Internal Control

Vocabulary & Terms Dictionary

ICI Brasil

Vocabulary & Terms

Terms	Definitions
Access Threats	Threats that unauthorized or improper processing will occur. External risks are frequently called security risks or accessibility risks. Unauthorized acts are those executed by a person or program, which does not have authority from management to execute that act.
Access to Assets	Access to assets is permitted only in accordance with management's authorization.
Activity	COSO uses the word activity to define an operational unit such as payroll. Both systems controls and transaction processing controls are included in the COSO Activity definition
Administrative Control	Administrative control includes, but is not limited to, the plan of an organization and the procedures and records that are concerned with the decision processes leading to management's authorization of transactions. Such authorization is a management function directly associated with the responsibility for achieving the objectives of the organization and is the starting point for establishing accounting control of transactions.
Assessment program	An assessment program is a "procedure" for conducting a system or activity evaluation. The assessment program is a series of steps for the examiner to follow in completing an assessment. Assessment programs are built around objectives and risks to the achievement of those objectives that need to be addressed during the process. During the assessment process evidence needs to be collected, documented and examined.
Asset Accountability	The recorded accountability for assets is compared with existing assets at reasonable intervals and appropriate action is taken with respect to any differences
Asset Safeguarding	The procedures an organization puts into place to ensure that the assets acquired/owned by the organization are adequately protected from theft and misuse.

Audit Committee	The Audit Committee of the Board is in a unique position. It normally has the authority to question top management regarding how it is carrying out its financial reporting responsibilities, and it also has authority to ensure that corrective action is taken. The audit committee, in conjunction with or in addition to a strong internal audit function, is often in the best position within an entity to identify and act in instances where top management overrides internal controls or otherwise seeks to misrepresent reported financial results.
Auditability Threats	Threats preventing the reconstruction of transaction processing. This threat deals with the storage of data for purposes other than processing. Data is stored for the audit trail, backup, and other historical purposes. The risk is that this type of information will not be available to substantiate processing for management, auditors, and regulatory agencies.
Authorization	Transactions are executed in accordance with management's general or specific authorization. Authorization can be either general of specific. Management makes various general authorizations when it establishes policies for the organization to follow. Subordinates are instructed to implement these general authorizations for transactions within the limits set by the policy. Specific authority has to do with individual transactions for which management is unwilling to establish a general authorization, preferring a case-by-case review. These are usually non-routine transactions (such as major capital expenditures) that are to be approved only by senior management
Board of Directors (including key Board Committees)	Management is accountable to the Board of Directors or **trustees, who provide** governance, guidance and oversight. By selecting and monitoring management, the Board has a major role in defining what it expects in integrity and ethical values, and can confirm its expectations through its oversight activities. .
Business System/Application Risk	Risks associated with the operations at the organization. This operation can be expressed as business cycles, which include such cycles as revenue and expense, as well as individual applications within

	those cycles, such as invoicing and purchasing.
Cascading of Errors	A unique problem in computerized business applications is the cascading of errors, which occurs when one error triggers a series of errors. It is also a difficult problem to prevent and sometimes to detect.
Certified Internal Control Specialist (CICS)	A program developed by leading internal control professionals as a means of recognizing those individuals who demonstrate a predefined level of internal control competency. The CICS program is directed by an independent Certification Board and administered by the Internal Control Institute (ICI).
Chief Executive Officer (CEO)	The CEO is accountable for the entire system of internal control. This includes all of the controls within the organization. It is through the Sarbanes-Oxley Act that the CEO is required to attest to the adequacy of the system of internal controls.
Chief Financial Officer (CFO)	The Chief Financial Officer has primary responsibility to the system of internal accounting controls. It is internal accounting controls govern the physical systems of the organization. These include the financial records, reports for stockholders, performance statements and so forth. .
Chief Operations Officer (COO)	The COO has responsibility for quality control and statistical process control. These are primarily control over the work processes and control over the quality of the products produced from those processes.
Code of Conduct Policy	The code of conduct of an organization is its code of ethics for employees. These are the basic principles and guidelines that employees are expected to use in their dealings as an employee of the organization.
Code of Ethics	The Code of Ethics outlines the ethical behaviors expected of all certified professionals. Failure to adhere to the requirements of the Code is grounds for decertification of the individual by the Certification Board.
Common Body of Knowledge (CBOK)	The Certification Board defines the skills upon which internal control certification is based. The current CBOK includes skill categories fully described in a collection of the disciplines and skills for a respective internal control discipline

Compensation Committee	This Board Committee can see that emphasis is placed on compensation arrangements that help the entity's objectives and that do not unduly emphasize short-term results at the expense of long-term performance
Compliance Hotline	While compliance matters can often be resolved at the local level, the Compliance Hotline provides another way to address matters that might not be adequately resolved there and, in general, provides a way to report a concern or get information or advice anonymously. The Compliance Hotline is usually available 24 hours a day, 7 days a week, 365 days a year
Computer Processing controls	Computer processing controls, which are used to ensure accuracy and completeness of data during computer processing, are the controls that govern computer process integrity and computer process error handling. These controls are applied after the entry of data into the computer application system as application programs process the data. File interface and program interfaces are also included in this chapter. The scope of computer processing controls discussed here includes application level controls that are built in and around the central processing unit. These controls are built into each individual application program and control application program data input, processing, and output. Application controls are unique and specific in one application and therefore may or may not be transferable between applications. During the continuing development of computer processing controls, it is important to ensure that the principles of internal control (e.g., separation of functions) are being carried forward to the functions performed by the computer application system.
Conflicts of Interest	A conflict of interest arises when you put your personal, social, financial, or political interests before the interests of the Company. Even the appearance of a conflict can damage your reputation or that of the Company. Any potential conflict of interest should be promptly disclosed to your manager. It should also be disclosed whenever you are asked to certify your understanding of and adherence to the standards in this booklet. Many conflicts of interest can be resolved in a simple and mutually acceptable way. The following

	are several types of conflicts of interest.
Continuing Professional Education (CICS)	The CICS is required to submit 120 credit hours of Continuing Professional Education (CPE) every three years to maintain certification or take an examination for re-certification. CPE may be gained by such activities as attending professional conferences, taking education and training courses, developing and offering training to share knowledge and skills with other professionals, publishing information, participating in the profession through active committee memberships and formal special interest groups.
Control	Any technique, method, or approach, which can minimize or eliminate risk in the attainment of an objective.
Control Activities	Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.
Control Environment	The core of any business is its people – their individual attributes, including integrity, ethical values and competence - and the environment in which they operate. They are the engine that drives the entity and the foundation on which everything rests. The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors.

Control Hierarchy	Internal control classification that shows a hierarchy of categories of control. At the apex of the hierarchy are environmental controls that "govern" the operation and effectiveness of the other two levels of control. Beneath environmental controls are system controls, and below them transaction processing controls
Control Objectives	Control objectives are a positive statement regarding risk. For example, if the risk is that business transactions would be lost, then the positive control objectives could be "All business transactions will be processed correctly". The generic system control objectives are those commonly described in accounting literature, the Foreign Corrupt Practices Act, and the Sarbanes-Oxley Act.
Control Point	That point within the application system where the exposure to loss is greatest and the point where the control will be installed.
Control Threats	Threats to the accuracy and completeness of data, as well as the operational performance of the application system. These are threats dealing with the integrity of data within the system and the effectiveness, economy and efficiency by which that system performs its functions.
Corporate Compliance Committee	The Corporate Compliance Committee has been created to broaden the reach of the Corporate Compliance Officer. Representatives from each business division make up the Committee. The members provide oversight to Corporation's compliance strategy and system and are charged with keeping the Corporate Compliance Officer, the Board of Directors, and senior management informed of significant compliance issues, risks, and trends.
Corporate Compliance Officer	The Corporate Compliance Officer is responsible for overseeing Corporation's compliance system, including the internal auditing, monitoring, and self-evaluation programs relating to the legal and regulatory obligations of the Company. The Corporate Compliance Officer ensures that there is broad application and consistent interpretation of our standards throughout the Company. The Corporate Compliance Officer often reports directly to the Chairman of the Board and Chief Executive Officer,

	as well as to the Audit Committee of the Board of Directors.
Corporate Governance	There is no common definition of corporate governance; and no one approach for corporate governance works for all corporations. The dictionary defines governance as "to control or to rule." Among the many definitions for govern are: (1) to exercise authority over; rule, control, manage, etc.; (2) to influence the action or conduct of; guide; (3) to hold in check; curb; (4) to be a rule or law Much of the literature on corporate governance is associated with the corporation's board of directors. Simplistically, we could define corporate governance as those practices followed by the Board of Directors and senior corporate officers to govern the corporation
Corporate Values	The values that the corporation wants considered in the performance of day-to-day operation. For example, if the value is "respect each employee" then when reprimanding an employee for inappropriate behavior in front of other employees would also be inappropriate behavior
Corrective Control	Corrective controls provide the necessary evidence and/or information to correct the undesirable event. Detection is basic to application of corrective controls.
COSO	COSO stands for the Committee of Sponsoring Organizations of the Treadway Commission. It was organized to provide guidance in evaluating internal control. The five member organizations of COSO are Financial Executives Institute, American Institute of Certified Public Accountants, American Accounting Association, The Institute of Internal Auditors, and The Institute of Management Accountants
COSO's Enterprise Risk Management Framework	Activities are designed to accomplish business objectives. Management is responsible for developing business objectives that are consistent with the mission and business constraints that produce a high probability of meeting the organizations business plan. The enterprise risk management framework, developed by COSO, provides a framework for creating business objectives.
COSO's Internal Control Framework	The COSO internal control framework is currently recognized by the Securities and Exchange Commission as a valid framework for evaluating

	internal control. The COSO internal control framework consists of five interrelated components. These are derived from the way management runs a business, and are integrated with the management process. The components are control environment, risk assessment, control activities, information and communication, and monitoring.. COSO's Internal Control Framework has become the most widely accepted internal control model.
Data Communications controls	Data communication controls are primarily concerned with ensuring the integrity of data as they pass through communication lines from the message input devices to the message reception devices. These controls are important because most data communication equipment is owned and controlled by organizations other than the sending or receiving organizations. These controls are also important because there is a fast-growing trend by many organizations to use data communication services as an integral part of their computer application systems to ensure the accuracy and completeness of data for the entire application system.
Data Storage and Retrieval controls	The scope of computer data storage and retrieval controls includes those controls in effect during file handling and file error handling. These controls govern the file-handling processes that are not directly associated with the computer processing of the application system. Data storage and retrieval controls are of particular importance because they involve a high degree of human intervention and data handling. For this reason it is important to provide for the facility and personnel procedures necessary to control the integrity of data files and programs during storage and retrieval.
Detective controls	Controls are often segregated for design purposes into two broad classifications: preventive and detective. Detective controls are designed to detect errors and ensure their prompt correction.
Disclosure controls and	The SEC Certification rule uses a new term

procedure	"disclosure controls and procedure" defined as: "Controls and other procedures of an issuer that are designed to ensure that information required to be disclosed by the issuer in the reports filed or submitted under the Exchange Act recorded, processed, summarized, and reported within the time periods specified in the Commission's rules and forms. 'Disclosure controls and procedures' include, without limitation, controls and procedures designed to ensure that information required to be disclosed by an issuer in the Exchange Act reports is accumulated and communicated to the issuer's management … as appropriate to allow timely decisions regarding required disclosure."
Enterprise Risk Management (ERM)	Enterprise risk management consists of eight interrelated components. These are derived from the way management runs a business, and are integrated with the management process. These components are internal environment, objective setting event identification, risk assessment, risk response, control activities, information and communication, and monitoring.
Environmental controls	Environmental controls are the responsibility of executive management. The word "environment" is used to represent the values established by executive management and the way in which management wants the business of the organization performed. This implies that work may be performed in different ways depending upon the environment established by executive management. Environmental controls significantly impacts the way organizations function
Environmental Risk	Risks associated with the organization's environment. This includes both external and internal risk factors.
Expenditures Cycle	The expenditures cycle is subdivided into purchasing, payroll, and disbursement functions.
Exposure	The word "exposure" indicates that there is an event, which could "expose" the organization to loss. Exposure does not mean that there will be loss, but rather that the potential for loss exists. For example, the exposure of "unauthorized transactions" does not conclude that a loss occurred, because somewhere in

	the system that unauthorized transaction may be detected and deleted from processing. In practical terms, it is the potential loss derived from a threat. Exposure can take the form of a quantitative monetary measure and/or an intangible value.
External Auditing	Independent certified public accountants play an important a role in contributing to achievement of the entity's financial reporting objectives. They bring to management and the Board of Directors a unique independence and objective view, and can contribute to an entity's achievement of its financial reporting responsibilities.
External Financial Reporting Cycle	The external financial reporting cycle covers the functions involved in preparing journal entries and posting transactions to the general ledger ; deciding the generally accepted accounting principles that the company should follow; gathering and consolidating the information required for the preparation of financial statements and other external historical financial reports, including related disclosures; preparing and reviewing the financial statements and other external reports. This external financial reporting cycle has taken on critical importance with the passage of the Sarbanes-Oxley Act
Finance Committee	This Board Committee is useful in controlling major commitments of funds and ensuring that capital expenditure budgets are consistent with operating plans.
Financial Officers	Finance and controllership officers and their staffs' activities cut across, up and down the operating units of an enterprise. These financial executives often are involved in developing entity-wide budgets and plans. They track and analyze performance, often from an operations and compliance perspectives, as well as a financial one. As such, the chief financial officer, chief accounting officer, controller and others in an entity's financial function are central to the way management exercises control.
Financing Cycle	The financing cycle covers the functions involved with the issuance and redemption of capital stock and the recording of transactions therein; the payment of

	dividends; the investigation and selection of appropriate forms of financing, including lease transactions; debt management, including monitoring compliance with covenants; investment management and physical custody of securities.
Foreign Corrupt Practice Act	The passage of the Foreign Corrupt Practice Act in 1977 made inadequate internal accounting control a federal offense. This, in effect, requires controls adequate to reduce most of the stated exposures to an "adequate" level.
Freedom of Information Act	The Freedom of Information Act requires federal agencies to publish in the Federal Register certain information related to personal files. This information must include the source and method by which the information retained by those agencies can be obtained.
ICI risk and control model	The ICI risk and control model is a three level model. The three levels are environmental, system, and transaction processing. Environmental controls are normally thought of as the responsibility of the Board of Directors and executive management and create an environment in which system and transaction processing control are executed as intended. System controls are the responsibility of middle management (i.e., those responsible for function activities such as payroll). Transaction processing controls are the responsibility of employees.
Information and Communication	Surrounding activities are information and communication systems. These enable the entity's people to capture and exchange the information needed to conduct, manage and control its operations.
Internal Audit Charter	A formal written document reviewed and approved by the Board of Directors that outlines the authority grated to internal auditing and the function's responsibility is to senior management and/or the board of directors.
Internal Auditing	A function within the organization that has authority and responsibility to evaluate the performance of the organization, as well as the adequacy of and compliance to controls. The Standards for the Professional Practice of Internal Auditing, adopted by the Institute of Internal Auditors provides the following definition 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."
Internal Auditors	Internal auditors directly examine internal controls and recommend improvements. Standards established by the Institute of Internal Auditors specify that the scope of internal auditing should encompass the examination and evaluation of the adequacy and effectiveness of the organization's system of internal control and the quality of performance in carrying out assigned responsibilities
Internal Control (as defined by COSO)	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 in the categories of effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.
Internal Control (as defined by the American Institute of Certified Public Accountants)	Internal control comprises the plan of organization and all of the coordinate methods and measures adopted within a business to safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies. This definition possibly is broader than the meaning sometimes attributed to the term. It recognizes that a "system" of internal control extends beyond those matters which relate directly to the functions of the accounting and financial departments.
Malcolm Baldrige National Quality Award	The Malcolm Baldrige National Quality Award Management Model was established as a basis for improving the effectiveness and efficiency of U.S. corporations. Prior to the establishment of the Baldrige model, Japan had established the Deming Prize which was based on a management model. The objective of the both the Deming Prize and the Malcolm Baldrige National Quality Award was two-fold. First, to recognize those corporations that are leaders in their fields; and second, to help share best practices to lift the effectiveness and efficiency of other corporations.

Materiality	The major determinate for controls is the materiality considerations of the transaction. Materiality is defined as the value of the event being protected in relationship to the total value of the corporation. The higher the value of the event being protected in relation to the total value of the organization, the more controls used to protect those events. There should be a high correlation in establishing control between strength of controls and dollar value protected by those controls.
Monitoring	Internal control systems need to be monitored – a process that assesses the quality of the activities performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board.
Nominating Committee	This Board Committee provides control over the selection of candidates for directors and perhaps for top management
Output Processing controls	Output processing controls are used to ensure the integrity of output data from the conclusion of computer processing until their delivery to the functional user. The functional user is dependent upon the timely delivery of complete and accurate data to conduct his/her day-to-day business functions. Output controls play an important part in achieving the control objectives associated with the overall computerized record-keeping system. The function of output control is to ensure that processed information includes authorized, complete, and accurate data. The scope of output controls includes the control areas of information technology balancing and reconciliation, output distribution, user balancing and reconciliation, record retention, accountable document control, and output error handling.

PDCA Cycle	A major premise of any quality program is an emphasis on continuous improvement. The approach to continuous improvement is illustrated using the PDCA cycle, which was developed in the 1930s by Dr. Shewhart of the Bell System. The cycle comprises the four steps of Plan, Do, Check, and Act . It is also called the Deming Wheel, and is one of the key concepts of quality.
Play script	Play script is a method that defines procedures in an easy-to-follow, step-by-step format. The play script concept comes literally from the scripts written for plays. This concept works well for writing procedures
Preventive controls	Controls are often segregated for design purposes into two broad classifications: Detective controls are designed to detect errors and ensure their prompt correction. preventive and detective. Preventive controls are designed to prevent errors from occurring. Preventive controls may not always be noticeable because of their built-in nature.
Privacy Act of 1974	The Privacy Act of 1974 imposes numerous requirements upon federal agencies to prevent the misuse or compromise of data containing personal information. Federal automatic data processing (ADP) organizations that process personal data must provide a reasonable degree of protection against unauthorized disclosure, destruction, or modification of personal data, whether intentionally caused or resulting from accident or carelessness.
Process Engineering Cycle	The process engineering cycle covers the activities involved in building individual systems or applications. It is during this cycle that risks are identified, measured, and the means for controlling those risks are identified, defined, and implemented. Also during this cycle the effectiveness and efficiency of business operations will be determined. The process engineering cycle also includes changing and upgrading applications to affect current business needs and regulatory requirements
Production or Conversion Cycle	The production or conversion cycle covers the functions involved in production planning and control, inventory planning and control, property and deferred cost accounting, and cost accounting.
Recording	Transactions are recorded as necessary to permit

	preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and to maintain accountability for assets.
Reference Letter	A letter from someone who can attest to your job experience in internal control design and/or assessment. Reference letters must describe job experience
Revenue Cycle	The revenue cycle covers the functions involved in receiving and accepting requests for goods or services; delivering or otherwise providing goods or services; credit granting, cash receipts, and collection activities; billing; accounting for revenues, accounts receivable, commissions, warranties, bad debts, returned goods, and other adjustments.
Risk	A risk is the likelihood of a potential threat materializing and causing an adverse effect in the organization. For example, the risk (likelihood) of destruction of the corporate computer center increases as the hurricane threat approaches. Risk has a probability or frequency of occurrence attached to it.
Risk Analysis	Risk analysis is a process used to identify, assess and quantify the likelihood of a threat occurring and estimating the adverse effect. Risk analysis, is intended to improve the probability of success in any given situation.
Risk appetite	Risk appetite is the degree of risk, on a broad-based level, that a company or other entity is willing to accept in pursuit of its goals.
Risk Assessment	The entity must be aware of and deal with the risks it faces. It must set objectives, integrated with the sales, production, marketing, financial and other activities. In concert with setting objectives it also must establish mechanisms to identify analyze and manage the related risks.
Risk Exposure – Threat Diagram	Risk is the probability that an unfavorable event may occur. A threat is an event or activity that triggers a loss (i.e., the potential loss being the exposure). The effect of that cause is a loss. Therefore, a Risk Exposure – Threat diagram shows this cause – effect relationships to better illustrate the components of risk.

Risk management	Risk management is a senior management responsibility. It is a formal process that involves identifying, measuring, and prioritizing risk in a sequence in which they need to be addressed. .
Risk Scoring (Using External Application characteristics)	A method of determining the risk of an application by evaluating the characteristics pertaining primarily to the environment in which the application is developed, operated, and used.
Risk Scoring (Using Internal Application characteristics)	A method of determining the risk of an application by evaluating the characteristics of the data processed by the application and the controls over that data.
Sarbanes-Oxley Act	The Sarbanes-Oxley Act was enacted in the United States largely in response to a number of major corporate and accounting scandals. The objective of the law was to establish new or enhanced standards for corporate accountability and penalties for corporate wrong doing. The legislation placed new demands on corporate executives and their board of directors.
Segregation of Duties	Segregation of employee tasks and duties is an arrangement of responsibilities such that the work of an employee is checked; it is a system of inherent checks and balances that separates custody from initiation and accountability. These characteristics affect the four types of segregation of duties that contribute to an effective internal control environment, segregating operations from recordkeeping, custody from accounting, custody from authorization, and accounting tasks from one another.
Segregation of Responsibilities Conflict Matrix	The traditional segregation of responsibility concepts may not be effective or even possible in computerized business applications. Segregation of responsibilities in a data processing environment can be achieved by limiting personnel's actions on elements of data. This is possible because control mechanisms can be installed in a computer system that permits control granularity (i.e., controlling at the data element level as opposed to the record level). The conflict matrix can be used for determining the functions to be segregated, and for assessing the adequacy of segregation.
Strategic Planning	Strategic planning is the high-level, long-term planning process, involving decisions as to the

	objectives of the enterprise and the nature of its business. It includes determining what lines of business to enter or terminate, capacity planning, long-range personnel hiring plans, and so on.
System Controls (process controls)	System controls are those controls that define the management aspects of individual application systems. These would include such things as assuring that the system is maintainable, that changes can be made to the payroll system effectively and efficiently. This would also involve the type of structure of the computer system and the types of documentation available. System controls would also define the key indicators needed by management to manage the overall system. It would include independent reconciliations to ensure that the items processed were correct. System controls are the responsibility of middle management - - the managers that manage individual business systems.
System of Control	A system of control is an integrated system of individual controls, which must be evaluated on how the total system functions. Single controls, while effective at a single point, do not provide the assurance necessary that the process is under control. For example, incoming checks could be controlled in the mail room, but without a total system of controls governing the movement of checks from receipt in the mail room to deposit in the bank, there is no assurance that cash receipts are under control. Thus, what is important is the system of controls, as opposed to individual controls.
Tactical Planning	Tactical or management planning comprises the activities used to implement strategic plans and determines the requirements for operational activities. Tactical planning, or the short-term planning and control cycle, includes setting yearly budgets and monitoring performances against such budgets. This is one of the most powerful of all management based control systems
Threat	A threat is an event that can occur under given circumstances, which could lead to a loss. Threats include inherent and environmental hazards and the triggering of vulnerabilities
Threat Point Matrix	The Threat Point Matrix is a tool used to identify points in systems that have high risks of loss due to

	control weaknesses. The technique has proven to be highly reliable when used by individuals knowledgeable in the area that may be subject to loss. The technique involves building a matrix. On one dimension are the control points and the other dimension potential points of threat.
Tone at the Top	The "tone at the top" implies that the appropriate message is sent to employees by senior management, and that senior management is, in fact, "walking the talk." Walking the talk means that senior management is doing those things that they are asking the organization's employees to do.
Transaction Conflict Matrix	The objective of the Transaction Conflict Matrix is to show the adequate segregation of duties for financially oriented transactions. The matrix shows the functions that transactions can perform and the financial accounts on which that action occurs. When the same transaction can perform too many functions on the same account, there is a potential "conflict" in the adequacy of the segregation of duties.
Transaction Entry controls (IT)	These are the controls that oversee the processing of individual business transactions from the point where transactions originate to the point where the results are delivered to the user. Transaction entry controls are used to ensure the accuracy and completeness of data during their entry into the computer application system. The scope of the transaction entry control area includes controls up to the point of data entering the communication link or, in a non-data communication environment, entry into computer application programs for further processing. Transaction entry controls are a combination of manual and automated control routines. They are of particular importance because they control two important application areas: data conversion and edit and validation. Increasingly, the emphasis is on automating as many control routines as possible, to take advantage of computer hardware capabilities as well as to promote consistency in the application of controls.
Transaction Origination	Transaction origination controls are used to ensure the

controls	accuracy and completeness of data before they enter the computer application system. The scope of the transaction origination control area includes controls up to the point of converting data to a machine-readable format. Management, systems personnel, and control designers are placing increasing emphasis on transaction origination controls to ensure that the information prepared for entry into the system is valid, reliable, cost-effective, and not subject to compromise.
Transaction Processing Risk	Risks associated with processing a single business event from its point of origination to its point of conclusion.
Transaction Use Matrix	The Transaction Use Matrix shows the relationship between data items and the computer programs that use the data. One side of the matrix lists each individual data item, such as employee name, employee number, net pay, social security number, etc. The other side lists the program broken into the function data access programs can perform.
Vulnerability	Vulnerability is a weakness in the flow of business systems (i.e., a processes) that "exposes" an organization to a loss. For example, a password taped on a computer terminal could be used inappropriately by someone not authorized access, to cause loss to the organization