

# 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 through 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 1 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 1 – ESSENTIALS OF INTERNAL AUDITING

Domain		Cognitive Level	Gleim Study Unit(s) or Subunit(s)	
<b>Foundations of Internal Auditing (15%)</b>				
I	A	Interpret The IIA's Mission of Internal Audit, Definition of Internal Auditing, and Core Principles for the Professional Practice of Internal Auditing, and the purpose, authority, and responsibility of the internal audit activity	Proficient	1.1
	B	Explain the requirements of an internal audit charter (required components, board approval, communication of the charter, etc.)	Basic	1.8
	C	Interpret the difference between assurance and consulting services provided by the internal audit activity	Proficient	1.1
	D	Demonstrate conformance with the IIA Code of Ethics	Proficient	1.2-1.7
<b>Independence and Objectivity (15%)</b>				
II	A	Interpret organizational independence of the internal audit activity (importance of independence, functional reporting, etc.)	Basic	2.1
	B	Identify whether the internal audit activity has any impairments to its independence	Basic	2.3
	C	Assess and maintain an individual internal auditor's objectivity, including determining whether an individual internal auditor has any impairments to his/her objectivity	Proficient	2.2-2.3
	D	Analyze policies that promote objectivity	Proficient	2.2-2.3
<b>Proficiency and Due Professional Care (18%)</b>				
III	A	Recognize the knowledge, skills, and competencies required (whether developed or procured) to fulfill the responsibilities of the internal audit activity	Basic	2.4-2.5
	B	Demonstrate the knowledge and competencies that an internal auditor needs to possess to perform his/her individual responsibilities, including technical skills and soft skills (communication skills, critical thinking, persuasion/negotiation and collaboration skills, etc.)	Proficient	2.4
	C	Demonstrate due professional care	Proficient	2.6
	D	Demonstrate an individual internal auditor's competency through continuing professional development	Proficient	2.6

Domain		Cognitive Level	Gleim Study Unit(s) or Subunit(s)
IV	<b>Quality Assurance and Improvement Program (7%)</b>		
	A	Describe the required elements of the quality assurance and improvement program (internal assessments, external assessments, etc.)	Basic 2.7-2.8
	B	Describe the requirement of reporting the results of the quality assurance and improvement program to the board or other governing body	Basic 2.9
	C	Identify appropriate disclosure of conformance vs. nonconformance with The IIA's <i>International Standards for the Professional Practice of Internal Auditing</i>	Basic 2.9
V	<b>Governance, Risk Management, and Control (35%)</b>		
	A	Describe the concept of organizational governance	Basic 3.1-3.2
	B	Recognize the impact of organizational culture on the overall control environment and individual engagement risks and controls	Basic 3.1
	C	Recognize and interpret the organization's ethics and compliance-related issues, alleged violations, and dispositions	Basic 3.1
	D	Describe corporate social responsibility	Basic 3.3
	E	Interpret fundamental concepts of risk and the risk management process	Proficient 4.1
	F	Describe globally accepted risk management frameworks appropriate to the organization (COSO - ERM, ISO 31000, etc.)	Basic 4.2-4.4
	G	Examine the effectiveness of risk management within processes and functions	Proficient SU 4
	H	Recognize the appropriateness of the internal audit activity's role in the organization's risk management process	Basic 4.1
	I	Interpret internal control concepts and types of controls	Proficient SUs 5-6
	J	Apply globally accepted internal control frameworks appropriate to the organization (COSO, etc.)	Proficient 5.3
K	Examine the effectiveness and efficiency of internal controls	Proficient SUs 5-6	
VI	<b>Fraud Risks (10%)</b>		
	A	Interpret fraud risks and types of frauds and determine whether fraud risks require special consideration when conducting an engagement	Proficient 7.1
	B	Evaluate the potential for occurrence of fraud (red flags, etc.) and how the organization detects and manages fraud risks	Proficient 7.1-7.2
	C	Recommend controls to prevent and detect fraud and education to improve the organization's fraud awareness	Proficient SUs 5-6, 7.2
D	Recognize techniques and internal audit roles related to forensic auditing (interview, investigation, testing, etc.)	Basic 7.3	



## APPENDIX C

# THE IIA EXAMINATION BIBLIOGRAPHY

The Institute has prepared a listing of references for Part 1 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
COSO – Internal Control – Integrated Framework (Framework) <i>URL: <a href="https://www.coso.org/Pages/ic.aspx">https://www.coso.org/Pages/ic.aspx</a></i>	Committee of Sponsoring Organizations of the Treadway Commission (COSO)
Enterprise Risk Management – Integrating with Strategy and Performance <i>URL: <a href="https://www.coso.org/Pages/ERM-Framework-Purchase.aspx">https://www.coso.org/Pages/ERM-Framework-Purchase.aspx</a></i>	Committee of Sponsoring Organizations of the Treadway Commission (COSO)
The Global Internal Audit Competency Framework <i>URL: <a href="https://na.theiia.org/about-us/about-ia/pages/competency-framework.aspx">https://na.theiia.org/about-us/about-ia/pages/competency-framework.aspx</a></i>	The Institute of Internal Auditors, Inc.
The IIA's Three Lines Model: An Update of the Three Lines of Defense	The Institute of Internal Auditors, Inc.
Internal Auditing: Assurance & Advisory Services <i>URL: <a href="https://bookstore.theiia.org/internal-auditing-assurance-advisory-services-fourth-edition-2">https://bookstore.theiia.org/internal-auditing-assurance-advisory-services-fourth-edition-2</a></i>	Urton L. Anderson, Michael J. Head, Sridhar Ramamoorti, Cris Riddle, Mark Salamasick, Paul J. Sobel
International Professional Practices Framework (IPPF), including <ul style="list-style-type: none"> <li>● Mission</li> <li>● Definition of Internal Auditing</li> <li>● Core Principles</li> <li>● Code of Ethics</li> <li>● <i>Standards</i></li> <li>● Implementation Guides</li> <li>● Practice Guides</li> <li>● Global Technology Audit Guides (GTAGs)</li> </ul> <i>URL: <a href="http://bit.ly/1AilTOC">http://bit.ly/1AilTOC</a></i>	The Institute of Internal Auditors, Inc.

-- Continued on next page --

**CIA EXAM REFERENCES – Continued**

Title/URL	Author
New Auditor's Guide to Internal Auditing	Bruce Turner
People-Centric Skills: Interpersonal and Communication Skills for Auditors and Business Professionals	Danny M. Goldberg and Manny Rosenfeld
Quality Assessment Manual URL: <a href="https://na.theiia.org/services/quality/pages/quality-assessment-manual.aspx">https://na.theiia.org/services/quality/pages/quality-assessment-manual.aspx</a>	The Institute of Internal Auditors, Inc.
Risk Appetite Critical to Success	Committee of Sponsoring Organizations of the Treadway Commission (COSO)
Sawyer's Internal Auditing URL: <a href="https://bookstore.theiia.org/sawyers-internal-auditing-enhancing-and-protecting-organizational-value-7th-edition">https://bookstore.theiia.org/sawyers-internal-auditing-enhancing-and-protecting-organizational-value-7th-edition</a>	L.B. Sawyer
Understanding Management URL: <a href="https://www.cengage.com/c/understanding-management-11e-daft/">https://www.cengage.com/c/understanding-management-11e-daft/</a>	Richard L. Daft and Dorothy Marcic

**AVAILABILITY OF PUBLICATIONS**

The listing above and 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](https://bookstore.theiia.org) or contact The IIA at [bookstore@theiia.org](mailto: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

## 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

## FOUNDATIONS OF INTERNAL AUDITING

1.1	<i>Applicable Guidance</i> .....	2
1.2	<i>Codes of Ethical Conduct for Professionals</i> .....	7
1.3	<i>Internal Audit Ethics -- Introduction and Principles</i> .....	8
1.4	<i>Internal Audit Ethics -- Integrity</i> .....	10
1.5	<i>Internal Audit Ethics -- Objectivity</i> .....	12
1.6	<i>Internal Audit Ethics -- Confidentiality</i> .....	14
1.7	<i>Internal Audit Ethics -- Competency</i> .....	16
1.8	<i>Internal Audit Charter</i> .....	17

This study unit covers **Domain I: Foundations of Internal Auditing** from The IIA's CIA Exam Syllabus. This domain makes up 15% of Part 1 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 APPLICABLE GUIDANCE

### 1. International Professional Practices Framework (IPPF)

- a. The Institute of Internal Auditors (The IIA) defines the **mission** of internal audit as follows:
  - 1) “To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.”
  - 2) Facilitating the achievement of this mission is the IPPF.
- b. The IPPF organizes The IIA’s authoritative guidance so that it is accessible and strengthens The IIA as a global standard setter.
- c. The IPPF contains **mandatory** guidance and **recommended** guidance.

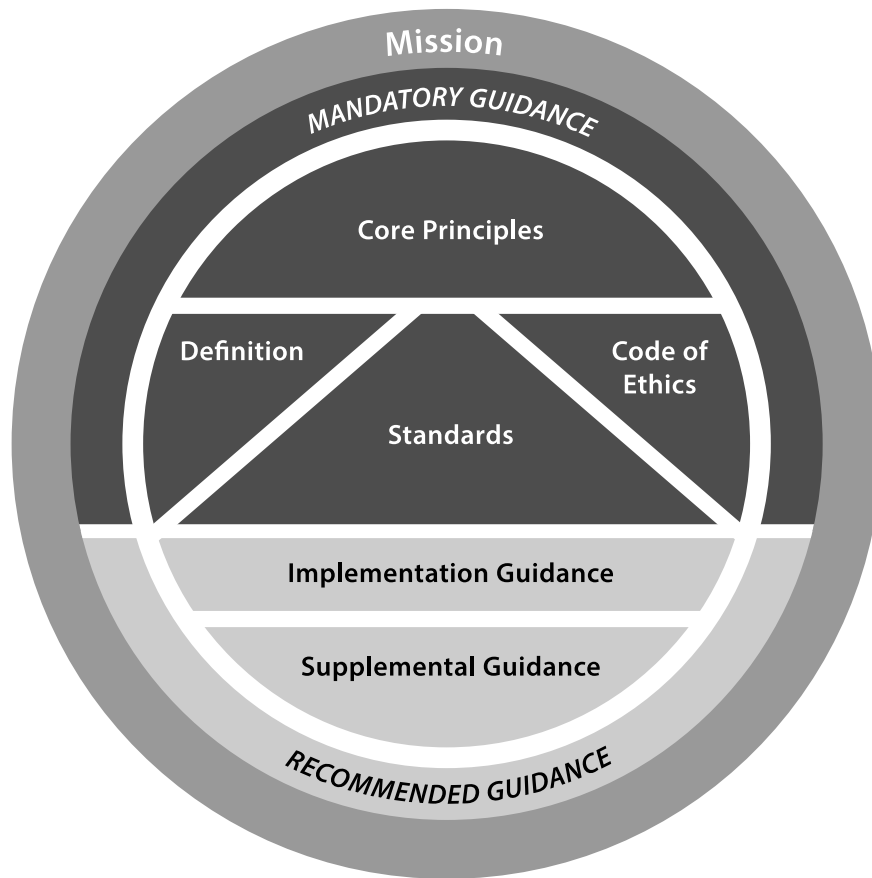


Figure 1-1. IPPF Standards




**SUCCESS TIP**

Knowledge of the IPPF is important for understanding and distinguishing among the elements of the authoritative guidance on internal auditing. But it is more important that you **understand** and can accurately **apply** the **content** contained in the IPPF. Parts 1 and 2 of the CIA exam primarily test understanding and application of IPPF content.

## 2. Mandatory Guidance

- a. Adherence to the mandatory guidance is essential for the professional practice of internal auditing.
  - 1) If the *Standards* are used with requirements of other authoritative bodies, internal audit communications also may cite the other requirements. But, if the *Standards* and other requirements are inconsistent, internal auditors must conform with the *Standards* and may conform with the other requirements if they are more restrictive.
- b. The mandatory guidance consists of four elements: the Core Principles for the Professional Practice of Internal Auditing, the Definition of Internal Auditing, the Code of Ethics, and the *Standards*.
  - 1) The **Core Principles** are the basis for internal audit effectiveness. The internal audit function is effective if all principles are present and operating effectively. The following are the Core Principles:
    - a) “Demonstrates integrity.
    - b) Demonstrates competence and due professional care.
    - c) Is objective and free from undue influence (independent).
    - d) Aligns with the strategies, objectives, and risks of the organization.
    - e) Is appropriately positioned and adequately resourced.
    - f) Demonstrates quality and continuous improvement.
    - g) Communicates effectively.
    - h) Provides risk-based assurance.
    - i) Is insightful, proactive, and future-focused.
    - j) Promotes organizational improvement.”
  - 2) The **Definition of Internal Auditing** is a concise statement of the role of the internal audit activity in the organization.
    - a) “Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of **risk management, control, and governance processes.**”
  - 3) The detailed text of the **Code of Ethics** is in Subunit 1.3.
  - 4) The **Standards** (known formally as the *International Standards for the Professional Practice of Internal Auditing*) serve the following four purposes described by The IIA:
    - a) “Guide adherence with the mandatory elements of the International Professional Practices Framework.
    - b) Provide a framework for performing and promoting a broad range of value-added internal auditing services.
    - c) Establish the basis for the evaluation of internal audit performance.
    - d) Foster improved organizational processes and operations.”

- c. The *Standards* are vital to the practice of internal auditing, but CIA candidates need not memorize them. However, the principles they establish should be thoroughly understood and appropriately applied.
- 1) **Attribute Standards**, numbered in the 1000s, govern the responsibilities, attitudes, and actions of the organization's internal audit activity and the people who serve as internal auditors. They appear in boxes with green highlighting (example below) throughout this text.



### **Attribute Standard 1000** **Purpose, Authority, and Responsibility**

The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Mission of Internal Audit and the mandatory elements of the International Professional Practices Framework (the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the *Standards*, and the Definition of Internal Auditing). The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.

- 2) **Performance Standards**, numbered in the 2000s, govern the nature of internal auditing and provide quality criteria for evaluating the internal audit function's performance. Performance Standards also appear in boxes with green highlighting (example below).



### **Performance Standard 2120** **Risk Management**

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

- 3) **Interpretations** are provided by The IIA to clarify terms and concepts referred to in Attribute or Performance Standards. Interpretations appear in boxes with blue highlighting (example below) throughout this text.



### **Interpretation of Standard 1000**

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, including the nature of the chief audit executive's functional reporting relationship with the board; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities. Final approval of the internal audit charter resides with the board.



- 4) **Implementation Standards** expand upon the individual Attribute or Performance Standards by providing the requirements applicable to assurance (.A) or consulting (.C) services. Implementation Standards appear in boxes with gray highlighting (example below) throughout this text.



#### **Implementation Standard 1110.A1**

The internal audit activity must be free from interference in determining the scope of internal auditing, performing work, and communicating results. The chief audit executive must disclose such interference to the board and discuss the implications.

- d. The Core Principles and the Definition of Internal Auditing are encompassed in the Code of Ethics and the *Standards*. Thus, conformance with the Code and the *Standards* demonstrates conformance with all mandatory elements of the IPPF.

### 3. Recommended Guidance

- a. The pronouncements that constitute recommended guidance have been developed by The IIA through a formal approval process. They describe practices for effective implementation of the Core Principles, the Definition of Internal Auditing, the Code of Ethics, and the *Standards*.

- 1) The two recommended elements of the IPPF are
- a) Implementation Guidance (IG) and
  - b) Supplemental Guidance.

### 4. Purpose, Authority, and Responsibility of the Internal Audit Activity

#### a. Purpose

- 1) As defined in The IIA Glossary, the purpose of the internal audit activity is to provide “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.”
- 2) Per 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. Accordingly, The IIA Glossary defines assurance services as an objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization.
  - a) The **nature and scope** of an assurance engagement are determined by the internal auditor.
  - b) Generally, **three parties** are participants in assurance services:
    - i) The process owner (i.e., the person or group directly involved with the entity, operation, function, process, system, or other subject matter),
    - ii) The internal auditor (i.e., the person or group making the assessment), and
    - iii) The user (i.e., the person or group using the assessment).
  - c) Assurance services include performing financial, performance, compliance, system security, and due diligence engagements.

- 3) Per the *Standards*, **consulting services** are advisory in nature and are generally performed at the specific request of an engagement client. Accordingly, The IIA Glossary defines consulting services as activities intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility.
  - a) The **nature and scope** of the consulting engagement are subject to agreement with the engagement client.
  - b) Generally, **two parties** are participants in consulting services:
    - i) The internal auditor (i.e., the person or group offering the advice)
      - When performing consulting services, the internal auditor should maintain objectivity and not assume management responsibility.
    - ii) The engagement client (i.e., the person or group seeking and receiving the advice)
  - c) Consulting services include providing counsel, advice, facilitation, and training.

b. **Authority**

- 1) The support of management and the board is crucial when inevitable conflicts arise between the internal audit activity and the department or function under review. Thus, the internal audit activity should be empowered to require auditees to grant access to all records, personnel, and physical properties relevant to the performance of every engagement.
  - a) A formal **charter** for the internal audit activity that defines the internal audit activity's purpose, authority, and responsibility must be adopted, and it should contain a grant of sufficient authority. Final approval of the charter resides with the board. (The internal audit charter is the subject of Subunit 1.8.)

c. **Responsibility**

- 1) The internal audit activity's responsibility is to provide the organization with assurance and consulting services that will add value and improve the organization's operations. Specifically, the internal audit activity must evaluate and improve the effectiveness of the organization's governance, risk management, and control processes.

## 1.2 CODES OF ETHICAL CONDUCT FOR PROFESSIONALS

### 1. Reasons for Codes of Ethical Conduct

- a. The primary purpose of a code of ethical conduct for a professional organization is to promote an ethical culture among professionals who serve others.
- b. Additional functions of a code of ethical conduct for a professional organization include
  - 1) Communicating acceptable values to all members,
  - 2) Establishing objective standards against which individuals can measure their own performance, and
  - 3) Communicating the organization's values to outsiders.

### 2. Aspects of Codes of Ethical Conduct

- a. The mere existence of a code of ethical conduct does not ensure that its principles are followed or that those outside the organization will believe that it is trustworthy.
  - 1) A measure of the cohesion and professionalism of an organization is the degree of voluntary compliance with its adopted code.
  - 2) A code of ethical conduct worded so as to reduce the likelihood of members being sued for substandard work would not earn the confidence of the public.
- b. A code of ethical conduct can help establish minimum standards of competence, but it is impossible to require equality of competence by all members of a profession.
- c. To enhance its effectiveness, the code should provide for disciplinary action for violators.

### 3. Typical Components of a Code of Ethical Conduct

- a. A code of ethical conduct for professionals should address at least the following:
  - 1) **Integrity.** A refusal to compromise professional values for personal gain. Another facet of integrity is performance of professional duties in accordance with relevant laws.
  - 2) **Objectivity.** A commitment to providing stakeholders with unbiased information. Another facet of objectivity is a commitment to independence from conflicts of economic or professional interest.
  - 3) **Confidentiality.** A refusal to use organizational information for private gain.
  - 4) **Competency.** A commitment to acquiring and maintaining an appropriate level of knowledge and skill.
- b. These four elements are principles of The IIA's Code of Ethics.

### 1.3 INTERNAL AUDIT ETHICS -- INTRODUCTION AND PRINCIPLES

#### 1. Introduction

- a. The IIA incorporates the Definition of Internal Auditing into the Introduction to the Code of Ethics and specifies the reasons for establishing the Code.

#### 2. Applicability

- a. The provisions of the Code are applied broadly to all organizations and persons who perform internal audit services, not just CIAs and members of The IIA.
- b. Violations of rules of ethics should be reported to The IIA's board of directors.

#### 3. Principles

- a. The Rules of Conduct in the Code are organized based on the principles of integrity, objectivity, confidentiality, and competency.

### **The Institute of Internal Auditors' Code of Ethics**

#### **Introduction to The IIA's Code of Ethics**

The purpose of The Institute's Code of Ethics is to promote an ethical culture in the profession of internal auditing.

*Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.*

A code of ethics is necessary and appropriate for the profession of internal auditing, founded as it is on the trust placed in its objective assurance about governance, risk management, and control.

The Institute's Code of Ethics extends beyond the Definition of Internal Auditing to include two essential components:

1. Principles that are relevant to the profession and practice of internal auditing.
2. Rules of Conduct that describe behavior norms expected of internal auditors. These rules are an aid to interpreting the Principles into practical applications and are intended to guide the ethical conduct of internal auditors.

"Internal auditors" refers to Institute members, recipients of or candidates for IIA professional certifications, and those who perform internal audit services within the Definition of Internal Auditing.

#### **Applicability and Enforcement of the Code of Ethics**

This Code of Ethics applies to both entities and individuals that perform internal audit services.

For IIA members and recipients of or candidates for IIA professional certifications, breaches of the Code of Ethics will be evaluated and administered according to The Institute's Bylaws and Administrative Directives. The fact that a particular conduct is not mentioned in the Rules of Conduct does not prevent it from being unacceptable or discreditable, and therefore, the member, certification holder, or candidate can be liable for disciplinary action.

-- Continued on next page --

**The Institute of Internal Auditors' Code of Ethics – Continued****Principles**

Internal auditors are expected to apply and uphold the following principles:

**1. Integrity**

The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment.

**2. Objectivity**

Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgments.

**3. Confidentiality**

Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so.

**4. Competency**

Internal auditors apply the knowledge, skills, and experience needed in the performance of internal audit services.

**Rules of Conduct****1. Integrity**

Internal auditors:

- 1.1. Shall perform their work with honesty, diligence, and responsibility.
- 1.2. Shall observe the law and make disclosures expected by the law and the profession.
- 1.3. Shall not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the profession of internal auditing or to the organization.
- 1.4. Shall respect and contribute to the legitimate and ethical objectives of the organization.

**2. Objectivity**

Internal auditors:

- 2.1. Shall not participate in any activity or relationship that may impair or be presumed to impair their unbiased assessment. This participation includes those activities or relationships that may be in conflict with the interests of the organization.
- 2.2. Shall not accept anything that may impair or be presumed to impair their professional judgment.
- 2.3. Shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.

**3. Confidentiality**

Internal auditors:

- 3.1. Shall be prudent in the use and protection of information acquired in the course of their duties.
- 3.2. 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.

-- Continued on next page --

**The Institute of Internal Auditors' Code of Ethics – Continued**

**4. Competency**

Internal auditors:

- 4.1. Shall engage only in those services for which they have the necessary knowledge, skills, and experience.
- 4.2. Shall perform internal audit services in accordance with the *International Standards for the Professional Practice of Internal Auditing*.
- 4.3. Shall continually improve their proficiency and the effectiveness and quality of their services.

**1.4 INTERNAL AUDIT ETHICS -- INTEGRITY**

**1. Rules of Conduct – Integrity**

**Integrity**

Internal auditors:

- 1.1. Shall perform their work with honesty, diligence, and responsibility.
- 1.2. Shall observe the law and make disclosures expected by the law and the profession.
- 1.3. Shall not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the profession of internal auditing or to the organization.
- 1.4. Shall respect and contribute to the legitimate and ethical objectives of the organization.

a. Further guidance on integrity is provided in Implementation Guide, *Code of Ethics: Integrity*.

- 1) “Integrity is the **foundation** of the other three principles in The IIA’s Code of Ethics; objectivity, confidentiality, and competency all depend on integrity. Integrity also underpins the *Standards*.”
- 2) The chief audit executive’s (CAE’s) responsibility for implementing integrity includes the following:
  - a) “[T]he CAE should cultivate a culture of integrity by acting with integrity and adhering to the Code of Ethics.”
  - b) “The CAE also establishes policies and procedures to guide the internal audit activity . . . to show diligence and responsibility.”
  - c) “[T]he CAE may also emphasize the importance of integrity by providing training that demonstrates integrity and other ethical principles in action.”
- 3) For internal auditors, the “best attempts to identify and measure integrity likely involve astute awareness and understanding of the Code of Ethics’ rules of conduct for integrity, the IPPF’s Mandatory Guidance, and supporting practices.”

- 4) “For internal auditors, behaviors that may not be illegal but may be **discreditable** include:
- a) Behavior that may be considered bullying, harassing, or discriminatory.
  - b) Failing to accept responsibility for making mistakes.
  - c) Issuing false reports or permitting others to do so.
  - d) Lying.
  - e) Making claims about one’s competency in a manner that is deceptive, false, or misleading.
  - f) Making disparaging comments about the organization, fellow employees, or its stakeholders, either in person or via media (e.g., in publications or social media posts).
  - g) Minimizing, concealing, or omitting observations or unsatisfactory conclusions and ratings from engagement reports or overall assessments.
  - h) Noncompliance with the *Standards* and other IPPF Mandatory Guidance.
    - i) Performing internal audit services for which one is not competent.
    - ii) Performing internal audit services with undeclared impairments to independence and objectivity.
    - iii) Soliciting or disclosing confidential information without proper authorization.
    - iv) Stating that the internal audit activity is operating in conformance with the *Standards* when the assertion is not supported by the results of the quality assurance and improvement program.
  - i) Overlooking illegal activities that the organization may tolerate or condone.
  - j) Using the CIA designation or other credentials after they have expired or been revoked.”
- 5) Conformance with integrity may be demonstrated by
- a) “[A] quality assurance and improvement program [maintained by the CAE].”
  - b) “Forms of acknowledgment, signed by individual internal auditors, [to] demonstrate that internal auditors have committed to follow the organization’s ethics policy or code of conduct, relevant laws and regulations, and The IIA’s Code of Ethics and other IPPF Mandatory Guidance.”
  - c) “[D]iligent supervision of engagements and performance of the self-assessments required by the *Standards*” to demonstrate the integrity of the internal audit activity as a whole.

**EXAMPLE 1-1 Conformance with the Integrity Rule**

An internal auditor is working for a cosmetics manufacturer that may be inappropriately testing cosmetics on animals. If, out of loyalty to the employer, no information about the testing is gathered, the auditor violated the Rules of Conduct by

1. Knowingly becoming a party to an illegal act,
2. Engaging in an act discreditable to the profession,
3. Failing to make disclosures expected by the law, and
4. Not performing the work diligently.

## 1.5 INTERNAL AUDIT ETHICS -- OBJECTIVITY



SUCCESS TIP

The objectivity principle is a frequently tested ethics topic. Mastery of the rules of conduct related to objectivity will increase your success on the exam.

### 1. Rules of Conduct – Objectivity

#### Objectivity

Internal auditors:

- 2.1. Shall not participate in any activity or relationship that may impair or be presumed to impair their unbiased assessment. This participation includes those activities or relationships that may be in conflict with the interests of the organization.
- 2.2. Shall not accept anything that may impair or be presumed to impair their professional judgment.
- 2.3. Shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.

- a. A material ownership interest in a competitor is allowable.
  - 1) An internal auditor seldom can during the course of employment take action to enhance the value of the ownership interest.
- b. For example, if management override of an important control creates exposure to a material risk, the internal auditor is ethically obligated to report the matter to senior officials charged with performing the governance function. Disclosure is not limited by time constraints.
- c. An internal auditor cannot assure anonymity. Information communicated to an internal auditor is not deemed to be privileged. However, promising merely to attempt to keep the source of the information confidential is allowed.
- d. Disclosure is not required when the internal auditor gathers sufficient information to dispel the suspicion of fraud.
- e. The CAE should share information and coordinate activities with other internal and external providers of relevant assurance and consulting services.

### 2. Conflict of Interest Policy

- a. A conflict of interest policy should prohibit the transfer of benefits between an employee and those with whom the organization deals.

### 3. Examples of violations of Rules 2.1., 2.2., and 2.3. include the following:

- a. **Rule of Conduct 2.1.**
  - 1) Excessive individual fraternizing outside of work with the organization's employees, management, third-party suppliers, and vendors.
  - 2) Certain dealings in commercial properties (excluding rental activity).
  - 3) Sales of services or products by the internal auditor to the organization.
  - 4) Participation in non-public service organizations may not be allowed, for example, serving as a consultant to third parties (vendors, suppliers, etc.) with which the organization conducts business.
  - 5) Performing an audit in a department managed by a family member.



- 6) Accepting a bonus based on work accomplished during an audit.
  - 7) Assuming management responsibilities and auditing an area in which the auditor had such responsibilities within 1 year.
- b. **Rule of Conduct 2.2.**
- 1) Accepting gifts, meals, trips, and special treatment that exceed policy limits or are not disclosed and approved
  - 2) Working in a non-audit position and accepting gifts not permitted by IIA code of conduct
- c. **Rule of Conduct 2.3.**
- 1) Intentional omission of disclosures of illegal activity from final engagement communications
  - 2) Withholding pertinent information
  - 3) Not communicating pertinent information to the chief audit executive
  - 4) Distorting facts reported in final engagement communications
4. Conformance with objectivity is demonstrated by the following:
- a. “[T]he CAE may provide evidence of relevant policies and procedures for the internal audit activity, the requirement for internal auditors to attend meetings or trainings about objectivity, and documentation of the rationale for allocating resources to the internal audit plan, including consideration of potential impairments.”
  - b. “Additional evidence may include documentation of research into potential conflicts of interest related to outsourced and cosourced activities for which the CAE has responsibility, as well as signed contracts and records of services provided with the rationale and evidence supporting results, observations, and conclusions.”
  - c. “Engagement workpapers that have been approved by the CAE or a designated engagement supervisor may evidence that internal auditors have conducted a balanced assessment. Feedback from post-engagement surveys and supervisory reviews of engagements may provide additional evidence that the internal auditors’ work appeared to be performed objectively. Assessments as part of the internal audit activity’s quality assurance and improvement program also lend support that appropriate objectivity was used in arriving at internal audit conclusions and opinions.”

#### **EXAMPLE 1-2 Conformance with the Objectivity Rule**

At the end of the year, an internal auditing team made observations and recommendations that an organization can use to improve operating efficiency. To express gratitude, the division manager presented the internal audit team with a gift of moderate value. The internal audit team meets to discuss whether to accept the gift. The following reasons for accepting or not accepting the gift were discussed:

One auditor said, “we *should* accept the gift because its value is insignificant.”

Another auditor said, “we *should not* accept the gift until after we submit our final engagement communication.”

A third auditor said, “we *should not* accept the gift.”

The lead auditor considered the opinions of the other auditors and the intent of the Rules of Conduct. The lead auditor then decided that acceptance of the gift would be inappropriate because of the presumed impairment of the internal auditor’s professional judgment.

## 1.6 INTERNAL AUDIT ETHICS -- CONFIDENTIALITY

### 1. Rules of Conduct – Confidentiality

#### Confidentiality

Internal auditors:

- 3.1. Shall be prudent in the use and protection of information acquired in the course of their duties.
- 3.2. 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.

- a. Further guidance on confidentiality is provided in Implementation Guide, *Code of Ethics: Confidentiality*.
  - 1) “Organizations usually issue **information security policies** to protect the data they acquire, use, and produce and to ensure compliance with the laws and regulations that pertain to the industry and jurisdiction within which they operate.”
    - a) “To protect proprietary information, policies and procedures may require internal auditors to take the following precautions, even when handling information internally:
      - i) Collect only the data required to perform the assigned engagement and use this information only for the engagement’s intended purposes.
      - ii) Protect information from intentional or unintentional disclosure through the use of controls such as data encryption, email distribution restrictions, and restriction of physical access to the information.
      - iii) Eliminate copies of or access to such data when it is no longer needed.”
  - 2) “To better understand the impact of legal and regulatory requirements and protections (e.g., legal privilege or attorney-client privilege), the chief audit executive (CAE) should **consult with legal counsel**. The organization’s policies and procedures may require that specific authorities review and approve business information before external release.”
  - 3) “Rule of Conduct 3.2 emphasizes that internal auditors must not use any information for personal gain. For example, internal auditors should not use insider financial, strategic, or operational knowledge of an organization to bring about personal financial gain by purchasing or selling shares in the organization. Another example is releasing insider knowledge to journalists or via other media without proper authorization. Using **insider information** to develop a competitive product or selling proprietary information to a competitor also violates this confidentiality rule. Furthermore, internal auditors should not abuse their privilege to access information, such as using access to customer records to look up a neighbor’s recent purchases or to view the health records of a celebrity.”

- 4) Conformance with confidentiality is demonstrated as follows:
- a) “The CAE may demonstrate support of internal audit confidentiality through evidence of policies, processes, procedures, and training materials implemented to cover confidentiality as it applies to the internal audit activity and the organization.”
  - b) “Regarding the release of engagement results, reports, or related information, the CAE demonstrates conformance with the confidentiality principle and rules of conduct by documenting and retaining records of disclosures approved by legal counsel, if applicable, and by senior management and the board.”
  - c) “Internal auditors demonstrate conformance with engagement record confidentiality by documenting distribution restrictions in engagement workpapers and reports and by retaining authorizations of all disclosures and approved distribution lists.”
  - d) “If there are no reports or investigations of individual auditors violating policies, procedures, and rules related to confidentiality, then it is likely that the internal audit activity as a whole is in conformance with the principle.”

**EXAMPLE 1-3 Conformance with the Confidentiality Rule**

Which of the following violate(s) The IIA’s Code of Ethics?

- Investigating a lead sales person’s expense reports based on rumors of overstatement.
  - Investigating potential instances of fraud is within the internal auditor’s normal responsibilities. It is not a violation.
- Purchasing stock in a target organization after reading reports that it may be acquired.
  - Rule of Conduct 3.2 states, “Internal auditors shall not use information for any personal gain.” The stock purchase is a violation.
- Disclosing confidential information in response to a court order.
  - The principle of confidentiality permits the disclosure of confidential information given a legal or professional obligation to do so. This disclosure is not a violation.

## 1.7 INTERNAL AUDIT ETHICS -- COMPETENCY

### 1. Rules of Conduct – Competency

#### Competency

Internal auditors:


- 4.1. Shall engage only in those services for which they have the necessary knowledge, skills, and experience.
- 4.2. Shall perform internal audit services in accordance with the *International Standards for the Professional Practice of Internal Auditing*.
- 4.3. Shall continually improve their proficiency and the effectiveness and quality of their services.

- a. Further guidance on competency is provided in Implementation Guide, *Code of Ethics: Competency*.
  - 1) Conformance with competency is demonstrated by the following:
    - a) “The CAE may demonstrate a culture supportive of competency and the continual improvement of proficiency, effectiveness, and quality through evidence that:
      - i) Engagements have been properly resourced and supervised.
      - ii) Feedback has been solicited from internal audit stakeholders and sufficiently considered.
      - iii) Performance reviews of internal auditors have been conducted regularly.
      - iv) Opportunities for training, mentoring, and professional education have been provided.
      - v) A quality assurance and improvement program is active.
      - vi) Internal audit services are performed in conformance with the IPPF’s Mandatory Guidance.”
    - 2) “The knowledge, skills, and experience of individual internal auditors may be evidenced, in part, through credentialed qualifications, such as university degrees and certifications, and relevant work history as detailed on the internal auditor’s resume, which the CAE and/or the organization’s human resources department should have on file.”
    - 3) “Additionally, internal auditors may maintain documentation of a skills self-assessment, a plan for professional development, and the completion of continuing professional education/development courses or trainings.”
    - 4) “Internal auditors also may provide evidence of experiences undertaken — such as specific work assignments (i.e., on-the-job training) or volunteering in professional organizations — to expand their competencies. Pursuing and completing professional education, whether new certifications or continuing professional education, further evidences an internal auditor’s commitment to continually improving their proficiency and the effectiveness and quality of their services.”

**EXAMPLE 1-4 Conformance with the Competency Rule**

Which of the following violate(s) The IIA's Code of Ethics?

- After obtaining evidence that an employee is embezzling funds, the internal auditor interrogates the suspect. The organization has a security department.
  - Internal auditors generally lack the knowledge, skills, or experience regarding interrogation of suspects possessed by security specialists. The lack of proficiency most likely is a violation.
- An internal auditor has been assigned to perform an engagement in the warehousing department next year. The auditor currently has no expertise in this area but accepted the assignment and plans to take continuing professional education courses in warehousing.
  - The internal auditor plans to acquire the required knowledge and skills prior to the start of this engagement. The internal auditor most likely did not violate the Code of Ethics.

**1.8 INTERNAL AUDIT CHARTER**

**Attribute Standard 1000  
Purpose, Authority, and Responsibility**

The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Mission of Internal Audit and the mandatory elements of the International Professional Practices Framework (the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the *Standards*, and the Definition of Internal Auditing). The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.

**1. Internal Audit Charter**

- a. The following Interpretation was issued by The IIA:


**Interpretation of Standard 1000**

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, including the nature of the chief audit executive's functional reporting relationship with the board; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities. Final approval of the internal audit charter resides with the board.

- 1) An auditee must not be able to place a **scope limitation** on the internal audit activity by refusing to make relevant records, personnel, and physical properties available to the internal auditors.

- b. Engagement clients must be informed of the internal audit activity's purpose, authority, and responsibility to prevent misunderstandings about access to records and personnel.
- c. IG 1000, *Purpose, Authority, and Responsibility*, further addresses the charter:
  - 1) "To create [the internal audit charter], the chief audit executive (CAE) must understand the Mission of Internal Audit and the mandatory elements of The IIA's International Professional Practices Framework (IPPF) — including the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the *International Standards for the Professional Practice of Internal Auditing*, and the Definition of Internal Auditing.
  - 2) This understanding provides the foundation for a discussion among the CAE, senior management, and the board to **mutually agree upon**:
    - a) Internal audit objectives and responsibilities
    - b) The expectations for the internal audit activity
    - c) The CAE's functional and administrative reporting lines
    - d) The level of authority (including access to records, physical property, and personnel) required for the internal audit activity to perform engagements and fulfill its agreed-upon objectives and responsibilities
  - 3) The CAE may need to confer with the organization's legal counsel or the board secretary regarding the preferred format for charters and how to effectively and efficiently submit the proposed internal audit charter for board approval.
  - 4) Once **drafted**, the proposed internal audit charter should be discussed with senior management and the board to confirm that it accurately describes the agreed-upon role and expectations or to identify desired changes. Once the draft has been **accepted**, the CAE **formally presents** it during a board meeting to be discussed and approve.
  - 5) The **minutes** of the board meetings during which the CAE initially discusses and then formally presents the internal audit charter provide documentation of conformance. In addition, the **CAE retains the approved charter.**"
- d. The charter must define the nature of assurance and consulting services provided by the internal audit activity.

#### Implementation Standard 1000.A1

The nature of assurance services provided to the organization must be defined in the internal audit charter. If assurances are to be provided to parties outside the organization, the nature of these assurances must also be defined in the internal audit charter.

#### Implementation Standard 1000.C1

The nature of consulting services must be defined in the internal audit charter.



- e. The charter must also refer to the mandatory guidance portion of the IPPF.

### Attribute Standard 1010 Recognizing Mandatory Guidance in the Internal Audit Charter

The mandatory nature of the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the *Standards*, and the Definition of Internal Auditing must be recognized in the internal audit charter. The chief audit executive should discuss the Mission of Internal Audit and the mandatory elements of the International Professional Practices Framework with senior management and the board.



- f. The IIA's model internal audit charter is available from The IIA; however, it is restricted to IIA members only.

## 2. Key Definitions from the Glossary

- a. The complete IIA Glossary is in Appendix A. The definitions do not need to be memorized, but they are useful to exam candidates and practitioners.
- 1) **Chief audit executive (CAE)** 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.
    - a) The chief audit executive or others reporting to the chief audit executive will have appropriate professional certifications and qualifications.
    - b) The specific job title or responsibilities of the chief audit executive may vary across organizations.
  - 2) The **board** is 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.
    - a) Although governance arrangements vary among jurisdictions and sectors, typically the board includes members who are not part of management.
    - b) If a board does not exist, the word "board" in the *Standards* refers to a group or person charged with governance of the organization.
    - c) 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).

## STUDY UNIT TWO

### INDEPENDENCE, OBJECTIVITY, PROFICIENCY, CARE, AND QUALITY

2.1	<i>Independence of the Internal Audit Activity (IAA)</i> .....	2
2.2	<i>Objectivity of Internal Auditors</i> .....	6
2.3	<i>Impairment to Independence and Objectivity</i> .....	8
2.4	<i>Auditor Proficiency</i> .....	12
2.5	<i>Internal Audit Resources</i> .....	16
2.6	<i>Due Professional Care and Continuing Professional Development</i> .....	17
2.7	<i>Quality Assurance and Improvement Program (QAIP)</i> .....	20
2.8	<i>Internal and External Assessments</i> .....	22
2.9	<i>Reporting on Quality Assurance</i> .....	26

This study unit covers three domains from The IIA's CIA Exam Syllabus: **Domain II: Independence and Objectivity**, **Domain III: Proficiency and Due Professional Care**, and **Domain IV: Quality Assurance and Improvement Program**. These domains make up 40% of Part 1 of the CIA exam and are 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 INDEPENDENCE OF THE INTERNAL AUDIT ACTIVITY (IAA)



### SUCCESS TIP

The examination uses acronyms for such frequently used terms as IIA and IAA. IIA and IAA are the acronyms for The Institute of Internal Auditors and internal audit activity, respectively.



### Attribute Standard 1100 Independence and Objectivity

The internal audit activity must be independent, and internal auditors must be objective in performing their work.

#### 1. Independence

- a. Independence is an organizational attribute of the internal audit activity as a whole. The IIA clarifies this distinction in the Interpretation below. (Objectivity is the subject of Subunit 2.2.)



### Interpretation of Standard 1100 (para. 1)

Independence is the freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner. To achieve the degree of independence necessary to effectively carry out the responsibilities of the internal audit activity, the chief audit executive has direct and unrestricted access to senior management and the board. This can be achieved through a dual-reporting relationship. Threats to independence must be managed at the individual auditor, engagement, functional, and organizational levels.

- 1) **Dual reporting** separates **functional** reporting and **administrative** reporting.

#### 2. Achieving Independence through Reporting to the Board

- a. In this Standard, the reporting level that assures independence is identified in general terms:



### Attribute Standard 1110 Organizational Independence

The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.

- b. The related Interpretation specifies a reporting relationship that effectively achieves independence:

### Interpretation of Standard 1110

Organizational independence is effectively achieved when the chief audit executive reports functionally to the board. Examples of functional reporting to the board involve the board:

- Approving the internal audit charter.
- Approving the risk based internal audit plan.
- Approving the internal audit budget and resource plan.
- Receiving communications from the chief audit executive on the internal audit activity's performance relative to its plan and other matters.
- Approving decisions regarding the appointment and removal of the chief audit executive.
- Approving the remuneration of the chief audit executive.
- Making appropriate inquiries of management and the chief audit executive to determine whether there are inappropriate scope or resource limitations.



### 3. Facilitating Independence through Dual Reporting



#### SUCCESS TIP

The dual-reporting relationship is the most frequently tested aspect of the independence attribute. The organizational independence of the internal audit activity is achieved when it reports functionally to the board and administratively to senior management. Memorization of the internal audit activity's functional and administrative reporting lines will increase your success on the exam.

- a. Further guidance on the dual-reporting relationship is provided in IG 1110, *Organizational Independence*:
- 1) “[T]he CAE works with the board and senior management to determine organizational placement of internal audit, including the CAE’s reporting relationships. To ensure effective organizational independence, the CAE has a direct functional reporting line to the board.”
    - a) But the CAE cannot solely determine organizational independence and placement.
  - 2) “A **functional reporting** line to the **board** provides the CAE with direct board access for sensitive matters and enables sufficient organizational status. It ensures that the CAE has unrestricted access to the board, typically the highest level of governance in the organization.”
  - 3) “Generally, the CAE also has an **administrative reporting** line to senior management, which further enables the requisite stature and authority of internal audit to fulfill responsibilities.”
    - a) “For example, the CAE typically **would not** report to a controller, accounting manager, or mid-level functional manager.”
    - b) “To enhance stature and credibility, The IIA recommends that the CAE report administratively to the **chief executive officer (CEO)** so that the CAE is clearly in a senior position, with the authority to perform duties unimpeded.”

- 4) Conformance with Attribute Standard 1110 may be demonstrated, among other means, through
  - a) “[T]he internal audit charter and the audit committee charter, which would describe the audit committee’s oversight duties.”
  - b) “The CAE’s job description and performance evaluation[, which] would note reporting relationships and supervisory oversight.”
  - c) “[A]n internal audit policy manual that addresses policies like independence and board communication requirements or an organization chart with reporting responsibilities. . . .”
- b. Graphical depiction of dual reporting:

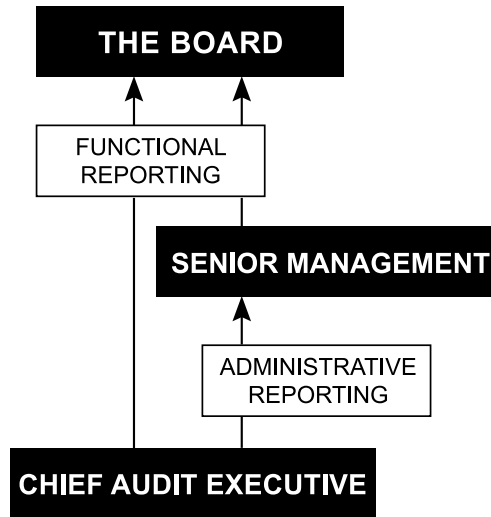


Figure 2-1

- c. The following Implementation Standard clarifies how internal audit’s independence is applied as a practical matter:



**Implementation Standard 1110.A1**

The internal audit activity must be free from interference in determining the scope of internal auditing, performing work, and communicating results. The chief audit executive must disclose such interference to the board and discuss the implications.

#### 4. Board Interaction

- a. The CAE's access to the board must not be limited.



##### **Attribute Standard 1111 Direct Interaction with the Board**

The chief audit executive must communicate and interact directly with the board.

- b. Further guidance on the CAE's direct communication with the board is provided in IG 1111, *Direct Interaction with the Board*:
- 1) "If the CAE has a direct functional reporting relationship with the board, then the board assumes responsibility for approving the internal audit charter, internal audit plan, internal audit budget and resource plan, evaluation and compensation of the CAE, and appointment and removal of the CAE. Further, the board monitors the ability of internal audit to operate independently and fulfill its charter."
  - 2) "[Under a functional] reporting relationship, the CAE will have many opportunities to communicate and interact directly with the board, as required by [Attribute Standard 1111]. For example, the CAE will participate in audit committee and/or full board meetings, generally quarterly, to communicate such things as the proposed internal audit plan, budget, progress, and any challenges. Further, the CAE will have the ability to contact the chair or any member of the board to communicate sensitive matters or issues facing internal audit or the organization. Typically, and **at least annually**, a private meeting with the board or audit committee and the CAE (without senior management present) is formally conducted to discuss such matters or issues. It is also helpful for the CAE to participate in one-on-one meetings or phone calls periodically with the board or audit committee chair, either prior to scheduled meetings or routinely during the year, to ensure direct and open communication."
  - 3) "Board meeting agendas and minutes are often sufficient to demonstrate whether the CAE has communicated and interacted directly with the board."

## 2.2 OBJECTIVITY OF INTERNAL AUDITORS

### 1. Objectivity



#### SUCCESS TIP

Independence is an attribute of the internal audit activity. In contrast, objectivity is an attribute of individual internal auditors. Knowledge of this distinction will increase your success on the exam.

- a. Internal auditors must be objective in performing their work.
  - 1) Objectivity is an attribute of individual internal auditors. The IIA clarifies this distinction in the following Interpretation:

#### Interpretation of Standard 1100 (para. 2)

Objectivity is 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. Threats to objectivity must be managed at the individual auditor, engagement, functional, and organizational levels.

- b. The importance of objectivity as an attribute of individual internal auditors is embodied in the following Standard:

#### Attribute Standard 1120 Individual Objectivity

Internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.

### 2. Conflict of Interest

- a. The IIA Glossary defines conflict of interest as 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.”
- b. The importance of identifying potential conflicts of interest of individual internal auditors is clarified in the following Interpretation:

#### Interpretation of Standard 1120

Conflict of interest is a situation in which an internal auditor, who is in a position of trust, has a competing professional or personal interest. Such competing interests can make it difficult to fulfill his or her duties impartially. A conflict of interest exists even if no unethical or improper act results. A conflict of interest can create an appearance of impropriety that can undermine confidence in the internal auditor, the internal audit activity, and the profession. A conflict of interest could impair an individual’s ability to perform his or her duties and responsibilities objectively.

### 3. Aspects of Objectivity

- a. Further guidance on the objectivity of internal auditors is provided in IG 1120, *Individual Objectivity*:
  - 1) “Objectivity refers to an internal auditor’s **impartial and unbiased mindset**, which is facilitated by avoiding conflicts of interest.”
  - 2) “To manage internal audit objectivity effectively, many CAEs have an internal audit **policy manual or handbook** that describes the expectation and requirements for an unbiased mindset for every internal auditor. Such a policy manual may describe:
    - a) The critical importance of objectivity to the internal audit profession.
    - b) Typical situations that could undermine objectivity, such as auditing in an area in where [*sic*] an internal auditor recently worked; auditing a family member or a close friend; or assuming, without evidence, that an area under audit is acceptable based solely on prior positive experiences.
    - c) Actions the internal auditor should take if he or she becomes aware of a current or potential objectivity concern, such as discussing the concern with an internal audit manager or the CAE.
    - d) Reporting requirements, where each internal auditor periodically considers and discloses conflicts of interest. Often, policies require internal auditors to indicate that they understand the conflict of interest policy and to disclose potential conflicts. Internal auditors sign annual statements indicating that no potential threats exist or acknowledging any known potential threats.”
  - 3) “To reinforce the importance of these policies and help ensure all internal auditors internalize their importance, many CAEs will hold **routine workshops or training** on these fundamental concepts. . . . For example, more senior auditors and managers may share personal experiences where objectivity was called into question or where they self-disclosed a relationship or experience that was a conflict. Another common related training topic is professional skepticism. Such training reinforces the nature of skepticism and the criticality of avoiding bias and maintaining an open and curious mindset.”
  - 4) “[W]hen **assigning internal auditors** to specific engagements, the CAE (or delegate) will consider potential objectivity impairments and avoid assigning team members who may have a conflict. . . .”
  - 5) Because “**performance and compensation** practices can significantly and negatively affect an individual’s objectivity[,] . . . the CAE needs to be thoughtful in designing the internal audit performance evaluation and compensation system and consider whether the measurements used could impair an internal auditor’s objectivity.”
- b. Review of internal audit work results before the related engagement communications are released assists in providing reasonable assurance that the work was performed objectively.

### 4. Assess Individual Objectivity

- a. The CAE must establish policies and procedures to assess the objectivity of individual internal auditors.
  - 1) These can take the form of periodic reviews of conflicts of interest or as-needed assessments during the staffing requirements phase of each engagement.

## 5. Maintain Individual Objectivity

- a. The responsibility to maintain objectivity rests with the CAE and with internal auditors themselves.
  - 1) Internal auditors should be aware of the possibility of new conflicts of interest that may result from changes in personal circumstances or the particular auditees to which an auditor may be assigned.

## 2.3 IMPAIRMENT TO INDEPENDENCE AND OBJECTIVITY



### SUCCESS TIP

The impairments frequently tested on the exam are those caused by the internal auditor or internal audit activity assessing activities for which they were previously responsible or will have responsibility over.

The disclosure requirements related to impairments are also frequently tested. Note that all impairments must be disclosed to the “appropriate” party.

Mastery of both of these frequently tested aspects of impairments will increase your success on the exam.



### Attribute Standard 1130 Impairment to Independence or Objectivity

If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.



### Interpretation of Standard 1130

Impairment to organizational independence and individual objectivity may include, but is not limited to, personal conflict of interest; scope limitations; restrictions on access to records, personnel, and properties; and resource limitations, such as funding.

The determination of appropriate parties to which the details of an impairment to independence or objectivity must be disclosed is dependent upon the expectations of the internal audit activity’s and the chief audit executive’s responsibilities to senior management and the board as described in the internal audit charter, as well as the nature of the impairment.

## 1. Specific Circumstances

- a. The IIA provides examples of and responses to impairments to both independence and objectivity in IG 1130, *Impairment to Independence or Objectivity*:
  - 1) “Impairment situations generally include self-interest, self-review, familiarity, bias, or undue influence.”
  - 2) “Internal audit examples of organizational **independence impairments** include the following, which, if in effect, can also undermine internal auditor objectivity:
    - a) The CAE has broader functional responsibility than internal audit and executes an audit of a functional area that is also under the CAE’s oversight.
    - b) The CAE’s supervisor has broader responsibility than internal audit, and the CAE executes an audit within his or her supervisor’s functional responsibility.
    - c) The CAE does not have direct communication or interaction with the board.
    - d) The budget for the internal audit activity is reduced to the point that internal audit cannot fulfill its responsibilities as outlined in the charter.”
  - 3) “Examples of **objectivity impairments** include:
    - a) An internal auditor audits an area in which he or she recently worked, such as when an employee transfers into internal audit from a different functional area of the organization and then is assigned to an audit of that function. . . .
    - b) An internal auditor audits an area where a relative or close friend is employed.
    - c) An internal auditor assumes, without evidence, that an area being audited has effectively mitigated risks based solely on prior positive audit or personal experiences (e.g., a lack of professional skepticism).
    - d) An internal auditor modifies the planned approach or results based on the undue influence of another person, often someone senior to the internal auditor, without appropriate justification.”
  - 4) “Both the nature of the impairment and board/senior management expectations will determine the **appropriate parties to be notified** of the impairment and the ideal **communication approach**. For example:
    - a) When the CAE believes the impairment is **not real**, but recognizes there could be a *perception* of impairment, the CAE may choose to discuss the concern in engagement planning meetings with the operating management, document the discussion (such as in an audit planning memo), and explain why the concern is without merit. Such a disclosure may also be appropriate for a final engagement report.
    - b) When the CAE believes the impairment **is real** and is affecting the ability of internal audit to perform its duties independently and objectively, the CAE is likely to discuss the impairment with the board and senior management and seek their support to resolve the situation.
    - c) When an impairment comes to light **after an audit has been executed**, and it impacts the reliability (or perceived reliability) of the engagement results, the CAE will discuss it with operating and senior management, as well as the board.”



- b. A **scope limitation** is a restriction placed on the internal audit activity that precludes the activity from accomplishing its objectives and plans. Among other things, a scope limitation may restrict (1) the scope defined in the internal audit charter; (2) the internal audit activity’s access to records, personnel, and physical properties relevant to the performance of engagements; (3) the approved engagement work schedule; (4) the performance of necessary engagement procedures; and (5) the approved staffing plan and financial budget.

**EXAMPLE 2-1                      Scope Limitation**

An internal audit activity was recently engaged to audit the final balance of inventory for the financial statements. During the audit, senior management contacted the lead auditor and stated that the internal audit activity would not be given access to the physical inventory.

The denial of access to the inventory is a scope limitation. The internal audit activity needs to communicate the nature of the scope limitation and its potential effects to the board. This communication should preferably be in writing.

- c. Internal auditors are not to **accept fees, gifts, or entertainment** from an employee, client, customer, supplier, or business associate that may create the appearance that the auditor’s objectivity has been impaired.
  - 1) The appearance that objectivity has been impaired may apply to current and future engagements conducted by the auditor.
  - 2) The status of engagements is not to be considered as justification for receiving fees, gifts, or entertainment.
  - 3) The receipt of promotional items (such as pens, calendars, or samples) that are available to employees and the general public and have minimal value does not hinder internal auditors’ professional judgments.
  - 4) Internal auditors are to report immediately the offer of all material fees or gifts to their supervisors.
- d. The internal auditor’s objectivity is not impaired when the auditor **recommends** standards of control for systems or reviews procedures before they are implemented.
- e. Certain responsibilities lead to the presumption that objectivity is impaired.
  - 1) These responsibilities include **designing, installing, implementing, or drafting** procedures for information systems.
    - a) The appearance of objectivity cannot be maintained when an internal auditor both (1) designs, installs, implements, or drafts procedures for an information system and (2) audits or reviews that system.
  - 2) The following chart contains examples of what may or may not be presumed to impair the objectivity of an internal auditor:

Responsibility	Presumption of Impairment
Recommending standards of control for a new information system application	<b>Not</b> presumed to impair objectivity
Performing reviews of the procedures for retiring capital equipment	<b>Not</b> presumed to impair objectivity
Drafting procedures for a new hiring system	Presumed to impair objectivity

## 2. Objectivity Impaired by Previous Assignment of Internal Audit Personnel

- a. Employees often hold several different positions within the organization in sequence, on both temporary and permanent bases.
  - 1) Organizations build competence and gain the advantages of new perspectives by such cross-training.
- b. On occasion, departments or functions in which current internal audit personnel were employed may be scheduled for an engagement in the internal audit work plan. These situations are addressed in the following Implementation Standard:

### Implementation Standard 1130.A1

Internal auditors must refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an auditor provides assurance services for an activity for which the auditor had responsibility within the previous year.

## 3. Objectivity Impaired by Assignment of Nonaudit Functions to Internal Audit Personnel

- a. The CAE may be assigned responsibility for one or more functions outside the scope of internal auditing.

### Attribute Standard 1112 Chief Audit Executive Roles Beyond Internal Auditing

Where the chief audit executive has or is expected to have roles and/or responsibilities that fall outside of internal auditing, safeguards must be in place to limit impairments to independence or objectivity.

### Interpretation of Standard 1112

The chief audit executive may be asked to take on additional roles and responsibilities outside of internal auditing, such as responsibility for compliance or risk management activities. These roles and responsibilities may impair, or appear to impair, the organizational independence of the internal audit activity or the individual objectivity of the internal auditor. Safeguards are those oversight activities, often undertaken by the board, to address these potential impairments, and may include such activities as periodically evaluating reporting lines and responsibilities and developing alternative processes to obtain assurance related to the areas of additional responsibility.

- b. The following Implementation Standard provides guidance for these situations:

### Implementation Standard 1130.A2

Assurance engagements for functions over which the chief audit executive has responsibility must be overseen by a party outside the internal audit activity.

#### 4. Objectivity Impaired by Performance of Consulting Services



##### Implementation Standard 1130.A3

The internal audit activity may provide assurance services where it had previously performed consulting services, provided the nature of the consulting did not impair objectivity and provided individual objectivity is managed when assigning resources to the engagement.


##### 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.

### 2.4 AUDITOR PROFICIENCY



#### Attribute Standard 1200 Proficiency and Due Professional Care

Engagements must be performed with proficiency and due professional care.

#### 1. Responsibility

- a. According to IG 1200, *Proficiency and Due Professional Care*,
  - 1) “The **CAE is responsible** for ensuring conformance with [Attribute Standard 1200] by the internal audit activity as a whole.”
  - 2) However, “[p]erforming engagements with proficiency and due professional care is the responsibility of **every internal auditor**.”

## 2. Proficiency



### SUCCESS TIP

The proficiency of the internal audit activity is frequently tested on the exam. To increase your success on the exam, remember the internal audit activity is considered proficient if it **collectively** possesses or obtains the competencies needed to perform its responsibilities.

- a. The internal audit activity as a whole, not each auditor individually, must be proficient in all necessary competencies.

### Attribute Standard 1210 Proficiency

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

- b. The Interpretation of Attribute Standard 1210 states, “Proficiency is a collective term that refers to the knowledge, skills, and other competencies required of internal auditors to effectively carry out their professional responsibilities. It encompasses consideration of current activities, trends, and emerging issues, to enable relevant advice and recommendations.”
- c. Proficiency includes knowledge sufficient to evaluate fraud risks and IT risks and controls.

### Implementation Standard 1210.A2

Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

### Implementation Standard 1210.A3

Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

### 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.

- d. Internal auditors become proficient through professional education (including continuing professional development), professional experience, and certifications.

### 3. Competency Framework

- a. The internal audit activity can obtain and maintain the proficiency required by the *Standards* if it effectively applies **The IIA’s Global Internal Audit Competency Framework**.
  - 1) “A **competency** is the ability to perform a task or job properly.” It is “a set of defined knowledge, skills, and behavior.”
- b. IG 1210, *Proficiency*, provides guidance on the relationship between internal audit proficiency and the Competency Framework.
  - 1) The Competency Framework “defines the core competencies needed to fulfill [International Professional Practices Framework (IPPF)] requirements for all occupational levels of the internal audit profession, including staff, management, and executive.”
  - 2) “To build and maintain the proficiency of the internal audit activity, the CAE may develop a competency assessment tool or skills assessment based on the Competency Framework or another benchmark (e.g., a mature internal audit activity).”
- c. The Competency Framework is described by The IIA as “a tool that defines the competencies needed to meet the requirements of the International Professional Practices Framework for the success of the internal audit profession.” The Framework describes 10 interdependent core competencies:
  - I. **Professional ethics**: Promotes and applies professional ethics
  - II. **Internal audit management**: Develops and manages the internal audit function
  - III. **IPPF**: Applies the International Professional Practices Framework (IPPF)
  - IV. **Governance, risk and control**: Applies a thorough understanding of governance, risk, and control appropriate to the organization
  - V. **Business acumen**: Maintains expertise of the business environment, industry practices, and specific organizational factors
  - VI. **Communication**: Communicates with impact
  - VII. **Persuasion and collaboration**: Persuades and motivates others through collaboration and cooperation
  - VIII. **Critical thinking**: Applies process analysis, business intelligence, and problem solving techniques
  - IX. **Internal audit delivery**: Delivers internal audit engagements
  - X. **Improvement and innovation**: Embraces change and drives improvement and innovation”

- d. The organization of the Competency Framework is presented below.

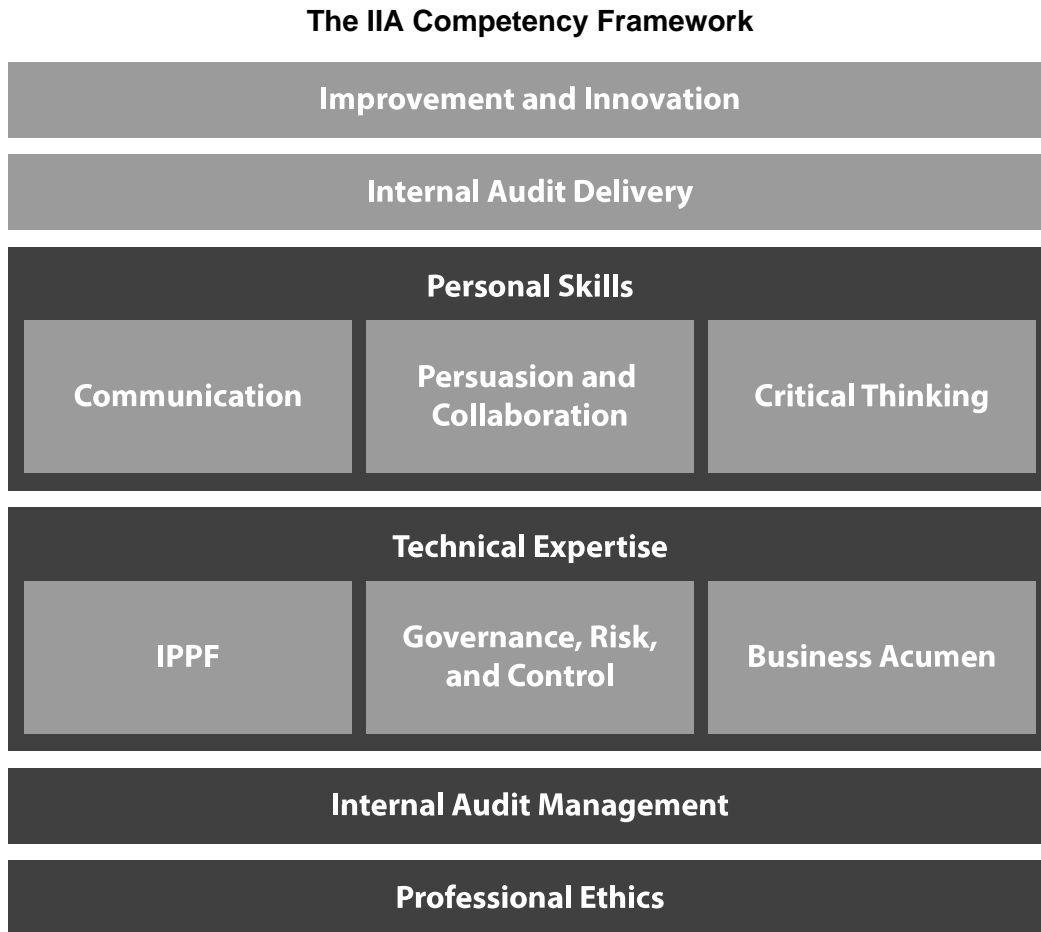


Figure 2-2

- 1) Professional ethics and internal audit management are the basis of service delivery.
- 2) The IPPF is the primary set of standards for internal auditors. Technical expertise in governance, risk, and control is needed to help achieve organizational objectives. Business acumen is an understanding of the organizational culture, the economy in which it operates, and the global and local conditions that affect its operations.
- 3) Competence in communication, persuasion, collaboration, and critical thinking is required to perform engagements and promote the organization's improvement and innovation.

## 2.5 INTERNAL AUDIT RESOURCES

### 1. Internal Resources

- a. The CAE must ensure that the internal audit activity is able to fulfill its responsibilities.
  - 1) Identifying the available knowledge, skills, and competencies within the internal audit activity will help the CAE determine whether the current staff is sufficient to satisfy those responsibilities.
- b. The following practices help the CAE identify the available resources:
  - 1) Hiring practices are an essential part of understanding the background of the internal audit staff. During this process, the CAE identifies the internal auditor's education, previous experience, and specialized areas of knowledge.
  - 2) The CAE should conduct periodic skills assessments to determine the specific resources available. Assessments should be performed at least annually.
  - 3) Staff performance appraisals are completed at the end of any major internal audit engagement. These appraisals help the CAE assess future training needs and current staff abilities.
  - 4) Continuing professional development encourages continued growth. Acquired training also should be considered when identifying internal audit resources.
- c. Databases can be used to store internal audit background information. The information stored can include lists of relevant skills, completed projects, acquired training, and development needs.
- d. If the internal audit staff is not able to fulfill internal audit responsibilities, the use of external service providers must be considered.

### 2. External Resources

#### a. Outsourcing and Cosourcing

- 1) An organization may outsource none, all, or some of the functions of the internal audit activity. However, oversight of and responsibility for the internal audit activity must **not** be outsourced.
  - a) Regardless of the degree of outsourcing, services still must be performed in accordance with the *Standards*, and the guidance for obtaining external service providers should be followed.
- 2) Outsourcing alternatives include the following:
  - a) Partial or total external sourcing on an ongoing basis
  - b) Cosourcing for a specific engagement or on an ongoing basis
    - i) Cosourcing is performance by internal audit staff of joint engagements with external service providers (*Position Paper, The Role of Internal Auditing in Resourcing the Internal Audit Activity*).

### b. CAE's Responsibility

- 1) The following Implementation Standard requires the use of expertise from outside the internal audit activity during assurance engagements when the internal auditors lack the necessary expertise.



#### Implementation Standard 1210.A1

The chief audit executive must 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.

- a) Each member of the internal audit activity need not be qualified in all disciplines. When necessary, the CAE can obtain necessary knowledge, skills, and competencies from external service providers.

### c. External Service Providers

- 1) Qualified external service providers may be recruited from many sources, such as the external audit firm, an external consulting firm, or a university.
- 2) However, an external service provider associated with the engagement client is unacceptable because the person would not be independent or objective.
- 3) External service providers may more easily accommodate engagement requirements in distant locations.

## 2.6 DUE PROFESSIONAL CARE AND CONTINUING PROFESSIONAL DEVELOPMENT



#### Attribute Standard 1220 Due Professional Care

Internal auditors must apply the care and skill expected of a **reasonably** prudent and competent internal auditor. Due professional care does not imply infallibility.



#### SUCCESS TIP

Due professional care questions on the exam frequently test the standard of care required of internal auditors. To increase your success on the exam, remember the standard of care required is **reasonable care**, not absolute assurance.

### 1. Due Care in Practice

- a. The IIA provides guidance for the application of due care in IG 1220, *Due Professional Care*:
  - 1) “[D]ue professional care requires conformance with The IIA’s Code of Ethics and may entail conformance with the organization’s code of conduct and any additional codes of conduct relevant to other professional designations attained.”



- 2) “[T]he internal audit activity’s policies and procedures provide a systematic and disciplined approach to planning, executing, and documenting internal audit work. By following this systematic and disciplined approach, internal auditors essentially apply due professional care. However, what constitutes due professional care partially depends upon the complexities of the engagement.”
  - 3) “Internal auditors demonstrate conformance with Standard 1220 through proper application of the IPPF’s Mandatory Guidance, which would be reflected in their engagement plans, work programs, and workpapers.”
- b. The following Implementation Standards provide guidance for the application of due care during assurance engagements:



**Implementation Standard 1220.A1**

Internal auditors must exercise due professional care by considering the:

- Extent of work needed to achieve the engagement’s objectives.
- Relative complexity, materiality, or significance of matters to which assurance procedures are applied.
- Adequacy and effectiveness of governance, risk management, and control processes.
- Probability of significant errors, fraud, or noncompliance.
- Cost of assurance in relation to potential benefits.

**Implementation Standard 1220.A2**

In exercising due professional care internal auditors must consider the use of technology-based audit and other data analysis techniques.

**Implementation Standard 1220.A3**

Internal auditors must be alert to the significant risks that might affect objectives, operations, or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified.

- c. The following Implementation Standard provides guidance for the application of due care during consulting engagements:



**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.
- Cost of the consulting engagement in relation to potential benefits.

- d. Due professional care can be demonstrated if the auditor applied the care and skill of a **reasonably competent and prudent** internal auditor in the same or similar circumstances.
  - 1) For example, any unexpected results from analytical procedures should be investigated and adequately explained.

## 2. Continuing Professional Development

- a. The IIA requires internal auditors to continue expanding their knowledge and abilities throughout their careers.



### Attribute Standard 1230 Continuing Professional Development

Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.

- b. IG 1230, *Continuing Professional Development*, gives specific advice regarding further education to enhance proficiency.
  - 1) “An individual internal auditor may use a self-assessment tool, such as the Competency Framework, as a basis for creating a professional development plan. The development plan may encompass on-the-job training, coaching, mentoring, and other internal and external training, volunteer, or certification opportunities.”
  - 2) “Opportunities for professional development include participating in conferences, seminars, training programs, online courses and webinars, self-study programs, or classroom courses; conducting research projects; volunteering with professional organizations; and pursuing professional certifications. . . .”
- c. Certified internal auditors (CIAs) demonstrate their continuing professional development by completing **continuing professional education (CPE)**.
  - 1) Practicing and nonpracticing CIAs must complete 40 hours and 20 hours, respectively, of CPE annually (including at least 2 hours of ethics training).
  - 2) Qualifying CPE activities are those that contribute to internal audit competence. They include the following:
    - a) Educational programs (e.g., seminars, conferences, or technical sessions provided by auditing or accounting organizations and chapters; formal in-house training programs; college or university courses passed; or self-study programs relevant to internal auditing)
    - b) Passing examinations
    - c) Authoring or contributing to publications
    - d) Translating publications
    - e) Delivering oral presentations
    - f) Participating as a subject matter expert volunteer
    - g) Performing external quality assessments

## 2.7 QUALITY ASSURANCE AND IMPROVEMENT PROGRAM (QAIP)



### Attribute Standard 1300 Quality Assurance and Improvement Program

The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.



### Interpretation of Standard 1300

A quality assurance and improvement program is designed to enable an evaluation of the internal audit activity's conformance with the *Standards* and an evaluation of whether internal auditors apply the Code of Ethics. The program also assesses the efficiency and effectiveness of the internal audit activity and identifies opportunities for improvement. The chief audit executive should encourage board oversight in the quality assurance and improvement program.

1. IG 1300, *Quality Assurance and Improvement Program*, describes the characteristics of a QAIP:
  - a. "The QAIP should encompass all aspects of operating and managing the internal audit activity—including consulting engagements—as found in the mandatory elements of the [IPPF]."
  - b. "A well-developed QAIP ensures that the concept of **quality** is embedded in the internal audit activity and **all** of its operations."
  - c. "[I]t must include ongoing and periodic internal assessments as well as external assessments by a qualified independent assessor or assessment team. . . ."
  - d. The QAIP consists of **five components**: (1) internal assessments, (2) external assessments, (3) communication of QAIP results, (4) proper use of a conformance statement, and (5) disclosure of nonconformance.
2. IG 1310, *Requirements of the Quality Assurance and Improvement Program*, states that
  - a. "[T]he QAIP also includes ongoing measurements and analyses of performance metrics such as accomplishment of the internal audit plan, cycle time, recommendations accepted, and customer satisfaction."

3. IG 1300 also addresses the **CAE's responsibilities** for the QAIP:

- a. "The CAE must have a thorough understanding of the mandatory elements of the IPPF, especially the *Standards* and Code of Ethics. Generally, the CAE meets with the board to gain an understanding of the expectations for the internal audit activity, to discuss the importance of the *Standards* and the QAIP, and to encourage the board's support of these."
- b. "The CAE periodically evaluates the QAIP and updates it as needed. For example, as the internal audit activity matures, or as conditions within the internal audit activity change, adjustments to the QAIP may become necessary to ensure that it continues to operate in an effective and efficient manner and to assure stakeholders that it adds value by improving the organization's operations."



#### Attribute Standard 1310

#### Requirements of the Quality Assurance and Improvement Program

The quality assurance and improvement program must include both internal and external assessments.

4. Further guidance is provided in IG 1310, *Requirements of the Quality Assurance and Improvement Program*:

- a. The CAE is responsible for ensuring that the internal audit activity conducts internal assessments and external assessments.
- b. "**Internal assessments** consist of ongoing monitoring and periodic self-assessments . . . , which evaluate the internal audit activity's conformance with the mandatory elements of the IPPF, the quality and supervision of audit work performed, the adequacy of internal audit policies and procedures, the value the internal audit activity adds to the organization, and the establishment and achievement of key performance indicators."
  - 1) "**Ongoing monitoring** is achieved primarily through continuous activities such as engagement planning and supervision, standardized work practices, workpaper procedures and signoffs, report reviews, as well as identification of any weaknesses or areas in need of improvement and action plans to address them."
  - 2) "**Periodic self-assessments** are conducted to validate that ongoing monitoring is operating effectively. . . ."
- c. "**External assessments** provide an opportunity for an **independent** assessor or assessment team to conclude as to the internal audit activity's conformance with the *Standards* and whether internal auditors apply the Code of Ethics, and to identify areas for improvement."
  - 1) "[T]he CAE is responsible for ensuring that the internal audit activity conducts an external assessment at least **once every five years**. . . ."
  - 2) "A self-assessment may be performed in lieu of a full external assessment, provided it is validated by a qualified, independent, competent, and professional external assessor."

5. The **Deming Cycle** (or Plan-Do-Check-Act Cycle) is a continuous improvement model popularized by W. Edwards Deming.
- a. The Deming Cycle consists of four steps:
    - 1) **Plan** establishes standards and expectations for operating a process to meet goals.
    - 2) **Do** executes the process and collects data for further analysis in the later steps.
    - 3) **Check** compares actual results with expected results and analyzes the difference.
    - 4) **Act** provides feedback by identifying and implementing improvements to the process.
  - b. The Deming Cycle can be used to establish the QAIP in a planned, methodical manner. The IIA's Practice Guide, *Quality Assurance and Improvement Program*, presents the application of the Deming Cycle to the QAIP:
    - 1) Formal documentation of standards and expected practices (PLAN)
    - 2) Development activities to define quality and build staff awareness of standards and expectations (DO)
    - 3) Various forms of assessment and review to measure product or process quality (CHECK)
    - 4) Undertaking improvement initiatives and documenting lessons learned (ACT)

## 2.8 INTERNAL AND EXTERNAL ASSESSMENTS

### Attribute Standard 1311 Internal Assessments

Internal assessments must include:

- Ongoing monitoring of the performance of the internal audit activity.
- Periodic self-assessments or assessments by other persons within the organization with sufficient knowledge of internal audit practices.

### Interpretation of Standard 1311

Ongoing monitoring is an integral part of the day-to-day supervision, review, and measurement of the internal audit activity. Ongoing monitoring is incorporated into the routine policies and practices used to manage the internal audit activity and uses processes, tools, and information considered necessary to evaluate conformance with the Code of Ethics and the *Standards*.

Periodic assessments are conducted to evaluate conformance with the Code of Ethics and the *Standards*.

Sufficient knowledge of internal audit practices requires at least an understanding of all elements of the International Professional Practices Framework.

## 1. Internal Assessments

- a. IG 1311, *Internal Assessments*, provides more extensive guidance.
  - 1) “The two interrelated parts of internal assessments—ongoing monitoring and periodic self-assessments—provide an effective structure for the internal audit activity to continuously assess its conformance with the *Standards* and whether internal auditors apply the Code of Ethics.”
  - 2) **Ongoing Monitoring**
    - a) “[O]ngoing monitoring is generally focused on reviews conducted at the **engagement level**.”
      - i) Thus, “ongoing monitoring helps the CAE determine whether internal audit processes are delivering quality on an **engagement-by-engagement basis**.”
      - ii) Compared with periodic self-assessments, ongoing monitoring emphasizes evaluating conformance with the performance standards.
    - b) “Generally, ongoing monitoring occurs routinely throughout the year. . . .”
    - c) “Ongoing monitoring is achieved **primarily** through **continuous activities** such as
      - i) Engagement planning and supervision,
      - ii) Standardized work practices,
      - iii) Workpaper procedures and signoffs, [and]
      - iv) Report reviews. . . .”
    - d) “Additional mechanisms commonly used for ongoing monitoring include:”
      - i) Checklists or automation tools,
      - ii) Feedback from internal audit clients and other stakeholders,
      - iii) Staff and engagement key performance indicators (e.g., “the number of certified internal auditors on staff, their years of experience in internal auditing, the number of continuing professional development hours they earned during the year, timeliness of engagements, and stakeholder satisfaction”).
  - 3) **Periodic Self-Assessments**
    - a) Compared with ongoing monitoring, periodic self-assessments “generally provide a more holistic, comprehensive review of the *Standards* and the internal audit activity.”
    - b) Periodic self-assessments are generally conducted by those with extensive internal auditing experience (e.g., senior internal auditors or certified internal auditors).
    - c) “The internal audit activity conducts periodic self-assessments to validate its continued conformance with the *Standards* and Code of Ethics and to evaluate:
      - i) The quality and supervision of work performed.
      - ii) The adequacy and appropriateness of internal audit policies and procedures.
      - iii) The ways in which the internal audit activity adds value.
      - iv) The achievement of key performance indicators.
      - v) The degree to which stakeholder expectations are met.”

- 4) “**Adequate supervision** is a fundamental element of any quality assurance and improvement program (QAIP). Supervision begins with planning and continues throughout the performance and communication phases of the engagement. Adequate supervision is ensured through expectation-setting, ongoing communications among internal auditors throughout the engagement, and workpaper review procedures, including timely sign-off by the individual responsible for supervising engagements.”
- b. The chief audit executive (CAE) establishes a structure for reporting results of internal assessments that maintains appropriate credibility and objectivity. Generally, those assigned responsibility for conducting ongoing and periodic reviews report to the CAE while performing the reviews and communicate results directly to the CAE.
- c. The CAE should report the results of internal assessments, necessary action plans, and their successful implementation to senior management and the board.

### Attribute Standard 1312 External Assessments

External assessments must be conducted at least once every five years by a qualified, independent assessor or assessment team from outside the organization. The chief audit executive must discuss with the board:

- The form and frequency of external assessments.
- The qualifications and independence of the external assessor or assessment team, including any potential conflict of interest.



## 2. External Assessments

- a. External assessments provide an independent and objective evaluation of the internal audit activity's conformance with the *Standards* and Code of Ethics.
- b. Relevant guidance is provided in IG 1312, *External Assessments*:
  - 1) “External assessments may be accomplished using one of two approaches: a full external assessment, or a self-assessment with independent external validation (SAIV).”
  - 2) “A **full external assessment** would be conducted by a qualified, independent external assessor or assessment team. The team should be comprised of competent professionals and led by an experienced and professional project team leader. The **scope** of a full external assessment typically includes three core components:
    - a) The level of conformance with the *Standards* and Code of Ethics. This may be evaluated via a review of the internal audit activity's charter, plans, policies, procedures, and practices. In some cases, the review may also include applicable legislative and regulatory requirements.
    - b) The efficiency and effectiveness of the internal audit activity. This may be measured through an assessment of the internal audit activity's processes and infrastructure, including the QAIP, and an evaluation of the internal audit staff's knowledge, experience, and expertise.
    - c) The extent to which the internal audit activity meets expectations of the board, senior management, and operations management, and adds value to the organization.”

- 3) “The second approach to meeting the requirement for an external assessment is an SAIV [**self-assessment with independent external validation**]. This type of external assessment typically is conducted by the internal audit activity and then validated by a qualified, **independent** external assessor. The scope of [this assessment] typically consists of:
  - a) A comprehensive and fully documented self-assessment process that emulates the full external assessment process, at least with respect to evaluating the internal audit activity’s conformance with the *Standards* and Code of Ethics.
  - b) Onsite validation by a qualified, independent external assessor.
  - c) Limited attention to other areas such as benchmarking; review, consultation, and employment of leading practices; and interviews with senior and operations management.”
- 4) “[External] assessors or assessment teams must be competent in two main areas:
  - a) [T]he professional practice of internal auditing (including current in-depth knowledge of the IPPF), and
  - b) [T]he external quality assessment process.”
- c. External assessors must have no real or apparent **conflict of interest** due to current or past relationships with the organization.
  - 1) Matters relating to independence include conflicts of **former employees** or of **firms** providing (a) the financial statement audit, (b) significant consulting services, or (c) assistance to the internal audit activity.
  - 2) An individual in another part of the organization or in a related organization (e.g., a parent or an affiliate) is not independent.
  - 3) **Peer review** among three unrelated organizations (but not between two) may satisfy the independence requirement.
  - 4) Given concerns about independence, one or more **independent individuals** may provide separate validation.



## 2.9 REPORTING ON QUALITY ASSURANCE

### 1. Reporting Results

- a. Senior management and the board must be kept informed about the degree to which the internal audit activity achieves the degree of professionalism required by The IIA.

#### Attribute Standard 1320

#### Reporting on the Quality Assurance and Improvement Program

The chief audit executive must communicate the results of the quality assurance and improvement program to senior management and the board. Disclosure should include:

- The scope and frequency of both the internal and external assessments.
- The qualifications and independence of the assessor(s) or assessment team, including potential conflicts of interest.
- Conclusions of assessors.
- Corrective action plans.



- b. The IIA addresses the frequency of reporting on the QAIP in the following excerpt from the Interpretation of Standard 1320:

*To demonstrate conformance with the Code of Ethics and the Standards, the results of external and periodic internal assessments are communicated **upon completion** of such assessments and the results of ongoing monitoring are communicated at least **annually**.*

- c. IG 1320, *Reporting on the Quality Assurance and Improvement Program*, provides further guidance.
  - 1) The expression of an opinion or conclusion on the results of the **external assessment** is included in the external assessment report. The report typically includes an assessment for each standard and an overall assessment for each standard series (attribute and performance). These assessments are in addition to the overall conformance results. The following is an example of a rating scale that may be used to show the degree of conformance:
    - a) **Generally conforms.** The top rating means that (1) an internal audit activity has a charter, policies, and processes, and (2) their execution and results conform with the *Standards*.
    - b) **Partially conforms.** Deficiencies in practice are judged to deviate from the *Standards*. But they do not preclude the internal audit activity from performing its responsibilities.
    - c) **Does not conform.** Deficiencies in practice are judged to be so significant as to seriously impair, or preclude, the internal audit activity's ability to perform adequately in all or in significant areas of its responsibilities.

- 2) During an external assessment, the assessor may provide recommendations to address (a) areas that were not in conformance with the *Standards* and (b) opportunities for improvement.
  - a) The CAE may provide management action plans to address recommendations from the external assessment.
  - b) The CAE also may consider (1) adding the recommendations and management action plans to the internal audit activity's existing monitoring of progress related to internal audit engagement findings and (2) reporting on resolutions.
  - c) Verification that recommendations identified during the external assessment have been implemented is communicated to the board either (1) as part of the internal audit activity's monitoring of progress or (2) by following up separately through the next QAIP internal assessment.

## 2. Importance of Conforming with the Standards

- a. The internal audit activity cannot claim to comply with the *Standards* unless it has a successfully functioning QAIP.

### Attribute Standard 1321

#### Use of "Conforms with the *International Standards for the Professional Practice of Internal Auditing*"

Indicating that the internal audit activity conforms 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.



## 3. Importance of Reporting Nonconformance

- a. The internal audit activity is a crucial part of the modern complex organization's governance processes. Senior management and the board must be informed when an assessment discovers a significant degree of nonconformance.

### Attribute Standard 1322

#### Disclosure of Nonconformance

When nonconformance with the Code of Ethics or the *Standards* impacts the overall scope or operation of the internal audit activity, the chief audit executive must disclose the nonconformance and the impact to senior management and the board.



- b. Nonconformance of this type refers to the overall internal audit activity and not to specific engagements.

# STUDY UNIT THREE

## GOVERNANCE

3.1	<i>Governance Principles</i> .....	1
3.2	<i>Roles of Internal Auditors in Governance</i> .....	9
3.3	<i>Corporate Social Responsibility (CSR)</i> .....	12

This study unit is the first of four covering **Domain V: Governance, Risk Management, and Control** from The IIA's CIA Exam Syllabus. This domain makes up 35% of Part 1 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.



### SUCCESS TIP

The roles of the board, senior management, and internal auditors in organizational governance are frequently tested on the exam. A sound understanding of their unique roles in organizational governance will increase your success on the exam.

### 3.1 GOVERNANCE PRINCIPLES

#### 1. Definition of Corporate Governance

- a. **Governance** is defined in the glossary of the *International Standards for the Professional Practice of Internal Auditing (Standards)* as “[t]he 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.”
  - 1) This definition of governance is consistent with the globally accepted definition of **corporate governance** stated by the Organization for Economic Co-operation and Development (OECD):
 

“Corporate governance involves a set of relationships between a company’s management, its board, its shareholders, and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined.”
  - 2) Stakeholders are persons or entities who are affected by the activities of the entity. Among others, these include shareholders, employees, suppliers, customers, neighbors of the entity’s facilities, and government regulators.
- b. Corporate governance can be influenced by internal or external mechanisms.
  - 1) Internal mechanisms include corporate charters and bylaws, boards of directors, and internal audit functions.
  - 2) External mechanisms include laws, regulations, and the government regulators who enforce them.

## 2. Governance Principles

- a. Governance does not exist independently of risk management and control. Rather, governance, risk management, and control (collectively referred to as GRC) are interrelated.

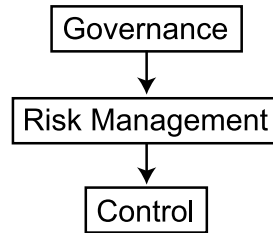


Figure 3-1

- 1) Effective governance considers risk when setting strategy, and risk management relies on effective governance (e.g., tone at the top, risk appetite and tolerance, risk culture, and the oversight of risk management).
  - 2) Effective governance relies on controls to manage risks and on communication of their effectiveness to the board.
- b. The following summary of governance principles is based on a publication of The IIA:
    - 1) An independent and objective board with sufficient expertise, experience, authority, and resources to conduct independent inquiries
    - 2) An understanding by senior management and the board of the operating structure, including structures that impede transparency
    - 3) An organizational strategy used to measure organizational and individual performance
    - 4) An organizational structure that supports accomplishing strategic objectives
    - 5) A governing policy for the operation of key activities
    - 6) Clear, enforced lines of responsibility and accountability
    - 7) Effective interaction among the board, management, and assurance providers
    - 8) Appropriate oversight by management, including strong controls
    - 9) Compensation policies—especially for senior management—that encourage appropriate behavior consistent with the organization’s values, objectives, strategy, and internal control
    - 10) Reinforcement of an ethical culture, including employee feedback without fear of retaliation
    - 11) Effective use of internal and external auditors, ensuring their independence, the adequacy of their resources and scope of activities, and the effectiveness of operations
    - 12) Clear definition and implementation of risk management policies and processes
    - 13) Transparent disclosure of key information to stakeholders
    - 14) Comparison of governance processes with national codes or best practices
    - 15) Oversight of related party transactions and conflicts of interest

### 3. Governance Process and Roles

- a. Governance has two major components: strategic direction and oversight.
  - 1) Strategic direction determines
    - a) The business model,
    - b) Overall objectives,
    - c) The approach to risk taking (including the risk appetite), and
    - d) The limits of organizational conduct.
  - 2) Oversight is the governance component with which internal auditing is most concerned. It is also the component to which risk management and control activities are most likely to be applied. The elements of oversight are
    - a) Risk management activities performed by senior management and risk owners and
    - b) Internal and external assurance activities.
- b. The **board** is defined by The IIA as 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.
  - 1) 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" refers to a group or person charged with governance of the organization.
  - 2) Furthermore, "board" may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee). Thus, the board is the source of overall direction to, and the authority of, management. It also has the **ultimate responsibility for oversight**.
    - a) Another responsibility is to identify stakeholders, whether directly involved with the business (employees, customers, and suppliers), indirectly involved (investors), or having influence over the business (regulators and competitors).
    - b) The board must determine the expectations of stakeholders and the outcomes that are unacceptable.
    - c) The board has the following duties:
      - i) Selection and removal of officers
      - ii) Decisions about capital structure (mix of debt and equity, consideration to be received for shares, etc.)
      - iii) Adding, amending, or repealing bylaws (unless this authority is reserved to the shareholders)
      - iv) Initiation of fundamental changes (mergers, acquisitions, etc.)
      - v) Decisions to declare and distribute dividends
      - vi) Setting of management compensation (sometimes performed by a subcommittee called the compensation committee)
      - vii) Coordinating audit activities (most often performed by a subcommittee called the audit committee)
      - viii) Evaluating and managing risk (sometimes performed by a subcommittee called the risk committee)

- d) A **risk committee** may be created that
  - i) Identifies key risks,
  - ii) Connects them to risk management processes,
  - iii) Delegates them to risk owners, and
  - iv) Considers whether tolerance levels delegated to risk owners are consistent with the organization's risk appetite.
- c. **Management** performs day-to-day governance functions. Senior management carries out board directives (within specified tolerances for unacceptable outcomes) to achieve objectives.
  - 1) Senior management determines
    - a) Where specific risks are to be managed,
    - b) Who will be **risk owners** (managers responsible for specific day-to-day risks), and
    - c) How specific risks will be managed.
  - 2) Senior management establishes reporting requirements for risk owners related to their risk management activities.
  - 3) Governance expectations, including tolerance levels, must be periodically reevaluated by the board and senior management. The result may be changes in risk management activities.
- d. The **internal audit activity** is responsible for assessing and improving governance processes. (The internal audit activity's responsibilities are described in items 6.a.5) and 6.a.6), beginning on page 7, and in Subunit 3.2.)
- e. **Risk owners** are responsible for
  - 1) Evaluating the adequacy of the design of risk management activities and the organization's ability to carry them out as designed;
  - 2) Determining whether risk management activities are operating as designed;
  - 3) Establishing monitoring activities; and
  - 4) Ensuring that information to be reported to senior management and the board is accurate, timely, and available.

4. The chart below depicts a typical U.S. corporate governance structure. [In the U.S., the Securities and Exchange Commission (SEC) enforces the securities laws and the Public Company Accounting Oversight Board (PCAOB) regulates the auditors of public companies.]

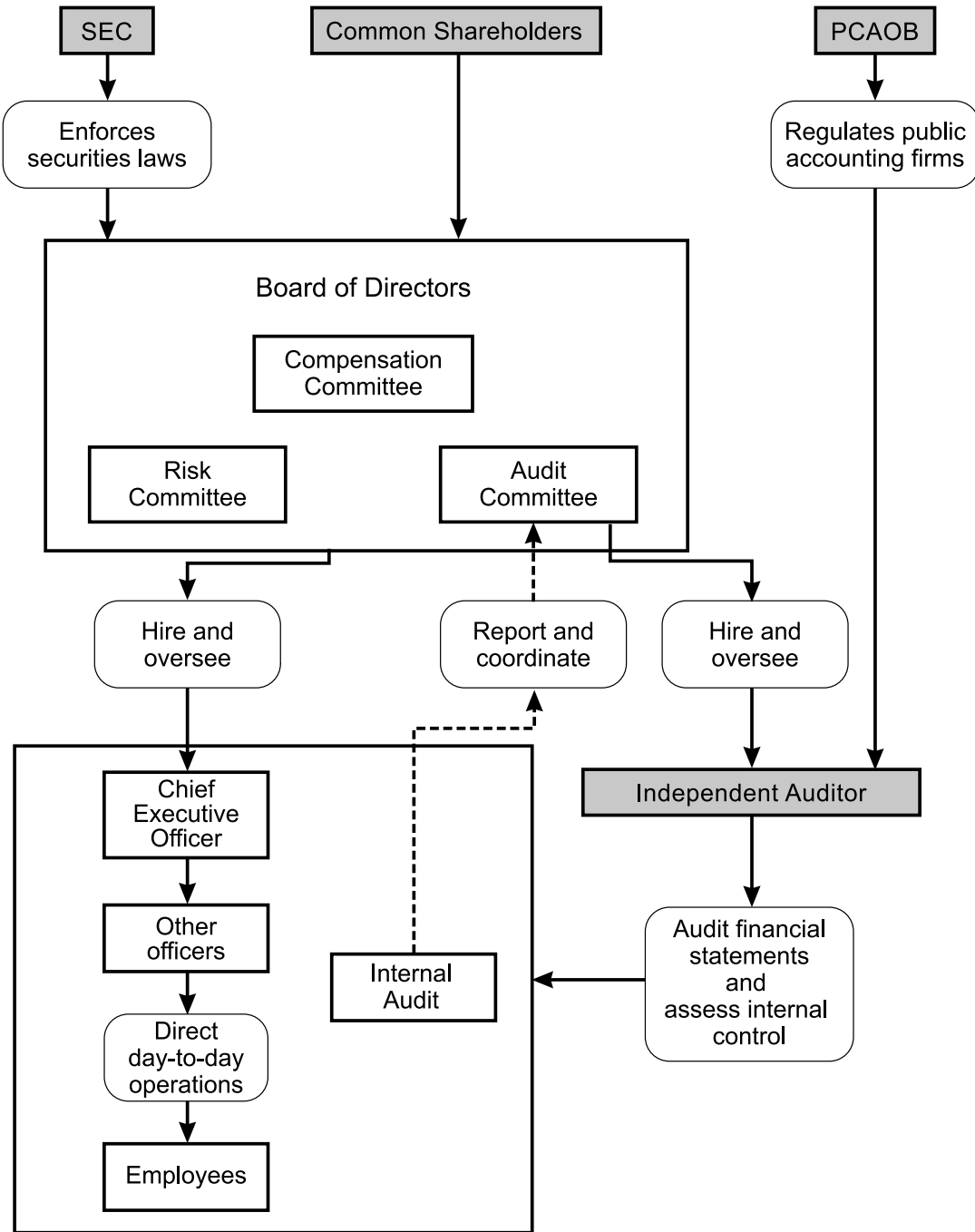


Figure 3-2

## 5. Governance Practices

- a. Governance applies to all organizational activities.
- b. Governance practices reflect the organization's unique culture and largely depend on it for effectiveness.
  - 1) According to the COSO Enterprise Risk Management framework, **culture** consists of the attitudes, behaviors, and understanding about risk, both positive and negative, that influence the decisions of management and personnel and reflect the mission, vision, and core values of the organization.
  - 2) Accordingly, organizational culture is reflected in
    - a) Setting values, objectives, and strategies;
    - b) Defining roles and behaviors;
    - c) Measuring performance;
    - d) Specifying accountability; and
    - e) Complying with corporate social responsibilities.
  - 3) Organizational culture affects the overall **control environment** and individual engagement risks and controls. (The control environment is defined in Appendix A.)
    - a) Organizational culture that is risk aggressive (risk averse) is more likely to regard the importance of control within the organization as low (high). Consequently, engagement risks are less (more) likely to be assessed as high.
  - 4) **Senior management** is primarily responsible for establishing and maintaining an organizational culture.
- c. Governance practices may use various legal forms, structures, strategies, and procedures. They ensure that the organization
  - 1) Complies with society's legal and regulatory rules;
  - 2) Satisfies the generally accepted business norms, ethical principles, and social expectations of society;
  - 3) Provides overall benefit to society and enhances the interests of the specific stakeholders in both the long and short term; and
  - 4) Reports fully and truthfully to its stakeholders, including the public, to ensure accountability for its decisions, actions, and performances.



## 6. Ethical Culture

- a. The ethical culture is an important component of the organizational culture and is crucial to the effectiveness of governance practices. Because decision making is complex and dispersed in most organizations, each person should be an ethics advocate, whether officially or informally.
  - 1) Codes of conduct and vision statements are issued to state
    - a) The organization's values and objectives;
    - b) The behavior expected; and
    - c) The strategies for maintaining a culture consistent with legal, ethical, and societal responsibilities.
  - 2) The **board** oversees the organization's ethical climate.
  - 3) **Senior management** has ultimate responsibility for promoting and setting the example of ethical behavior (i.e., setting the tone at the top).
    - a) Senior management is also responsible for establishing and maintaining sound ethics-related objectives and programs.
  - 4) Organizations may designate a chief ethics officer.
  - 5) **Internal auditors** may have an active role in support of the organization's ethical culture. Roles may include chief ethics officer, member of an ethics council, or assessor of the ethical climate.
    - a) In some circumstances, the role of chief ethics officer may conflict with the independence attribute of the internal audit activity.
      - i) The organizational independence of the internal audit activity is necessary because it performs internal assurance services.
      - ii) External assurance may be provided by external auditors, consultants, industry groups, or regulators.
    - b) The role of, and advice given by, the internal audit activity depend on the maturity of the governance system.
      - i) In a **less mature** system, the internal audit activity emphasizes compliance with policies, procedures, laws, etc. It also addresses the basic risks to the organization.
      - ii) In a **more mature** governance system, the internal audit activity's emphasis is on optimizing structure and practices.
    - c) The responsibility of the internal audit activity in an assurance engagement for ethics-related matters is described in the following standard:

### Implementation Standard 2110.A1

The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities.



- 6) The internal audit activity periodically assesses the elements of the ethical climate of the organization and its effectiveness in achieving legal and ethical compliance. Internal auditors therefore evaluate the effectiveness of the following:
- a) A formal code of conduct and related statements and policies (including procedures covering fraud and corruption)
  - b) Frequent demonstrations of ethical attitudes and behavior by influential leaders
  - c) Explicit strategies to support the ethical culture
  - d) Confidential reporting of alleged misconduct
  - e) Regular declarations by employees, suppliers, and customers about the requirements of ethical behavior
  - f) Clear delegation of responsibilities for providing counsel, investigation, and reporting
  - g) Easy access to learning opportunities
  - h) Personnel practices that encourage contributions by employees
  - i) Regular surveys of employees, suppliers, and customers to determine the state of the ethical climate
  - j) Regular reviews of the processes that undermine the ethical culture
  - k) Regular reference and background checks

### 3.2 ROLES OF INTERNAL AUDITORS IN GOVERNANCE

1. Governance is one of the three basic processes identified in the Definition of Internal Auditing.
  - a. The board and management are responsible for the design and implementation of governance processes.

#### Performance Standard 2110 Governance

The internal audit activity must assess and make appropriate recommendations to improve the organization's governance processes for:

- Making strategic and operational decisions.
- Overseeing risk management and control.
- Promoting appropriate ethics and values within the organization.
- Ensuring effective organizational performance management and accountability.
- Communicating risk and control information to appropriate areas of the organization.
- Coordinating the activities of, and communicating information among, the board, external and internal auditors, other assurance providers, and management.



#### Implementation Standard 2110.A2

The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.



- b. Understanding the role of the internal audit activity begins with understanding the nature of governance in a specific organization.
  - 1) Governance has a range of definitions depending on the circumstances.
    - a) The CAE should work with the board and senior management to determine how governance should be defined for audit purposes.
  - 2) Governance models generally treat governance as a process or system that is not static.
    - a) The approach in the *Standards* emphasizes the board and its governance activities.
  - 3) Governance requirements vary by entity type and regulatory jurisdiction. Examples include publicly traded companies, not-for-profits, governments, private companies, and stock exchanges.
  - 4) The design and practice of effective governance vary with
    - a) The size, complexity, and life-cycle maturity of the organization;
    - b) Its stakeholder structure; and
    - c) Legal and cultural requirements.

- c. The internal audit activity's **ultimate responsibility** is to evaluate and improve governance.
- 1) The unique position of internal auditors in the organization enables them to observe and formally assess governance processes while remaining independent.
  - 2) The definition of governance should be agreed upon with the board and senior management. The internal auditors should understand governance processes and the relationships among governance, risk, and control.
  - 3) Internal auditors assess the design and operating effectiveness of governance processes. They also provide advice on improving those processes.
    - a) Internal auditors may facilitate board self-assessments of governance.
  - 4) The audit plan should be based on an assessment of risks that considers governance processes and related controls. The plan should include the higher-risk governance processes.
    - a) Moreover, inclusion of an assessment of processes or risk areas should be considered if the board or senior management has requested that work be performed.
    - b) The plan should define
      - i) The nature of the work;
      - ii) The governance processes; and
      - iii) The nature of the assessments, e.g., consideration of specific risks, processes, or activities.
  - 5) The CAE should consider the following in planning assessments of governance:
    - a) An audit should address controls in governance processes that are designed to prevent or detect events that could have a negative effect on the organization.
    - b) Controls within governance processes often are significant in managing multiple risks. For example, controls related to the code of conduct may be relied upon to manage compliance and fraud risks.
    - c) If other audits assess controls in governance processes, the auditor should consider relying on their results.
  - 6) Assessments of governance are likely to be based on numerous audits. The internal auditor should consider
    - a) Audits of specific processes,
    - b) Governance issues arising from audits not focused on governance,
    - c) The results of other assurance providers' work, and
    - d) Such other information as adverse incidents indicating an opportunity to improve governance.

- 7) When control issues are known or the governance process is not mature, the CAE may consider different methods for improving control or governance through consulting services.
  - 8) During the planning, evaluating, and reporting phases, the internal auditor should be sensitive to the consequences of the results and ensure appropriate communications with the board and senior management.
    - a) The internal auditor should consider consulting legal counsel both before the audit and before issuing the final report.
- d. Other roles of internal auditors in governance include the following:
- 1) Obtain the board's approval of the internal audit charter.
  - 2) Communicate the plan of engagements.
  - 3) Report significant audit issues.
  - 4) Communicate key performance indicators to the board on a regular basis.
  - 5) Discuss areas of significant risk.
  - 6) Support the board in enterprise-wide risk assessment.
  - 7) Review the positioning of the internal audit activity within the risk management framework within the organization.
  - 8) Monitor compliance with the corporate code of conduct/business practices.
  - 9) Report on the effectiveness of the control framework.
  - 10) Assess the ethical climate of the board and the organization.
  - 11) Conduct a follow-up and report on management's response to regulatory body reviews.
  - 12) Conduct a follow-up and report on management's response to external audit.
  - 13) Assess the adequacy of the performance measurement system and achievement of organizational objectives.
  - 14) Support a culture of fraud awareness and encourage the reporting of improprieties.

### 3.3 CORPORATE SOCIAL RESPONSIBILITY (CSR)



#### SUCCESS TIP

CSR is a frequently tested governance topic. Mastery of this topic will increase your success on the exam.

#### 1. Characteristics of CSR

- a. Stakeholders increasingly expect organizations to accept responsibility and implement strategies and controls that (1) manage their effects on the environment and society, (2) engage stakeholders in their efforts, and (3) report results to the public.
- b. CSR is a response to stakeholder expectations.
  - 1) CSR refers to (a) social responsibility, (b) sustainable development, and (c) corporate citizenship.
  - 2) The International Organization for Standardization (ISO) has issued guidance on social responsibility in its ISO 26000. CSR is defined, in part, as “the willingness of an organization to incorporate social and environmental considerations in its decision making and be accountable for the impacts of its decisions and activities on society and the environment.”
  - 3) Similarly, an IIA Practice Guide defines CSR as “the way firms integrate social, environmental, and economic concerns into their values, culture, decision-making, strategy and operations in a transparent and accountable manner and thereby establish better practices within the firm, create wealth, and improve society.”
- c. Business ethics scholar Archie B. Carroll has identified four responsibilities that an organization must fulfill to be called socially responsible:
  - 1) Economic responsibility to be profitable, or to do what is required by capitalism
  - 2) Legal responsibility to obey the law, or to do what is required by stakeholders
  - 3) Ethical responsibility to be ethical in its practices, given local and global standards, or to do what is expected by stakeholders
  - 4) Philanthropic responsibility to be a good corporate citizen, or to do what is desired by stakeholders
- d. Despite increasing pressure from stakeholders for organizations to be more socially and environmentally responsible, CSR is largely a **voluntary** practice.
  - 1) In most jurisdictions, public companies are not required to disclose their CSR performance.
  - 2) Furthermore, organizations exercise significant discretion in deciding what to disclose about their CSR performance.

#### 2. CSR Frameworks

- a. Two major frameworks exist that provide guidance on CSR implementation.
  - 1) The Global Reporting Initiative (GRI) has developed a sustainability **reporting** framework that provides specific guidance on measuring CSR performance against predefined criteria.
  - 2) While GRI guidance emphasizes reporting, ISO 26000 emphasizes how to **implement and manage a CSR initiative**.

- b. ISO 14000 standards are a set of criteria for certification of an environmental management system.
  - 1) According to ISO, the benefits of using ISO 14000 can include the following:
    - a) Reduced cost of waste management
    - b) Savings in consumption of energy and materials
    - c) Lower distribution costs
    - d) Improved corporate image among regulators, customers, and the public

### 3. Responsibility for CSR

- a. The board is responsible for overseeing CSR and the effectiveness of governance, risk management, and internal control processes related to CSR.
- b. Management is responsible for establishing CSR objectives, assessing and managing risks, measuring performance, and monitoring and reporting activities.
- c. The internal auditor is responsible for evaluating whether controls over CSR are adequate to achieve CSR objectives.
- d. All employees are responsible for the success of CSR initiatives.

### 4. CSR Strategies

- a. The following are four alternative strategies:
  - 1) Reaction. The organization denies responsibility and tries to maintain the status quo.
  - 2) Defense. The organization uses legal action or public relations efforts to avoid additional responsibilities.
  - 3) Accommodation. The organization assumes additional responsibilities only when pressured.
  - 4) Proaction. The organization takes the initiative in implementing a CSR program that serves as an example for the industry.

### 5. Risks

- a. The risks of failing to implement an effective CSR program include the following, among others:
  - 1) Loss of reputation. The organization's brand or reputation could be damaged.
  - 2) Noncompliance. The organization may fail to comply with regulations or contractual obligations.
  - 3) Lawsuits. The organization may be held liable for alleged harms.
  - 4) Operational failures. Operational pressure points (e.g., environmental effects of processes or products) may indicate risks. Risks also result from, for example, not achieving CSR objectives because of inappropriate CSR strategies or over-emphasis on CSR strategies.
  - 5) Stock market. The organization may lose investors.
  - 6) Employment market. Employees may leave the organization, or attracting new employees may be difficult.
  - 7) Sales decline. Customers may boycott services or products.

## 6. CSR Business Activities

- a. CSR business activities generally include the following:
  - 1) Establishing and communicating policies and procedures
  - 2) Setting objectives, performance goals, and strategies
  - 3) Communicating and integrating CSR principles and controls into the business decision-making processes
  - 4) Monitoring, evaluating results, and benchmarking
  - 5) Engaging stakeholders (e.g., through satisfaction surveys, focus groups, and complaint management processes)
  - 6) Auditing (e.g., public disclosures, internal controls, and contractual compliance with CSR terms and conditions)
  - 7) External and internal reporting of results

## 7. Evaluating and Auditing CSR

- a. The internal audit activity must maintain its independence and objectivity while performing CSR audits.
  - 1) The internal audit activity's independence and objectivity is not impaired if it
    - a) Provides advice on the design and implementation of CSR programs or
    - b) Facilitates a management self-assessment of CSR controls and results.
- b. Any internal audit activity that collectively lacks the appropriate skill and knowledge should not perform CSR audits.
- c. The chief audit executive (CAE) considers CSR risks, and the internal audit activity evaluates whether the organization has adequate controls to achieve its CSR objectives.
  - 1) Evaluation criteria may include compliance with internal control frameworks (e.g., COSO), quality frameworks (e.g., ISO), or contractual obligations.
- d. **CSR Maturity Model**
  - 1) The CAE compares the organization's CSR maturity level [using a 5-level maturity scale (level 1 is "initial" and level 5 is "optimizing")] at the time of the internal audit with the level the organization desires to achieve.
- e. Two common approaches to auditing CSR are auditing by element and by stakeholder group.
  - 1) **Element.** Separate audits of each element are performed. The following are typical CSR elements with example audit questions:
    - a) Governance (Do board members have sufficient and relevant information to fulfill their roles and responsibilities?)
    - b) Community investment (What philanthropic practices are in place, and how are decisions made?)
    - c) Environment (Are social and environmental impact assessments performed?)
    - d) Ethics (Is an anti-corruption culture included in the organization's risk assessment, code of conduct, and policies?)



- e) Health, safety, and security (Are incidents reported, communicated, managed, and resolved appropriately?)
  - f) Transparency (Does the organization follow appropriate accounting standards?)
  - g) Working conditions and human rights (Is compensation based on fair pay, living wages, and job opportunities?)
- 2) **Stakeholder group.** Separate audits of CSR programs related to each significant stakeholder group are performed that consider compliance with laws, regulations, and contracts. The following are typical stakeholder groups with example audit questions:
- a) Customers (Does the organization have product safety and recall processes?)
  - b) Employees and their families (Does the organization prohibit discrimination and harassment?)
  - c) Environment (Are social and environmental impact assessments performed?)
  - d) Neighboring communities (Does the organization give to local economic support programs?)
  - e) Shareholders (Does the organization abide by shareholder rights?)
  - f) Suppliers (Are rates and payment terms fair?)

## 8. Reporting CSR

- a. Every organization must make a business decision about (1) the **cost or benefit** of producing a CSR report and (2) what information to include in the report.
- b. Many organizations use **verification and assurance processes** for all or parts of the report to increase accountability and reduce the likelihood that the report will appear to be a marketing tool.
- c. Reporting methods include the following:
  - 1) Providing a standalone CSR report
  - 2) Integrating the CSR report with the annual financial report
  - 3) Providing CSR information booklets on special topics
- d. Distribution formats include the following:
  - 1) Web pages
  - 2) Booklets
  - 3) Press releases
  - 4) Regulatory filings

# STUDY UNIT FOUR

## RISK MANAGEMENT

4.1	<i>Risk Management Processes</i> .....	2
4.2	<i>COSO Framework -- Enterprise Risk Management (ERM) Overview</i> .....	11
4.3	<i>COSO Framework -- ERM Components and Limitations</i> .....	14
4.4	<i>ISO 31000 Risk Management Framework</i> .....	25

This study unit is the second of four covering **Domain V: Governance, Risk Management, and Control** from The IIA's CIA Exam Syllabus. This domain makes up 35% of Part 1 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 MANAGEMENT PROCESSES

1. **Risk** is “[t]he possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood” (The IIA Glossary).
  - a. Risk management is “a process to identify, assess, manage, and control potential events or situations to provide **reasonable assurance** regarding the achievement of the organization’s objectives” (The IIA Glossary).
    - 1) It is one of the three processes specifically addressed in the Definition of Internal Auditing.



### Performance Standard 2120 Risk Management

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

## 2. The Risk Management Process

- a. Risk management processes include (1) identification of context, (2) risk identification, (3) risk assessment and prioritization (i.e., risk analysis), (4) risk response, and (5) risk monitoring.
  - 1) Management must focus on risks at all levels of the entity and take the necessary action to manage them.
  - 2) All risks that could affect achievement of objectives must be considered.
- b. Step 1 – Identification of context
  - 1) A precondition to risk identification is identifying the significant contexts within which risks should be managed.
  - 2) Contexts include the following:
    - a) Laws and regulations
    - b) Capital projects
    - c) Business processes
    - d) Technology
    - e) Market risk (e.g., interest rates, foreign exchange rates, equity investments)
    - f) Organizations

## c. Step 2 – Risk identification

- 1) Risk identification should be performed at every level of the entity (entity-level, division, business unit) relevant to the identified context(s).
  - a) Examples of external risk factors at the entity level include technological changes and changes in customer wants and expectations.
  - b) Examples of internal risk factors at the entity level include
    - i) Interruptions in automated systems,
    - ii) The quality of personnel hired, and
    - iii) The level of training provided.
- 2) Some occurrences may be inconsequential at the entity level but disastrous for an individual unit.
- 3) Risk identification should consider past events (trends) and future possibilities. Methods used include the following:
  - a) **Event inventories.** Certain events are common to particular industries. Software is available that provides lists that can be used as a starting point for event identification.
  - b) **Questionnaires and surveys.** Responses can be evaluated to identify potential events.
  - c) **Leading event indicators and escalation triggers.** Leading event indicators are measures that provide insight into potential events. An escalation trigger, also known as a threshold trigger, is a condition that a leading event indicator must satisfy before the potential event is escalated to management. For example,
    - i) Potential event: Manufacturing equipment breakdown, resulting in decreases in production
    - ii) Leading event indicator: Maintenance requests
    - iii) Escalation trigger: Two maintenance requests outside of regularly scheduled maintenance within a 3-month period
  - d) **Facilitated workshops and interviews.** A facilitator leads a discussion group consisting of management, staff, or other stakeholders through a structured process of conversation and exploration about potential events.
  - e) **Process flow analysis.** A single business process, such as vendor authorization and payment, is studied in isolation to identify the events that affect its inputs, tasks, responsibilities, and outputs.
  - f) **Loss event data methodologies.** The losses associated with adverse events in the past can be used to make predictions. An example is matching workers' compensation claims with the frequency of accidents.
- 4) Other methods for identifying risks are
  - a) Brainstorming,
  - b) SWOT (strengths, weaknesses, opportunities, and threats) analysis, and
  - c) Scenario analysis (what-if analysis).

d. Step 3 – Risk assessment and prioritization

- 1) The risk assessment process may be formal or informal. It involves (a) assessing the significance of an event, (b) assessing the event’s likelihood, and (c) considering the means of managing the risk.
- 2) The results of assessing the likelihood and impact of the risk events identified are used to prioritize risks and produce decision-making information.
- 3) Risk assessment methods may be qualitative or quantitative.
  - a) Qualitative methods include (1) lists of all risks, (2) risk rankings, and (3) risk maps.
    - i) Heat maps present risk levels by color. Risks that have the same likelihood (e.g., remote, unlikely, possible, likely, or certain) and impact (e.g., negligible, low, medium, high, or extreme), or that fall in the same range of severity (i.e., combined assessment of likelihood and impact), are assigned the same color. (An illustration is provided in Figure 4-2 in Subunit 4.3.)
    - ii) Matrix risk maps plot risks on a chart with a likelihood on one axis and an impact on the other axis. (An illustration is provided in Example 4-1.)
  - b) Quantitative methods include probabilistic models. For example, some organizations focus on earnings at risk by examining how variables influence earnings.
- 4) **Risk modeling** is a method of risk assessment and prioritization.
  - a) Risk modeling ranks and validates risk priorities when setting the priorities of engagements in the audit plan.
  - b) Risk factors may be weighted based on professional judgments to determine their relative significance, but the weights need not be quantified.
  - c) This simple model and the resulting risk assessment process can be depicted as in Example 4-1 below.

**EXAMPLE 4-1 Risk Modeling**

A chief audit executive is reviewing the following enterprise-wide **risk map**:

<b>I M P A C T</b>		<b>LIKELIHOOD</b>		
		<b>Remote</b>	<b>Possible</b>	<b>Likely</b>
	<b>Critical</b>	Risk A	Risk B	
	<b>Major</b>			Risk D
	<b>Minor</b>		Risk C	

To establish priorities for the use of limited internal audit resources, the CAE makes the following analysis:

- Risk D clearly takes precedence over Risk C because D has both a higher likelihood and a greater impact.
- Risk B also clearly has a higher priority than Risk A because B has a higher likelihood and the same impact.

Choosing the higher priority between Risk D and Risk B 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 D 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 B.

- d) Open channels of communication with senior management and the board are necessary to ensure the audit plan is based on the appropriate risk assessments and audit priorities. The audit plan should be reevaluated as needed.
- e) Risk modeling in a consulting service is done by ranking the engagement's potential to (1) improve management of risks, (2) add value, and (3) improve the organization's operations.
  - i) Senior management assigns a weight to each item based on organizational objectives.
  - ii) The engagements with the appropriate weighted values are included in the annual audit plan.
- e. Step 4 – Risk response
  - 1) Risk responses are the means by which an organization elects to manage individual risks.
    - a) Each organization selects risk responses that align risks with the organization's risk appetite (the level of risk the organization is willing to accept).
    - b) Strategies for risk response are covered in Subunit 4.3.
  - 2) **Controls** are actions taken by management to manage risk and ensure risk responses are carried out.
    - a) **Control risk** is the risk that controls fail to effectively manage controllable risks.
  - 3) **Residual risk** is the risk that remains after risk responses are executed.
  - 4) In large or complex entities, senior management may appoint a **risk committee** to (a) review the risks identified by the various operating units and (b) create a response plan.
    - a) All personnel must be aware of the importance of the risk response appropriate to their levels of the entity.
- f. Step 5 – Risk monitoring
  - 1) Risk monitoring (a) tracks identified risks, (b) evaluates current risk response plans, (c) monitors residual risks, and (d) identifies new risks.
  - 2) The two most important sources of information for ongoing assessments of the adequacy of risk responses (and the changing nature of the risks) are
    - a) Those closest to the activities. The manager of an operating unit is in the best position to monitor the effects of the chosen risk response strategies.
    - b) The audit function. Operating managers may not always be objective about the risks facing their units, especially if they helped design a particular response strategy. Analyzing risks and responses are among the normal responsibilities of internal auditors.

### 3. Responsibility for Aspects of Organizational Risk Management

- a. Risk management is a key responsibility of senior management and the board.
  - 1) **Boards** have an oversight function. They determine that risk management processes are in place, adequate, and effective.
  - 2) **Management** ensures that sound risk management processes are functioning.
  - 3) The **internal audit activity** may be directed to examine, evaluate, report, or recommend improvements.
    - a) It also has a consulting role in identifying, evaluating, and implementing risk management methods and controls.
- b. Senior management and the board determine the internal audit activity's role in risk management based on factors such as (1) organizational culture, (2) abilities of the internal audit activity staff, and (3) local conditions and customs.
  - 1) That role may range from no role; to auditing the process as part of the audit plan; to active, continuous support and involvement in the process; to managing and coordinating the process.
    - a) But assuming management responsibilities and the threat to internal audit activity independence must be fully discussed and board-approved.
- c. The CAE must understand management's and the board's expectations of the internal audit activity in risk management. The understanding is codified in the charters of the internal audit activity and the board.
  - 1) If the organization has no formal risk management processes, the CAE has formal discussions with management and the board about their obligations for understanding, managing, and monitoring risks.
- d. Risk management processes may be formal or informal, quantitative or subjective, or embedded in business units or centralized. They are designed to fit the organization's culture, management style, and objectives. For example, a small entity may use an informal risk committee.
  - 1) The internal audit activity determines that the methods chosen are comprehensive and appropriate for the organization.

#### 4. Internal Audit's Role in Risk Management

- a. The IIA issued the following Interpretation to clarify internal audit's role:

##### 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; and
- 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.

- b. Two Implementation Standards link the assessment of risk to specific risk areas.

##### 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; and
- 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.



- c. In accordance with IG 2120, *Risk Management*, the CAE and internal auditors should
- 1) Obtain a clear **understanding** of the organization's
    - a) Risk appetite.
    - b) Business missions and objectives.
    - c) Business strategies.
    - d) Risks identified by management.
      - i) Risks may be financial, operational, legal or regulatory, or strategic.
    - e) Current risk management environment and prior corrective actions.
    - f) Means of identifying, assessing, and overseeing risks.
  - 2) Consider risk management frameworks and models and IG 2100, *Nature of Work*.
  - 3) Consider the characteristics of the organization. Examples are size, life cycle, maturity, stakeholders, environment, and changes in that environment (e.g., new management or products).
  - 4) Review the maturity of the organization's risk management process and determine the reliance on management's risk assessment.
    - a) The IIA's Practice Guide, *Assessing the Risk Management Process*, contains a risk management maturity model for measuring an organization's risk management maturity.
      - i) The **risk management maturity model** consists of the following maturity levels, presented in order of maturity: (a) initial, (b) repeatable, (c) defined, (d) managed, and (e) optimized.
      - ii) The maturity level of risk management can be measured using various elements, including risk culture, risk governance, and risk management process. Elements may have different maturity levels. For example, an organization's risk culture may be at the defined maturity level, but risk governance and risk management process may be at the repeatable maturity level.
      - iii) The common characteristics of a **mature** risk management (i.e., at the optimized maturity level) can be described as follows:

<b>Risk culture</b>
Risk is considered and built into decision-making, objective-setting, and compensation structure.
<b>Risk governance</b>
Across the organization, personnel who are competent and skilled participate in the risk management process.
<b>Risk management process</b>
Assessment, treatment, monitoring, and reporting of risk are aggregated across the organization.

- iv) Not every organization must reach the highest maturity level. Operating below the optimized maturity level may be acceptable. Each organization should decide its own optimal maturity level according to its unique needs and circumstances.
    - 5) Have an established process for planning, auditing, and reporting risk management issues.
  - d. Implementing Standard 2120
    - 1) The CAE should speak with the board and senior management about risk appetite, risk tolerance, and risk management.
      - a) After reviewing the strategic plan, business plan, and policies, the CAE may determine whether strategic objectives align with the mission, vision, and risk appetite. Mid-level managers may give insight into alignment at the business-unit level.
    - 2) The internal audit activity
      - a) Alerts management to new risks or inadequately mitigated risks
      - b) Provides recommendations and action plans for risk responses
      - c) Evaluates risk management processes
    - 3) Internal auditors review risk assessments by senior management, external auditors, and regulators. The purpose is to learn how the organization identifies, addresses, and determines the acceptability of risks.
      - a) The responsibilities and risk processes of the board and key managers also are evaluated.
    - 4) The internal audit actively performs its own risk assessments.
      - a) The discussions with the board and management permit alignment of recommended risk responses with the risk appetite.
      - b) An established framework (e.g., COSO or ISO 31000) may be used for risk identification.
      - c) (1) New developments in the industry and (2) processes for monitoring, assessing, and responding to risks (or opportunities) may be researched.
    - 5) The foregoing procedures allow internal auditors to perform gap analyses (whether risks are identified and assessed adequately).
    - 6) Internal auditors should identify risks and corresponding responses. “For example, management may choose to accept risk, and the CAE would need to determine whether the decision is appropriate, according to the organization’s risk appetite or risk management strategy. If the CAE concludes that management has accepted a level of risk that may be unacceptable . . . , the CAE must discuss the matter with senior management and may need to communicate the matter to the board.”
    - 7) If management uses a risk mitigation strategy, “the internal audit activity may evaluate the adequacy and timeliness of remedial actions” by “reviewing the control designs and testing the controls and monitoring procedures.”

- 8) “To assess whether relevant risk information is captured and communicated timely across the organization, internal auditors may interview staff at various levels and determine whether the organization’s objectives, significant risks, and risk appetite are . . . understood throughout the organization. Typically, the internal audit activity also evaluates the adequacy and timeliness of . . . risk management results. The internal audit activity may review board minutes to determine whether the most significant risks are communicated timely to the board and whether the board is acting to ensure that management is responding appropriately.”
- 9) The internal audit activity also should
  - a) Ensure management of its risks (e.g., audit failure, false assurance, and damage to reputation) and
  - b) Monitor all corrective actions.
- e. Conformance with Standard 2120
  - 1) The internal audit charter and audit plan are relevant documents.
  - 2) Also relevant are minutes of meetings in which the elements of the standard (e.g., recommendations by the internal auditors) were discussed with the board, senior management, task forces, and committees.
  - 3) Internal audit risk assessments and action plans demonstrate evaluation and improvement.
- f. Three Implementation Standards address the risk management responsibilities of internal auditors when performing consulting engagements.



**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.

## 4.2 COSO FRAMEWORK -- ENTERPRISE RISK MANAGEMENT (ERM) OVERVIEW

### 1. COSO Risk Management Framework

- a. *Enterprise Risk Management – Integrating with Strategy and Performance* (COSO ERM framework) is a framework that complements, and incorporates some concepts of, the COSO internal control framework.
- b. The COSO ERM framework provides a basis for coordinating and integrating all of an organization's risk management activities. Effective integration
  - 1) Improves **decision making** and
  - 2) Enhances **performance**.
- c. Effective enterprise risk management can
  - 1) Increase the range of opportunities
  - 2) Identify and manage risk entity wide
  - 3) Increase positive outcomes
  - 4) Reduce performance variability
  - 5) Improve resource deployment
  - 6) Enhance enterprise resilience

### 2. ERM Definition and Concepts

- a. ERM is based on the premise that every organization exists to provide **value** for its stakeholders. Accordingly, ERM is defined as

*The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to **manage risk** in creating, preserving, and realizing **value**.*

- b. Key Concepts and Phrases
  - 1) **Culture** consists of “[t]he attitudes, behaviors, and understanding **about risk**, both positive and negative, that influence the decisions of management and personnel and reflect the mission, vision, and core values of the organization.”
    - a) **Mission** is the organization's core purpose.
    - b) **Vision** is the organization's aspirations for what it intends to achieve over time.
    - c) **Core values** are the organization's essential beliefs about what is acceptable or unacceptable.
  - 2) **Capabilities** are the skills needed to carry out the entity's mission and vision.
  - 3) **Practices** are the collective methods used to manage risk.
  - 4) **Integrating strategy setting and performance**.
    - a) Risk must be considered in setting strategy, business objectives, performance targets, and tolerance.
      - i) **Strategy** communicates how the organization will (a) achieve its mission and vision and (b) apply its core values. ERM enhances strategy selection.
      - ii) **Business objectives** are the steps taken to achieve the strategy.
      - iii) **Tolerance** is the range of acceptable variation in performance results. (This term is identical to “risk tolerance” in the COSO internal control framework.)

- b) The organization considers the effect of strategy on its risk profile and portfolio view.

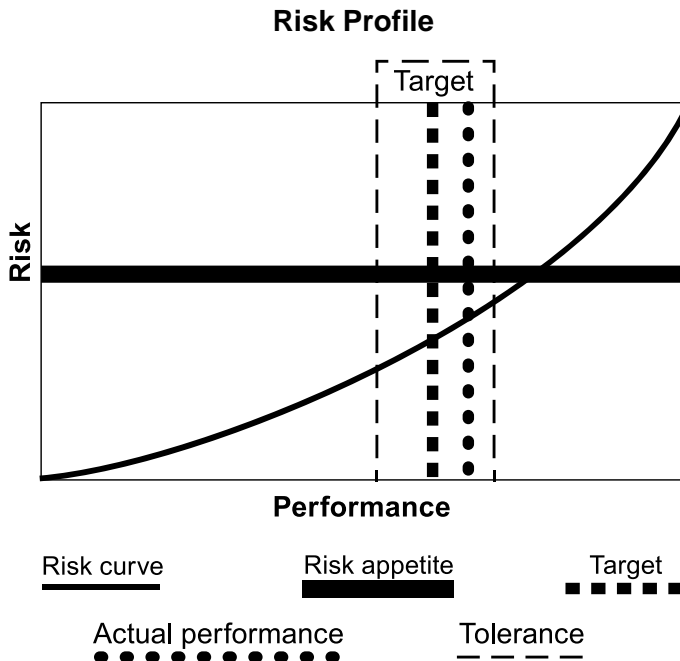


Figure 4-1

- i) **Risk profile** is a composite view of the types, severity, and interdependencies of **risks** related to a specific strategy or business objective and their effect on **performance**.
- A risk profile may be created at any level (e.g., entity, division, operating unit, or function) or aspect (e.g., product, service, or geography) of the organization.
- ii) **Portfolio view** is similar to a risk profile.
- The difference is that it is a composite view of the risks related to **entity-wide** strategy and business objectives and their effects on **entity** performance.

5) **Managing risk.**

- a) **Risk** is “[t]he possibility that events will occur and affect the achievement of strategy and business objectives.”
- b) **Opportunity** is any action or potential action that creates or alters goals or approaches for the creation, preservation, or realization of value.
- c) **Reasonable expectation** (not absolute assurance) that the risk assumed is appropriate is provided by effective ERM practices.
- d) **Risk inventory** consists of all identified risks that affect strategy and business objectives.
- e) **Risk capacity** is the maximum amount of risk the organization can assume.
- f) **Risk appetite** consists of the amount and types of risk the organization is willing to accept in pursuit of value.
- g) **Actual residual risk** is the risk remaining after taking management actions to alter its severity. Actual residual risk should be equal to or less than target residual risk.
- h) **Inherent risk** is the risk in the absence of management actions to alter its severity.
- i) Actual residual risk remains after management actions to alter its severity.
- i) **Risk response** is an action taken to bring identified risks within the organization’s risk appetite.
- i) A **residual risk profile** includes risk responses.
- j) **Target residual risk** is the risk the entity prefers to assume knowing that management has acted or will act to alter its severity.

6) **Value** is

- a) **Created** when the benefits obtained from the resources used exceed their costs.
- b) **Preserved** when the value of resources used is sustained.
- c) **Realized** when benefits are transferred to stakeholders.
- d) **Eroded** when management's strategy does not produce expected results or management does not perform day-to-day tasks.

3. **ERM Roles and Responsibilities**

- a. The **board** provides risk oversight of ERM culture, capabilities, and practices. ERM can enhance enterprise resilience (the ability to anticipate and respond to change), and it provides a framework for boards to assess risk and embrace a mindset of resilience. Certain board committees may be formed for this purpose. Examples are
  - 1) An **audit** committee (often required by regulators),
  - 2) A **risk** committee that directly oversees ERM,
  - 3) An **executive compensation** committee, and
  - 4) A **nomination or governance** committee that oversees selection of directors and executives.
- b. **Management** has **overall responsibility** for ERM and is generally responsible for the **day-to-day** managing of risk, including the implementation and development of the COSO ERM framework.
  - 1) Within management, the **CEO** has **ultimate responsibility** for ERM and achievement of strategy and business objectives.
- c. An organization may designate a **risk officer** as a centralized coordinating point to facilitate risk management across the entire enterprise. This risk officer is commonly referred to as a centralized coordinator.
- d. **Three Lines Model**
  - 1) **The first line** consists of the principal owners of risk. They manage performance and risks taken to achieve strategy and objectives.
  - 2) **The second line** consists of the supporting (business-enabling) functions, e.g., a risk officer or centralized coordinator. This level of management provides guidance on performance and ERM requirements, evaluates adherence to standards, and challenges the first line to take prudent risks.
  - 3) **The third line** is the assurance function: internal auditing. The internal auditor audits (or reviews) ERM, identifies issues and improvements, and informs the board and executives of matters needing resolution.

### 4.3 COSO FRAMEWORK -- ERM COMPONENTS AND LIMITATIONS

#### 1. ERM Components

- a. The COSO ERM framework consists of **five interrelated components**. Twenty principles are distributed among the components.
  - 1) The **supporting aspect** components are
    - a) Governance and culture and
    - b) Information, communication, and reporting.
  - 2) The **common process** components are
    - a) Strategy and objective-setting,
    - b) Performance, and
    - c) Review and revision.

#### 2. Governance and Culture

- a. Governance sets the organization's tone and establishes responsibilities for ERM. Culture relates to the desired behaviors, values, and overall understanding about risk held by personnel within the organization. **Five principles** relate to governance and culture.
  - 1) The **board** exercises **risk oversight**.
    - a) The full board ordinarily is responsible for risk oversight. However, the board may delegate risk oversight to a board committee, such as a **risk committee**.
      - i) **Management** generally has day-to-day responsibility for managing performance and risks taken to achieve strategy and business objectives.
    - b) The board's oversight role may include, but is not limited to,
      - i) Reviewing and challenging decisions related to strategy, risk appetite, and significant business decisions (e.g., mergers and acquisitions).
      - ii) Approving management compensation.
      - iii) Participating in stakeholder relations.
    - c) Risk oversight is most effective when the board
      - i) Has the necessary **skills, experience, and business knowledge** to (a) understand the organization's strategy and industry and (b) maintain this understanding as the business context changes.
      - ii) Is **independent** of the organization.
      - iii) Determines whether ERM capabilities and practices enhance value.
      - iv) Understands the **organizational biases** (e.g., a tendency for excessive risk avoidance or risk taking) influencing decision making and challenges management to minimize them.

- 2) The organization establishes **operating structures**.
  - a) They describe how the entity is organized and carries out its day-to-day operations.
  - b) They generally are aligned with the entity's legal structure and management structure.
    - i) The **legal structure** determines how the entity operates (e.g., as a single legal entity or as multiple, distinct legal entities).
    - ii) The **management structure** establishes reporting lines (e.g., direct reporting versus secondary reporting), roles, and responsibilities. Management is responsible for clearly defining roles and responsibilities.
  - c) Factors to consider when establishing and evaluating operating structures include the entity's
    - i) Strategy and business objectives, including related risks.
    - ii) Nature, size, and geographic distribution.
    - iii) Assignment of authority, accountability, and responsibility at all levels.
    - iv) Types of reporting lines and communication channels.
    - v) Reporting requirements (e.g., financial, tax, regulatory, and contractual).
- 3) The organization defines the desired **culture**.
  - a) The board and management are responsible for defining culture.
  - b) Culture is shaped by internal and external factors.
    - i) **Internal** factors include (a) the level of judgment and autonomy allowed to personnel, (b) standards and rules, and (c) the reward system in place.
    - ii) **External** factors include (a) legal requirements and (b) expectations of stakeholders (e.g., customers and investors).
  - c) The organization's definition of culture determines its placement on the **culture spectrum**, which ranges from risk averse to risk aggressive.
  - d) Judgment has a significant role in defining the desired culture and management of risk. Judgment is a function of personal experiences, risk appetite, capabilities and the level of information available, and organizational bias.
  - e) Culture is not static and will change over time.
- 4) The organization demonstrates commitment to **core values**.
  - a) The organization's core values should be reflected in all its actions and decisions.
  - b) The **tone of the organization** is the manner in which core values are communicated across the organization.
  - c) When risk-aware culture and tone are aligned, stakeholders have confidence that the organization is abiding by its core values.
  - d) Leadership helps establish and enforce accountability and a common purpose.



- 5) The organization **attracts, develops, and retains** capable individuals.
  - a) Management is responsible for defining the human capital necessary (the needed competencies) to achieve strategy and business objectives.
  - b) The **human resources function** assists management in developing competency requirements through processes that attract, train, mentor, evaluate, reward, and retain competent individuals.
  - c) **Contingency plans** should be developed to prepare for succession. Such plans train selected personnel to assume responsibilities vital to ERM. An example is training a risk manager to assume the position of risk officer.

### 3. Strategy and Objective Setting

- a. Strategy must support the organization's mission, vision, and core values. The integration of ERM with strategy setting helps to understand the risk profile related to strategy and business objectives. **Four principles** relate to strategy and objective setting.
  - 1) The organization analyzes **business context** and its effect on the risk profile.
    - a) Business context pertains to the relationships, events, trends, and other factors that influence the organization's strategy and business objectives. Accordingly, business context includes the organization's internal and external environments.
      - i) The **internal environment** consists of factors related to four categories: (a) capital (e.g., assets), (b) people (e.g., skills and attitudes), (c) processes (e.g., tasks, policies, and procedures), and (d) technology (e.g., adopted technology).
      - ii) The **external environment** consists of factors related to the following six categories: (a) political (government intervention and influence), (b) economic (e.g., interest rates and availability of credit), (c) social (e.g., consumer preferences and demographics), (d) technological (e.g., R&D activity), (e) legal (laws, regulations, and industry standards), and (f) environmental (e.g., climate change).
    - b) Business context may be
      - i) **Dynamic.** New, emerging, and changing risks can appear at any time (e.g., low barriers of entry allow new competitors to emerge).
      - ii) **Complex.** A context may have many interdependencies and interconnections (e.g., a transnational company has several operating units around the world, each with unique external environmental factors).
      - iii) **Unpredictable.** Change occurs rapidly and in unanticipated ways (e.g., currency fluctuations).
  - c) The effect of business context on the risk profile may be analyzed based on past, present, and future performance.

- 2) The organization defines **risk appetite** (the amount of risk it is willing to accept in pursuit of value).
  - a) The organization considers its mission, vision, culture, prior strategies, and risk capacity (the maximum risk it can assume) to set its risk appetite.
  - b) In setting risk appetite, the optimal balance of opportunity and risk is sought.
    - i) Risk appetite is rarely set above risk capacity.
  - c) Risk appetite may be expressed **qualitatively** (e.g., low, moderate, high) or **quantitatively** (e.g., as a percentage of a financial amount). But it should reflect how risk assessment results are expressed.
  - d) Entities may express risk appetite in terms of targets, ranges, ceilings, or floors.
  - e) The board approves the risk appetite, and management communicates it throughout the organization.
- 3) The organization evaluates **alternative strategies** and their effects on the risk profile.
  - a) Approaches to evaluating strategy include SWOT (Strengths-Weaknesses-Opportunities-Threats) analysis, competitor analysis, and scenario analysis.
  - b) The organization must evaluate
    - i) The strategy's alignment with its mission, vision, core values, and risk appetite and
    - ii) The implications of the chosen strategy (its risks, opportunities, and effects on the risk profile).
  - c) Strategy should be changed if it fails to create, realize, or preserve value.
- 4) The organization establishes **business objectives** that align with and support strategy.
  - a) Business objectives are
    - i) Specific,
    - ii) Measurable,
    - iii) Observable, and
    - iv) Obtainable.
  - b) Business objectives may relate to, among others, financial performance, operational excellence, or compliance obligations.
  - c) Performance measures, targets, and **tolerances** (the range of acceptable variation in performance) are established to evaluate the achievement of objectives.

#### 4. Performance

- a. Performance relates to ERM practices that support the organization's decisions in pursuit of value. Those practices consist of identifying, assessing, prioritizing, responding to, and developing a portfolio view of risk. **Five principles** relate to performance.
  - 1) The organization **identifies risks** that affect the performance of strategy and business objectives.
    - a) The organization should identify risks that disrupt operations and affect the **reasonable expectation** of achieving strategy and business objectives.
    - b) **New, emerging, and changing** risks are identified. Examples are risks resulting from changes in business objectives or the business context.
      - i) The organization also identifies **opportunities**. These are actions or potential actions that create or alter goals or approaches for the creation, preservation, or realization of value. They differ from **positive events**, occurrences in which performance exceeds the original target.
    - c) Risk identification **methods** and **approaches** include
      - i) Day-to-day activities (e.g., budgeting, business planning, or reviewing customer complaints),
      - ii) Simple questionnaires,
      - iii) Facilitated workshops,
      - iv) Interviews, or
      - v) Data tracking.
    - d) The **risk inventory** consists of all risks that could affect the entity.
    - e) Risk and opportunity identification should be comprehensive across all levels and functions of the entity.
  - 2) The organization assesses the **severity of risk**. Severity is a measure of such considerations as impact, likelihood, and the time to recover from events.
    - a) Common measures of severity include combinations of impact and likelihood.
      - i) **Impact** is the result or effect of the risk. Impact may be positive or negative.
      - ii) **Likelihood** is the possibility that an event will occur. Likelihood may be expressed qualitatively (e.g., a remote probability), quantitatively (e.g., a 75% probability), or in terms of frequency (e.g., once every 6 months).
    - b) The **time horizon** to assess risk should be identical to that of the related strategy and business objective. For example, the risk affecting a strategy that takes 2 years to achieve should be assessed over the same period.
    - c) Risk is assessed at **multiple levels** (e.g., entity, division, operating unit, and function) of the organization and linked to the related strategy and business objective.
      - i) The severity of a risk may vary across levels. For example, a risk with high severity at the operating unit level may have low or moderate severity at the entity level.

- d) Qualitative and quantitative methods may be used to assess risk.
  - i) **Qualitative** methods are more efficient and less costly than quantitative methods. Examples are interviews, surveys, and benchmarking.
  - ii) **Quantitative** methods are more precise than qualitative methods. Examples are decision trees, modeling (probabilistic and nonprobabilistic), and Monte Carlo simulation.
- e) The organization should **reassess severity** whenever triggering events occur, such as changes in business context and risk appetite.
- f) The risk assessment should consider inherent risk, target residual risk, and actual residual risk.
- g) Assessment results may be presented using a **heat map**, which highlights the relative severity of each risk. The warmer the color, the more severe the risk.

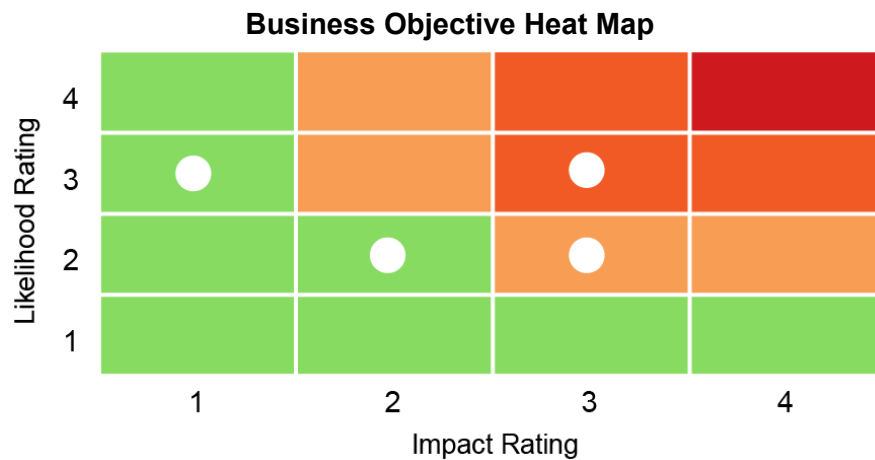


Figure 4-2

- 3) The organization **prioritizes risks** at all levels.
  - a) Risk prioritization enables the organization to optimize the allocation of its limited resources.
  - b) In addition to severity (e.g., impact and likelihood), the following factors are considered when prioritizing risks:
    - i) Agreed-upon criteria
    - ii) Risk appetite
    - iii) The importance of the affected business objective(s)
    - iv) The organizational level(s) affected

- c) **Agreed-upon criteria** are used to evaluate the characteristics of risks and to determine the entity's capacity to respond appropriately. Higher priority is given to risks that most affect the criteria. Example criteria include the following:
    - i) **Complexity** is the nature and scope of a risk, e.g., interdependence of risks.
    - ii) **Velocity** is the speed at which a risk affects the entity.
    - iii) **Persistence** is how long a risk affects the entity, including the time it takes the entity to recover.
    - iv) **Adaptability** is the entity's capacity to adjust and respond to risks.
    - v) **Recovery** is the entity's capacity (not the time) to return to tolerance.
  - d) Higher priority also is assigned to risks that
    - i) Approach or exceed risk appetite,
    - ii) Cause performance levels to approach the outer limits of tolerance, or
    - iii) Affect the entire entity or occur at the entity level.
- 4) The organization identifies and selects **risk responses**, recognizing that risk may be managed but not eliminated. Risks should be managed within the business context and objectives, performance targets, and risk appetite.


**SUCCESS TIP**

Risk response is a frequently tested risk management topic. Having a sound knowledge and understanding of the risk response strategies (avoidance, retention, reduction, and sharing) and examples for each will increase your success on the exam.

- a) The following are the five categories of risk responses:
  - i) **Acceptance (retention).** No action is taken to alter the severity of the risk. Acceptance is appropriate when the risk is within the risk appetite. This term is synonymous with self-insurance.
  - ii) **Avoidance.** Action is taken to remove the risk. Avoidance typically suggests no response would reduce the risk to an acceptable level. For example, the risk of pipeline sabotage can be avoided by selling the pipeline.
  - iii) **Pursuit.** Action is taken to accept increased risk to improve performance without exceeding acceptable tolerance.
  - iv) **Reduction (mitigation).** Action is taken to reduce the severity of the risk so that it is within the target residual risk profile and risk appetite. For example, the risk of systems penetration can be reduced by maintaining an effective information security function within the entity.
  - v) **Sharing (transfer).** Action is taken to reduce the severity of the risk by transferring a portion of the risk to another party. Examples are insurance; hedging; joint ventures; outsourcing; and contractual agreements with customers, vendors, or other business partners.

- b) The following are the **factors** considered in selecting and implementing risk responses:
    - i) They should be chosen for, or adapted to, the **business context**.
    - ii) **Costs and benefits** should be proportionate to the severity of the risk and its priority.
    - iii) They should further **compliance** with obligations (e.g., industry standards) and achievement of **expectations** (e.g., mission, vision, and stakeholder expectations).
    - iv) They should bring risk within **risk appetite** and result in performance outcomes within **tolerance**.
    - v) Risk response should reflect risk severity.
  - c) **Control activities** are designed and implemented to ensure risk responses are carried out. (COSO guidance for control activities is outlined in Study Unit 5, Subunit 3.)
- 5) The organization develops and evaluates its **portfolio view of risk**.
- a) The culmination of risk identification, assessment, prioritization, and response is the full portfolio view of risk.
  - b) The following four risk views have different levels of risk integration:
    - i) **Risk view (minimal integration)**. Risks are identified and assessed. Emphasis is on the event, not the business objective. For example, the risk of a breach may impact the entity's compliance with local regulations.
    - ii) **Risk category view (limited integration)**. Identified and assessed risks are categorized, e.g., based on operating structures. For example, the accounting department will have responsibilities for helping the organization manage its risks related to potential accounting rule changes.
    - iii) **Risk profile view (partial integration)**. Risks are linked to the business objectives they affect, and any dependencies between objectives are identified and assessed. For example, an objective of increased sales may depend on an objective to introduce a new product line.
    - iv) **Portfolio view (full integration)**. This composite view of risks relates to **entity-wide** strategy and business objectives and their effect on **entity** performance. At the top level, greater emphasis is on strategy. Thus, responsibility for business objectives and specific risks **cascades** through the entity.
  - c) Using a portfolio view of risk, management determines whether the entity's **residual risk profile** (risk profile inclusive of risk responses) aligns with overall **risk appetite**.
  - d) Qualitative and quantitative methods may be used to evaluate how changes in risk may affect the portfolio view of risk.
    - i) **Qualitative** methods include benchmarking, scenario analysis, and stress testing.
    - ii) **Quantitative** methods include statistical analysis.

## 5. Review and Revision

- a. The organization reviews and revises its current ERM capabilities and practices based on changes in strategy and business objectives. **Three principles** relate to review and revision.
  - 1) The organization identifies and assesses **changes** that may substantially affect strategy and business objectives.
    - a) Changes in the organization's **business context** and **culture** are most likely to substantially affect strategy and business objectives.
    - b) Such changes may result from changes in the organization's internal or external environment.
      - i) Substantial changes in the **internal environment** include those due to rapid growth, innovation, and turnover of key personnel.
      - ii) Substantial changes in the **external environment** include those in the economy or regulations.
  - 2) The organization reviews **entity performance** results and considers **risk**.
    - a) Performance results that deviate from target performance or tolerance may indicate
      - i) Unidentified risks,
      - ii) Improperly assessed risks,
      - iii) New risks,
      - iv) Opportunities to accept more risk, or
      - v) The need to revise target performance or tolerance.
    - b) In reviewing performance, the organization seeks to answer questions such as
      - i) Has the entity performed as expected and achieved its target?
      - ii) What risks are occurring that may be affecting performance?
      - iii) Was the entity taking enough risks to attain its target?
      - iv) Was the estimate of the amount of risk accurate?
  - 3) The organization pursues **improvement** of ERM.
    - a) The organization must continually improve ERM at all levels, even if actual performance aligns with target performance or tolerance.
    - b) Methods of identifying areas for improvement include **continual** or **separate evaluations** and peer comparisons (reviews of industry peers). (COSO guidance for monitoring activities is outlined in Study Unit 5, Subunit 3.)

## 6. Information, Communication, and Reporting

- a. The organization must capture, process, manage (organize and store), and communicate timely and relevant information to **identify risks** that could affect strategy and business objectives. **Three principles** relate to information, communication, and reporting.
  - 1) The organization leverages its **information systems** to support ERM.
    - a) **Data** are raw facts collectible for analysis, use, or reference. **Information** is processed, organized, and structured data about a fact or circumstance. Information systems transform data (e.g., risk data) into relevant information (e.g., risk information).
      - i) **Knowledge** is data transformed into information.
      - ii) Information is **relevant** if it helps the organization be more agile in decision making, giving it a competitive advantage.

- b) **Structured** data are generally well organized and easily searchable (e.g., spreadsheets, public indexes, or database files).
    - i) **Unstructured** data are unorganized or lack a predefined pattern (e.g., word processing documents, videos, photos, or email messages).
  - c) **Data management** practices help ensure that risk information is useful, timely, relevant, and of high quality. The following are the elements of effective data management:
    - i) **Data and information governance.** Standards are established for the delivery, quality, timeliness, security, and architecture of data. Roles and responsibilities also are defined for risk information owners and data owners.
    - ii) **Processes and controls.** Activities are implemented to ensure established data standards are reinforced and corrections are made as necessary.
    - iii) **Data management architecture.** Information technology is designed that determines what data are collected and how the data are used.
  - d) Information systems must be **adaptable to change**. As the organization adapts its strategy and business objectives in response to changes in the business context, its information systems also must change.
- 2) The organization uses **communication channels** to support ERM.
- a) Communications about risk.
    - i) Management communicates the organization's strategy and business objectives to internal (e.g., personnel and the board) and external (e.g., shareholders) stakeholders.
    - ii) Communications between management and the board should include continual discussions about **risk appetite** and adjust strategy and business objectives accordingly.
  - b) Channels and methods.
    - i) Organizations should adopt **open communication channels** to allow risk information to be sent and received both ways (e.g., to and from personnel or suppliers).
    - ii) Communication **methods** include written documents (e.g., policies and procedures), electronic messages (e.g., email), public events or forums (e.g., town hall meetings), and informal or spoken communications (e.g., one-on-one discussions).
    - iii) The board may hold **formal** quarterly meetings or call **extraordinary** meetings (special meetings to discuss urgent matters).



- 3) The organization **reports** on risk, culture, and performance at multiple levels and across the entity.
  - a) The purpose of reporting is to **support** personnel in their
    - i) Understanding of the relationships among risk, culture, and performance.
    - ii) Decision making related to (a) setting strategy and objectives, (b) governance, and (c) day-to-day operations.
  - b) Reporting combines qualitative and quantitative risk information, with greater emphasis on information that supports **forward-looking** decisions.
  - c) **Management** is responsible for implementing **controls** to ensure reports are accurate, complete, and clear.
  - d) The **frequency of reporting** is based on the severity and priority of the risk.
  - e) Reports on **culture** may be communicated, among other means, in surveys and lessons-learned analyses.
  - f) **Key indicators of risk** should be reported with key performance indicators to emphasize the relationship of risk and performance.

## 7. Assessing ERM

- a. The COSO ERM framework provides criteria for assessing whether the organization's ERM culture, capabilities, and practices together effectively manage risks to strategy and business objectives.
- b. When the **components, principles**, and supporting **controls** are present and functioning, ERM is **reasonably expected** to manage risks effectively and to help create, preserve, and realize **value**.
  - 1) **Present** means the components, principles, and controls exist in the design and implementation of ERM to achieve objectives.
  - 2) **Functioning** means the components, principles, and controls continue to operate to achieve objectives.

## 8. ERM Limitations

- a. Limitations of ERM result from the possibility of
  - 1) Faulty human judgment,
  - 2) Cost-benefit considerations,
  - 3) Simple errors or mistakes,
  - 4) Collusion, and
  - 5) Management override of ERM practices.

## 4.4 ISO 31000 RISK MANAGEMENT FRAMEWORK



SUCCESS TIP

The ISO 31000 risk management framework is a frequently tested risk management topic. Accordingly, mastery of this framework will increase your success on the exam.

### 1. ISO 31000 – Principles, Framework, and Process

- a. ISO 31000 is a **principles-based** approach to risk management. Its principles are the foundation for risk management. They also communicate the characteristics, value, and purpose of effective and efficient risk management. **Value creation and protection** are the purposes of risk management. The principles are described below:
- 1) Integrated. Risk management is integrated into all organizational activities.
  - 2) Structured and comprehensive. The risk management approach needs to be structured and comprehensive.
  - 3) Customized. The risk management framework and process should be customized to the organizational objectives.
  - 4) Inclusive. Appropriate involvement of stakeholders enables informed risk management.
  - 5) Dynamic. Risk management foresees, recognizes, and reacts to changing risks.
  - 6) Best available information. Risk management considers past, current, and future information and any related limitations of such information.
  - 7) Human and cultural factors. Human behavior and culture affect all facets and each level of risk management.
  - 8) Continual improvement. Learning and experience constantly improve risk management.

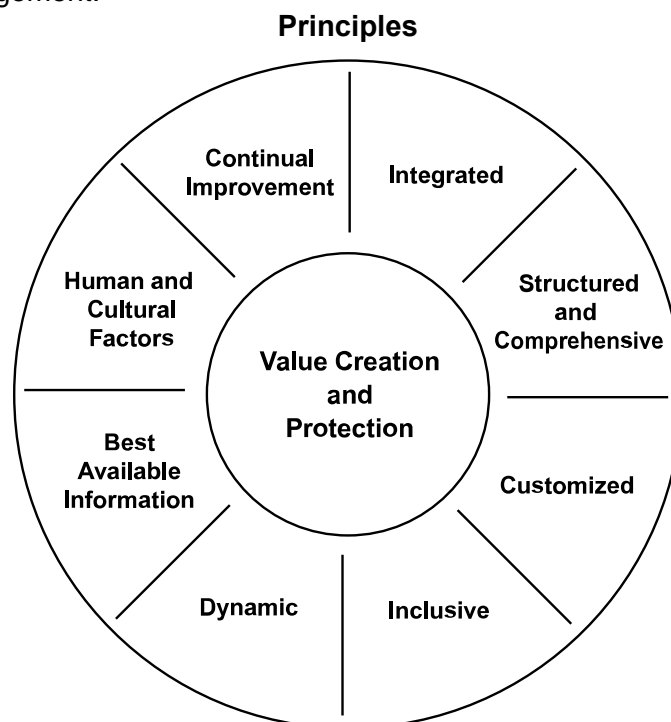


Figure 4-3

- b. A risk management **framework** is a set of components that includes leadership and commitment, integration, design, implementation, evaluation, and improvement of risk management. The six components are described as follows:
- 1) The board and senior management demonstrate **leadership and commitment** by implementing the framework's components; adopting a policy that establishes a risk management plan or approach; committing resources to risk management; and assigning accountability, authority, and responsibility at each organizational level.
  - 2) The **integration** of the framework into all facets of an organization, including its objectives, structure, governance, and culture, is a dynamic process. All personnel in the organization are responsible for managing risks.
  - 3) The **design** of the framework involves the following:
    - a) Understanding the organization and its context
    - b) Articulating commitment to risk management
    - c) Assigning and communicating authorities, responsibilities, and accountabilities for risk management roles at all levels
    - d) Allocating resources (e.g., people, experience, processes, and information systems) to support risk management while recognizing the limitations of existing resources
    - e) Establishing communication and consultation
  - 4) The **implementation** of the framework can be achieved by developing a plan; identifying decision making processes; modifying decision making processes as change occurs; and ensuring stakeholders' understanding of, and engagement with, the organization's risk management arrangement.
  - 5) The **evaluation** of the framework's effectiveness involves measuring performance against expectations.
  - 6) The **improvement** of the framework is through monitoring and updating the framework in response to changes, thereby enhancing organization performance.

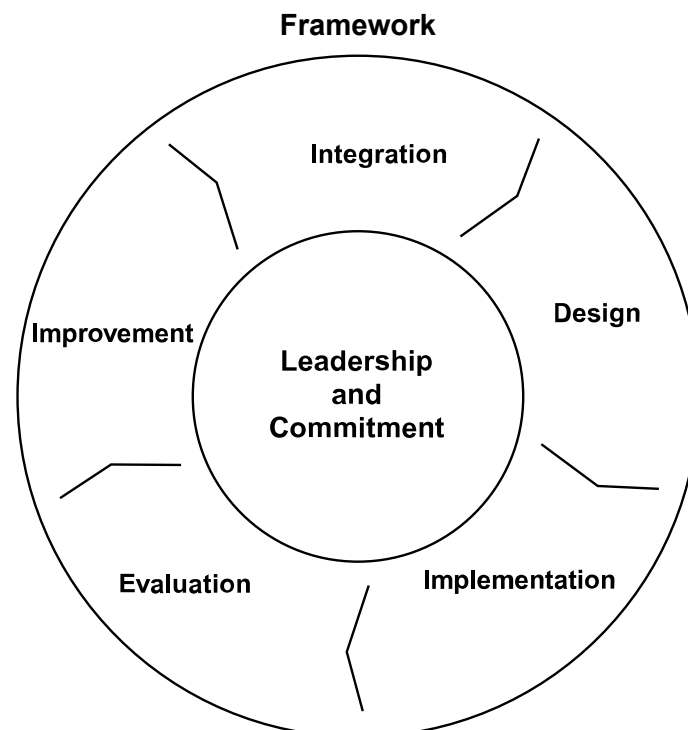


Figure 4-4

- c. The risk management **process** consists of the following elements:
- 1) To improve understanding of risks and decisions made, **communication** to raise awareness and **consultation** to obtain feedback and information require ongoing, structured coordination with stakeholders.
  - 2) The **scope, context, and criteria** should be established to customize risk management. This element includes defining the scope of the risk management process, understanding its external and internal context, and defining risk criteria.
    - a) The context of the risk management process derives from the understanding of the specific external and internal environment of the organization.
  - 3) **Risk assessment** is the process of identifying, analyzing, and evaluating risk.
    - a) **Risk identification** finds risks that can contribute to or prevent achieving organizational objectives. For example, it considers risk sources, changes in context, threats and opportunities, emerging risk indicators, and consequences and their effects on objectives.
    - b) **Risk analysis** examines the nature, characteristics, and level of risk. It considers such factors as likelihood of events and consequences, control effectiveness, and confidence level.
    - c) **Risk evaluation** supports decision making by comparing the defined risk criteria with the risk analysis outcome and determining whether any action is required.
  - 4) **Risk treatment** is a repetitive process of selecting risk treatments (e.g., accept, avoid, reduce, share, or pursue), implementing the treatment, assessing the treatment's effectiveness, determining whether the residual risk is acceptable, and adopting another treatment if the first was unacceptable.
  - 5) **Monitoring and review** should occur in all phases of the risk management process to improve its quality and effectiveness.
  - 6) **Recording and reporting** of the risk management process and its results should be facilitated to communicate and improve risk management activities, support decisions, and enhance communications with stakeholders.

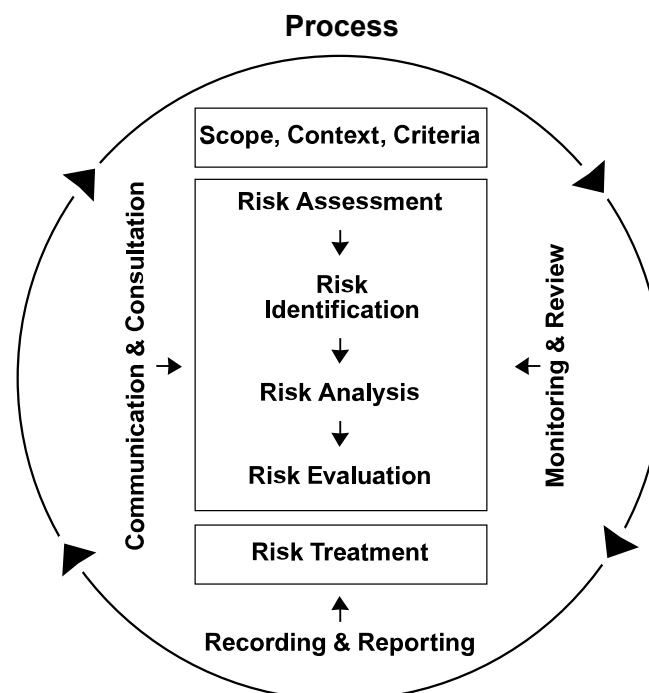


Figure 4-5

## 2. ISO 31000 – Responsibilities for Risk Management

- a. The **board** is responsible for overseeing risk management and has overall responsibility for ensuring that risks are managed and the risk management system is effective.
- b. **Management** is responsible for setting the organization's **risk attitude**, which is defined by ISO as an "organization's approach to assess and eventually pursue, retain, take, or turn away from risk." Management also identifies and manages risks.
- c. The **internal audit activity** is responsible for providing assurance regarding the entire risk management system.

## 3. ISO 31000 – Assurance Approaches

- a. ISO 31000 describes three approaches to providing assurance on the risk management process: (1) key principles, (2) process element, and (3) maturity model.
  - 1) The **key principles** approach evaluates whether the risk management principles are in practice.
  - 2) The **process element** approach evaluates whether the risk management elements have been put into practice.



SUCCESS TIP

The maturity model approach is a frequently tested assurance approach. Having a thorough understanding of this approach will increase your success on the exam.

- 3) The **maturity model** approach is based on the principle that effective risk management processes develop and improve with time as value is added at each phase in the maturation process. The basic principle is that risk management must add value.
  - a) Accordingly, this approach determines where the risk management process is on the maturity curve and evaluates whether it (1) is progressing as expected, (2) adds value, and (3) meets organizational needs.
  - b) An example maturity curve (i.e., maturity model) is the **capability maturity model (CMM)**. It consists of the following maturity levels presented in order of maturity: initial, repeatable, defined, managed, and optimizing.

<b>Level 1</b>	<b>Initial:</b> Few processes are defined.
<b>Level 2</b>	<b>Repeatable:</b> Basic processes are established.
<b>Level 3</b>	<b>Defined:</b> Standards are developed.
<b>Level 4</b>	<b>Managed:</b> Performance measures are defined.
<b>Level 5</b>	<b>Optimizing:</b> Continuous improvement is enabled.

- c) The **Capability Maturity Model Integration (CMMI) Development V2.0** focuses on organizational performance at each maturity level. This model consists of the following maturity levels presented in order of maturity: incomplete, initial, managed, defined, quantitatively managed, and optimizing.

<b>Level 0</b>	<b>Incomplete:</b> Whether work can be completed is not known.
<b>Level 1</b>	<b>Initial:</b> Work can be completed, but not on time or within the budget.
<b>Level 2</b>	<b>Managed:</b> Projects are planned, implemented, managed, and monitored.
<b>Level 3</b>	<b>Defined:</b> Standards for projects are defined throughout the organization.
<b>Level 4</b>	<b>Quantitatively managed:</b> The organization quantifies performance improvement goals to meet stakeholder needs.
<b>Level 5</b>	<b>Optimizing:</b> The organization pursues continuous improvement, responds to change, and innovates.

- d) A critical aspect of the maturity model approach is that risk management performance and progress in executing the risk management plan should be linked with a **performance measurement system**, which typically consists of
- i) Performance standards,
  - ii) Criteria on how the standards can be satisfied,
  - iii) A method of comparing actual performance with each standard,
  - iv) A method of recording and reporting performance and improvements in performance, and
  - v) Periodic independent verification of management's assessment.

#### 4. **Turnbull Risk Management Framework**

- a. In contrast with the ISO 31000 principles-based approach, the Turnbull risk management framework emphasis is on **internal control**, the assessment of its effectiveness, and risk analysis.

# STUDY UNIT FIVE

## CONTROLS: TYPES AND FRAMEWORKS

5.1	Overview of Control .....	1
5.2	Types of Controls .....	6
5.3	Control Frameworks -- Overview and COSO .....	12
5.4	Control Frameworks -- CoCo Model, COBIT, VAL IT, and eSAC Model .....	19

This study unit is the third of four covering **Domain V: Governance, Risk Management, and Control** from The IIA's CIA Exam Syllabus. This domain makes up 35% of Part 1 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.



### SUCCESS TIP

Many questions on the CIA exam address controls. Few such questions are answerable based on memorization of lists. Moreover, no text can feasibly present comprehensive lists of procedures. Thus, candidates must be able to apply reasoning processes and knowledge of auditing concepts to unfamiliar situations involving controls. By answering our questions, you will be able to synthesize, understand, and apply internal control theory.

**Analysis** results in an understanding of a situation, set of circumstances, or process.

**Synthesis** involves developing standards and generalizations for a situation, set of circumstances, or a process. It is a means of combining individual components or parts to produce a whole. Synthesis requires inductive reasoning, which is reaching a generalized conclusion from particular instances.

**Evaluation** is relating a situation, set of circumstances, or process to predetermined or synthesized standards. Evaluation usually includes both analysis and synthesis. This skill set will allow you to answer any question on the CIA exam with confidence.

### 5.1 OVERVIEW OF CONTROL

1. **Definitions from The IIA Glossary** (Appendix A contains the complete IIA Glossary.)
  - a. **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.”
  - b. **Control processes** are “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.”
  - c. **Control environment** is “[t]he 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:
    - 1) Integrity and ethical values
    - 2) Management’s philosophy and operating style
    - 3) Organizational structure
    - 4) Assignment of authority and responsibility
    - 5) Human resource policies and practices
    - 6) Competence of personnel”

## 2. The Control Process

- a. Control requires feedback on the results of organizational activities for the purposes of measurement and correction.
- b. The control process includes
  - 1) Establishing standards for the operation to be controlled,
  - 2) Measuring performance against the standards,
  - 3) Examining and analyzing deviations,
  - 4) Taking corrective action, and
  - 5) Reappraising the standards based on experience.
- c. An evaluation-reward system should be implemented to encourage compliance with the control system.
- d. Internal control only provides reasonable assurance of achieving objectives. It cannot provide absolute assurance because any system of internal control has the following inherent limitations:
  - 1) **Human judgment** is faulty, and controls may fail because of simple errors or mistakes.
  - 2) **Management** may inappropriately override internal controls, e.g., to fraudulently achieve revenue projections or hide liabilities.
  - 3) Manual or automated controls can be circumvented by **collusion**.
  - 4) The **cost** of internal control must not be greater than its **benefits**.

## 3. Characteristics of Automated Processing

- a. The use of computers in business information systems has fundamental effects on the nature of business transacted, the procedures followed, the risks incurred, and the methods of mitigating those risks.
  - 1) These effects result from the characteristics that distinguish computer-based from manual processing.
- b. **Transaction Trails**
  - 1) A complete trail useful for audit and other purposes might exist for only a short time or only in computer-readable form.
  - 2) The nature of the trail is often dependent on the transaction processing mode. For example, transactions may be batched prior to processing or processed immediately as they happen.
- c. **Uniform Processing of Transactions**
  - 1) Computer processing uniformly subjects similar transactions to the same processing instructions and thus virtually eliminates clerical error.
    - a) But programming errors (or other similar systematic errors in either the hardware or software) will result in all similar transactions being processed incorrectly when they are processed under the same conditions.
- d. **Segregation of Functions**
  - 1) Many controls once performed by separate individuals may be concentrated in computer systems. Thus, an individual who has access to the computer may perform incompatible functions.
    - a) As a result, other controls may be necessary to achieve the control objectives ordinarily accomplished by segregation of functions.



**e. Potential for Errors and Fraud**

- 1) The potential for individuals, including those performing control procedures, to gain unauthorized access to data, to alter data without visible evidence, or to gain access (direct or indirect) to assets may be greater in computer systems.
- 2) Decreased human involvement in handling transactions can reduce the potential for observing errors and fraud. Errors or fraud in the design or changing of application programs can remain undetected for a long time.

**f. Potential for Increased Management Supervision**

- 1) Computer systems offer management many analytical tools for review and supervision of operations. These additional controls may enhance internal control.
  - a) For example, traditional comparisons of actual and budgeted operating ratios and reconciliations of accounts are often available for review on a more timely basis.
  - b) Furthermore, some programmed applications provide statistics regarding computer operations that may be used to monitor actual processing.

**g. Initiation or Subsequent Execution of Transactions by Computer**

- 1) Certain transactions may be automatically initiated or certain procedures required to execute a transaction may be automatically performed by a computer system.
  - a) The authorization of these transactions or procedures may not be documented in the same way as those in a manual system. Accordingly, management's authorization may be implicit in its acceptance of the design of the system.

**h. Dependence of Controls in Other Areas on Controls over Computer Processing**

- 1) Computer processing may produce reports and other output that are used in performing manual control procedures.
  - a) The effectiveness of these controls can be dependent on the effectiveness of controls over the completeness and accuracy of computer processing. For example, the effectiveness of a manual review of a computer-produced exception listing is dependent on the controls over the production of the listing.

**i. Manual Controls vs. Automated Controls**

- 1) Manual controls may be more suitable where judgment and discretion are required, such as
  - a) For large, unusual, or nonrecurring transactions;
  - b) For circumstances where misstatements are difficult to define, anticipate, or predict;
  - c) In changing circumstances that require a control response outside the scope of an existing automated control; and
  - d) In monitoring the effectiveness of automated controls.
- 2) Automated controls are suitable for
  - a) High-volume transactions that require additional calculations.
  - b) Routine errors that can be predicted and corrected.
  - c) Circumstances that require a high degree of accuracy.

## 4. Roles of Internal Auditors in Control


**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.

**Implementation Standard 2130.C1**

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

**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.

- a. 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 (1) resources used exceed the benefits and (2) 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 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

## 5.2 TYPES OF CONTROLS

### 1. Primary Controls

- a. **Preventive controls** deter the occurrence of unwanted events.
  - 1) Storing petty cash in a locked safe and segregating duties, e.g., using a lockbox system, are examples.
  - 2) IT examples include
    - a) Designing a database so that users cannot enter a letter in the field that stores a Social Security number and
    - b) Requiring the number of invoices in a batch to be entered before processing begins.
- b. **Detective controls** alert the proper people after an unwanted event. They are effective when detection occurs before material harm occurs.
  - 1) For example, a batch of invoices submitted for processing may be rejected by the computer system if it includes identical payments to a single vendor. A detective control provides for automatic reporting of all rejected batches to the accounts payable department.
  - 2) A burglar alarm is another example.
- c. **Corrective controls** correct the negative effects of unwanted events.
  - 1) An example is a requirement that all cost variances over a certain amount be justified.
- d. **Directive controls** cause or encourage the occurrence of a desirable event. These include the following:
  - 1) Policy and procedure manuals
  - 2) Employee training
  - 3) Job descriptions

### 2. Secondary Controls

- a. **Compensatory (mitigative) controls** may reduce risk when the primary controls are ineffective. However, they do not, by themselves, reduce risk to an acceptable level.
  - 1) An example is the lack of segregation of duties when a store clerk is the only employee present at closing. Accordingly, the clerk counts cash at the end of the day without supervision. The compensating control performed the next morning is for a supervisor to reconcile the count with the cash register data.
- b. **Complementary controls** work with other controls to reduce risk to an acceptable level. In other words, their synergy is more effective than either control by itself.
  - 1) For example, separating the functions of accounting for and custody of cash receipts is complemented by obtaining deposit slips validated by the bank.

### 3. Two Basic Processing Modes

#### a. Batch Processing

- 1) In this mode, transactions are accumulated and submitted to the computer as a single batch. In the early days of computers, this was the only way a job could be processed.
- 2) In batch processing, the user cannot influence the process once the job has begun (except to ask that it be aborted completely). (S)he must wait until the job is finished running to see whether any transactions were rejected and failed to post.
- 3) Despite huge advances in computer technology, this accumulation of transactions for processing on a delayed basis is still widely used. It is very efficient for such applications as payroll because large numbers of routine transactions must be processed on a regular schedule.
- 4) **Memo posting** is used by banks for financial transactions when batch processing is used. It posts temporary credit or debit transactions to an account if the complete posting to update the balance will be done as part of the end-of-day batch processing. Information can be viewed immediately after updating.
  - a) Memo posting is an intermediate step between batch processing and real-time processing.

#### b. Online, Real-Time Processing

- 1) In some systems, having the latest information available at all times is crucial to the proper functioning of the system. An airline reservation system is a common example.
- 2) In an online, real-time system, the database is updated immediately upon entry of the transaction by the operator. Such systems are referred to as **online transaction processing**, or **OLTP**, systems.

### 4. IT General Controls

- a. Controls over information and related technologies can be broadly classified into two categories: (1) IT general controls and (2) application controls.
- b. According to The IIA's Global Technology Audit Guides (GTAGs), IT general controls are those that pertain to all systems components, processes, and data present in an organization's IT environment.
  - 1) The objectives of IT general 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.
- c. The most common IT general controls are
  - 1) Logical access controls (e.g., passwords) over infrastructure, applications, and data
  - 2) System development life cycle controls
  - 3) Program change management controls
  - 4) Physical security controls over the data center
  - 5) System and data backup and recovery controls

## 5. Application Controls

- a. Per the GTAGs, application controls are those that pertain to the scope of individual business processes or application systems. The objective of application controls is to ensure that
  - 1) Input data is accurate, complete, authorized, and correct.
  - 2) Data is processed as intended in an acceptable time period.
  - 3) Data stored is accurate and complete.
  - 4) Outputs are accurate and complete.
  - 5) A record is maintained to track the process of data from input to storage and to the eventual output.
- b. When designing data input controls, primary consideration should be given to authorization, validation, and error notification.
- c. The most economical point for correcting input errors in an application is the time at which the data are entered into the system.
  - 1) For this reason, input controls are a primary focus of an internal auditor's assessment of application controls. Each of the two major types of processing modes has its own controls.
- d. **Batch Input Controls**
  - 1) **Financial totals** summarize monetary amounts in an information field in a group of records. The total produced by the system after the batch has been processed is compared to the total produced manually beforehand.
  - 2) **Record counts** track the number of records processed by the system for comparison to the number the user expected to be processed.
  - 3) **Hash totals** are control totals without a defined meaning, such as the total of vendor numbers or invoice numbers, that are used to verify the completeness of the data.

### EXAMPLE 5-1 Batch Input Controls

A company has the following invoices in a batch:

<u>Invoice Number</u>	<u>Product</u>	<u>Quantity</u>	<u>Unit Price</u>
303	G7	100	US \$15
305	A48	200	5
353	L30	125	10
359	Z26	150	20

The hash total is a control total without a defined meaning, such as the total of employee numbers or invoice totals, that is used to verify the completeness of data. Using invoice numbers, the hash total would be 1320.

e. **Online Input Controls**

- 1) **Preformatting** of data entry screens, i.e., to make them imitate the layout of a printed form, can aid the operator in keying to the correct fields.
- 2) **Field/format checks** are tests of the characters in a field to verify that they are of an appropriate type for that field. For example, the system is programmed to reject alphabetic characters entered in the field for Social Security number.
- 3) **Validity checks** compare the data entered in a given field with a table of valid values for that field. For example, the vendor number on a request to cut a check must match the table of current vendors, and the invoice number must match the approved invoice table.
- 4) **Limit (reasonableness) and range checks** are based on known limits for given information. For example, hours worked per week must be between 0 and 100, with anything above that range requiring management authorization.
- 5) **Check digits** are an extra reference number that follows an identification code and bears a mathematical relationship to the other digits. This extra digit is input with the data. The identification code can be subjected to an algorithm and compared to the check digit.
- 6) **Sequence checks** are based on the logic that processing efficiency is greatly increased when files are sorted on some designated field, called the “key,” before operations such as matching. If the system discovers a record out of order, it may indicate that the files were not properly prepared for processing.
- 7) **Zero balance checks** will reject any transaction or batch thereof in which the sum of all debits and credits does not equal zero.

f. **Processing controls** ensure that data are complete and accurate during updating.

- 1) **Concurrency controls** manage situations where two or more users attempt to access or update a file or database simultaneously. These controls ensure the correct results are generated while getting those results as quickly as possible.

g. **Output controls** ensure that processing results are complete, accurate, and properly distributed.

- 1) An important output control is user review. Users should be able to determine when output is incomplete or not reasonable, particularly when the user prepared the input. Thus, users as well as computer personnel have a quality assurance function.

h. **Integrity controls** monitor data being processed and in storage to ensure it remains consistent and correct.

i. **Management trail** (or audit trail) are processing history controls that enable management to track transactions from their source to their output.

## 6. Entity-Level, Process-Level, and Transaction-Level Controls

- a. **Entity-level controls** are designed to achieve organizational objectives and to address entity-wide risks. They include governance controls and management oversight controls.
  - 1) Entity-level **governance controls** are established by the board of directors at the highest level (governance level). They include organizational policies and procedures that define the entity's culture and communicate its expectations. Examples include IT policies, the code of conduct, oversight of controls, and setting the risk appetite.
  - 2) Entity-level **management oversight controls** are implemented by management at the business unit level to achieve business unit objectives and address business unit risks. Examples include IT general controls and period-end controls.
- b. **Process-level controls** are designed to achieve process objectives and to address process risks. Examples include physical inventory counts, performance assessment, and review of revenue center reports.
- c. **Transaction-level controls** are designed to achieve transaction objectives and to address risks specific to transactions. Examples include application controls, exception reports, and segregation of duties.

## 7. Time-Based Classification

- a. **Feedback controls** report information about completed activities. They permit improvement in future performance by learning from past mistakes.
  - 1) For example, the inspection of completed goods followed by performing variance analysis procedures helps identify deviations from what was expected. Thus, inspection and the analysis of variance provide feedback on how well the completion of goods meets expectations.
- b. **Concurrent controls** adjust ongoing processes. These real-time controls monitor activities in the present to prevent them from deviating too far from standards. An example is close supervision of production-line workers.
- c. **Feedforward controls** anticipate and prevent problems. These controls require a long-term perspective. Organizational policies and procedures are examples.

## 8. Financial vs. Operating Controls

- a. **Financial controls** should be based on relevant established accounting principles.
  - 1) Objectives of financial controls may include
    - a) Proper authorization;
    - b) Appropriate recordkeeping;
    - c) Safeguarding of assets; and
    - d) Compliance with laws, regulations, and contracts.
- b. **Operating controls** apply to production and support activities.
  - 1) Because they may lack established criteria or standards, they should be based on management principles and methods. They also should be designed with regard to the management functions of planning, organizing, directing, and controlling.



9. **People-Based vs. System-Based Controls**

- a. **People-based controls** are dependent on the intervention of humans for their proper operation, for example, regular performance of bank reconciliations.
  - 1) Checklists, such as lists of required procedures for month-end closing, can be valuable to ensure that people-based controls are executed when needed.
- b. **System-based controls** are executed whenever needed with no human intervention.
  - 1) An example is code in a computerized purchasing system that prevents any purchase order over a certain monetary threshold from being submitted to the vendor without managerial approval.

10. **Use of a Control Matrix**

- a. Controls do not necessarily match risks one-to-one. Certain controls may address more than one risk, and more than one control may be needed to adequately address a single risk.
  - 1) For example, assume all petty cash custodians must present expense vouchers periodically. This control helps ensure that
    - a) Petty cash accounts are maintained at the established level and
    - b) Petty cash expenditures are reviewed for appropriateness.
  - 2) A control matrix is useful for matching controls with risks in these circumstances. The following is an example:

**Control Matrix**

	Control A	Control B	Control C	Control D
Risk 1	●			
Risk 2	●			
Risk 3		●		
Risk 4		●	●	
Risk 5	●			
Risk 6				●

Figure 5-1

### 5.3 CONTROL FRAMEWORKS -- OVERVIEW AND COSO

#### 1. Available Control Frameworks

- a. Several bodies have published control frameworks that provide a comprehensive means of ensuring that the organization has considered all relevant aspects of internal control.
  - 1) The use of a particular model or control design not mentioned here may be specified by regulatory or legal requirements.
  - 2) Some of the better-known frameworks are described below.
- b. **United States**
  - 1) The 1973-74 Watergate investigations revealed that U.S. companies were bribing government officials, politicians, and political parties in foreign countries. The result was the Foreign Corrupt Practices Act of 1977.
  - 2) The private sector also responded by forming the National Commission on Fraudulent Financial Reporting (NCFRR) in 1985.
    - a) The NCFRR is known as the Treadway Commission because James C. Treadway was its first chair.
    - b) The Treadway Commission was originally sponsored and funded by five professional accounting organizations based in the United States.
    - c) This group of five became known as the Committee of Sponsoring Organizations of the Treadway Commission (COSO).
    - d) The Commission recommended that this group of five organizations cooperate in creating guidance for internal control.
  - 3) The result was the *COSO Internal Control – Integrated Framework*, published in 1992, which was modified in 1994 and again in 2013.
- c. **Canada**
  - 1) *Guidance on Control* (commonly referred to as CoCo based on its original title *Criteria of Control*), published by the Canadian Institute of Chartered Accountants (CICA).
- d. **United Kingdom**
  - 1) *Internal Control: Guidance for Directors on the Combined Code* (commonly referred to as the Turnbull Report after Nigel Turnbull, chair of the committee that drafted the report), published by the Financial Reporting Council (FRC) of the UK and re-released as *Internal Control: Revised Guide for Directors on the Combined Code*.
  - 2) The UK Committee on the Financial Aspects of Corporate Governance (known informally as the Cadbury Committee after its chairman Sir Adrian Cadbury) issued its report about the same time as the Treadway Commission in the U.S.
  - 3) It was subsequently blended with the reports of two other organizations. The resulting *Combined Code* includes recommendations for sound governance, such as requiring that the CEO and chairperson be separate individuals.
- e. **Information Technology**
  - 1) *Control Objectives for Information and Related Technology* (COBIT) is the best-known framework specifically for IT controls. COBIT 2019 is the most recent version.
  - 2) Covered within the scope of the COBIT 2019 framework is the VAL IT framework. It addresses the governance of IT-enabled business investments.
  - 3) *Electronic Systems Assurance and Control* (eSAC), published by The Institute of Internal Auditors Research Foundation, is an alternative control model for IT.

## 2. COSO Framework

### a. Definition of Internal Control

- 1) The COSO model defines internal control as follows:

*Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.*

- 2) Thus, internal control is

- a) Intended to achieve three classes of objectives
- b) An ongoing process
- c) Effected by people at all organizational levels, e.g., the board, management, and all other employees
- d) Able to provide reasonable, but not absolute, assurance
- e) Adaptable to an entity's structure

### b. Objectives

- 1) The three classes of objectives direct organizations to the different (but overlapping) elements of control.

#### a) Operations

- i) Operations objectives relate to achieving the entity's mission.
  - Appropriate objectives include improving (1) financial performance, (2) productivity, (3) quality, (4) innovation, and (5) customer satisfaction.
- ii) Operations objectives also include **safeguarding of assets**.
  - Objectives related to protecting and preserving assets assist in risk assessment and development of mitigating controls.
  - Avoidance of waste, inefficiency, and bad business decisions relates to broader objectives than safeguarding of assets.

#### b) Reporting

- i) To make sound decisions, stakeholders must have reliable, timely, and transparent financial information.
- ii) Reports may be prepared for use by the organization and stakeholders.
- iii) Objectives may relate to
  - Financial and nonfinancial reporting
  - Internal or external reporting

c) **Compliance**

- i) Entities are subject to laws, rules, and regulations that set minimum standards of conduct.
  - Examples include taxation, environmental protection, and employee relations.
  - Compliance with internal policies and procedures is an operational matter.

d) The following is a useful memory aid for the COSO classes of objectives:

<b>O</b>	<b>Operations</b>
<b>R</b>	<b>Reporting</b>
<b>C</b>	<b>Compliance</b>

2) Achievement of Objectives

- a) An internal control system is more likely to provide reasonable assurance of achieving the reporting and compliance objectives than the operational objectives.
- b) Reporting and compliance objectives are responses to standards established by external parties, such as regulators.
  - i) Thus, achieving these objectives depends on actions almost entirely within the entity’s control.
- c) However, operational effectiveness may not be within the entity’s control because it is affected by human judgment and many external factors.

c. **Components of Internal Control**

- 1) Supporting the organization in its efforts to achieve objectives are the following five components of internal control:
  - a) Control environment
  - b) Risk assessment
  - c) Control activities
  - d) Information and communication
  - e) Monitoring
- 2) A useful memory aid for the COSO components of internal control is “Controls stop **CRIME.**”

<b>C</b>	<b>Control activities</b>
<b>R</b>	<b>Risk assessment</b>
<b>I</b>	<b>Information and communication</b>
<b>M</b>	<b>Monitoring</b>
<b>E</b>	<b>Control environment</b>

**d. Control Environment**

- 1) The control environment is a set of standards, processes, and structures that pervasively affects the system of internal control. Five principles relate to the control environment.
  - a) The organization demonstrates a commitment to **integrity and ethical values** by
    - i) Setting the tone at the top. Through words and actions, the board of directors and management communicate their attitude toward integrity and ethical values.
    - ii) Establishing standards of conduct. The board and management create expectations that should be understood at all organizational levels and by outside service providers and business partners.
    - iii) Evaluating the performance of individuals and teams based on the established standards of conduct.
    - iv) Correcting deviations in a timely and consistent manner.
  - b) The board demonstrates independence from management and exercises **oversight** for internal control. The board
    - i) Establishes oversight responsibility. The board identifies and accepts its oversight responsibilities.
    - ii) Applies relevant experience by defining, maintaining, and periodically evaluating the skills and expertise needed among its members to ask difficult questions of management and take appropriate actions.
    - iii) Operates independently. The board includes enough members who are independent and objective in evaluations and decision making.
      - For example, in some jurisdictions, all members of the audit committee must be outside directors.
    - iv) Provides oversight. The board is responsible for oversight of management's design, implementation, and conduct of internal control.
  - c) Management establishes, with board oversight, **structures, reporting lines, and appropriate authorities and responsibilities**. Management
    - i) Considers all structures of the entity. Variables considered in establishing organizational structures include the following:
      - Nature of the business
      - Size and geographic scope of the entity
      - Risks, some of them outsourced, and connections with outside service providers and partners
      - Assignment of authority to different management levels
      - Definition of reporting lines
      - Reporting requirements
    - ii) Establishes and evaluates reporting lines. The trend in corporate governance has been to allow employees closer to day-to-day operations to make decisions.
    - iii) Designs, assigns, and limits authorities and responsibilities.

- d) The organization demonstrates a **commitment to attract, develop, and retain competent individuals** in alignment with objectives.
  - i) Policies and practices reflect expectations of competence. Internal control is strengthened when management specifies what competencies are needed for particular jobs.
  - ii) The board and management evaluate competence and address shortcomings. Employees and outside service providers have the appropriate skills and knowledge to perform their jobs.
  - iii) The organization attracts, develops, and retains individuals. The organization is committed to hiring individuals who are competent and have integrity. Ongoing training and mentoring are necessary to adapt employees to the control requirements of a changing environment.
  - iv) Senior management and the board plan and prepare for succession.
- e) The **organization holds individuals accountable** for their internal control responsibilities in pursuit of objectives. Management and the board
  - i) Enforce accountability through structures, authorities, and responsibilities
  - ii) Establish performance measures, incentives, and rewards
  - iii) Evaluate performance measures, incentives, and rewards for ongoing relevance
  - iv) Consider excessive pressures
  - v) Evaluate performance and reward or discipline individuals

#### e. Risk Assessment

- 1) The risk assessment process encompasses an assessment of the risks themselves and the need to manage organizational change. It is a basis for determining how the risks should be managed. Four principles relate to risk assessment.
  - a) The organization **specifies objectives** with sufficient clarity to enable the identification and assessment of risks relating to five types of objectives.
    - i) Operations
    - ii) External financial reporting
    - iii) External nonfinancial reporting
    - iv) Internal reporting
    - v) Compliance
  - b) The organization **identifies** risks to the achievement of its objectives across the entity and **analyzes** risks to determine how the risks should be managed. Management must focus carefully on risks at all levels of the entity and take the necessary actions to manage them.
  - c) The organization considers the potential for fraud in **assessing fraud risks** to the achievement of objectives. The organization must
    - i) Consider various types of fraud,
    - ii) Assess incentives and pressures,
    - iii) Assess opportunities, and
    - iv) Assess attitudes and rationalizations.
  - d) The organization **identifies and assesses changes** that could significantly affect the system of internal control.
    - i) Significant changes could occur in an organization's external environment, business model, and leadership. Thus, internal controls must be adapted to the entity's changing circumstances.

#### f. Control Activities

- 1) These policies and procedures help ensure that management directives are carried out. Whether automated or manual, they are applied at various levels of the entity and stages of processes. They may be preventive or detective, and segregation of duties is usually present. Three principles relate to control activities.
  - a) The organization selects and develops control activities that contribute to the **mitigation of risks** to the achievement of objectives to acceptable levels.
  - b) The organization selects and develops general control activities over **technology** to support the achievement of objectives.
  - c) The organization deploys control activities through **policies** that establish what is expected and **procedures** that put policies into action.

#### g. Information and Communication

- 1) Information systems enable the organization to obtain, generate, use, and communicate information to (a) maintain accountability and (b) measure and review performance. Three principles relate to information and communication.
  - a) The organization obtains or generates and uses **relevant, quality information** to support the functioning of internal control.
  - b) The organization **internally communicates** information, including objectives and responsibilities for internal control, necessary to support the function of internal control.
  - c) The organization **communicates with external parties** regarding matters affecting the functioning of internal control.

#### h. Monitoring Activities

- 1) Control systems and the way controls are applied change over time. Monitoring is a process that assesses the quality of internal control performance over time to ensure that controls continue to meet the needs of the organization. The following are two principles related to monitoring activities:
  - a) The organization selects, develops, and performs **ongoing or separate evaluations (or both)** to determine whether the components of internal control are present and functioning.
  - b) The organization **evaluates and communicates control deficiencies** in a timely manner.
- 2) Changes in the external or internal environment create risks to the organization's internal control system. To ensure the internal control system remains capable of achieving its objectives, the organization should maintain an effective monitoring program. The stages in the monitoring-for-change continuum are as follows:
  - a) Control Baseline
    - i) Monitoring must begin with an understanding of internal control's design and whether the controls that have been implemented are effective at accomplishing the organization's objectives.
    - ii) This baseline understanding of internal control provides a starting place for making suggestions on how to improve efficiency and effectiveness.

- b) Change Identification
  - i) Ongoing or separate evaluation (or both) are used to identify whether changes in process or risks are being addressed. As part of these evaluations, the organization should confirm that controls continue to meet their objectives of helping to manage or mitigate related risks.
- c) Change Management
  - i) The organization should verify that the internal control system manages the changes and establishes a new control baseline for the modified controls.
- d) Control Revalidation
  - i) Control revalidation is the process of using monitoring procedures to confirm the conclusion that controls are effective. This is a form of continuous monitoring.

i. **Relationship of Objectives, Components, and Organizational Structure**

- 1) The COSO model may be displayed as a cube with rows, slices, and columns. The rows are the five components, the slices are the three objectives, and the columns represent an entity’s organizational structure.

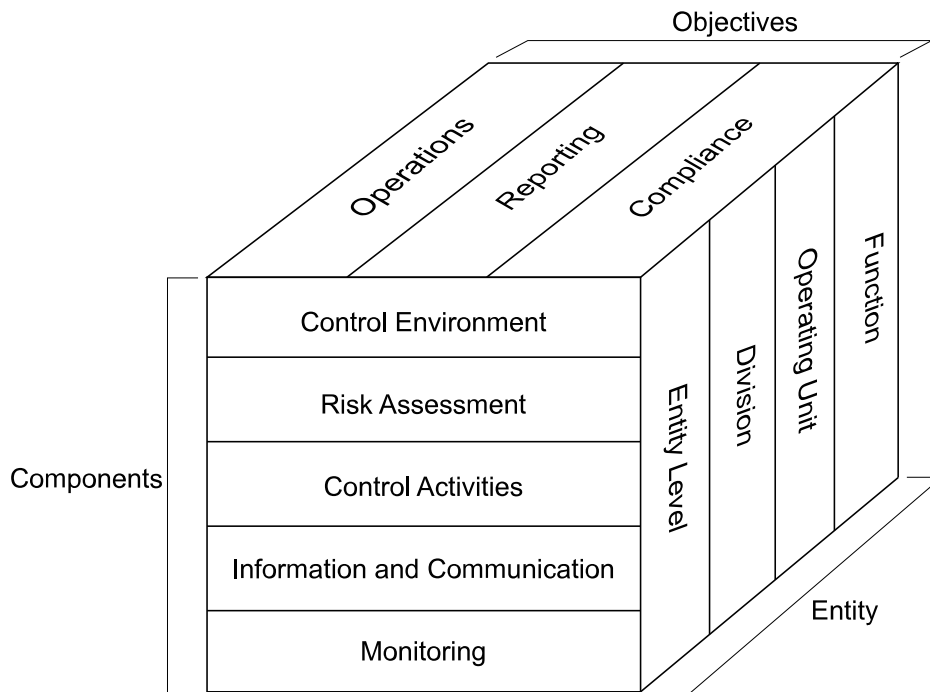


Figure 5-2



## 5.4 CONTROL FRAMEWORKS -- CoCo MODEL, COBIT, VAL IT, AND eSAC MODEL

### 1. CoCo Model

- a. The CoCo model is thought to be more suited for internal auditing purposes. It consists of 20 criteria grouped into 4 components:
  - 1) Purpose
  - 2) Commitment
  - 3) Capability
  - 4) Monitoring and Learning
- b. The following is a useful memory aid for the components of the CoCo model:

<b>P</b> olice	<b>P</b> urpose
<b>C</b> an	<b>C</b> ommitment
<b>C</b> atch	<b>C</b> apability
<b>M</b> any	<b>M</b> onitoring
<b>L</b> awbreakers	<b>L</b> earning

### 2. COBIT -- A Framework for IT Governance and Management

- a. COBIT is the best-known control and governance framework that addresses information technology.
  - 1) In its original version, COBIT was focused on controls for specific IT processes.
  - 2) Over the years, information technology has gradually come to pervade every facet of the organization's operations. IT can no longer be viewed as a function distinct from other aspects of the organization.
    - a) The evolution of COBIT has reflected this change in the nature of IT within the organization.

### 3. COBIT 5 -- Five Key Principles

#### a. Principle 1: Meeting Stakeholder Needs

- 1) COBIT 5 asserts that value creation is the most basic stakeholder need. Thus, the creation of stakeholder value is the fundamental goal of any enterprise, commercial or not.
  - a) Value creation in this model is achieved by balancing three components:
    - i) Realization of benefits
    - ii) Optimization (not minimization) of risk
    - iii) Optimal use of resources

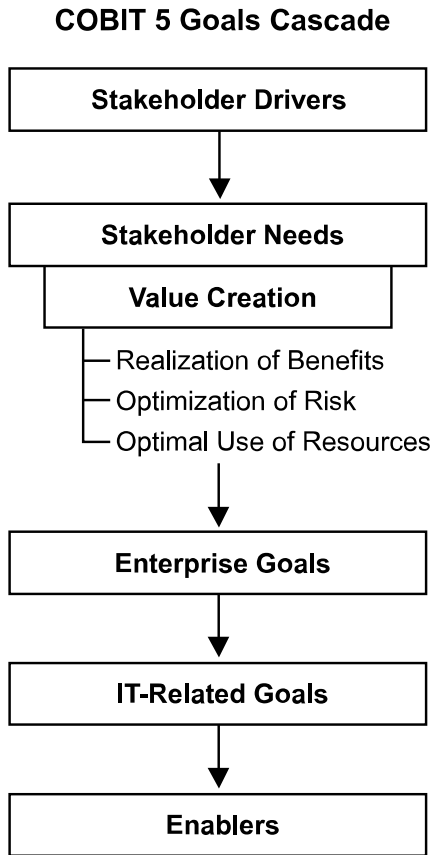


Figure 5-3

- 2) COBIT 5 also recognizes that stakeholder needs are not fixed.
  - a) They evolve under the influence of both internal factors (e.g., changes in organizational culture) and external factors (e.g., disruptive technologies).
  - b) These factors are collectively referred to as stakeholder drivers.
- 3) In response to the identified stakeholder needs, enterprise goals are established.
  - a) COBIT 5 supplies 17 generic enterprise goals that are tied directly to the balanced scorecard model.
- 4) Next, IT-related goals are drawn up to address the enterprise goals.
  - a) COBIT 5 translates the 17 generic enterprise goals into IT-related goals.
- 5) Finally, enablers are identified that support pursuit of the IT-related goals. An enabler is broadly defined as anything that helps achieve objectives.
  - a) The seven categories of enablers are listed in item 3.d. on the next page.
- 6) The process described above is the goals cascade. It can be depicted as in the graphic to the left.

**b. Principle 2: Covering the Enterprise End-to-End**

- 1) COBIT 5 takes a comprehensive view of all of the enterprise's functions and processes. Information technology pervades them all; it cannot be viewed as a function distinct from other enterprise activities.
  - a) Thus, IT governance must be integrated with enterprise governance.
- 2) IT must be considered enterprise-wide and end-to-end, i.e., all functions and processes that govern and manage information "wherever that information may be processed."

**c. Principle 3: Applying a Single, Integrated Framework**

- 1) In acknowledgment of the availability of multiple IT-related standards and best practices, COBIT 5 provides an overall framework for enterprise IT within which other standards can be consistently applied.
- 2) COBIT 5 was developed to be an overarching framework that does not address specific technical issues; i.e., its principles can be applied regardless of the particular hardware and software in use.

d. **Principle 4: Enabling a Holistic Approach**

- 1) COBIT 5 describes seven categories of enablers that support comprehensive IT governance and management:
  - a) Principles, policies, and frameworks
  - b) Processes
  - c) Organizational structures
  - d) Culture, ethics, and behavior
  - e) Information
  - f) Services, infrastructure, and applications
  - g) People, skills, and competencies
- 2) The last three of these enablers also are classified as resources, the use of which must be optimized.
- 3) Enablers are interconnected because they
  - a) Need the input of other enablers to be fully effective and
  - b) Deliver output for the benefit of other enablers.

e. **Principle 5: Separating Governance from Management**

- 1) The complexity of the modern enterprise requires governance and management to be treated as distinct activities.
  - a) In general, governance is the setting of overall objectives and the monitoring of progress toward those objectives. COBIT 5 associates governance with the board of directors.
    - i) Within any governance process, three practices must be addressed: evaluate, direct, and monitor.
  - b) Management is the carrying out of activities in pursuit of enterprise goals. COBIT 5 associates these activities with executive management under the leadership of the CEO.
    - i) Within any management process, four responsibility areas must be addressed: plan, build, run, and monitor.

4. **COBIT 5 Conversion to COBIT 2019**

- a. COBIT 2019 expands on COBIT 5's key principles for a governance system applicable to IT governance to include six **governance system** principles and three **governance framework** principles. A governance system is the rules, practices, and processes that direct and regulate an entity. A governance framework is the structure upon which the governance system is built.
  - 1) The six principles for a **governance system** are summarized as follows:
    - a) Provide **stakeholder value**. Achieving value requires a strategy and a governance system.
    - b) **Holistic** approach. Create synergies among the components interconnected in the system.
      - i) Governance system **components** were called "enablers" under COBIT 5. Components can be **generic** (components applied in principle to any circumstances) or **variant** (components designed for a given purpose or context in a focus area).

- c) **Dynamic** governance system. The governance system must be dynamic when dealing with a change in design factors (e.g., personnel, infrastructure, applications, etc.) and must be accompanied by consideration of its systemic effects.
  - d) Governance **distinct** from management. Governance tasks should be differentiated from management tasks.
  - e) Tailored to **enterprise needs**. The governance system must be designed to meet an organization's requirements.
    - i) **Design factors** affect the blueprint of a governance system.
    - ii) Design factors include, but are not limited to, threat landscape, technology adoption strategy, and enterprise strategy and goals.
  - f) **End-to-end** enterprise coverage. The emphasis is not solely on the IT function but on all information, processes, and technology that contribute to organizational goal achievement.
- 2) The following are three principles for a governance **framework**:
- a) It is **based on a conceptual model**. The governance framework achieves consistency and automation by identifying components and their relationships.
  - b) It is **open and flexible**. The governance framework is flexible and permits inclusion of new content and issues without loss of consistency and integrity.
  - c) It is **aligned with major standards**. The governance framework aligns with relevant regulations, standards, frameworks, and best practices (e.g., the latest IT standards and compliance regulations).
- 3) An IT governance program has two separate phases.
- a) Phase 1. Pre-planning is the development stage. It includes identifying all stakeholders and their needs and designing a course of action to create stakeholder value.
  - b) Phase 2. Program implementation involves activating the system, comparing the status of the system with the system's goals, and making any necessary adjustments to ensure acceptable value is produced.
- b. COBIT 2019 expanded the COBIT model to include 40 governance and management objectives organized into 5 domains.
- 1) Candidates need not memorize these elements. They are included here because they represent one of the foundational shifts from COBIT 5 to COBIT 2019.

- c. Performance management is a crucial element of a governance and management system. It directs all of the components at work toward accomplishing the goals of the organization by providing reliable and relevant outcomes.
- 1) The **COBIT Performance Management (CPM)** model measures performance using capability and maturity levels. CPM concepts and methods align with and extend the Capability Maturity Model Integration Development V2.0 capability and maturity levels (discussed in Study Unit 4, Subunit 4).
    - a) **Capability levels.** The CPM measures performance by using the capability level to quantify how well a **process** is operating, ranging from 0 (no capability or not meeting the intent of any process practices) to 5 (well-defined process or continuous improvement enabled).
    - b) **Maturity levels.** The CPM measures performance by using focus area maturity levels. The six maturity levels, presented in order of maturity, are
      - 0 – Incomplete
      - 1 – Initial
      - 2 – Managed
      - 3 – Defined
      - 4 – Quantitative
      - 5 – Optimizing
    - i) A **focus area** is a governance issue, domain, or topic that is associated with a group of objectives and their components. COBIT 2019 added new focus areas, including cloud computing, cybersecurity, privacy, and small and medium enterprises.

## 5. VAL IT

- a. VAL IT is based on, and complements, COBIT.
- b. Its objective is to establish best practices that contribute to the process of **value** creation. It measures, monitors, and maximizes the realization of business value from investment in IT.
- c. According to ISACA, the VAL IT framework consists of the following three domains:
  - 1) Value governance. This domain defines the relationship between IT and the organization, which includes those functions in the organization with governance responsibilities.
  - 2) Investment management. This domain manages the organization's portfolio of IT-enabled business investments.
  - 3) Portfolio management. This domain maximizes the quality of **business cases** for IT-enabled business investments.
- d. Based on the "Four Ares" (as described by John Thorp in his book, *The Information Paradox—Realizing the Business Benefits of Information Technology*, written jointly with Fujitsu, first published in 1998 and revised in 2003, McGraw-Hill, Canada), business cases must include answers to the following four questions:
  - 1) Is the organization doing the right things?
  - 2) Is the organization doing them the right way?
  - 3) Is the organization getting them done well?
  - 4) Is the organization getting the benefits?

6. **The eSAC Model**

- a. In the eSAC (*Electronic Systems Assurance and Control*) model, the entity’s internal processes accept inputs and produce outputs.
  - 1) **Inputs:** Mission, values, strategies, and objectives
  - 2) **Outputs:** Results, reputation, and learning
- b. The eSAC model’s **broad control objectives** are influenced by the COSO Framework:
  - 1) Operating effectiveness and efficiency
  - 2) Reporting of financial and other management information
  - 3) Compliance with laws and regulations
  - 4) Safeguarding of assets
- c. The following are eSAC’s IT **business assurance objectives**:
  - 1) Availability. The entity must ensure that information, processes, and services are available at all times.
  - 2) Capability. The entity must ensure reliable and timely completion of transactions.
  - 3) Functionality. The entity must ensure that systems are designed to user specifications to fulfill business requirements.
  - 4) Protectability. The entity must ensure that a combination of physical and logical controls prevents unauthorized access to system data.
  - 5) Accountability. The entity must ensure that transactions are processed under firm principles of data ownership, identification, and authentication.
- d. The following is a useful memory aid for the eSAC IT business assurance objectives:

<b>A</b>	<b>A</b> vailability
<b>C</b> ourt	<b>C</b> apability
<b>F</b> inds	<b>F</b> unctionality
<b>P</b> eople	<b>P</b> rotectability
<b>A</b> ccountable	<b>A</b> ccountability

7. **Guides to the Assessment of IT Risks (GAIT)**

- a. GAIT methodology gives management and auditors guidance for assessing the scope of IT general controls using a top-down and risk-based approach.
  - 1) GAIT methodology is consistent with the Public Company Accounting Oversight Board’s Auditing Standard 5 and other control frameworks, e.g., COSO.

- b. The four principles of the GAIT methodology are as follows:
- 1) The identification of risks and related controls in IT general control processes should be a continuation of the top-down and risk-based approach used to identify significant accounts, risks to those accounts, and key controls in the business processes.
  - 2) The IT general control process risks that need to be identified are those that affect critical IT functionality in financially significant applications and related data.
  - 3) The IT general control process risks that need to be identified exist, for example, in application program code, networks, and operating systems.
  - 4) Risks in IT general control processes are mitigated by the achievement of IT control objectives, not individual controls.

## 8. Soft Controls

- a. The COSO and CoCo models emphasize soft controls (also covered in Roth, "Taking a Hard Look at Soft Controls," *Internal Auditor*, February 1998).
- 1) For example, the communication of ethical values and the fostering of mutual trust are soft controls in the CoCo model. In the COSO model, soft controls are part of the control environment.
  - 2) Soft controls should be distinguished from hard controls, such as compliance with specific policies and procedures imposed upon employees from above.
- b. Soft controls have become more necessary as technology advances have empowered employees. Technology has given them access to large amounts of critical information and enabled them to make decisions formerly made by those higher in the organizational structure.
- 1) In addition to making many hard controls obsolete, technology advances also have permitted the automation of hard controls, for example, the embedding of audit modules in computer programs.
- c. One approach to auditing soft controls is **control self-assessment (CSA)**. It is the involvement of management and staff in the assessment of internal controls within their workgroup.
- d. Hard and soft controls can be associated with particular risks and measured. The vulnerability addressed can be stated as the product of the probability of occurrence and the significance of the occurrence ( $V = P \times S$ ).

# STUDY UNIT SIX

## CONTROLS: APPLICATION

6.1	<i>Flowcharts and Process Mapping</i> .....	1
6.2	<i>Accounting Cycles and Associated Controls</i> .....	6
6.3	<i>Management Controls</i> .....	20

This study unit is the fourth of four covering **Domain V: Governance, Risk Management, and Control** from The IIA's CIA Exam Syllabus. This domain makes up 35% of Part 1 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 FLOWCHARTS 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:












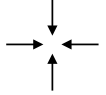



	Starting or ending point or point of interruption
	Input or output of a document or report
	Computer operation or group of operations
	Manual processing operation, e.g., prepare document
	Generalized symbol for input or output used when the medium is not specified
	Hard drive used for input or output
	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 6-1

### 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. Accordingly, activities, controls, and document flows that are the responsibility of a given department or function are shown in the same column. **PO** is a purchase order, and **AP** is accounts payable. The following is an example:

**Horizontal (System) Flowchart**

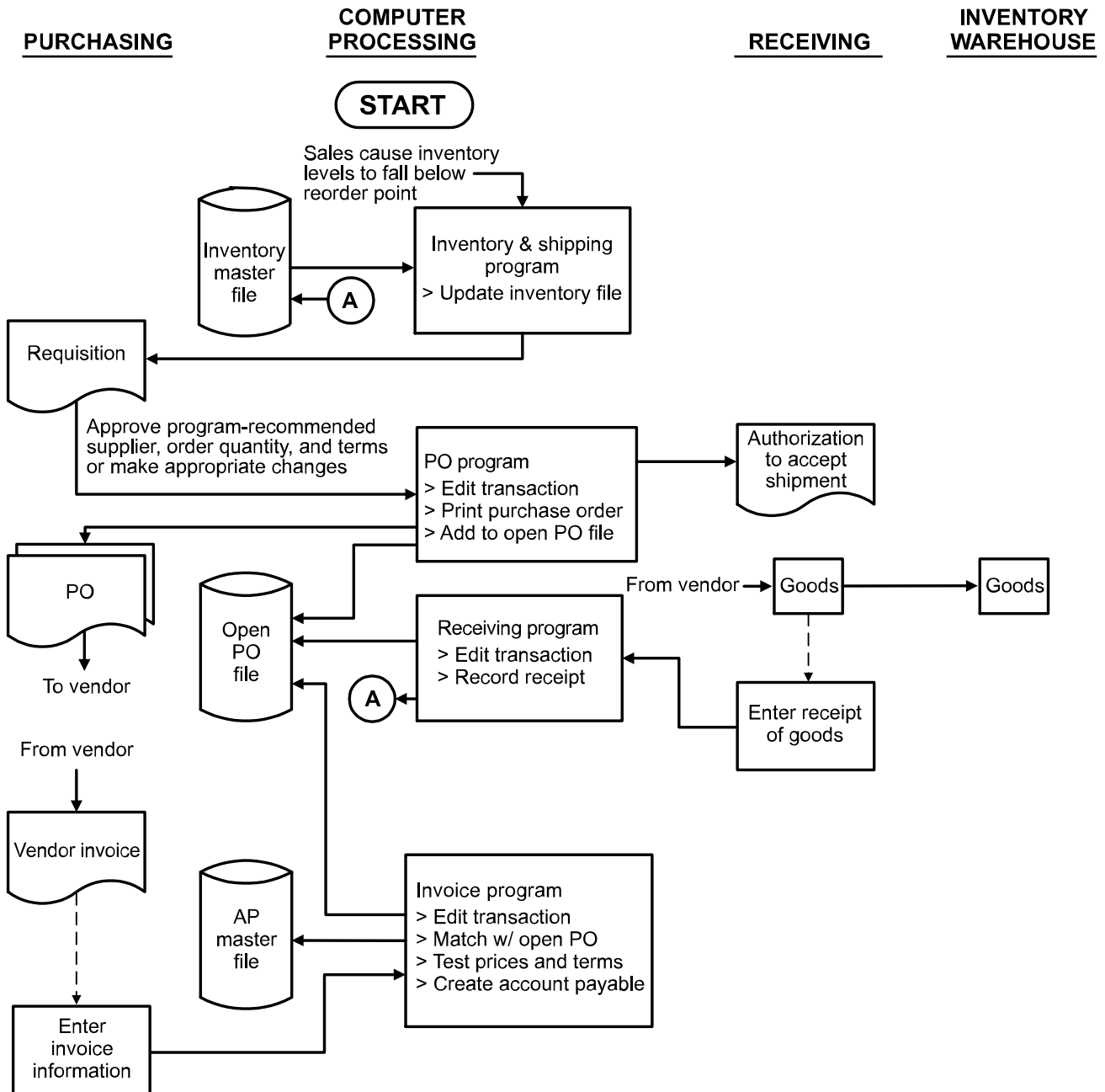


Figure 6-2

#### 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

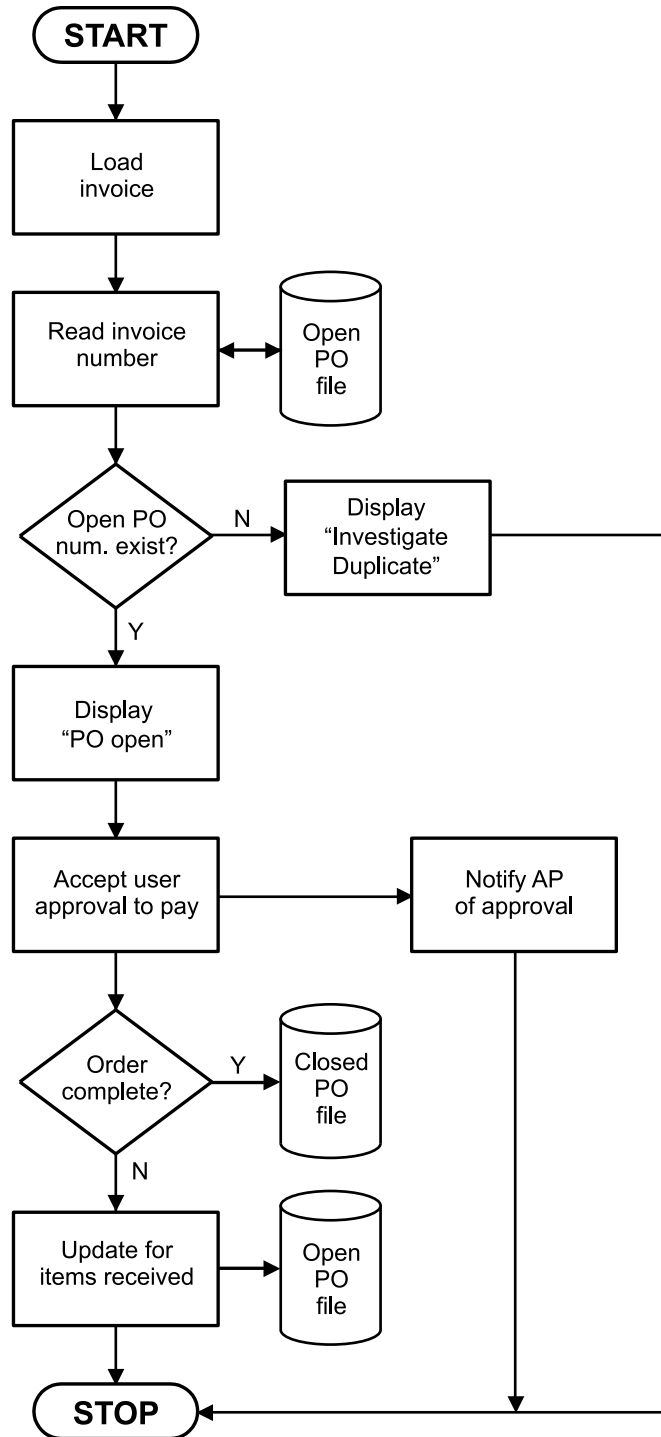


Figure 6-3

**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 to the right:
  - 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.

**Data Flow Diagram Symbols**

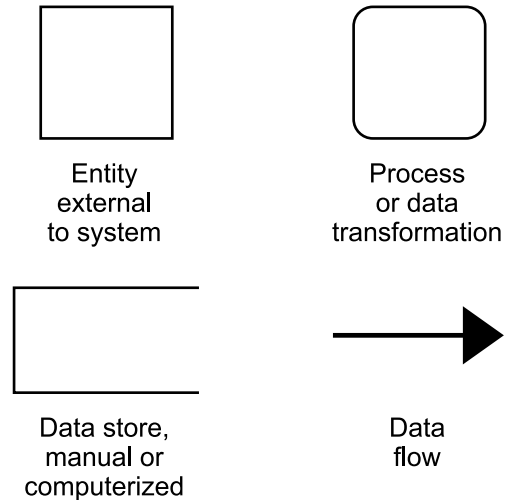


Figure 6-4

**6. Process Mapping**

a. Process mapping is a simple form of flowcharting used to depict a client process. Below is an example of a process map.

**Process Map for Invoice Processing in Purchasing Department**

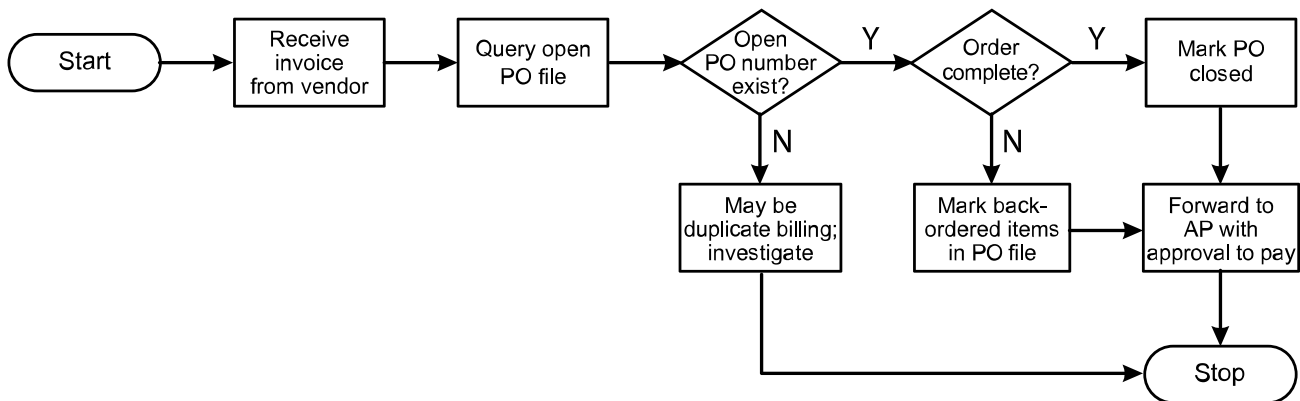


Figure 6-5

## 6.2 ACCOUNTING CYCLES AND ASSOCIATED CONTROLS

### 1. Internal Controls

- a. A properly designed system of internal controls should reduce the risk of errors and prevent an individual from perpetrating and concealing fraud. The structure of an organization and the assignment of job duties should be designed to segregate certain functions within this environment.
  - 1) Cost-benefit criteria must be considered.

### 2. Segregation of Duties

- a. For any given transaction, the following three functions preferably should be performed by separate individuals in different parts of the organization:
  - 1) Authorization of the transaction
  - 2) Recording of the transaction
  - 3) Custody of the assets associated with the transaction
    - a) The following memory aid is for the functions that should be kept separate for proper segregation of duties:

<b>A</b>	Authorization
<b>R</b>	Recordkeeping
<b>C</b>	Custody

- b. The internal control system is designed to detect fraud by one person but not fraud by collusion or management override.



**SUCCESS TIP**

CIA candidates must understand segregation of duties, a basic principle of internal control. Expect multiple questions on this topic.

### 3. Organizational Hierarchy

- a. In a medium-sized or larger organization, adequate segregation of duties can be achieved by separating the responsibilities of the following corporate-level executives:

VP of Operations	Chief Accounting Officer (Controller)	Treasurer	VP of Administration	VP of Human Resources
Sales Inventory Warehouse Receiving Shipping Production Purchasing	Accounts Receivable Billing Accounts Payable General Ledger Inventory Control Cost Accounting Payroll	Cash Receipts Cash Disbursements Credit	Mail Room	Human Resources

- b. Please note that not all questions on the CIA exam will follow this format.

#### 4. Accounting Cycles

- a. The accounting process can be described in terms of five cycles:
  - 1) Sales to customers on credit and recognition of receivables
  - 2) Collection of cash from customer receivables
  - 3) Purchases on credit and recognition of payables
  - 4) Payment (disbursement) of cash to satisfy trade payables
  - 5) Payment of employees for work performed and allocation of costs
- b. On the following pages are five flowcharts and accompanying tables depicting the steps in the 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.



#### SUCCESS TIP

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

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

The following detailed explanations of the accounting cycles do **not** need to be memorized. However, you should be able to understand them, and you may be able to relate these generic cycles to how the organization you work for handles them. If you understand these cycles and their respective control techniques, you should be able to answer any type of question about accounting cycles and their controls on the CIA exam.

Please note that not all questions on the CIA exam will follow the exact cycles described on the following pages.

#### 5. Sales-Receivables-Cash Receipts – Responsibilities of Personnel

- a. The following are the responsibilities of personnel or departments in the sales-receivables-cash receipts cycle:
  - 1) **Sales** prepares sales orders based on customer orders.
  - 2) **Credit** reports to the treasurer, authorizes credit for all new customers, and initiates write-off of credit losses. Credit checks should be performed before credit approval.
  - 3) **Inventory Warehouse** maintains physical custody of products.
  - 4) **Inventory Control** maintains records of quantities of products in the Inventory Warehouse.
  - 5) **Shipping** prepares shipping documents and ships products based on authorized sales orders.
  - 6) **Billing** prepares customer invoices based on goods shipped.
  - 7) **Accounts Receivable** maintains the accounts receivable subsidiary ledger.
  - 8) **Mail Room** receives mail and prepares initial cash receipts records.
  - 9) **Cash Receipts** safeguards and promptly deposits cash receipts.
  - 10) **General Ledger** maintains the accounts receivable control account and records sales. Daily summaries of sales are recorded in a sales journal. Totals of details from the sales journal are usually posted monthly to the general ledger.
  - 11) **Receiving** prepares receiving reports and handles all receipts of goods or materials, including sales returns.

6. Sales-Receivables Flowchart

- a. Study the flowchart below. Understand and visualize the sales-receivables process and controls. The flowchart begins at "Start." Read the business activity and internal control descriptions in the table on the next page as needed.

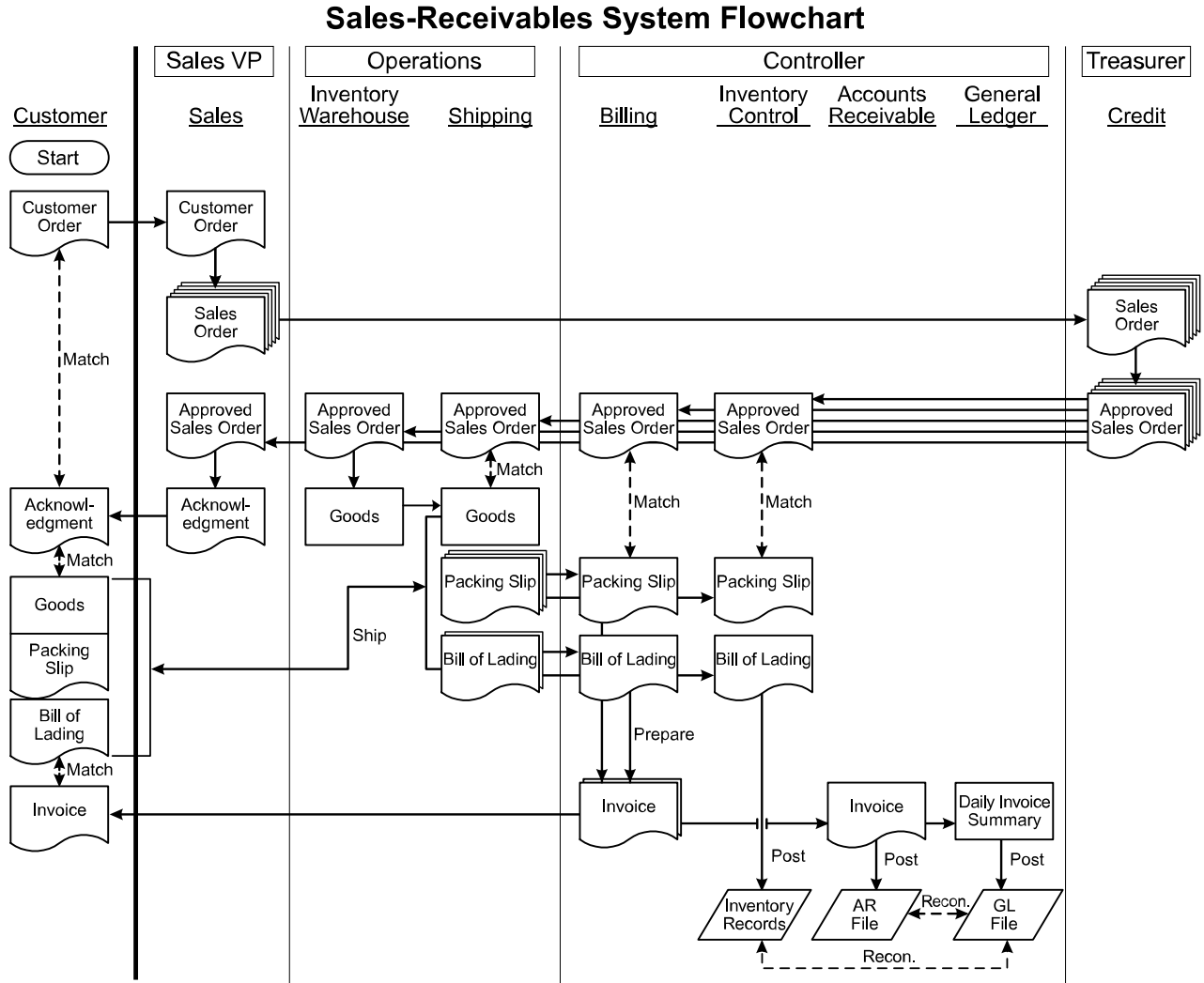


Figure 6-6

**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 <b>customer order</b> and prepares a multi-part <b>sales order</b> 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 <b>sales order</b> .					Ensures that goods are shipped only to actual customers and that the account is unlikely to become delinquent.			
3	Credit sends copies of the <b>approved sales order</b> to Sales, Inventory Warehouse, Shipping, Billing, and Inventory Control.					Notifies these departments that a legitimate sale has been made.			
4	Upon receipt of the <b>approved sales order</b> , Sales sends an <b>acknowledgment</b> to the customer.					The customer's expectation of receiving goods reduces the chances of misrouting or misappropriation.			
5	Upon receipt of the <b>approved sales order</b> , 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 <b>approved sales order</b> , prepares a <b>packing slip</b> and a <b>bill of lading</b> , and ships the goods to the customer.					Ensures that the correct goods are shipped.			
7	Shipping forwards a copy of the <b>packing slip</b> and <b>bill of lading</b> to Inventory Control and Billing.					Notifies these departments that the goods have been shipped.			
8	Upon receipt of the <b>packing slip</b> and <b>bill of lading</b> , Inventory Control matches them with the <b>approved sales order</b> and updates the inventory records.					Ensures that inventory records are updated once the goods have been shipped.			
9	Upon receipt of the <b>packing slip</b> and <b>bill of lading</b> , Billing matches them with the <b>approved sales order</b> , prepares a multi-part <b>invoice</b> , and sends a copy to the customer. Typically, a <b>remittance advice</b> 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 <b>invoice</b> copy from Billing and posts a journal entry to the AR file.					Ensures that customer accounts are kept current.			
11	Accounts Receivable prepares a <b>daily invoice summary</b> 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 <b>daily invoice summary</b> 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.			



7. Cash Receipts Flowchart

- a. Study the flowchart below. Understand and visualize the cash receipts process and controls. The flowchart begins at "Start." Read the business activity and internal control descriptions in the table on the next page as needed.

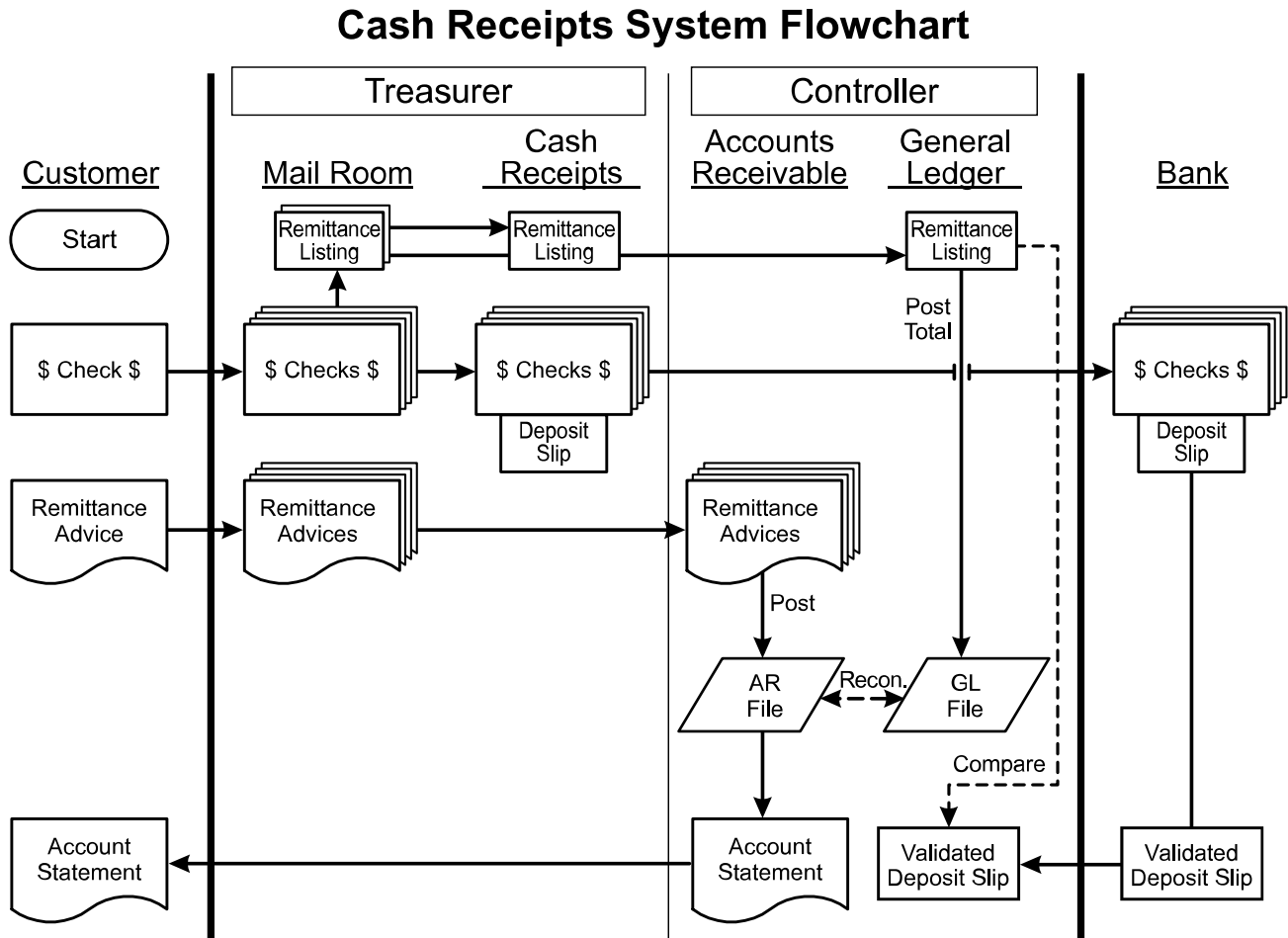


Figure 6-7

**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 <b>checks</b> are immediately endorsed "For Deposit Only into Account XXX." <b>Remittance advices</b> 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 <b>remittance listing</b> of all <b>checks</b> 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 <b>deposit slip</b> and deposits checks in Bank. Bank validates the <b>deposit slip</b> .	Bank provides independent evidence that the full amount was deposited.
4	Mail Room sends <b>remittance advices</b> 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 <b>remittance listing</b> 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	<b>Validated deposit slip</b> is returned to General Ledger to compare with <b>remittance listing</b> .	Ensures that all cash listed on the remittance listing from the Mail Room was deposited.
7	Accounts Receivable periodically sends an <b>account statement</b> to customers showing all sales and payment activity.	Customers will complain about mistaken billings or missing payments.

## 8. Purchases-Payables-Cash Disbursements – Responsibilities of Personnel

- a. Responsibilities of personnel and departments in the purchases-payables-cash disbursements cycle include the following:
  - 1) **Inventory Control** provides authorization for the purchase of goods and performs an accountability function (e.g., Inventory Control is responsible for maintaining perpetual records for inventory quantities and costs).
  - 2) **Purchasing** issues purchase orders for required goods.
  - 3) **Receiving** accepts goods for approved purchases, counts and inspects the goods, and prepares the receiving report.
  - 4) **Inventory Warehouse** provides physical control over the goods.
  - 5) **Accounts Payable** (vouchers payable) assembles the proper documentation to support a payment voucher (and disbursement) and records the account payable.
  - 6) **Cash Disbursements** evaluates the documentation to support a payment voucher and signs and mails the check.
    - a) This department cancels the documentation to prevent duplicate payment.
  - 7) **General Ledger** maintains the accounts payable control account and other related general ledger accounts.

- b. Study the flowchart below. Understand and visualize the purchases-payables process and controls. The flowchart begins at "Start." Read the business activity and internal control descriptions in the table on the next page as needed.

### Purchases-Payables System Flowchart

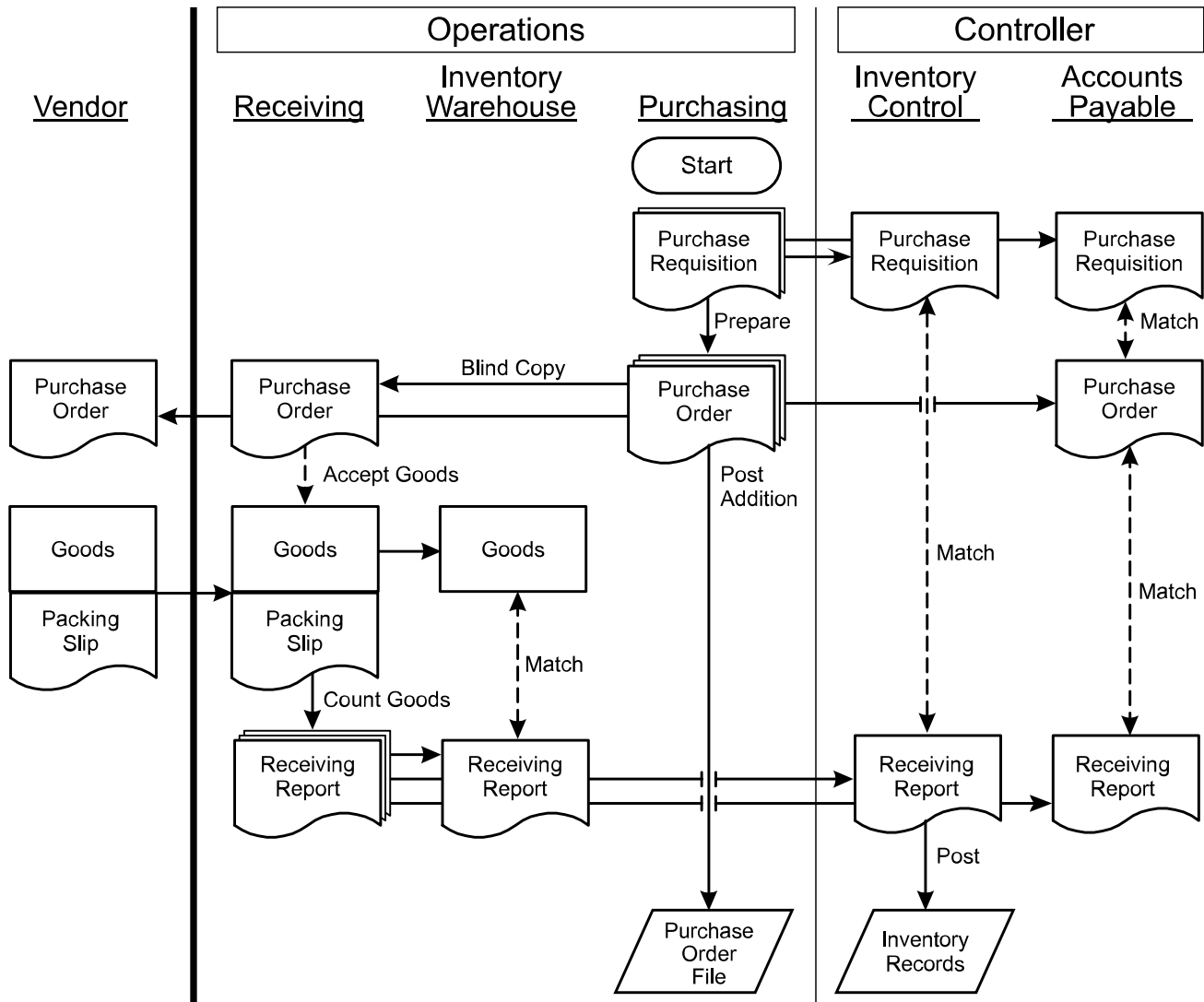


Figure 6-8

NOTE: Nothing is recorded in the general ledger for issuing a purchase order. A liability is not created until the goods and invoice are received (see the Cash Disbursements System Flowchart in Figure 6-9).

**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 <b>purchase requisition</b> 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 <b>purchase order</b> , and updates the purchase order file.	<ul style="list-style-type: none"> <li>• Purchasing ensures that goods are bought only from vendors who have been preapproved for reliability.</li> <li>• Reconciling sequentially numbered purchase orders helps ensure that orders are legitimate.</li> </ul>
3	Purchasing sends the <b>purchase order</b> to Vendor, Receiving, and Accounts Payable. Receiving's copy has blank quantities.	<ul style="list-style-type: none"> <li>• Receiving is put on notice to expect shipment.</li> <li>• Accounts Payable is put on notice that liability to this vendor will increase when goods arrive.</li> </ul>
4	When goods arrive, Receiving accepts goods based on the file copy of the <b>purchase order</b> , prepares a <b>receiving report</b> , and forwards the <b>receiving report</b> 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 <b>receiving report</b> .	Detects any loss or damage between Receiving and the Inventory Warehouse. Inventory Warehouse accepts responsibility for safeguarding received goods.
6	Receiving sends the <b>receiving report</b> to Inventory Control for matching with the <b>purchase requisition</b> and updating of inventory records.	Ensures that inventory records are current.
7	Receiving also sends a copy of the <b>receiving report</b> to Accounts Payable for matching with the <b>purchase order</b> and <b>purchase requisition</b> .	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).

- c. Study the flowchart below. Understand and visualize the cash disbursements process and controls. The flowchart begins at "Start." Read the business activity and internal control descriptions in the table on the next page as needed.

### Cash Disbursements System Flowchart

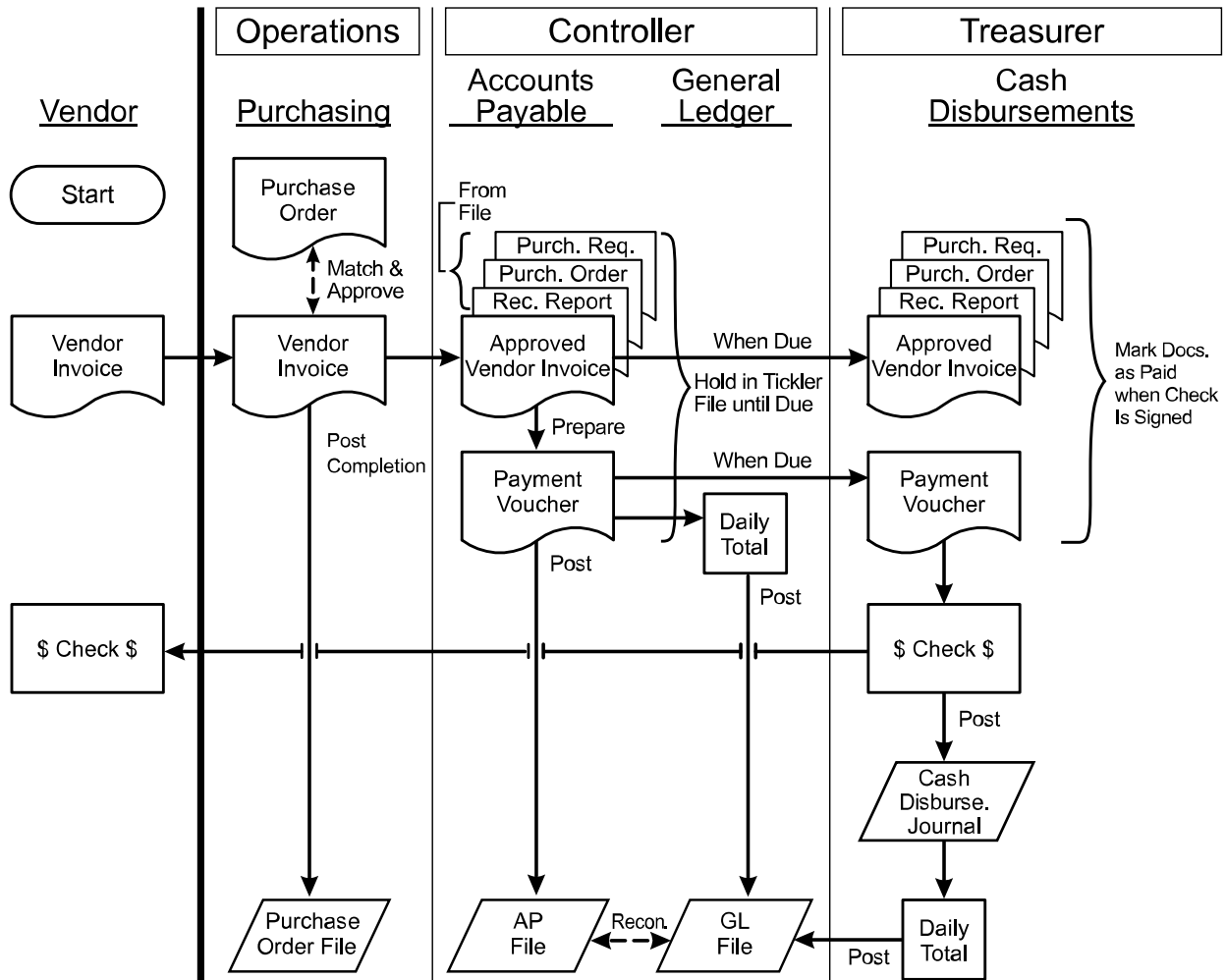


Figure 6-9

**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 <b>vendor invoice</b> . The <b>vendor invoice</b> is matched with the <b>purchase order</b> and approved for payment. The <b>purchase order</b> is marked as closed in the purchase order file if completed, and the <b>approved vendor invoice</b> is forwarded to Accounts Payable.	<ul style="list-style-type: none"> <li>• Purchasing ensures the vendor invoiced for the proper amount and the terms are as agreed.</li> <li>• Purchasing can follow up on partially filled orders.</li> </ul>
2	Accounts Payable matches the <b>approved vendor invoice</b> with the file copies of the <b>purchase requisition, purchase order, and receiving report</b> and prepares a <b>payment voucher</b> . The <b>payment voucher</b> is recorded in the accounts payable file.	<ul style="list-style-type: none"> <li>• Matching all documents provides assurance that only goods that were appropriately ordered, received, and invoiced are recorded as a liability.</li> <li>• 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.</li> </ul>
3	The <b>payment voucher</b> , with the attached documents, is filed in a tickler file by due date. The <b>daily total</b> 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 <b>payment voucher</b> and attached documents are removed from the tickler file sent to Cash Disbursements for <b>check</b> preparation, signing, and mailing. The <b>check</b> is recorded in the cash disbursements journal.	<ul style="list-style-type: none"> <li>• Cash Disbursements cannot issue a check without an approved payment voucher.</li> <li>• Large payments may require two signatures on the check to provide additional oversight.</li> </ul>
5	The <b>payment voucher</b> and attached documents are stamped "Paid," and the <b>check</b> is mailed to the vendor.	Stamping the documents "Paid" prevents them from supporting a second, illicit payment voucher.
6	The <b>daily total</b> 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.

d. Other Payment Authorizations

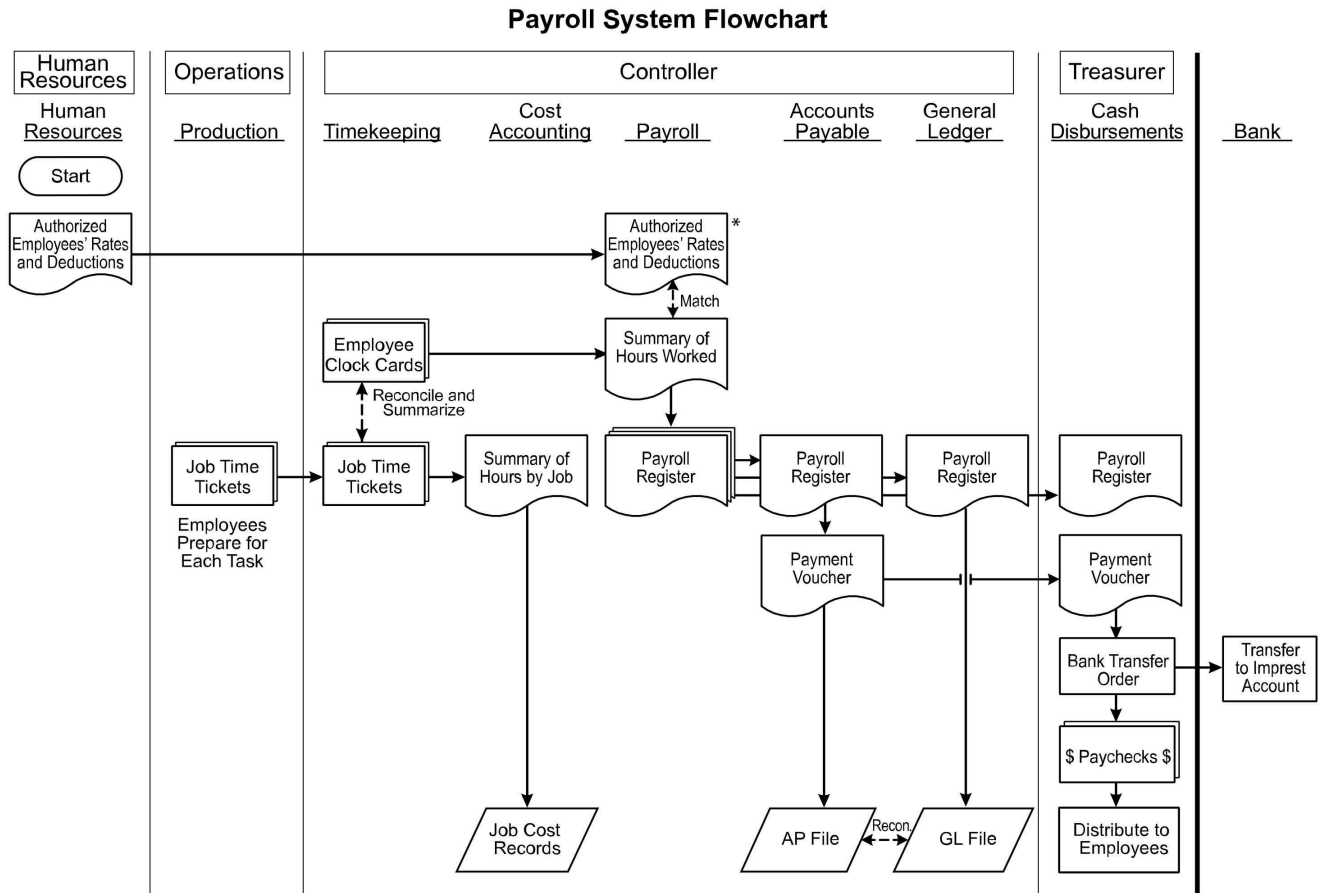
- 1) This voucher disbursement system is applicable to virtually all required payments by the entity, not just purchases of inventory as described previously. The following are additional considerations:
  - a) The authorizations may come from other departments based on a budget or policy (e.g., a utility bill might need authorization by the plant manager).
  - b) Accounts Payable requires different document(s) (e.g., a utility bill with the signature of the plant manager) to support the preparation of the payment voucher and check.
  - c) A debit other than inventory (e.g., utilities expense) is entered on the payment voucher and recorded in the general ledger. Accounts payable is still credited.
  - d) The use of the tickler file and the functions of Cash Disbursements do not change when other types of payments are made.

9. **Payroll – Responsibilities of Personnel**

- a. The following are the responsibilities of organizational subunits in the payroll cycle:
  - 1) **Human Resources** provides an authorized list of employees and associated pay rates, deductions, and exemptions.
  - 2) **Payroll** is an accounting function responsible for calculating the payroll (i.e., preparing the payroll register) based on authorizations from Human Resources and the authorized time records from Timekeeping.
  - 3) **Timekeeping** is an accounting function that oversees the employees' recording of hours on clock cards (using the time clock) and that receives and reconciles the job time tickets from Production.
  - 4) **Production** manufactures the products.
  - 5) **Cost Accounting** is an accounting function that accumulates direct materials, direct labor, and overhead costs on job order cost sheets to determine the costs of production.
  - 6) **Accounts Payable** prepares the payment voucher based on the payroll register prepared by Payroll.
  - 7) **Cash Disbursements** signs and deposits a check based on the payment voucher into a separate payroll account, prepares individual employee paychecks, and distributes paychecks.
  - 8) **General Ledger** records the payroll.



- b. Study the flowchart below. Understand and visualize the payroll process and controls. The flowchart begins at "Start." Read the business activity and internal control descriptions in the table on the next page as needed.



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

Figure 6-10

Payroll System Flowchart Table

Function	Authorization		Custody		Recording				
Department	Human Resources	Production	Cash Disbursements	Bank	Time-keeping	Cost Accounting	Payroll	Accounts Payable	General Ledger
Step	Business Activity				Internal Control				
1	Human Resources sends an <b>authorized employees' rates and deductions</b> 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 <b>employee clock cards</b> held in Timekeeping.				The recording process mechanically or electronically captures employee work hours.				
3	Production employees record time worked on various tasks on <b>job time tickets</b> .				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 <b>job time tickets</b> and forwards them to Timekeeping, where they are reconciled with the <b>employee clock cards</b> .				Ensures that employees worked only authorized hours. Reconciles the time allocated to direct and indirect labor with total time worked.				
5	Timekeeping prepares a <b>summary of hours worked</b> by employee and forwards it to Payroll. Payroll matches it with the <b>authorized employees' rates and deductions</b> list and prepares a <b>payroll register</b> .				Ensures that employees are paid the proper amount.				
6	Timekeeping prepares a <b>summary of hours worked by job</b> 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 <b>payroll register</b> from Payroll, prepares a <b>payment voucher</b> , and forwards it along with the <b>payroll register</b> to Cash Disbursements.				Ensures that a payable is accrued. Authorizes the transfer of cash to the payroll imprest account.				
8	Payroll also forwards the <b>payroll register</b> 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 <b>payment voucher</b> with the <b>payroll register</b> 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	<b>Paychecks</b> 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.				

## 6.3 MANAGEMENT CONTROLS

### 1. Roles and Responsibilities

#### a. Management

- 1) The chief executive officer (CEO) should establish the tone at the top. Organizations reflect the ethical values and control consciousness of the CEO.
- 2) The chief accounting officer also has a crucial role to play. Accounting staff have insight into activities across all levels of the organization.

#### b. Board of Directors

- 1) The entity's commitment to integrity and ethical values is reflected in the board's selections for senior management positions.
- 2) To be effective, board members should be capable of objective judgment, have knowledge of the organization's industry, and be willing to ask the relevant questions about management's decisions.
- 3) Important subcommittees of the board in organizations of sufficient size and complexity include the audit committee, the compensation committee, the finance committee, and the risk committee.

#### c. Internal Auditors

- 1) Management is ultimately responsible for the design and function of the system of internal controls. However, an organization's internal audit function may play an important consulting and advisory role.
- 2) The internal audit function also evaluates the soundness of the system of internal control by performing systematic reviews according to professional standards.
- 3) To remain independent in the conduct of these reviews, the internal audit function cannot be responsible for selecting and executing controls.

#### d. Other Personnel

- 1) Everyone in the entity must be involved in internal control and is expected to perform his or her appropriate control activities.
- 2) In addition, all employees should understand that they are expected to inform those higher in the entity of instances of poor control when controls are not functioning as intended.

### 2. Imposed Control and Self-Control

- a. Imposed control is the traditional, mechanical approach. It measures performance against standards and then takes corrective action through the individual responsible for the function or area being evaluated.
  - 1) Though common, it has the drawback that corrective action tends to come after performance. The result may be a response to poor performance rather than its prevention.
- b. Self-control evaluates the entire process of management and the functions performed. Thus, it attempts to improve that process instead of simply correcting the specific performance of the manager. Management by objectives is an example.
- c. Well-designed procedures that are set aside at management's discretion are not adequate controls.
  - 1) Control procedures must be followed consistently to be effective.
- d. The cost of internal auditing must not be greater than its benefit.

### 3. Alternative Definition of Control

- a. Sawyer, Dittenhofer, and Scheiner, in *Sawyer's Internal Auditing* (Altamonte Springs, FL, The Institute of Internal Auditors, 5th ed., 2003, pages 82-86), define control and describe the means of achieving control. Their definition of control is as follows:

*The employment of all the means devised in an enterprise to promote, direct, restrain, govern, and check upon its various activities for the purpose of seeing that enterprise objectives are met. These means of control include, but are not limited to, form of organization, policies, systems, procedures, instructions, standards, committees, charts of accounts, forecasts, budgets, schedules, reports, records, checklists, methods, devices, and internal auditing.*

NOTE: The author prefers the definition in Sawyer's 5th edition rather than those in later editions. It may be more helpful to CIA candidates.

### 4. Organization

- a. Organization, as a means of control, is an approved intentional structuring of roles assigned to people within the organization so that it can achieve its objectives efficiently and economically.
  - 1) Responsibilities should be divided so that no one person will control all phases of any transaction (this is discussed in further detail in Subunit 6.2).
  - 2) Managers should have the authority to take the action necessary to discharge their responsibilities.
  - 3) Individual responsibility always should be clearly defined so that it can be neither sidestepped nor exceeded.
  - 4) An official who assigns responsibility and delegates authority to subordinates should have an effective system of follow-up. Its purpose is to ensure that tasks assigned are properly carried out.
  - 5) The individuals to whom authority is delegated should be allowed to exercise that authority without close supervision. But they should check with their superiors in case of exceptions.
  - 6) People should be required to account to their superiors for the manner in which they have discharged their responsibilities.
  - 7) The organization should be flexible enough to permit changes in its structure when operating plans, policies, and objectives change.
  - 8) Organizational structures should be as simple as possible.
  - 9) Organization charts and manuals should be prepared. They help plan and control changes in, as well as provide better understanding of, the organization, chain of authority, and assignment of responsibilities.

## 5. Policies

- a. A policy is any stated principle that requires, guides, or restricts action. Policies should follow certain principles.
  - 1) Policies should be clearly stated in writing in systematically organized handbooks, manuals, or other publications and should be properly approved. But when the organizational culture is strong, the need for formal, written policies is reduced. In a strong culture, substantial training results in a high degree of acceptance of the organization's key values. Thus, such values are intensely held and widely shared.
  - 2) Policies should be systematically communicated to all officials and appropriate employees of the organization.
  - 3) Policies must conform with applicable laws and regulations. They should be consistent with objectives and general policies prescribed at higher levels.
  - 4) Policies should be designed to promote the conduct of authorized activities in an effective, efficient, and economical manner. They should provide a satisfactory degree of assurance that resources are suitably safeguarded.
  - 5) Policies should be periodically reviewed. They should be revised when circumstances change.

## 6. Procedures

- a. Procedures are methods employed to carry out activities in conformity with prescribed policies. The same principles applicable to policies also are applicable to procedures. In addition,
  - 1) To reduce the possibility of fraud and error, procedures should be coordinated so that one employee's work is automatically checked by another who is independently performing separate prescribed duties. The extent to which automatic internal checks should be built into the system of control depends on many factors. Examples are (a) degree of risk, (b) cost of preventive procedures, (c) availability of personnel, (d) operational impact, and (e) feasibility.
  - 2) For nonmechanical operations, prescribed procedures should not be so detailed as to stifle the use of judgment.
  - 3) To promote maximum efficiency and economy, prescribed procedures should be as simple and as inexpensive as possible.
  - 4) Procedures should not be overlapping, conflicting, or duplicative.
  - 5) Procedures should be periodically reviewed and improved as necessary.

## 7. Personnel

- a. People hired or assigned should have the qualifications to do the jobs assigned to them. The best form of control over the performance of individuals is supervision. Hence, high standards of supervision should be established. The following practices help improve control:
  - 1) New employees should be investigated as to honesty and reliability.
  - 2) Employees should be given training that provides the opportunity for improvement and keeps them informed of new policies and procedures.
  - 3) Employees should be given information on the duties and responsibilities of other segments of the organization. They will better understand how and where their jobs fit into the organization as a whole.
  - 4) The performance of all employees should be periodically reviewed to see whether all essential requirements of their jobs are being met. Superior performance should be given appropriate recognition. Shortcomings should be discussed with employees so that they are given an opportunity to improve their performance or upgrade their skills.

## 8. Accounting

- a. Accounting is the indispensable means of financial control over activities and resources. It is a framework that can be fitted to assignments of responsibility. Moreover, it is the financial scorekeeper of the organization. The problem lies in what scores to keep. Some basic principles for accounting systems follow:
  - 1) Accounting should fit the needs of managers for rational decision making rather than the dictates of a textbook or check list.
  - 2) Accounting should be based on lines of responsibility.
  - 3) Financial reports of operating results should parallel the organizational units responsible for carrying out operations.
  - 4) Accounting should permit controllable costs to be identified.

## 9. Budgeting

- a. A budget is a statement of expected results expressed in numerical terms. As a control, it sets a standard for input of resources and what should be achieved as output and outcomes.
  - 1) Those who are responsible for meeting a budget should participate in its preparation.
  - 2) Those responsible for meeting a budget should be provided with adequate information that compares budgets with actual events and shows reasons for any significant variances.
    - a) Management should ensure it receives prompt feedback on performance variances.
  - 3) All subsidiary budgets should tie into the overall budget.
  - 4) Budgets should set measurable objectives. Budgets are meaningless unless managers know why they have a budget.
  - 5) Budgets should help sharpen the organizational structure. Objective budgeting standards are difficult to set in a confused combination of subsystems. Budgeting is therefore a form of discipline and coordination.

**10. Reporting**

- a. In most organizations, management functions and makes decisions on the basis of reports it receives. Thus, reports should be timely, accurate, meaningful, and economical. The following are some principles for establishing a satisfactory internal reporting system:
  - 1) Reports should be made in accordance with assigned responsibilities.
  - 2) Individuals or units should be required to report only on those matters for which they are responsible.
  - 3) The cost of accumulating data and preparing reports should be weighed against the benefits to be obtained from them.
  - 4) Reports should be as simple as possible and consistent with the nature of the subject matter. They should include only information that serves the needs of the readers. Common classifications and terminology should be used as much as possible to avoid confusion.
  - 5) When appropriate, performance reports should show comparisons with predetermined standards of cost, quality, and quantity. Controllable costs should be segregated.
  - 6) When performance cannot be reported in quantitative terms, the reports should be designed to emphasize exceptions or other matters requiring management attention.
  - 7) For maximum value, reports should be timely. Timely reports based partly on estimates may be more useful than delayed reports that are more precise.
  - 8) Report recipients should be polled periodically to see whether they still need the reports they are receiving or whether the reports could be improved.

**11. Examples of Management Controls**

- a. The following charts present examples of some management controls, their objectives, the related assertions, and the reasons for implementing the controls.

<b>Production</b>		
<b>Objective</b>	<b>Assertion</b>	<b>Control(s)</b>
<p>Only quality materials are used in production.</p>	<p>Occurrence →</p> <p><b>WHY?</b></p>	<p>Require materials specifications for all purchases.</p>
<p>Materials specifications minimize defects in finished goods.</p>		
<p>Identify the cause of defects in finished goods inventory.</p>	<p>Occurrence →</p> <p><b>WHY?</b></p>	<p>Timely follow-up on all unfavorable usage variances.</p>
<p>Follow-up on unfavorable usage variances may lead to detection and correction of the use of substandard materials.</p>		
<p>-- Continued on next page --</p>		

<b>Production (Continued)</b>		
<b>Objective</b>	<b>Assertion</b>	<b>Control(s)</b>
Detect production problems and excessive costs and inventories.	Existence →	Compare actual production with management forecasts.
<p><b>WHY?</b></p> <p>Comparing actual costs with budgeted costs detects unfavorable cost variances and production problems.</p>		

<b>Debt and Equity Instruments</b>		
<b>Objective</b>	<b>Assertion</b>	<b>Control(s)</b>
Safeguard debt and equity instruments from unauthorized use (e.g., pledge as security for personal financing).	Existence →	Segregation of responsibility for custody of assets and recording of transactions.
<p><b>WHY?</b></p> <p>One individual with no accounting responsibilities or power to authorize transactions should have custody of liquid assets.</p>		
The proper execution of debt and equity transactions in accordance with management's wishes.	Existence →	Written policies requiring review of major funding or repayment proposals by the board.
<p><b>WHY?</b></p> <p>When a decision affects the capitalization of the entity, a policy should require review at the highest level.</p>		

<b>Cash</b>		
<b>Objective</b>	<b>Assertion</b>	<b>Control(s)</b>
Identify cash receipts recorded in the general ledger but not deposited.	Completeness →	Bank reconciliations performed by a third party.
<p><b>WHY?</b></p> <p>A bank reconciliation compares the bank statement with the organization's records and resolves differences caused by deposits in transit, outstanding checks, NSF checks, bank charges, errors, etc. An independent third party should prepare bank reconciliations to detect unexplained discrepancies between recorded deposits and the bank statements.</p>		



<b>Inventory</b>		
<b>Objective</b>	<b>Assertion</b>	<b>Control(s)</b>
<p>Physically protect assets such as tools, equipment, and vehicles from unauthorized access.</p>	<p>Existence →</p>	<p>Place tools, equipment, and vehicles in a secured area; install a keycard access system for all employees; and record each keycard access transaction on a report for the production superintendent.</p>
<p><b>WHY?</b></p> <p>Tools, equipment, and vehicles should be secured from theft using physical controls.</p>		
<p>Safeguard tools, equipment, and vehicles from unauthorized use.</p>	<p>Existence →</p>	<p>Tools, equipment, and vehicles inventory should be in the custody of inventory staging supervisors. Special requisitions should be required to issue tools, equipment, and vehicles to assist with recording the amount of tools removed from the inventory.</p>
<p><b>WHY?</b></p> <p>Assigning functional responsibility for custody of assets to one individual with no ability to authorize transactions or record them establishes accountability. Requiring that requisitions be submitted by appropriate persons is a control to ensure that their use is properly authorized. Moreover, items requisitioned should be consistent with the items typically used in the process performed.</p>		
<p>Items ordered are received by authorized locations.</p>	<p>Existence →</p>	<p>The receiving function verifies that the items received are those actually sent by the shipper.</p>
<p><b>WHY?</b></p> <p>Without verification of the receiving function, items could be lost, stolen, or sent to the wrong recipients.</p>		
<p>Confirm that inventory items (including financial instruments) listed on inventory reports actually exist.</p>	<p>Existence →</p>	<p>Physical inventories should be periodically reconciled with accounting records.</p>
<p><b>WHY?</b></p> <p>Auditors should make test counts of inventory.</p>		
<p>-- Continued on next page --</p>		

<b>Inventory (Continued)</b>		
<b>Objective</b>	<b>Assertion</b>	<b>Control(s)</b>
<p>Reduce risks associated with disposal of obsolete and scrap materials.</p>	<p>Existence →</p>	<p>Require managerial approval for materials to be declared scrap or obsolete. A commission is paid to the individual or organization assisting with selling obsolete or scrap materials.</p>
<b>WHY?</b>		
<p>Management approval of disposal reduces the risk of misappropriation of materials. Specifying that a commission be paid to the individual or organization assisting with selling the materials is an incentive to maximize the organization's return.</p>		
<p>Ensure prompt delivery of out-of-stock items.</p>	<p>Existence →</p>	<p>Match the back order file with goods received daily.</p>
<b>WHY?</b>		
<p>Matching back orders with daily receipts determines whether out-of-stock items are promptly replaced and identifies goods received that require immediate deliveries to customers.</p>		
<p>Maintain adequate inventory quantities.</p>	<p>Existence →</p>	<p>Increase inventory levels. Implement electronic data interchange with suppliers. Reconcile the sum of filled and back orders with the total of all orders placed daily.</p>
<b>WHY?</b>		
<p>Determining appropriate inventory levels and economic order quantities, expediting deliveries by using EDI, and reconciling orders with filled and back orders minimize stockouts.</p>		
<p>Safeguard raw materials.</p>	<p>Existence →</p>	<p>Only storeroom personnel have custody of raw materials.</p>
<b>WHY?</b>		
<p>Access to raw materials should only be given to personnel responsible for the custody of assets, not to individuals responsible for execution functions, such as a production line supervisor.</p>		
<p>Data entry is accurate and complete.</p>	<p>Existence →</p>	<p>Inventory reconciliations of material requisitions and material receipts are performed daily.</p>
<b>WHY?</b>		
<p>The parts requested should be consistent with the parts used in the maintenance activities. Unexplained variances should be investigated.</p>		

<b>Insurance</b>		
<b>Objective</b>	<b>Assertion</b>	<b>Control(s)</b>
Prevent overcharging by service providers.	Existence →	Develop a program that identifies services performed in excess of expectations for particular age categories, duplicate or equivalent services performed recently, and claims exceeding the average cost per claim.
<b>WHY?</b>		
Unusual claims should be identified and followed up to determine whether they are legitimate. This control is a reasonableness test, a type of IT input control.		
Effective administration of the insurance function.	Existence →	Receipt of billings and the disbursement of payments should be segregated. Final settlements are negotiated after claims are submitted.
<b>WHY?</b>		
The maximum probable compensable loss that the insurer must pay should be assessed and reported. Adjustment for inflation alone is not sufficient to determine the degree of risk that should be insured.		
Insurance coverage is adequate.	Existence →	Policy coverage should be systematically evaluated each year (periodic appraisals). Safeguarding assets includes insuring them. The types and amounts of insurance should be supported by periodic appraisals.
<b>WHY?</b>		
Policy coverage should be systematically evaluated each year. Coverage is a function of risk and the probability and amount of loss. They should be assessed to determine what insurance coverage is adequate. Adjustment for inflation alone is not sufficient.		
Insurance carrier has the means to pay claims.	Existence →	The financial resources of the carrier should be evaluated to determine whether the insurance carrier has the resources to pay claims.
<b>WHY?</b>		
The ability of the insurance carrier to pay claims may necessitate a change in the insurance carrier.		

<b>Sales Invoices</b>		
<b>Objective</b>	<b>Assertion</b>	<b>Control(s)</b>
Sales invoice amounts are properly reflected in accounting ledgers.	Completeness  →	Generate a control total (total monetary amount of all sales invoices) and compare it with the total amount posted to the individual accounts.
<b>WHY?</b>		
Total monetary amounts listed on sales invoices should match the total amount posted to the general ledger and accounts receivable subsidiary ledger. Discrepancies should be investigated and resolved.		

<b>Compensation Programs</b>		
<b>Objective</b>	<b>Assertion</b>	<b>Control(s)</b>
Long-term administration of a compensation program.	Existence  →	Job classifications based on predefined evaluation criteria.
<b>WHY?</b>		
Job classifications and grades are established during the job analysis phase, and the general level of compensation in the community and in the industry must be determined. Compensation is then fixed based on the job classifications, usually within a range for each grade. A range is necessary to allow for flexibility.		

# STUDY UNIT SEVEN

## FRAUD RISKS AND CONTROLS

7.1	<i>Fraud -- Risks and Types</i> .....	1
7.2	<i>Fraud -- Controls</i> .....	6
7.3	<i>Fraud -- Investigation</i> .....	10

This study unit covers **Domain VI: Fraud Risks** from The IIA's CIA Exam Syllabus. This domain makes up 10% of Part 1 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 FRAUD -- RISKS AND TYPES

#### 1. Fraud and Fraud Risk

- a. **Fraud** is “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.”
  - 1) Stated differently, fraud is any act characterized by **intentional** deception or misrepresentation.
- b. **Fraud risk** is the possibility that fraud will occur and the potential effects to the organization when it occurs.

#### 2. Characteristics of Fraud

- a. **Pressure or incentive** is the need a person tries to satisfy by committing the fraud.
  - 1) Situational pressure can be personal (e.g., financial difficulties in an employee's personal life) or organizational (e.g., the desire to release positive news to the financial media).
- b. **Opportunity** is the ability to commit the fraud.
  - 1) Opportunity to commit is a factor in low-level employee fraud. Lack of controls over cash, goods, and other organizational property, as well as insufficient segregation of duties, are enabling factors.
  - 2) Opportunity is the characteristic that the organization can most influence, e.g., by means of controls.
- c. **Rationalization** is the ability to justify the fraud. It occurs when a person attributes his or her actions to rational and creditable motives without analysis of the true and, especially, unconscious motives.
  - 1) Feeling underpaid is a common rationalization for low-level fraud.
  - 2) Fraud awareness training minimizes rationalization by
    - a) Supporting the ethical tone at the top,
    - b) Promoting an environment averse to fraud, and
    - c) Emphasizing that the organization does not tolerate misconduct of any kind.

### 3. Effects of Fraud

- a. Monetary losses from fraud are significant, but its full cost is immeasurable in terms of time, productivity, and reputation, including customer relationships.
- b. Thus, an organization should have a fraud program that includes awareness, prevention, and detection programs. It also should have a fraud risk assessment process to identify fraud risks.

### 4. Types of Fraud

- a. **Asset misappropriation** is stealing cash or other assets (supplies, inventory, equipment, and information). The theft may be concealed, e.g., by adjusting records.
  - 1) For example, entering fraudulent journal entries can help conceal asset theft (e.g., when an asset is purchased, the perpetrator debits an expense account instead of an asset account).
  - 2) However, selecting a vendor based on a blanket purchase order with an approved vendor(s) is a common business practice.
- b. **Skimming** is theft of cash before it is recorded, for example, accepting payment from a customer but not recording the sale.
- c. **Payment fraud** involves payment for fictitious goods or services, overstatement of invoices, or use of invoices for personal reasons.
- d. **Expense reimbursement fraud** is payment for fictitious or inflated expenses, for example, an expense report for personal travel, nonexistent meals, or extra mileage.
- e. **Payroll fraud** is a false claim for compensation, for example, overtime for hours not worked or payments to fictitious employees. One control used to detect the addition of fictitious persons to the payroll is for the auditor to make periodic comparisons of the names on the payroll with persons observed working for the company.
- f. **Financial statement misrepresentation** often overstates assets or revenue or understates liabilities and expenses. Management may benefit by selling stock, receiving bonuses, or concealing another fraud.
- g. **Information misrepresentation** provides false information, usually to outsiders in the form of fraudulent financial statements.
- h. **Corruption** is an improper use of power, e.g., bribery. It often leaves little accounting evidence. These crimes usually are uncovered through tips or complaints from third parties. Corruption often involves the purchasing function.
- i. **Bribery** is offering, giving, receiving, or soliciting anything of value to influence an outcome (e.g., kickbacks). Bribes may be offered to key employees such as purchasing agents. Those paying bribes tend to be intermediaries for outside vendors.
- j. A **conflict of interest** is an undisclosed personal economic interest in a transaction that adversely affects the organization or its shareholders.
- k. A **diversion** redirects to an employee or outsider a transaction that normally benefits the organization.
- l. **Wrongful use** of confidential or proprietary information is fraudulent.
- m. A **related-party fraud** is receipt of a benefit not obtainable in an arm's-length transaction.
- n. **Tax evasion** is intentionally falsifying a tax return.

## 5. Low-Level Fraud vs. Executive Fraud

- a. Fraud committed by staff or line employees most often consists of theft of property or embezzlement of cash. The incentive might be relief of economic hardship, the desire for material gain, or a drug or gambling habit. This type of fraud is intended to benefit individuals and is generally committed by an individual or individuals living outside their apparent means of support.
  - 1) Stealing petty cash or merchandise, lapping accounts receivable, and creating nonexistent vendors are common forms of low-level fraud.
- b. Fraud at the executive level is different. The incentive is usually either maintaining or increasing the stock price, receiving a large bonus, or both. This type of fraud is intended to benefit the organization.
  - 1) Executive level fraud ordinarily consists of materially misstating financial statements because promotion and compensation are tied to profits.

## 6. Symptoms of Fraud

- a. A **document symptom** is any tampering with the accounting records to conceal a fraud. Keeping two sets of books or forcing the books to reconcile are examples.
- b. A **lifestyle symptom** is an unexplained rise in an employee's social status or level of material consumption.
- c. A **behavioral symptom** (i.e., a drastic change in an employee's behavior) may indicate the presence of fraud. Guilt and other forms of stress associated with perpetrating and concealing the fraud may cause noticeable changes in behavior.

## 7. Some Indicators of Possible Fraud

- a. Frauds and their indicators (red flags) have different forms, including
  - 1) Lack of employee rotation in sensitive positions, such as cash handling
  - 2) Inappropriate combination of job duties (e.g., cash collections and disbursements responsibilities)
  - 3) Unclear lines of responsibility and accountability
  - 4) Unrealistic sales or production goals
  - 5) An employee who refuses to take vacations or refuses promotion
  - 6) Established controls not applied consistently
  - 7) High reported profits when competitors are suffering from an economic downturn
  - 8) High turnover among supervisory positions in finance and accounting areas
  - 9) Excessive or unjustifiable use of sole-source procurement
  - 10) An increase in sales far out of proportion to the increase in cost of goods sold (e.g., sales increase by 30% and cost of goods sold increase by 3%)
  - 11) Material contract requirements in the actual contract differ from those in the request for bids
  - 12) Petty cash transactions are not handled through an imprest fund

## 8. Types of Fraudulent Processes

### a. Lapping Receivables

- 1) In this fraud, a person (or persons) with access to customer payments and accounts receivable records steals a customer's payment. The shortage in that customer's account then is covered by a subsequent payment from another customer.
- 2) The process continues until
  - a) A customer complains about his or her payment not being posted,
  - b) An absence by the perpetrator allows another employee to discover the fraud, or
  - c) The perpetrator covers the amount stolen.

### b. Check Kiting

- 1) Kiting exploits the delay between (a) depositing a check in one bank account and (b) clearing the check through the bank on which it was drawn. This practice is only possible when manual checks are used. The widespread use of electronic funds transfer and other networked computer safeguards make electronic kiting difficult.
- 2) A check is kited when (a) a person (the kiter) writes an insufficient funds check on an account in one bank and (b) deposits the check in another bank.
- 3) The second bank immediately credits the account for some or all of the amount of the check, enabling the kiter to write other checks on that (nonexistent) balance. The kiter then covers the insufficiency in the first bank with another source of funds. The process can proceed in a circle of accounts at any number of banks.

## 9. Roles of Internal Auditors

- a. Internal auditors are not responsible for the detection of all fraud, but they always must be alert to the possibility of fraud.



### Implementation Standard 1210.A2

Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

- 1) According to Implementation Standard 1220.A1, internal auditors must exercise due professional care by, among other things, considering the "probability of significant errors, fraud, or noncompliance."
- 2) Internal auditors therefore must consider the probability of fraud when developing engagement objectives (Impl. Std. 2210.A2).



**Implementation Standard 2120.A2**

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

- b. The internal auditor should consider the potential for fraud risks in the assessment of control design and the choice of audit procedures.
  - 1) Internal auditors should obtain reasonable assurance that objectives for the process under review are achieved and material control deficiencies are detected.
  - 2) The consideration of fraud risks and their relation to specific audit work are documented.
- c. Internal auditors should have sufficient knowledge of fraud to identify indicators of fraud (red flags). However, internal auditors do not normally perform procedures specifically to gather red flag information.
  - 1) This knowledge includes
    - a) The characteristics of fraud,
    - b) The methods used to commit fraud, and
    - c) The various fraud schemes associated with the activities reviewed.
- d. Internal auditors should be alert to opportunities that could allow fraud, such as control deficiencies.
  - 1) If significant control deficiencies are detected, additional procedures may be performed to determine whether fraud has occurred.
- e. Internal auditors should evaluate the indicators of fraud and decide whether any further action is necessary or whether an investigation should be recommended.
- f. Internal auditors should evaluate whether
  - 1) Management is actively overseeing the fraud risk management programs,
  - 2) Timely and sufficient corrective measures have been taken with respect to any noted control deficiencies, and
  - 3) The plan for monitoring the program is adequate.
- g. If appropriate, internal auditors should recommend an investigation.

## 7.2 FRAUD -- CONTROLS

### 1. Fraud Management Program

- a. The components of an effective fraud management program include the following:
  - 1) Company ethics policy
  - 2) Fraud awareness
  - 3) Fraud risk assessment
  - 4) Ongoing reviews
  - 5) Prevention and detection
  - 6) Investigation

### 2. Controls

- a. Control is the principal means of managing fraud and ensuring the components of the fraud management program are present and functioning. (Control and types of control are covered in detail in Study Unit 5.)
- b. The **COSO Internal Control Framework** (covered in detail in Study Unit 5, Subunit 3) can be applied in the fraud context to promote an environment in which fraud is effectively managed.
  - 1) The control environment includes such elements as a code of conduct, ethics policy, or fraud policy to set the appropriate tone at the top; hiring and promotion guidelines and practices; and board oversight.
  - 2) A **fraud risk assessment** generally includes the following:
    - a) Identifying and prioritizing fraud risk factors and fraud schemes
    - b) Determining whether existing controls apply to potential fraud schemes and identifying gaps
    - c) Testing operating effectiveness of fraud prevention and detection controls
    - d) Documenting and reporting the fraud risk assessment
  - 3) Control activities are policies and procedures for business processes that include authority limits and segregation of duties.
  - 4) Fraud-related information and communication practices promote the fraud risk management program and the organization's position on risk. The means used include fraud awareness training and confirming that employees comply with the organization's policies.
  - 5) Monitoring evaluates antifraud controls through independent evaluations of the fraud risk management program and use of it.
- c. **Preventing fraud.** Essential elements in preventing fraud are setting the correct tone at the top and instilling a strong ethical culture.
- d. **Detecting fraud.** An essential element in detecting fraud is employee feedback, as fraud tips from employees is the most common way to detect fraud. Sources of employee feedback include a whistleblower hotline, exit interviews, and employee surveys.

### 3. Responsibility for Controls

- a. Management is primarily responsible for establishing and maintaining control.
- b. Internal auditors must assist the organization by evaluating the effectiveness and efficiency of controls and promoting continuous improvement (Perf. Std. 2130).
  - 1) In an assurance engagement, internal auditors must assist the organization by evaluating the adequacy and effectiveness of controls in responding to risks (Impl. Std. 2130.A1).
  - 2) Internal auditors are not responsible for designing and implementing fraud prevention controls.
  - 3) However, internal auditors acting in a consulting role can help management identify and assess risk and determine the adequacy of the control environment.
    - a) Internal auditors also are in a unique position within the organization to recommend changes to improve the control environment.

### 4. Fraud Awareness

- a. Fraud awareness is having an understanding of the nature, causes, and characteristics of fraud.
  - 1) Fraud awareness is developed through periodic fraud risk assessments, training of employees, and communications between management and employees.
- b. Employee training about fraud should be tailored to each organization's fraud risks.
  - 1) Training typically covers the organization's values and code of conduct, types of fraud, and employee roles and responsibilities to report violations of ethical behavior.
- c. Fraud essentially is the falsification of transactions. Thus, an auditor's examination of transactions for fraud tests the existence assertion.

5. The following charts describe examples of some controls (including their objectives) and provide a reason for their existence.

<b>Purchases</b>	
<b>Objective</b>	<b>Control</b>
<p>Confirm purchases are properly authorized.</p>	<p>Prepare an Accounts Payable signature authorization list showing the signatures for authorized individuals who may initiate and approve purchase orders.</p> <p>Persons authorized to initiate or approve purchase orders have full responsibility for ensuring that each purchase, including the price, specifications, quality, and quantity, is appropriate.</p> <p>Purchases can only be transacted by approved vendors or evidenced by approved contracts.</p> <p>A policy prohibits receipt of kickbacks, gifts, and other items of value from vendors.</p> <p>Expenditures transacted via credit or debit cards and electronic payments (Venmo, PayPal, Zelle, Square, etc.) are subject to expense-type code restrictions.</p> <p>Separation of duties between the ordering and receiving of merchandise.</p> <p>Receiving department does not accept goods unless it has a blind copy of a properly approved purchase order for the items.</p> <p>Credit card charges are subject to the expenditure controls used on purchases transacted through the accounts payable process cycle.</p> <p>Receiving reports and vendor invoices are required to be sent to accounts payable.</p> <p style="text-align: center;"><b>WHY?</b></p> <p>Prevent a purchasing agent from purchasing items for personal use with the organization's funds.</p>

<b>Computer Fraud</b>	
<b>Objective</b>	<b>Control</b>
<p>Only those persons with a bona fide purpose and authorization have access to data files and programs.</p>	<p>Programmers do not have access to programs used in processing.</p> <p>Lists of authorized persons are maintained online and should constantly be updated after personnel changes (e.g., promotion or resignation).</p> <p style="text-align: center;"><b>WHY?</b></p> <p>The risk of inappropriate use is reduced when only authorized personnel access programs used in processing. Use should be necessary to fulfill job obligations.</p>
<p>Only those persons with a bona fide purpose and authorization have access to data files and programs.</p>	<p>Use a device authorization table to grant access only to those physical devices that should logically need access.</p> <p>Restrict the ability of employees to gain access to and change sensitive information.</p> <p style="text-align: center;"><b>WHY?</b></p> <p>For example, it is illogical for anyone to access the accounts receivable file from a manufacturing terminal. Accordingly, the device authorization table should deny access to the accounts receivable file even when a valid password is used from a manufacturing terminal.</p>
<p>Convert data into unreadable code so that unauthorized individuals cannot use the data inappropriately.</p>	<p>Encrypt data so that only authorized users can decode (decipher) the information.</p> <p style="text-align: center;"><b>WHY?</b></p> <p>Encoding data before transmission over communication lines makes understanding or modifying the content more difficult for someone with access.</p>
<p>Adequate control over program changes.</p>	<p>Redesign programs using a working copy, not the version in use.</p> <p>Systems analyst is made responsible for communicating the purpose of the design to the programmer.</p> <p>Actual users test new programs.</p> <p>Programmers do not have access to operational processes, and librarians are not able to program.</p> <p style="text-align: center;"><b>WHY?</b></p> <p>Prevent opportunities for an individual with malicious or fraudulent intent to create and insert code within the program under development.</p>

<b>Segregation of Duties</b>	
<b>Objective</b>	<b>Control</b>
<p>Minimize the opportunities for a person to be able to perpetrate and conceal fraud or errors in the normal course of his or her duties.</p>	<p>Separate contract negotiation from approval of invoices for payment.</p> <p>Person(s) responsible for signing checks or approving electronic payments verify that a service or product was received.</p> <p>Separate contract negotiation, approval of invoices for payment, and budget preparation.</p> <p>Separate vendor setup responsibility from the purchasing function.</p> <p>Separate employee and contractor setup from the position responsible for processing payroll and contractor payments.</p> <p style="text-align: center;"><b>WHY?</b></p> <p>When feasible, segregation of duties divides responsibility for recording of the transaction, authorization, and custody of the assets associated with the transaction. The effect is to minimize the opportunities for a person to be able to perpetrate and conceal fraud or error.</p>

**7.3 FRAUD -- INVESTIGATION**

1. **Forensic auditing** uses accounting and auditing knowledge and skills in matters having civil or criminal legal implications. Engagements involving fraud, litigation support, and expert witness testimony are examples. Forensic auditing procedures include interviewing, investigating, and testing.
2. **Fraud Investigation**
  - a. An investigation gathers sufficient information to determine (1) whether fraud has occurred, (2) the loss exposures, (3) who was involved, and (4) how fraud occurred. It should discover the full nature and extent of the fraud.
  - b. Internal auditors, lawyers, and other specialists usually conduct fraud investigations.
  - c. The investigation and resolution activities must comply with local law, and the auditors should work effectively with legal counsel and become familiar with relevant laws.

- d. Management implements controls over the investigation. They include (1) developing policies and procedures, (2) preserving evidence, (3) responding to the results, (4) reporting, and (5) communications.
- 1) These matters may be documented in a **fraud policy** that the internal auditors may assist in evaluating.
  - 2) Policies and procedures address
    - a) The rights of individuals;
    - b) The qualifications of investigators;
    - c) The relevant laws; and
    - d) The disciplining of employees, suppliers, or customers, including legal measures.
  - 3) The authority and responsibilities of those involved in the investigation, especially the investigator and legal counsel, should be clear.
  - 4) Internal communications about an ongoing investigation should be minimized.
  - 5) A policy should specify the investigator's responsibility for determining whether a fraud has been committed. Either the investigator or management decides whether fraud has occurred, and management decides whether to notify outside authorities.
- e. The responsibility of the **internal audit activity** for investigations should be defined in its charter and in fraud policies and procedures.
- 1) For example, internal auditing may
    - a) Be primarily responsible,
    - b) Act as a resource, or
    - c) Avoid involvement because it is responsible for assessing investigations or lacks resources.
  - 2) Any role is acceptable if its effect on independence is recognized and managed appropriately.
  - 3) Internal auditors typically not only assess investigations but also advise management about the process, including control improvements.
  - 4) To be proficient, fraud investigation teams must obtain sufficient knowledge of
    - a) Fraud schemes,
    - b) Investigation methods, and
    - c) The applicable law.
  - 5) The internal audit activity may use in-house staff, outsourcing, or both.

- f. An **investigation plan** is developed for each investigation.
- 1) The lead investigator determines the knowledge, skills, and other competencies needed.
  - 2) The process includes obtaining assurance that no potential conflict of interest exists with those investigated or any employees of the organization.
  - 3) Planning should consider the following:
    - a) Gathering evidence using surveillance, interviews, or written statements
    - b) Documenting and preserving evidence, the legal rules of evidence, and the business uses of the evidence
    - c) Determining the extent of the fraud
    - d) Determining the methods used to perpetrate the fraud
    - e) Evaluating the cause of the fraud
    - f) Identifying the perpetrators
  - 4) All evidence obtained should be recorded chronologically in a log or inventory. Examples of evidence include the following:
    - a) Letters, memos, and correspondence (in hard copy or electronic form)
    - b) Financial records
    - c) IT or systems access records
    - d) Phone records
    - e) Customer or vendor information (e.g., contracts, invoices, and payment information)
    - f) Public records (e.g., property records or business registrations filed with government agencies)
    - g) News articles
    - h) Websites (e.g., social networking sites)
  - 5) The investigation should be coordinated with management, legal counsel, and other specialists.
  - 6) Investigators need to be prudent, consistent, and knowledgeable of the rights of persons within the scope of the investigation and the reputation of the organization itself.
  - 7) The level and extent of complicity in the fraud throughout the organization needs to be assessed. This assessment can be critical to avoid
    - a) Destroying or tainting crucial evidence and
    - b) Obtaining misleading information from persons who may be involved.
  - 8) The investigation needs to secure evidence collected and follow chain-of-custody procedures.



### 3. Interrogation of Employees

- a. A fraud-related interrogation differs significantly from a normal interview.
  - 1) The purpose of a typical interview is to gather facts.
    - a) In an interrogation, the internal auditor has already gathered pertinent facts and is seeking confirmation.
  - 2) At no time should the internal auditor accuse the employee of committing a crime.
    - a) If the accusation is unprovable, the organization could have legal liability.
  - 3) The accused generally is interrogated after most relevant evidence has been obtained.
    - a) The objective often is to use the evidence to obtain a confession.
  - 4) All information received during the interview must be correctly documented.
    - a) All evidence should be subject to effective chain-of-custody procedures.
  - 5) Two persons should conduct the interview, one of whom takes notes and may serve as a witness.
- b. The internal auditor should guide the conversation from the general to the specific.
  - 1) Open questions generally are used early in the interrogation, and closed questions are used later as the auditor comes closer to obtaining a confession.
    - a) Open questions are of the type, "Describe your role in the vendor approval process."
    - b) Closed questions are of the type, "Do you personally verify the existence of every vendor who seeks approval?"
  - 2) Normal interviewing methods regarding nonthreatening tone and close observation of body language apply.
- c. The employee should not be allowed to return to his or her normal work area upon completion of the interrogation.
  - 1) Because the employee is now alert to the fraud investigation, (s)he might be tempted to destroy valuable evidence.

#### 4. **Fraud Reporting**

- a. The chief audit executive is responsible for fraud reporting. It consists of the various oral or written, interim or final communications to management or the board regarding the status and results of fraud investigations.
  - 1) A formal communication may be issued at the conclusion of the investigation that includes
    - a) Time frames,
    - b) Observations,
    - c) Conclusions,
    - d) Resolution, and
    - e) Corrective action to improve controls.
  - 2) It may need to be written to protect the identities of some of the people involved.
  - 3) The needs of the board and management, legal requirements, and policies and procedures should be considered.
- b. A draft of the proposed final communication should be submitted to legal counsel for review. To be covered by the attorney-client privilege, the report must be addressed to counsel.
- c. Any incident of significant fraud, or incident that leads the internal auditors to question the level of trust placed in one or more individuals, must be timely reported to senior management and the board.
- d. If previously issued financial statements for 1 or more years may have been adversely affected, senior management and the board also should be informed.

#### 5. **Resolution of Fraud Incidents**

- a. Resolution consists of determining actions to be taken after the investigation is complete.
  - 1) Management and the board are responsible for resolving fraud incidents.
- b. Resolution may include the following:
  - 1) Providing closure to persons who were found innocent or reported a problem
  - 2) Disciplining an employee
  - 3) Requesting voluntary financial restitution
  - 4) Terminating contracts with suppliers
  - 5) Reporting the incident to law enforcement or regulatory bodies, encouraging them to prosecute, and cooperating with them
  - 6) Filing a civil suit to recover the amount taken
  - 7) Filing an insurance claim
  - 8) Complaining to the perpetrator's professional association
  - 9) Recommending control improvements

## 6. Communication of Fraud Incidents

- a. Management or the board determines whether to inform parties outside the organization after consultation with such individuals as legal counsel, human resources personnel, and the CAE.
  - 1) The organization may need to notify government agencies of certain types of fraudulent acts. It also may need to notify its insurers, bankers, and external auditors of instances of fraud.
- b. Internal communications are a strategic tool used by management to reinforce its position relating to integrity and to show why internal controls are important.

## 7. Opinion on Fraud-Related Controls

- a. The internal auditor may be asked by management or the board to express an opinion on internal controls related to fraud. The following provide relevant guidance:
  - 1) Standards and Implementation Guides applying to communication of results (Performance Standard 2400, etc.)
  - 2) Practice Guide, *Formulating and Expressing Internal Audit Opinions*
- b. An opinion on fraud-related controls is acceptable, but it is inappropriate for an internal auditor to express an opinion on the culpability of a fraud suspect.