provide the internal auditor with an efficient and effective means of obtaining evidence. The assessment results from comparing information with expectations identified or developed by the internal auditor.

8.4 WORKPAPERS -- PURPOSE AND CHARACTERISTICS

Performance Standard 2330
Documenting Information

Internal auditors must document sufficient, reliable, relevant, and useful information to support the engagement results and conclusions.

1. **General Guidelines**

a. Engagement workpapers

1) Aid in the planning, performance, and review of engagements
2) Provide the principal support for engagement results
3) Document whether engagement objectives were achieved
4) Support the accuracy and completeness of the work performed
5) Provide a basis for the internal audit activity's quality assurance and improvement program
6) Facilitate third-party review

2. **Workpapers**

   a. The content of workpapers is prescribed in IG 2330, *Documenting Information*.

      1) **Purpose.** Workpapers document the engagement process from planning to drawing conclusions.

      2) **Uniformity.** The content, organization, and format of workpapers depend on the organization and the engagement.

         a) But consistency should be maintained within the internal audit activity to permit sharing of information and coordination of activities.

      3) **Responsibility.** In accordance with Standard 2040 and Standard 2050, the CAE should establish policies and procedures for workpapers for different engagements.

         a) Standard formats with any needed flexibility improve efficiency and consistency.

      4) **Characteristics.** Standard 2310 requires internal auditors to identify sufficient, reliable, relevant, and useful information.

         a) This requirement also applies to information in workpapers that relates to objectives, observations, conclusions, and recommendations.

         b) The sufficiency and relevance characteristics “enable a prudent, informed person, such as another internal auditor or an external auditor, to reach the same conclusions.”

         c) Well-organized workpapers allow reperformance of the work and support conclusions and results.

      5) **Content.** Workpapers may include the following:

         a) Indexing
         b) Titles indicating the subject matter of the engagement
         c) Time of the engagement
         d) Scope of work
         e) Purpose
         f) Sources of information
         g) The population, sample size, and means of selection
         h) Analytical methods
         i) Results of tests and analyses
         j) Conclusions cross-referenced to observations
         k) Recommended follow-up
         l) Names of the internal auditor(s)
         m) Review notation and name of the reviewer(s)

      6) **Review.** Review of workpapers is a means of staff development.

         a) The review may determine compliance with the *Standards* and quality control guidelines.

3. **Best Practices**

   a. Each workpaper must, at a minimum, identify the engagement and describe the contents or purpose of the workpaper, for example, in the heading.

      1) Also, each workpaper should be signed (initialed) and dated by the internal auditor and contain an index or reference number.

   b. Workpapers should be consistently and efficiently prepared to facilitate review. They should be

      1) Neat, not crowded, and written on only one side (if written at all).
      2) Uniform in size and appearance.
      3) Economical, avoiding unnecessary copying, listing, or scheduling.

         a) They should use copies of engagement clients' records if applicable.

      4) Arranged in a logical and uniform style.

         a) The best organization is that of the work program. Each section should have statements of purpose and scope followed by observations, conclusions, recommendations, and corrective action.

      5) Clear, concise, and complete.
      6) Restricted to matters that are relevant and significant.
      7) Written in a simple style.

   c. While clarity, concision, and accuracy are desirable qualities of workpapers, completeness and support for conclusions are the most important considerations.

4. **Other Content**

   a. Workpapers should document such matters as how sampling populations were defined and how statistical samples were selected.

   b. Furthermore, verification symbols (tick marks) are likely to appear on most workpapers and should be explained.

5. **Indexing**

   a. Indexing permits cross-referencing. It is important because it simplifies supervisory review either during the engagement or subsequently by creating a trail of related items through the workpapers.

      1) Indexing facilitates preparation of final engagement communications, later engagements for the same client, and internal and external assessments of the internal audit activity.

6. **Summaries**

   a. Internal auditors summarize information in workpapers. Summaries help to coordinate workpapers related to a subject by providing concise statements of the most important information. Thus, they provide for an orderly and logical flow of information and facilitate efficient supervisory review.

7. **Permanent Files**

   a. The following are typical items contained in the permanent or carry-forward files:

      1) Previous engagement communications, responses, and results of follow-up
      2) Engagement communications provided by other organizational subunits
      3) Reviews of the long-term engagement work schedule by senior management
      4) Results of post-engagement reviews
      5) Auditor observations during past engagements that may have future relevance
      6) The chart of accounts with items referenced to engagement projects
      7) Management's operating reports
      8) Applicable engagement work programs and questionnaires
      9) Long-term contracts
      10) Flowcharts of operations
      11) Historical financial information
      12) Project control information
      13) Correspondence about the engagement project
      14) Updated organizational charter, bylaws, minutes, etc.

8. **Computerized Workpapers**

   a. Electronic workpapers have the following advantages:

      1) Uniformity of format
      2) Ease of storage
      3) Searchability and automated cross-indexing
      4) Backup and recovery functions
      5) Built-in audit methodologies, such as sampling routines

   b. However, the use of electronic media involves security issues that do not arise when workpapers exist only on paper.

      1) Electronic workpapers and reviewer comments should be protected from unauthorized access and change.

      2) Information recorded by scanning workpapers should be adequately controlled to ensure its continued integrity.

      3) Workpaper retention policies should consider changes made in the original operating system, other software, and hardware to ensure the continued retrievability of electronic workpapers throughout the retention cycle.

   c. Software packages have moved beyond the simple storage and retrieval of workpapers.

8.5 WORKPAPERS -- REVIEW, CONTROL, AND RETENTION

Implementation Standard 2330.A1

The chief audit executive must control access to engagement records. The chief audit executive must obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate.

1. **Review of Workpapers**
   - a. Workpapers facilitate supervision of the engagement. They are a means of communication between internal auditors and the auditor in charge.
   - b. All workpapers are reviewed to ensure that (1) they support engagement communications and (2) all necessary procedures are performed.
     - 1) The reviewer initials and dates each workpaper to provide evidence of review. Other methods include
       - a) Completing a review checklist,
       - b) Preparing a memorandum on the review, or
       - c) Evaluating and accepting reviews within the workpaper software.
   - c. Written review notes record questions arising from the review. When clearing review notes, the auditor ensures that the workpapers provide adequate evidence that questions raised have been resolved. The reviewer may
     - 1) Retain the notes as a record of questions raised, steps taken, and results.
     - 2) Discard the notes after questions are resolved and workpapers are amended to provide requested information.
2. **Control of Workpapers**
   - a. The primary objective of maintaining security over workpapers is to prevent unauthorized changes or removal of information.
     - 1) The workpapers are essential to the proper functioning of the internal audit activity. Among many other purposes, they document the information obtained, the analyses made, and the support for the conclusions and engagement results.
     - 2) Unauthorized changes or removal of information would seriously compromise the integrity of the internal audit activity’s work. For this reason, the chief audit executive must ensure that workpapers are kept secure.
   - b. Workpapers contain sensitive information, but they generally are not protected from disclosure in civil and criminal legal matters.
     - 1) Thus, auditors do not have the equivalent of the attorney-client privilege.
   - c. Engagement records include reports, supporting documents, review notes, and correspondence, regardless of storage media.
     - 1) These records or workpapers are the property of the organization.
     - 2) The internal audit activity controls workpapers and provides access to authorized personnel only.

3. **Access**

   a. When engagement objectives will not be compromised, the internal auditor may show all or part of the workpapers to the client.

      1) For instance, the results of certain engagement procedures may be shared with the client to encourage corrective action.

   b. One potential use of engagement workpapers is to provide support in the organization's pursuit of insurance claims, fraud cases, or lawsuits.

      1) In such cases, management and other members of the organization may request access to engagement workpapers.

         a) This access may be necessary to substantiate or explain engagement observations and recommendations or to use engagement documentation for other business purposes.

   c. Internal auditors are encouraged to consult legal counsel in matters involving legal issues. Requirements may vary significantly in different jurisdictions.

4. **Retention of Workpapers**

> **Implementation Standard 2330.A2**
>
> The chief audit executive must develop retention requirements for engagement records, regardless of the medium in which each record is stored. These retention requirements must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

   a. Record retention requirements vary among jurisdictions and legal environments.

   b. The CAE should develop a written retention policy that meets organizational needs and legal requirements of the jurisdictions where the organization operates.

   c. The record retention policy should include appropriate arrangements for the retention of records related to engagements performed by external service providers.

   d. Workpapers should be destroyed after they have served their purpose. Any parts having continuing value should be brought forward to current workpapers or to the permanent file.

8.6 DRAWING CONCLUSIONS

1. After performing procedures, the internal auditor applies experience, logic, and professional skepticism to analyzing and evaluating the evidence obtained (findings). The internal auditor then draws conclusions.
   a. Conclusions and opinions are evaluations of the effects of the observations and recommendations regarding the activities reviewed. Conclusions and opinions put the observations and recommendations in perspective based upon their overall implications and are clearly identified in the report.
      1) The terms “conclusion” and “opinion” are interchangeable.

   b. Conclusions may address the entire scope of an engagement or its specific elements. Thus, the internal auditor may draw conclusions based on the results of a procedure, a group of procedures, or the whole engagement.

2. **Root Cause Analysis**
   a. When audit procedures detect an unfavorable condition (noncompliance, fraud, opportunity loss, misstatement, etc.), internal auditors are encouraged to identify the root cause. IG 2320, *Analysis and Evaluation*, provides the following guidance on root cause analysis:
      1) **Purpose.** A root cause analysis identifies the underlying reason for the unfavorable condition.
         a) The analysis improves the effectiveness and efficiency of governance, risk management, and controls.
      2) **Cost-benefit.** Due professional care should be exercised by weighing effort (e.g., time, cost, and expertise) against possible benefits.
         a) Root cause analysis is subject to a cost (effort) – benefit constraint.
      3) **Application.** A root cause analysis may be difficult and subjective or as simple as asking one or more “why” questions to identify variance.
      4) **Professional judgment.** Root causes generally result from decisions, acts, or failures to act by a person or group.
         a) But a root cause may be elusive even after extensive analysis of quantitative or qualitative information. Furthermore, two or more mistakes of varying significance may collectively be the root cause. In other cases, the search for the root cause may involve a broader problem, e.g., organizational culture. Accordingly, input may be sought from internal and external stakeholders.
      5) **Multiple root causes.** In some circumstances, the internal auditors’ objective and independent analysis may identify multiple root causes for management’s consideration.
      6) **Management assistance.** The resources (e.g., time and expertise) of the internal audit activity may be inadequate to complete a root cause analysis. In these cases, the CAE may recommend that management determine the root cause.
      7) **Communication.** Results or relationships that are not adequately explained may indicate a situation to be communicated to senior management and the board.

3. **Examples**

   a. Below is an example of the process of moving from a finding to a conclusion for a specific engagement objective:

      1) The engagement work program called for the auditor to examine all purchase orders exceeding US $100,000 to determine whether they were approved by the appropriate division vice president. The results of the procedure are stated as a finding:

         Of 38 purchase orders over US $100,000 examined, 3 lacked required vice presidential approval, an exception rate of 7.9%.

         a) The finding (observation) is a relevant statement of fact about the results of audit work without interpretation or commentary.

      2) From the finding, the internal auditor can draw a conclusion that informs the reader of the implications of the finding for one or more engagement objectives:

         The system of internal controls over purchases of material dollar amounts in the Eastern Division is not functioning as designed.

      3) The relationship of a finding and a conclusion need not be one-to-one. If the auditor finds it useful, multiple findings can be used to support a single conclusion:

         Of 38 purchase orders over US $100,000 examined, 3 lacked required vice presidential approval, an exception rate of 7.9%. Of 115 purchase orders less than US $100,000 randomly selected and examined, 12 lacked required approvals, an exception rate of 10.4%. Given these findings, the system of internal controls over all purchases in the Eastern Division is not functioning as designed.

   b. Auditor judgment is essential when moving from a finding to a conclusion. No formula can tell an auditor whether a certain exception rate is indicative of a working or failing control.

      1) Depending on context, decisions about materiality, and auditee knowledge, the findings in the example above could have resulted in positive, not negative, conclusions.

4. **Report Test Results to Auditor in Charge**

   a. The auditor in charge of the engagement is responsible for coordinating the results of audit work and ensuring that work performed supports conclusions and opinions.

      1) For this reason, internal audit staff must report the results of audit work to the auditor in charge.

8.7 SUPERVISION

1. Supervision at the Engagement Level

Performance Standard 2340
Engagement Supervision

Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed.

a. Supervision is needed at all levels of the internal audit activity from planning to performance to reporting results. The CAE may delegate the task of supervision on individual engagements.

Interpretation of Standard 2340

The extent of supervision required will depend on the proficiency and experience of internal auditors and the complexity of the engagement. The chief audit executive has overall responsibility for supervising the engagement, whether performed by or for the internal audit activity, but may designate appropriately experienced members of the internal audit activity to perform the review. Appropriate evidence of supervision is documented and retained.

b. Further guidance is provided in IG 2340, *Engagement Supervision*.

   1) Supervision by the CAE is relevant to all phases of the engagement. The process includes

      a) Ensuring auditors collectively possess the required knowledge, skills, and other competencies.

      b) Providing instructions during planning and approving the engagement program.

      c) Ensuring the work program is completed (unless changes are justified and authorized) and objectives are met.

      d) Determining workpapers support observations, conclusions, and recommendations.

      e) Ensuring communications are accurate, objective, clear, concise, constructive, and timely.

      f) Developing internal auditors' proficiency.

2) The CAE is responsible for all internal audit engagements and significant professional judgments.

   a) The CAE adopts suitable means to

      i) Minimize the risk of inconsistent professional judgments or other actions inconsistent with those of the CAE and

      ii) Resolve differences in professional judgment between the CAE and staff members.

   b) The means of conflict resolution may include

      i) Discussion of facts,
      ii) Inquiries or research,
      iii) Workpaper documentation of differences, and,
      iv) For an ethical issue, referral to an individual responsible for such matters.

2. **Relationships**

   a. To ensure complete cooperation, senior management is responsible for notifying other departments of the existence of the internal audit activity.

      1) Partnering with management at all levels is one of the best ways for internal auditors to obtain information.

      2) Employees are another source of information.

   b. Internal auditors need effective interpersonal skills to promote the internal audit activity throughout the organization. According to The IIA Competency Framework, internal auditors nurture relationships when they

      1) Cultivate and maintain extensive informal networks,
      2) Create opportunities and events to help people build relationships with each other,
      3) Compliment and affirm others,
      4) Build relationships by sharing personal experiences and perspectives,
      5) Keep others in the loop,
      6) Seek opportunities for contact that build relationships,
      7) Initiate and participate in conversations that enhance approachability,
      8) Are recognized as approachable and resourceful individuals, and
      9) Use diplomacy and tact.

   c. Internal auditors rely on collaboration and cooperation among departments and other groups to work toward shared goals. During an engagement, internal auditors have a unique opportunity to build credibility and to promote the goals of adding value and improving the organization’s operations.

3. **Coordination during the Engagement**

   a. The auditor-in-charge should coordinate work assignments among audit team members during the engagement.

   b. Coordination during the engagement ensures that engagement objectives will be met efficiently and effectively.

4. **Staff Performance Evaluations**

   a. The CAE is responsible for ensuring that the internal audit activity has sufficient resources, including employees with the knowledge, skills, and other competencies appropriate for planned activities.

      1) Thus, as part of the resource management process, a written appraisal of each internal auditor’s performance is required at least annually.

      2) Furthermore, at the conclusion of any major audit engagement, supervisory personnel should complete performance appraisals for all audit staff who worked on the engagement.

         a) Such appraisals help (1) the CAE to assess future training needs and current staff abilities and (2) staff to identify areas of personal strength and weakness.

   b. Best practices include the following:

      1) It is appropriate and advisable to notify internal auditors of an upcoming appraisal.

      2) Evaluators should use objective language and not use generalizations. Rather, the evaluators should cite specific information and be prepared to support assertions with evidence.

      3) All appraisals should be documented.

   c. The **halo effect** is a generalization from the perception of one trait to others.

      1) If an employee’s performance appraisal of any given subordinate tends to be consistently high, low, or in the middle across the performance dimensions, a halo bias may exist in the way the subordinate is being rated.

         a) Appraisal ratings are not likely to remain consistent if the forms have too many leading questions.

STUDY UNIT NINE

COMMUNICATING RESULTS AND MONITORING PROGRESS

This study unit covers **Domain IV: Communicating Engagement Results and Monitoring Progress** from The IIA's CIA Exam Syllabus. This domain makes up 20% of Part 2 of the CIA exam and is tested at the **basic** and **proficient** cognitive levels. Refer to the complete syllabus located in Appendix B to view the relevant sections covered in Study Unit 9.

9.1 COMMUNICATION WITH CLIENTS

1. **Engagement Communications**
    a. The following are purposes of engagement communications:
        1) Inform (tell what was found),
        2) Persuade (convince management of the worth and validity of the audit findings), and
        3) Get results (move management toward change and improvement).
    b. Providing useful and timely information and promoting improvements in operations are goals of internal auditors.
        1) To accomplish these goals, engagement communications should meet the expectations, perceptions, and needs of operating and senior management.
        2) For the benefit of senior management, the communication should provide appropriately generalized information regarding matters of significance to the organization as a whole.
        3) For the benefit of operating management, the communication should emphasize details of operations.
        4) A written engagement communication should be made even if all issues have been resolved.
    c. Internal auditors should be skilled in oral and written communications to clearly and effectively convey such matters as engagement objectives, preliminary surveys, evaluations, conclusions, and recommendations.

2. **Preliminary Communication**
   - a. The CAE generally notifies client management about the timing of the audit, the reasons for it, the preliminary scope, procedures to be used, and the estimated client resources needed.
     - 1) For an assurance service, the person or group directly involved with the entity, operation, function, system, or other subject matter under review is the process owner.
     - 2) For a consulting service, the person or group seeking advice is the engagement client (Introduction to the *International Standards for the Professional Practice of Internal Auditing*).
     - 3) For the sake of convenience, The IIA and this text use the term **engagement client** for both assurance and consulting services.
   - b. Before this communication, the internal audit activity gathers basic information about the client, for example, about its industry, principal personnel, processes, major inputs and outputs, and control environment.
     - 1) Some information may be acquired by sending a questionnaire or survey to the client early in the audit process. The answers are then discussed at the preliminary meeting.
     - 2) This preliminary notice is omitted when the engagement involves such activities as a surprise cash count or procedures related to suspected fraud.
   - c. If the results of a preliminary survey and limited testing reveal no deficiencies, the internal audit activity should send a memorandum communication to the client summarizing the preliminary survey results and indicating that the engagement has been canceled.

3. **Interim Communication**
   - a. Interim or progress communications provide a prompt means of documenting a situation requiring immediate action as a result of significant observations.
     - 1) They are preliminary and should indicate that
       - a) Only current information, that is, an incomplete study, is the basis for such communications.
       - b) The final engagement communication will follow up on the topics covered.
     - 2) Progress communications prepared by the internal audit staff should be reviewed by the chief audit executive or other supervisory personnel.
     - 3) Progress communications about deficiency observations should have the same structure as communications on observations.
       - a) Deficiencies are described in records of engagement observations and are communicated to management in the form of a single-page executive summary.
     - 4) Progress communications also may be used to report the status of long, sensitive, or otherwise special engagements to the clients and senior management.
     - 5) Progress communications may reveal that an engagement or additional work may not be necessary if the survey and limited testing were conducted with due professional care.
       - a) The costs of an engagement may exceed the benefits.

b. **Interim reports** (oral or written) transmitted formally or informally communicate

1) Information needing immediate attention (e.g., noncompliance with government regulations and laws and evidence of fraud),

2) A change in the scope of the engagement, or

3) The progress of a long-duration engagement.

c. The most appropriate use of an oral communication is an interim report to communicate conditions that demand immediate action.

d. The use of interim reports does not reduce or eliminate the need for a final report.

9.2 OBSERVATIONS AND RECOMMENDATIONS

1. After identifying, analyzing, evaluating, and documenting engagement information, the internal auditor makes observations and forms conclusions about the engagement objectives based on the information.

a. Recommendations are based on observations and conclusions and may be general or specific. They are made to enhance and protect organizational value.

1) Specifically, recommendations call for action to correct existing conditions or improve operations and may suggest approaches to correcting or enhancing performance as a guide for management in achieving desired results.

NOTE: The word “findings” is often used as a synonym for “observations” on the CIA exam.

2. **Four Attributes of Observations and Recommendations**

a. Observations and recommendations result from comparing criteria (the correct state) with condition (the current state). When conditions meet the criteria, communication of satisfactory performance may be appropriate.

b. Observations and recommendations are based on the following attributes:

1) **Criteria** are the standards, measures, or expectations used in making an evaluation or verification (the correct state). Examples of criteria for evaluating operations include

a) Organizational policies and procedures delegating authority and assigning responsibilities,

b) Textbook illustrations of generally accepted practices, and

c) Codification of best practices in similar organizations.

2) The **condition** is the factual evidence that the internal auditor found in the examination (the current state).

3) The **cause** is the reason for the difference between expected and actual conditions.

a) A recommendation in a final engagement communication should address the cause attribute.

4) The **effect** is the risk or exposure the organization or others encounter because the condition is not consistent with the criteria (the impact of the difference).

a) In determining the risk or exposure, internal auditors consider the effect their observations and recommendations may have on the organization’s operations and financial statements.

c. Observations and recommendations also may include client accomplishments, related issues, and supportive information.

3. **Favorable observations** should be short and simple. For example, “Production schedules, levels, and quality were at or ahead of budgeted levels in every case.”
4. **Unfavorable observations** need further explanation to justify recommended changes. The following are examples:
   a. **Summary**
      1) Because of inaccurate inventory records, the supply department bought unneeded supplies costing US $75,000.

   b. **Criteria**
      1) Established procedures provide that excess materials returned by the production department shall be entered on the records of the supply department to show the levels of inventory currently on hand and available for issuance.

   c. **Condition (facts)**
      1) Our tests disclosed that, for a period of 6 months, supplies returned from production had not been entered on the supply department’s records.

   d. **Cause**
      1) We found that the employees responsible for the posting of returned supplies had not been instructed in their duties. In addition, supervisors had not been monitoring the process.

   e. **Effect**
      1) As a result of the inaccurate inventory records, the organization bought unneeded supplies costing about US $75,000.

   f. **Recommendation**
      1) We reviewed the conditions with the manager of the supply department, and he agreed to bring the inventory records up to date, issue job instructions to the workers spelling out the need to record returned supplies, and instruct supervisors to monitor the process in the future and to submit written reports on their periodic reviews.

   g. **Corrective action taken**
      1) Before we concluded our examination, the manager took all three steps. Our subsequent spot checks showed that the action was effective. We therefore consider this observation closed.

9.3 COMMUNICATING ENGAGEMENT RESULTS

1. **Final Engagement Communication**
   a. Internal auditors are expected to make known the results of their work.

Performance Standard 2400
Communicating Results

Internal auditors must communicate the results of engagements.

   b. The CAE, auditor-in-charge of the engagement, or other auditor with sufficient experience communicates results to the engagement client.
   c. The IIA provides specific criteria to be included with the results of engagements.

Performance Standard 2410
Criteria for Communicating

Communications must include the engagement's objectives, scope, and results.

Implementation Standard 2410.A1

Final communication of engagement results must include applicable conclusions, as well as applicable recommendations and/or action plans. Where appropriate, the internal auditors' opinion should be provided. An opinion must take into account the expectations of senior management, the board, and other stakeholders and must be supported by sufficient, reliable, relevant, and useful information.

   d. According to IG 2410, *Criteria for Communicating*, planning of the final communication includes consideration of all discussions with management of the area audited.
      1) Thus, the final engagement communication should consider client responses to audit observations that are received before the final communication has been issued.
   e. Specific guidance on the elements of final communications is provided below and on the next page.
      1) A final communication may vary by organization or type of engagement. However, it contains at least the purpose, scope, and results of the engagement.
      2) A final communication may include background information, such as activities reviewed and the status of observations, conclusions, recommendations from prior reports, and summaries of the communication's content.
      3) **Purpose** statements describe the objectives and may explain why the engagement was conducted and what it was expected to achieve.
      4) **Scope** statements identify the audited activities and may include the time period reviewed and related activities not reviewed to define the engagement.
         a) They also may describe the nature and extent of engagement work.
      5) **Results** include observations, conclusions, opinions, recommendations, and action plans.

6) **Observations** (findings) are relevant statements of fact. A final communication contains those observations necessary for understanding the conclusions and recommendations. Less significant matters may be communicated informally.

7) **Conclusions and opinions** are evaluations of the effects of the observations and recommendations. They are clearly identified. Conclusions may address the entire engagement scope or specific aspects. They may cover (but are not limited to) whether

   a) Operating or program objectives conform with the organization's,
   b) Those objectives are being met, and
   c) The activity under review is functioning as intended.

8) An overall opinion on the engagement is **not mandatory**. An opinion should only be included when it is appropriate, for example, when it improves communication with the users of the reports.

   a) An opinion may include an overall assessment of controls or be limited to specific controls or aspects of the engagement.

9) The internal auditor reaches agreement with the client about results and any necessary plan of corrective action. Disagreements are fully disclosed, including both positions and the reasons.

   a) The client's comments about results may be presented in the report.

10) A signed report is issued at the end of the engagement.

   a) Summary reports, which provide highlights of the engagement results, are appropriate for levels above the client.

      i) They may be issued separately from, or with, the final communication.

   b) The auditor authorized to sign is designated by the CAE.
   c) If reports are distributed electronically, the internal audit activity keeps a signed report on file.

      i) The term "signed" means a manual or electronic signature in the report or on a cover letter.

Implementation Standard 2410.A2

Internal auditors are encouraged to acknowledge satisfactory performance in engagement communications.

f. Internal auditors should provide positive feedback to engagement clients when appropriate. This practice helps to develop good relations with clients and may improve their receptiveness to the audit findings.

g. Additionally, client accomplishments included in the final communication may be necessary to present fairly the existing conditions and provide perspective and balance.

9.4 COMMUNICATION QUALITIES AND OVERALL OPINIONS

1. Definitions of the Qualities of Communications

Performance Standard 2420
Quality of Communications

Communications must be accurate, objective, clear, concise, constructive, complete, and timely.

a. The IIA issued an Interpretation of the Performance Standard above to define each quality.

Interpretation of Standard 2420

- Accurate communications are free from errors and distortions and are faithful to the underlying facts.
- Objective communications are fair, impartial, and unbiased and are the result of a fair-minded and balanced assessment of all relevant facts and circumstances.
- Clear communications are easily understood and logical, avoiding unnecessary technical language and providing all significant and relevant information.
- Concise communications are to the point and avoid unnecessary elaboration, superfluous detail, redundancy, and wordiness.
- Constructive communications are helpful to the engagement client and the organization and lead to improvements where needed.
- Complete communications lack nothing that is essential to the target audience and include all significant and relevant information and observations to support recommendations and conclusions.
- Timely communications are opportune and expedient, depending on the significance of the issue, allowing management to take appropriate corrective action.

b. Consistent with the *Standards* and IG 2420, *Quality of Communications*, the following are characteristics of high-quality communications:

1) Data and evidence are processed with care and precision.
2) Observations, conclusions, and recommendations are unbiased.
3) Unnecessary technical language is avoided, and context for all significant and relevant information is provided.
4) Communications are meaningful but concise.
5) The content and tone are useful and positive, and objectives are focused.
6) Communications are consistent with the entity’s style and culture.
7) Results are not unduly delayed.

2. **Other Characteristics of Effective Communications**

   a. The presentation should be **coherent**, that is, logically ordered and integrated.

   b. Sentences should be short and use simple but appropriate vocabulary.

   c. Good writing is **consistent**. Inconsistent style, sentence structure, format, and vocabulary are confusing.

   d. Active-voice verbs are generally (not always) preferable to passive-voice verbs. The active voice is more concise, vivid, and interesting.

   e. The Seven Seas (7 Cs) is a useful memory aid. Good writing is

      1) Clear.
      2) Correct (accurate and objective).
      3) Concise.
      4) Consistent.
      5) Constructive.
      6) Coherent.
      7) Complete and timely.

   f. Emphasis

      1) Successful communication between the internal auditor and the engagement client partially depends on achieving appropriate emphasis. Both parties should be aware of the most important points in their discussion.

      2) Graphic illustrations (e.g., pictures, charts, or graphs), oral and written repetition (e.g., summaries) and itemized lists (bulleted or numbered) are good ways of emphasizing information.

      3) Using audiovisual aids to support a discussion of major points results in the most retention of information. One study concluded that 85% of the information presented in this way will be remembered after 3 hours, and 65% after 3 days.

   g. Word selection (diction) can affect the recipient of an engagement communication in either written or oral form.

      1) In general, language should be fact-based and neutral. But if the internal auditor’s objective is to persuade an individual to accept recommendations, words with strong or emotional connotations should be used.

         a) However, words that are connotation-rich have strong but unpredictable effects. A common example is using the word “fraud” rather than the more neutral “irregularity.”

      2) Using too strong a word or a word inappropriate for the particular recipient may induce an unwanted response. Thus, high-connotation language should be chosen carefully to appeal to the specific recipient.

3. **Errors and Omissions**

> **Performance Standard 2421**
> **Errors and Omissions**
>
> If a final communication contains a significant error or omission, the chief audit executive must communicate corrected information to all parties who received the original communication.

a. The correction of an error or omission in an internal audit communication need not be in written form.

4. **The Conformance Phrase**

> **Performance Standard 2430**
> **Use of "Conducted in Conformance with the *International Standards for the Professional Practice of Internal Auditing*"**
>
> Indicating that engagements are "conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*" is appropriate only if supported by the results of the quality assurance and improvement program.

5. **Nonconformance**

> **Performance Standard 2431**
> **Engagement Disclosure of Nonconformance**
>
> When nonconformance with the Code of Ethics or the *Standards* impacts a specific engagement, communication of the results must disclose the:
>
> - Principle(s) or rule(s) of conduct of the Code of Ethics or Standard(s) with which full conformance was not achieved.
> - Reason(s) for nonconformance.
> - Impact of nonconformance on the engagement and the communicated engagement results.

6. **Overall Opinions**

   a. In contrast to an engagement opinion, an overall opinion considers multiple engagements. The IIA Glossary defines an overall opinion as follows:

   The rating, conclusion, and/or other description of results provided by the chief audit executive addressing, at a broad level, governance, risk management, and/or control processes of the organization. An overall opinion is the professional judgment of the chief audit executive based on the results of a number of individual engagements and other activities for a specific time interval.

Performance Standard 2450
Overall Opinions

When an overall opinion is issued, it must take into account the strategies, objectives, and risks of the organization; and the expectations of senior management, the board, and other stakeholders. The overall opinion must be supported by sufficient, reliable, relevant, and useful information.

Interpretation of Standard 2450

The communication will include:

- The scope, including the time period to which the opinion pertains.
- Scope limitations.
- Consideration of all related projects, including the reliance on other assurance providers.
- A summary of the information that supports the opinion.
- The risk or control framework or other criteria used as a basis for the overall opinion.
- The overall opinion, judgment, or conclusion reached.

The reasons for an unfavorable overall opinion must be stated.

   b. The outline in this section is based on Practice Guide, *Formulating and Expressing Internal Audit Opinions*.

   c. Internal auditors may be asked by stakeholders to express macro opinions or micro opinions, depending on the scope of the engagement.

      1) The assurance for the organization as a whole is a **macro opinion**. It is usually based on multiple audit projects. For example, a macro opinion may be expressed on

         a) The overall system of internal control over financial reporting

         b) Controls over compliance with laws and regulations, such as health and safety, when they are performed in multiple countries or subsidiaries

         c) Controls, such as budgeting and performance management, when they are performed in multiple subsidiaries and coverage extends to the majority of assets, revenues, etc.

2) The assurance for a component of operations is a **micro opinion**. It is usually based on one or a few audit projects. For example, a micro opinion may be expressed on

   a) An individual business process or activity in one organization, department, or location

   b) Internal control at a reporting unit when all work is performed in one audit

   c) Compliance with policies, laws, and regulations regarding data privacy when the work is performed in one or a few business units

3) The need for audit opinions and the ability to express them depends on, among other things,

   a) The needs of stakeholders;
   b) The scope, nature, timing, and extent of audit work;
   c) The sufficiency of resources to complete the work; and
   d) Assessing the results.

d. **Stakeholder requirements** for opinions should be clarified by the CAE with senior management and the board. Thus, the nature of the service to be performed should be determined prior to the engagement.

1) Discussions with stakeholders about an opinion may include

   a) Why it is being requested

   b) The timing for issuance and type of opinion

   c) The form of opinion (e.g., written or verbal)

   d) The level of assurance

   e) The period covered

   f) The scope (e.g., whether it is limited to operational controls)

      i) The scope definition commonly extends to (a) the parts of the entity covered, (b) controls addressed, and (c) the time period or moment in time for which the opinion is expressed.

   g) Suitable criteria to be used, i.e., a framework of factors relevant to the auditee against which outcomes may be measured

      i) The internal audit activity determines whether the entity has identified appropriate governance, risk management, and control practices. Thus, the auditee should provide a statement of risk tolerance or risk appetite and materiality thresholds. Without these principles, an opinion should not be expressed.

   h) Potential users

e. The following are factors that affect the expression of an opinion.

   1) The characteristics of macro and micro opinions.

   2) Whether positive or negative assurance will be expressed.

   3) The purpose and use of any special requests.

   4) The audit evidence to support the opinion and the time required for the work.

   5) Agreement with stakeholders on the criteria used.

   6) The need to develop an approach to provide sufficient, relevant evidence. This approach may combine the results of previous audits or identify areas of significance and risk.

      a) If multiple projects are required, they should be identified.

   7) The consideration of related projects (including reliance on the work of others or self-assessments) and allowing time for the final assessment.

   8) Whether resources and skills are adequate. If not, the auditor may (a) decline to express the opinion or (b) qualify the opinion (by excluding certain areas or risks from the scope).

      a) Discussions with management and communication of the plan, including its timing and scope and the criteria to be used.

f. **Evaluating results** of audit work completed may involve rating individual audit findings and their significance relative to a project, risk category, or the organization as a whole.

   1) The auditor considers the magnitude or significance (materiality) of a key business objective that is fundamental to the opinion, including the residual risk that it will not be achieved.

   2) The implications of audit issues or findings (impact) are considered and understood in the context of the opinion to be given (micro or macro).

   3) Another factor to be considered in a macro opinion is rating the risks that the controls in place will not permit management’s objectives to be achieved.

g. The **use of grades** in expressing an opinion requires careful wording, particularly terms such as “adequate” or “inadequate” and “satisfactory” or “unsatisfactory.” Wording should be clear and well defined.

   1) General terms may not sufficiently define the meaning. For example, the term “effective” usually refers to effectiveness in design and operation. The opinion needs to indicate whether both meanings are included.

   2) Clarity is improved if the organization has adopted a broadly understood definition of internal controls, such as the COSO model.

   3) Use of a grading scale generally requires a well-defined evaluation structure. For example, an opinion may state how much better or worse controls are than a defined benchmark.

   4) Increased precision in the information provided in an opinion normally increases the amount of evidence needed to support the opinion.

h. Macro opinions are generally in writing and in the form of **positive assurance**.

   1) The CAE provides macro opinions because (s)he has an overview of micro audit results.

   2) Positive assurance (reasonable assurance) is the highest level and requires the highest level of evidence.

      a) The assertion may be binary, for example, that controls are (are not) effective, or risks are (are not) effectively managed.

   3) Variations in positive assurance may include the use of commonly understood grades of the effectiveness of control or risk management.

      a) Examples include color coding (red-yellow-green) or a grading scale (1 to 4).

   4) A **qualified opinion** indicates an exception to the general opinion, for example, that controls were satisfactory with the exception of accounts payable controls.

i. **Negative assurance**, sometimes referred to as limited assurance, is a statement that nothing came to the auditor’s attention about an objective, such as the effectiveness of internal control or adequacy of a risk management process.

   1) The internal auditor takes no responsibility for the sufficiency of the audit scope and procedures.

   2) Occasionally, internal auditing may be asked for an informal opinion (oral opinion) on the adequacy of governance, risk management, or control policies and processes, either at the macro or micro level.

      a) If possible, the expression of such an opinion should be based on objective evidence.

      b) The same factors are considered as in expressing a written opinion.

      c) In some instances, internal auditing should decline to issue an oral opinion, especially given a lack of sufficient evidence or work to support the opinion.

j. If the CAE intends to rely on the **work of others**, appropriate steps should be taken, including assessing the competency, independence, and objectivity of the other assurance providers.

   1) Such reliance should be included in discussions with key stakeholders and, if significant, the board.

k. The use of opinions has **legal** significance because of the increased reliance on internal audit reports. However, reliance might result in legal liability if a control failure is discussed after issuance of the report. Moreover, the CAE’s certification credentials may have legal implications if noncompliance issues arise.

   1) Thus, the CAE should use appropriate language in the report and provide a disclaimer that notifies the reader of any limitations on the assurance given.

      a) The CAE should state that it is not possible to provide absolute assurance and should encourage readers to consider all legal implications.

9.5 EXIT CONFERENCE AND MANAGEMENT'S RESPONSE

1. **Exit Conferences**
   a. Internal auditors discuss observations, conclusions, and recommendations with engagement clients and appropriate levels of management before the CAE issues the final communication. The discussion usually occurs during the engagement or at post-engagement (exit) conferences.
      1) Internal auditors are in charge of the exit conference and therefore should lead the discussions.
      2) The conference participants should include representatives from management who have detailed knowledge about the process or area under review and who can authorize implementation of corrective action.

   b. The primary purpose of an exit conference is to present audit findings (i.e., observations, conclusions, and recommendations). Secondary purposes are, among others, to
      1) Improve relations with the engagement client(s).
      2) Review and verify the appropriateness of the engagement communication based upon client input, which ensures the accuracy of the information used by internal auditors.
      3) Resolve conflicts.
      4) Identify management's actions and responses or generate commitment for appropriate managerial action.
      5) Enhance the effectiveness of internal auditing engagements.

   c. The internal auditor should document the exit conference because the information may be needed if a dispute later arises.

2. **Management's Review and Response**
   a. Reviews of drafts of communications with engagement clients (management or others) are a courtesy to them and a form of insurance for the engagement.
   b. Clients may have discussed all such matters during the engagement. They should be given the opportunity to read what will be sent to their superiors. Moreover, seeing the draft report may cause clients to view the results differently.
   c. Reviewing results in draft form with the client may detect omissions or inaccuracies before the final communication is issued.
      1) Documenting these discussions and reviews can be valuable in preventing or resolving disputes.

   d. The auditor carefully considers the following before the review:
      1) The person(s) with whom the draft should be reviewed.
      2) The feasibility of performing some reviews on a group basis.
      3) The timing and order of the reviews.
      4) Sending the draft to the client before the meeting.
      5) The need for face-to-face discussions. Sending copies of the draft to interested parties and receiving their written comments may be sufficient.

e. The auditor should be prepared for conflicts and questions.

   1) When the auditor has previously experienced difficulty with an individual, that individual's superior may be invited to attend.

   2) To be able to answer questions promptly, the auditor may wish to prepare notes.

   3) The auditor should be flexible on matters not affecting the substance of the matters communicated. However, the focus of discussions should always remain on the substantive issues.

      a) Additionally, the auditor should never negotiate the opinion.

f. Disagreements are explained in the engagement communications.

g. When the reviews result in significant changes, the other people with whom the draft was reviewed should have an opportunity to see, or be told of, the revisions.

h. The auditor maintains careful records of the post-engagement meeting, of any objections, and of the manner in which conflicts were resolved.

i. When copies of the draft are sent to concerned parties for review, the auditor

   1) Asks for the timely return of the draft with any appropriate comments
   2) Sets a specific due date for the return of the draft
   3) Offers to meet with those who wish to discuss the draft further

j. Responses by clients about internal auditors' actions should go to both management and the internal auditors to ensure the accountability of the internal audit activity. This process is a way of

   1) Judging the internal auditors' performance,
   2) Improving future engagements by identifying areas of weak performance,
   3) Bettering internal auditor-client relations through a greater sense of participation,
   4) Minimizing conflicts, and
   5) Helping clients to understand the difficulties faced by the internal auditors.

9.6 APPROVE AND DISTRIBUTE REPORTS

Performance Standard 2440
Disseminating Results

The chief audit executive must communicate results to the appropriate parties.

Interpretation of Standard 2440

The chief audit executive is responsible for reviewing and approving the final engagement communication before issuance and for deciding to whom and how it will be disseminated. When the chief audit executive delegates these duties, he or she retains overall responsibility.

1. **Disseminating Results**
   a. Generally, final communications are distributed to persons having a business need for the results or responsibility for action plans. They include persons able to ensure due consideration of engagement results, that is, those who can take corrective action or ensure that it is taken. Organizational protocol also may dictate recipients.
      1) The board ordinarily receives summary reports only.
      2) Each communication should contain a distribution sheet listing the distributees and indicating with whom it has been reviewed in draft. Distributees may include the following:
         a) The executive to whom the internal audit activity reports
         b) The person or persons to whom replies will be addressed
         c) Persons responsible for the activity or activities reviewed, e.g., auditee management
         d) Persons required to take corrective action
   b. Results may be communicated orally or in writing, with the format varying with the recipient.

2. **Sensitive Information**

   a. The auditors may possess critically sensitive and substantial information with significant potential adverse consequences. If the new information is substantial and credible, the auditors normally communicate it on a timely basis to senior management and the board.

      1) The communication is typically through the internal audit activity’s usual chain of command, i.e., from staff to supervisor to chief audit executive.

   b. If the CAE then concludes that senior management is exposing the organization to unacceptable risk and is not taking appropriate action, (s)he presents the information and differences of opinion to the board.

   c. Laws, regulations, or common practices may require immediate reporting of sensitive occurrences, e.g., fraudulent financial reporting or illegal acts, to the board.

   d. Auditors may need to consider communicating outside the chain of command or the organization (internal or external whistleblowing, respectively).

      1) Most whistleblowers act internally. However, those who act outside the organization typically mistrust its response, fear retaliation, or have health or safety concerns.

         a) If an internal auditor elects internal whistleblowing, (s)he must cautiously evaluate the evidence, the reasonableness of the conclusions, and the merits of possible actions.

            i) Such action may be appropriate if it results in responsible action by senior management or the board.

      2) The decision to communicate outside the chain of command should be based on a well-informed opinion that the wrongdoing is supported by the evidence and that a legal, professional, or ethical obligation requires action.

         a) The auditor must make a professional decision about his or her obligation to the employer.

   e. Public servants may be required to report illegal or unethical acts, and some laws protect citizen whistleblowers. Thus, auditors need to be aware of applicable laws and must obtain legal advice if uncertain of legal requirements or consequences.

      1) Members of The IIA and CIAs also follow the provisions of The IIA’s Code of Ethics.

      2) An auditor’s professional duty and ethical responsibility is to evaluate the evidence and the reasonableness of his or her conclusions. The auditor then decides whether further actions may be needed to protect

         a) The organization,
         b) Its stakeholders,
         c) The outside community, or
         d) The institutions of society.

      3) The auditor also needs to consider the duty of confidentiality. The advice of legal counsel and other experts may be needed.

   f. Information that is privileged, proprietary, or related to improper or illegal acts is disclosed in a separate communication and distributed to the board.

      1) If senior management is involved, report distribution is to the board.

3. Communications Outside the Organization

Implementation Standard 2440.A2

If not otherwise mandated by legal, statutory, or regulatory requirements, prior to releasing results to parties outside the organization the chief audit executive must:

- Assess the potential risk to the organization.
- Consult with senior management and/or legal counsel as appropriate.
- Control dissemination by restricting the use of the results.

a. Auditors review guidance for disseminating information outside the organization. Such information could affect the organization's market value, reputation, earnings, or competitiveness. If guidance does not exist, auditors facilitate adoption of policies. These policies address

1) Authorization requirements,
2) The approval process,
3) Guidelines for types of information that may be reported,
4) Authorized recipients and what they may receive,
5) Legal considerations, and
6) Other information includible in outside communications (e.g., nature of assurance, opinions, guidance, advice, or recommendations).

b. Requests for existing information are reviewed to determine its suitability for disclosure. A request for information that must be created or determined results in a new internal audit engagement.

1) It may be possible to create a special-purpose report based on existing information that is suitable for outside disclosure.

c. Outside dissemination considers

1) The need for a written agreement;
2) Identifying persons related to the report or information;
3) Identification of objectives, scope, and procedures;
4) Nature of the report or other communication; and
5) Copyright issues.

d. The internal auditor may discover information reportable to senior management or the board during an engagement that requires outside disclosure. As a result, the CAE needs to communicate suitably to the board.

e. Engagements to generate internal audit reports or communications outside the organization need to be conducted in accordance with applicable standards. The report or other communication should refer to such standards.

EXAMPLE 9-1 Whistleblowing

An internal auditor discovered fraud committed by members of management and is unsure of whom to disclose this information.

In most cases of whistleblowing, whistleblowers will disclose sensitive information internally, even if not within the normal chain of command. If they trust the policies and mechanisms of the organization to investigate the problem, information can be shared with the appropriate internal parties. However, if the whistleblower doubts the problem will be properly investigated by the corporation, (s)he may consider disclosing the problem to an outside party.

9.7 MONITOR ENGAGEMENT OUTCOMES

Performance Standard 2500
Monitoring Progress

The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

1. **Monitor Outcomes**

    a. Further guidance is provided in IG 2500, *Monitoring Progress*.

    1) In establishing and maintaining a monitoring system for engagement results, the CAE first considers the type of information and the detail the board and senior management expect.

    2) The CAE is guided by professional judgment and the expectations of the board and senior management in determining the timing and means of monitoring.

    3) At a minimum, the system should include recording (a) pertinent observations, (b) corrective action, and (c) current status.

    a) The factors that influence the nature of monitoring include the organization's size and complexity and the availability of exception tracking software.

    b. Specific characteristics of monitoring processes may include the following:

    1) The CAE establishes procedures to monitor the disposition of reported results. They include a(n)

    a) Time frame for management's response,

    b) Evaluation and verification of the response (if appropriate),

    c) Follow-up (if appropriate), and

    d) Communications process that reports unsatisfactory responses (including assumption of risk) to the appropriate senior management or the board.

    2) Observations and recommendations needing immediate action are monitored until correction or implementation, respectively.

    3) Observations and recommendations are addressed to managers responsible for corrective action.

    4) Management responses and action plans are received and evaluated during the engagement or within a reasonable time afterward.

    a) Responses need to be sufficient for the CAE to evaluate the adequacy and timeliness of proposed actions.

    5) The internal audit activity receives periodic updates from management to evaluate the status of its efforts to correct observations or implement recommendations.

    6) Information from other units involved in follow-up or correction is received and evaluated.

    7) The status of responses is reported to senior management or the board.

2. Follow-Up Process

Implementation Standard 2500.A1

The chief audit executive must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

a. Follow-up is the element of monitoring that evaluates the adequacy, effectiveness, and timeliness of actions on reported observations and recommendations, including those by other auditors.

   1) The **internal audit activity charter** defines the responsibility for follow-up. The CAE defines its nature, timing, and extent after considering the

      a) Significance of what is reported,
      b) Effort and cost of correction,
      c) Effect of failure of correction,
      d) Complexity of correction, and
      e) Time period involved.

   2) The CAE includes follow-up as part of the work schedule. Scheduling depends on the risk involved and the difficulty and timing of corrective action.

   3) If action already taken suffices, follow-up may be part of the next engagement.

   4) Auditors verify that actions remedy underlying conditions.

   5) Follow-up should be documented.

   6) Follow-up also includes determining whether senior management or the board has assumed the risk of not taking corrective action on reported observations.

b. The following is a more detailed description of the follow-up process:

   1) The internal auditor should

      a) Receive all replies by the engagement client to the engagement communications

      b) Evaluate the adequacy of those replies

      c) Be convinced that the action taken will cure the defects

   2) The internal auditor is in the best position to carry out the follow-up responsibility. (S)he is

      a) Better acquainted with the facts than senior management or other control centers in the organization

      b) More objective than the operating manager who must take the corrective action

3) The responsibility for determining whether corrective action is adequate should include the authority to evaluate the adequacy of replies to engagement communications. The internal auditor should
    a) Report to management when corrective actions are not timely or effective.
    b) Submit periodic reports to management on open engagement observations and recommendations.
4) The adequacy of a response depends on the circumstances in each case. In general, a satisfactory response
    a) Addresses itself to the complete problem, not just to specific items included in the internal auditor's sample.
    b) Shows that action also has been taken to prevent a recurrence of the deficient condition.
5) In evaluating the reply, the internal auditor should be satisfied that the action promised is actually taken. The auditor should
    a) Obtain copies of revised procedures issued to correct conditions.
    b) Make any field tests needed to provide assurance that the condition has been corrected.
6) A formal system should be designed to keep engagements open until adequate corrective action is assured. For example,
    a) Provisions should be made for the formal opening and closing of engagements.
    b) The internal auditors should issue a formal statement of closure, supported by copies of replies to engagement communications and explanations of the action taken to ensure the adequacy and effectiveness of corrective measures.
        i) Closure reports are directed to the chief audit executive.
    c) Engagements should not be removed from the internal audit activity's open engagements listing until all required corrective actions have been taken and evaluated.

3. **Acceptance of Excessive Risk**

   a. The CAE is responsible for assessing the risk that remains after client management has taken action, or no action, to reduce its severity (i.e., residual risk).

Performance Standard 2600
Communicating the Acceptance of Risks

When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.

Interpretation of Standard 2600

The identification of risk accepted by management may be observed through an assurance or consulting engagement, monitoring progress on actions taken by management as a result of prior engagements, or other means. It is not the responsibility of the chief audit executive to resolve the risk.

   b. Management decides the action to be taken in response to engagement results. The CAE assesses this action for timely resolution. The extent of follow-up also is a function of follow-up work done by others.

   c. Senior management may assume the risk of noncorrection. The decisions on all significant engagement observations and recommendations are reported to the board.