INTERNAL CONTROL

- Internal Control means different things to different people. The wide variety of meanings prevents a common understanding of internal control. An important goal therefore is to integrate the various internal control concepts into a framework in which a common definition is established and control components are identified.
Internal Control Defined

Internal Control (COSO Framework) is defined as follows:

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.
• Reliability of financial reporting.
• Compliance with applicable laws and regulations.
Internal Control Defined - cont’d

This definition reflects certain fundamental concepts:

• Internal control is a **process**. It is a means to an end, not an end in itself.

• Internal control is effected by **people**. It is not merely policy manuals and forms, but people at every level of an organization.

• Internal control can be expected to provide only **reasonable assurance**, not absolute assurance, to an entity's management and board.

• Internal control is geared to the achievement of **objectives** in one or more separate but overlapping categories.
Internal Control Is A Process

- Internal control is not one event or circumstance, but a series of actions that permeate an entity's activities. These actions are pervasive, and are inherent in the way management runs the business.

- Business processes are managed through the basic management processes of planning, executing and monitoring. Internal control is a part of these processes and is integrated with them.

- The internal control system is intertwined with an entity’s operating activities and exists for fundamental business reasons.

- Internal controls are most effective when they are built into the entity’s infrastructure and are part of the essence of the enterprise. They should be “built in” rather than “built on”
Internal Control Is Effected By People

- Internal control is effected by a board of directors, management and other personnel in an entity. It is accomplished by the people of an organization, by what they do and say. People establish the entity's objectives and put control mechanisms in place.

- Similarly, internal control affects people's actions. Internal control recognizes that people do not always understand, communicate or perform consistently.

- Accordingly, a clear and close linkage needs to exist between people's duties and the way in which they are carried out, as well as with the entity's objectives.

- The organization's people include the board of directors, as well as management and other personnel.
Internal Control Fundamental Concepts Explained

**Internal Control Only Provides Reasonable Assurance**

- Internal control, no matter how well designed and operated, can provide only reasonable assurance to management and the board of directors regarding achievement of an entity's objectives.
- Additionally, controls can be circumvented by collusion of two or more people.
- Finally, management has the ability to override the internal control system.
Internal Control Fundamental Concepts Explained

**Internal Control Is Geared Towards Objectives**

- Every entity sets out on a mission, establishing objectives it wants to achieve and strategies for achieving them.

- Objectives may be set for an entity as a whole, or be targeted to specific activities within the entity.

- Though many objectives are specific to a particular entity, some are widely shared.
Components of Internal Control

Internal control (COSO 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
- Monitoring
COSO Components

- *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.
COSO Components

- **Risk Assessment** - The entity must be aware of and deal with the risks it faces. It must set objectives, so that the organization is operating in concert. It also must establish mechanisms to identify, analyze and manage the related risks.
COSO Components

• **Control Activities** - Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to achievement of the entity’s objectives are effectively carried out.
COSO Components

- **Information and Communication** - Surrounding these 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.
**COSO Components**

- **Monitoring** – The entire process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant.
| The Committee of Sponsor-ing Organizations of the Treadway Commission's (COSO's) Internal Control--Integrated Framework | COSO's *Internal Control-Integrated Framework* was introduced in 1992 as guidance on how to establish better controls so companies can achieve their objectives with minimal surprises. COSO categorizes entity-level objectives into operations, financial reporting, and compliance. The framework includes more than 20 basic principles representing the fundamental concepts associated with its five components: control environment, risk assessment, control activities, information and communication, and monitoring. Some of the principles include key elements for compliance, such as integrity and ethical values, authorities and responsibilities, policies and procedures, and reporting deficiencies. |
| **Canadian Institute of Chartered Accountants' (CICA's) Criteria of Control Framework (CoCo)** | CoCo was introduced in 1992 with the objective of improving organizational performance and decision-making with better controls, risk management, and corporate governance. In 1995, *Guidance on Control* was produced and described the CoCo framework and defining controls. The framework includes 20 criteria for effective control in four areas of an organization: purpose (direction), commitment (identity and values), capability (competence), and monitoring and learning (evolution). |
The Basel Committee on Banking Supervision's Framework for Internal Control Systems

The Basel Committee on Banking Supervision, which includes supervisory authorities from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Sweden, Switzerland, the United Kingdom, and the United States, introduced the Framework for Internal Control Systems in 1998. Regulatory compliance is an integral part of the framework. The five elements of internal control are: management oversight and control culture, risk recognition and assessment, control activities and segregation of duties, information and communication, and monitoring activities and correcting deficiencies. The effective functioning of these five elements is key to an organization achieving its performance, information, and compliance objectives.
Control Objectives for Information and Related Technology (COBIT)

COBIT is an internationally accepted controls-based framework for IT governance that was first released by ISACA in 1996. COBIT has 34 high-level processes that cover 210 control objectives categorized in four domains: planning and organization, acquisition and implementation, delivery and support, and monitoring and evaluation. The framework guides an organization on how to use IT resources (i.e., applications, information, infrastructure, and people) to manage IT domains, processes, and activities to respond to business requirements, which include compliance, effectiveness, efficiency, confidentiality, integrity, availability, and reliability. Well-governed IT practices can assist businesses in complying with laws, regulations, and contractual arrangements.
| International Organization for Standardization (ISO) | ISO has developed more than 16,000 international standards for stakeholders such as industry and trade associations, science and academia, consumers and consumer associations, governments and regulators, and societal and other interest groups. The ISO 9000 series focuses on quality management systems, including ensuring controls are in place to comply with applicable regulatory requirements. The ISO 14000 series focuses on environmental management systems, including complying with applicable environmental regulatory requirements. ISO 9001 (introduced in 2000) and ISO 14001 (introduced in 1996) have been implemented by organizations in more than 160 countries. The ISO 27000 series focuses on information security management systems. The 27000 series helps organizations establish information security standards that meet business needs while ensuring compliance with regulatory and contractual requirements. |
### Standards for Internal Control In the U.S. Federal Government

| The U.S. Government Accountability Office issued the Standards for Internal Control in the Federal Government in 1999. The standards provide guidance on assessing risks and internal controls in programmatic, financial, and compliance operations. They are similar to COSO's 1992 framework |
BUSINESS AND IT CONTROLS

- The enterprise's system of internal controls impacts IT at three levels:
  - At the executive management level
  - At the business process level
  - To support the business processes
BUSINESS AND IT CONTROLS

Executive management level

- At the executive management level, business objectives are set, policies are established and decisions are made on how to deploy and manage the resources of the enterprise to execute the enterprise strategy. The overall approach to governance and control is established by the board and communicated throughout the enterprise. The IT control environment is directed by this top-level set of objectives and policies.
At the business process level, controls are applied to specific business activities.

Most business processes are automated and integrated with IT application systems, resulting in many of the controls at this level being automated as well.

These controls are known as application controls. However, some controls within the business process remain as manual procedures, such as authorisation for transactions, separation of duties and manual reconciliations.

Therefore, controls at the business process level are a combination of manual controls operated by the business and automated business and application controls.
BUSINESS AND IT CONTROLS
Support Business processes

• To support the business processes, IT provides IT services, usually in a shared service to many business processes, as many of the development and operational IT processes are provided to the whole enterprise, and much of the IT infrastructure is provided as a common service (e.g., networks, databases, operating systems and storage). The controls applied to all IT service activities are known as IT general controls. The reliable operation of these general controls is necessary for reliance to be placed on application controls. For example, poor change management could jeopardise (accidentally or deliberately) the reliability of automated integrity checks.
IT GENERAL CONTROLS AND APPLICATION CONTROLS

General controls are controls embedded in IT processes and services. Examples include:

- Systems development
- Change management
- Security
- Computer operations

Controls embedded in business process applications are commonly referred to as application controls. Examples include:

- Completeness
- Accuracy
- Validity
- Authorisation
- Segregation of duties
Limitations of Internal Control

Internal control, no matter how well designed and operated can provide only reasonable assurance to management and the board of directors regarding achievement of an entity’s objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include:

- The realities that human judgment in decision-making can be faulty, and that breakdowns can occur because of such human failures as simple error or mistake.
- Controls can be circumvented by the collusion of two or more people.
- Management has the ability to override the internal control system
- Costs versus Benefits – Resources always have constraints, and entities must consider the relative costs and benefits of establishing controls.
Roles and Responsibilities

- **Everyone** in an organization has some responsibility for internal control.
- Management, however, is responsible for an entity’s internal control.
- The chief executive officer is ultimately responsible and should assume ‘ownership’ of the control system.
- A number of external parties, such as external auditors, often contribute to the achievement of the entity’s objectives and provide information useful in effecting internal control. However, they are not responsible for the effectiveness of, nor are they a part of, the entity’s internal control system.
Evaluating Internal Control

• Evaluating internal controls is one of the auditor’s primary responsibilities.

• In evaluation internal controls, the auditor uses various tools and techniques. Example of such tools is the COSO Internal Control Evaluation Tools. The auditor may also develop and conduct audit tests as a means of evaluating the effectiveness of an internal control system.
Evaluating Internal Control

The COSO Model: How IT Auditors Can Use IT to Evaluate the Effectiveness of Internal Controls

- The COSO Model of Internal Controls uses five elements of internal controls: control environment, risk assessment, information and communication, control activities and monitoring.
Evaluating Internal Control - Control Environment

What is the risk of material misstatement occurring within the current entity and its environment? Some of the ways the control environment can be evaluated regarding the risks associated with the control environment include:

• Communication and enforcement of integrity and ethical values
• Commitment to competence
Evaluating Internal Control - Risk Assessment

• Has the entity made an effective effort to identify areas of risk that would allow a material misstatement to occur?

• The risk assessment aspect of COSO, in general, refers to the entity's ability to properly assess risks and, for major ("significant") risks, mitigate them to an acceptable level using controls.
Evaluating Internal Control - Information and Communication

• Does the entity have sufficient controls to ensure the timely and proper notification of a material misstatement if and when one occurs?

• The financial reporting information not only should have reliability, but should also be communicated in a timely manner and accurately to managers and decision makers. Therefore, in general, this aspect of controls deals with effective communication.
Evaluating Internal Control - Control Activities

• Are there sufficient controls that, in the aggregate, effectively mitigate the risk of a material misstatement in the financial statements to an acceptable level?
Evaluating Internal Control - Monitoring

• Does the entity have a system of monitoring activities to continuously evaluate and improve the effectiveness of its internal controls?

• Some of the various ways in which controls over monitoring of control effectiveness could be evaluated regarding the risks associated with those activities include:
  □ Ongoing and separate evaluations on internal controls over financial reporting
  □ Identifying and reporting deficiencies
  □ Assessing the quality of internal control performance over time
  □ Putting procedures in place to modify the control system as needed (add, change, delete)
AUDITING IN IT ENVIRONMENT
IT ENVIRONMENT EXPLAINED

- An IT environment exists when one or more computers of any type or size is involved in the processing of financial information, including quantitative data of significance to the audit whether those computers are operated by the entity or by a third party.
- Auditing in an IT environment is of two main types:
  - Operational audits of the functional business processes and activities
  - IT audits of the information systems infrastructure and applications.
Objective of Operational Audit in IT Environment

• The overall objective and scope of an audit does not change in an IT environment. The auditor’s audit objectives therefore do not change whether accounting data is processed manually or by computer.
The use of a computer changes the processing, storage, retrieval and communication of financial information and may affect the accounting and internal control systems employed by the entity.

The methods of applying audit procedures to gather evidence may therefore be influenced by the methods of computer processing.

The auditor can use manual audit procedures, or computer-assisted audit techniques, or a combination of both to obtain sufficient evidential matter.

However, in some accounting systems that use a computer for processing significant applications, it may be difficult or impossible for the auditor to obtain certain data for inspection, inquiry, or confirmation without computer assistance.
Effect of an IT Environment on The Audit

• In this regard, an IT environment may affect:
  ▫ The procedures followed by the auditor in obtaining sufficient understanding of the accounting and internal control system.
  ▫ The auditor's design and performance of tests of control and substantive procedures appropriate to meet the audit objective.
Effect of an IT Environment on The Audit

- The auditor should therefore consider the effect of IT environment on the audit. The auditor should evaluate, inter alia, the following factors to determine the effect of the IT environment on the audit:
  - The extent to which the IT environment is used to record, compile and analyse accounting information
  - The system of internal control in existence in the entity with regard to:
    - flow of authorized, correct and complete data to the processing center
    - processing, analysis and reporting tasks undertaken in the installation
  - The impact of computer-based accounting system on the audit trail.
Skills and Competence Required

- The auditor should have sufficient knowledge of the computer information systems to plan, direct, supervise, control and review the work performed. The sufficiency of knowledge would depend on the nature and extent of the IT environment.

- The auditor should consider whether any specialized IT skills are needed in the conduct of the audit. Specialized skills may be needed, inter alia, to:
  - obtain sufficient understanding of the effect of the IT environment on accounting
  - determine the effect of the IT environment on the assessment of risk; and
  - design and perform appropriate tests of control and procedures.
Skills and Competence Required (2)

- If specialised skills are needed, the auditor would seek the assistance of an expert possessing such skills, who may either be the auditor's staff or an outside professional.
- If the use of such a professional is planned, the auditor should obtain sufficient appropriate audit evidence that the work performed by the expert is adequate for the purposes of the audit.
Planning the Audit

- The auditor should obtain an understanding of the accounting and internal control systems sufficient to plan the audit and to determine the nature, timing and extent of the audit procedures. Such an understanding would help the auditor to develop an effective audit approach.
In planning the audit which may be affected by the IT environment, the auditor should obtain an understanding of the significance and complexity of the IT activities and the availability of the data for use in the audit. This understanding would include such matters as:

- the computer information systems infrastructure [hardware, operating system(s), etc., and application software(s) used by the entity, including changes, if any,
Planning the Audit (cont’d)

- the significance and complexity of computerised processing in each significant accounting application. An application may be considered to be complex when, for example:
  - the volume of transactions is such that users would find it difficult to identify and correct errors in processing.
  - the computer automatically generates material transactions or entries directly to another application.
  - the computer performs complicated computations of financial information and/or automatically generates material transactions or entries that cannot be (or are not) validated independently.
Assessment of Risk

• The auditor should make an assessment of risks inherent in the client’s operations.
Audit Procedures

• The auditor should consider the IT environment in designing audit procedures to reduce audit risk to an acceptably low level. He should make enquiries and particularly satisfy himself whether:
  ▫ adequate procedures exist to ensure that the data transmitted is correct and complete; and
  ▫ cross-verification of records, reconciliation statements and control systems between primary and subsidiary ledgers do exist and are operative and that accuracy of computer compiled records are not assumed.
Examples of Operational audits conducted by the Internal Audit Department of Bank of Ghana are:

- Government Accounts
- Payment Systems
- Foreign Exchange Operations
- Banking Services
- Currency Operations
- Domestic Treasury Operations
- Human Resources
- Payroll Administration etc.
What IT Auditing is All About?

- **IT auditing** is a branch of general auditing concerned with governance (control) of information and communications technologies (computers). IT auditors primarily study computer systems and networks from the point of view of examining the effectiveness of their technical and procedural controls to minimise risks.
What do IT Auditors actually do?

In short, IT auditors review risks relating to IT systems and processes including:

- Inadequate information security (e.g. missing or out of date antivirus controls)
- Inefficient use of corporate resources, or poor governance (e.g. spending large sums on unnecessary IT projects)
- Ineffective IT strategies, policies and practices (including lack of policies etc.)
- IT-related frauds
STAGES OF THE IT AUDIT PROCESS

• **Scoping and pre-audit survey** - the auditors determine the main area/s of focus and any areas that are explicitly out-of-scope, based normally on some form of risk-based assessment. Information sources at this stage include background reading, previous audit reports etc.

• **Planning and preparation** - during which the scope is broken down into greater levels of detail, usually involving the generation of an audit workplan or risk-control-matrix.

• **Fieldwork** - gathering evidence by interviewing staff and managers, reviewing documents, printouts and data, observing processes *etc*. This step may include the use of Computer Aided Audit Techniques (CAATs)
STAGES OF THE IT AUDIT PROCESS (2)

- **Analysis** - this step involves desperately sorting out, reviewing and trying to make sense out of the evidence gathered earlier.

- **Reporting** - Reviewing and trying to make sense out of the analysis and writing a report making the necessary recommendations for improvement. The report should include the auditee’s responses.

- **Follow up** – Conduct follow up to ensure implementation of audit recommendations.
Main types of IT Audits

• **Network / Operational computer system audits:** review the controls within and surrounding networks and operational computer systems at various levels *e.g.* network, operating system, application software, databases, logical/procedural controls, preventive/detective/corrective controls.

• **IT installation audits:** take a look at the computer building, room, including aspects such as physical security (*walls, CCTV, locks, guards, barbed wire, visitor procedures ...*), environmental controls (*fire and flood protection, power supply*), computer and network operations processes and the IT equipment itself.
Main types of IT Audits (cont’d)

- **IT Management Audits**: review the organization, structure, strategy, work planning, resource planning, budgeting, cost controls *etc.* and, where applicable, relationships with outsourced IT providers (in some cases, these aspects may be audited by operations and financial auditors, leaving the IT auditors to do the more technological aspects).

- **IT process audits**: review processes which take place within IT such as application development, testing, implementation, operations, maintenance, housekeeping (backups, preventive maintenance *etc.*), support, incident handling.
Main types of IT Audits (cont’d)

- **Change Management Audits**: review the planning and control of changes to systems, networks, applications, processes, facilities *etc.*, including configuration management, control over the promotion of code from development through testing to production, and the management of changes to the organisation as a result of ICT.

- **Information Security & Control Audits**: review controls relating to confidentiality, integrity and availability of systems and data.

- **IT legal compliance audits**: review legal and regulatory aspects of IT systems (*e.g.* software copyright compliance, protection of personal data).
Main types of IT Audits (cont’d)

• **Certification and other compliance audits**: compliance to information security standards such as [ISO27k](http://ISO27k) is normally audited by IT auditors.

• **Disaster contingency/business continuity planning/disaster recovery audits**: review arrangements to restore some semblance of normality after a disaster affecting the IT systems, and perhaps assess the organisation’s approach to risk management.

• **IT strategy audits**: review various aspects of IT strategy, vision and plans, including their relationship to other strategies, visions and plans.
Examples of IT Audits conducted by the Internal Audit Department of Bank of Ghana are:

- Information Security,
- Network Administration,
- Oracle Application,
- T24 Application,
- Other Applications Audit.
Computer Aided Audit Techniques (CAATs)

- CAATs are tools/utilities to help auditors select, gather, analyse and report audit findings. Starting with the basics, many computer applications have useful built-in data analysis/audit facilities.
- Database programs typically have custom reporting facilities and sometimes include pre-configured reports intended for use by auditors.
- Specialised CAAT tools such as ACL (Audit Control Language) and IDEA (Interactive Data Extraction and Analysis) include libraries of prewritten queries to ask typically meaningful questions on data sets.
Here are the sorts of questions an IT auditor (or an ‘ordinary’ auditor working on a computer system) might want to ask:

- How many changes have been made to the customer details file during the year?
- Are there any out-of-range or unusual data values, or any suspicious data patterns?
- Are any of our suppliers also employees?

CAATs are wonderful for asking bizarre audit questions that ordinary system users, managers, analysts and developers have probably never even considered, some of which can lead to the identification of frauds or confirmation that control weaknesses have not been exploited.
Examples of uses of IDEA at Internal Audit - BOG

• **T24 AUDIT**
  ▫ IDEA was used to extract system access logs and check for the following
  ▫ Duplication of users
  ▫ Users whose assigned functions did not match their work schedule

• **GOVERNMENT ACCOUNTS AUDIT**
  ▫ Used To Extract Overdrawn Positions
  ▫ Used to select a sample of transactions for audit review

• **CURRENCY OPERATIONS AUDIT**
  ▫ Used to select samples of various transactions for audit review
  ▫ Used to check the computation of Agency commission
End of Lecture

Have a nice day