Robust Internal Controls including COBIT 2019: Must to achieve Enterprise Mission – Role of CAs

CA. (Dr.) Rajkumar Adukia

Author of more than 300 books,

Business Growth and Motivational Coach,

Member IFRS SMEIG London 2018-2020

Ex director - SBI mutual fund, BOI mutual fund

Ph. D , LL.B, LLM (Constitution), FCA,FCS, MBA, MBF , FCMA, Dip Criminology, Dip in IFR(UK) Justice (Harvard) , CSR, Dip IPR, Dip Criminology ,dip in CG , Dip Cyber, dip data privacy B. Com , M. Com., Dip LL & LW

Student of – MA (psychology), MA (Economics), IGNOU PGDCR, PGCAP etc.

Chairman western region ICAI 1997, Council Member ICAI 1998-2016

Internal Controls are systematic and procedural steps adopted by an organization to mitigate risks, primarily in the areas of financial accounting and reporting, operational processing and compliance with laws and regulations. They are steps taken to strengthen the organization's systems and processes, as well as help to prevent and detect errors and irregularities and thus essentially risk mitigation exercise. The ***Committee of Sponsoring Organizations of the Tread way Commission (COSO)***, in its 2013 *Internal Control – Integrated FrameworkReport*, defines internal control as: "A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives related to operations, reporting, and compliance." An effective internal control is a prerequisite for any organization to realize its mission. If we look back, all major scandals and business failures in India or abroad are result of failure of Internal Control. Be it Waste Management Scandal of 1998 which happened due to fraud of internal employees of the organization, orEnron Scandal of 2001 which is remembered as epitome of corporate fraud on it investors, or Satyam Fiasco in India investigation of all indicate failure of internal control at one level or the other. It can safely be said internal control is a must for any kind of organization, irrespective of its size, setup or culture even though its significance in big corporate increases many folds due to involvement of public money and disassociation of management with ownership.

Role of Chartered Accountants in Internal Control

Chartered Accountants are professionals who play vital role in an organization in fields of accounting, internal and external audit, tax planning, capital budgeting, budget forecasting, financing and many other activities.They work in many roles, in all industries and across the public, private and not-for-profit sectors. However, it is felt in matters of internal control, there

still lots of scope awaiting Chartered Accountants. One of the most essential traits of this profession is skepticism. Chartered Accountants by their education, training and experience in field of audit/assurance develop a level of professional skepticism which means:

- having a questioning mind;
- being alert to anything that may indicate misstatement due to error or fraud; and
- Critically assessing audit evidence.

Besides, the Chartered Accountants are also expected to have keen and analytical brain which enables them to analyze situations and results quickly and correctly. They generally are good communicator and quick learners. All of the above features are core values expected of any person given the onus of developing an Internal Control system in any organization.

With above traits, Chartered Accountants can assist management in developing internal control standards and procedures within the organization by understanding vital processes in business and detecting loophole and potential security gaps. A list of opportunities that a CA can explore in area of Internal Control:

1. Improvement of Internal Controlto bring it in compliance with regulatory requirements which will essentially involve following steps:
    a. Proper guidance for developing a clear communication about the statement of Risk Appetite and measures for Risk Management;
    b. Analyzing the current control environment in line with the statement of Risk Appetite and identifying inherent gaps;
    c. Developing a strong board and specific processes to fulfill the identified gaps;
    d. Document the process flows and controls to support the relevant regulations;
    e. Arranging the training of internal control to management and staff; and
    f. Monitoring the internal control process.
2. Implementation of an Enterprise Resource Planning (ERP) System

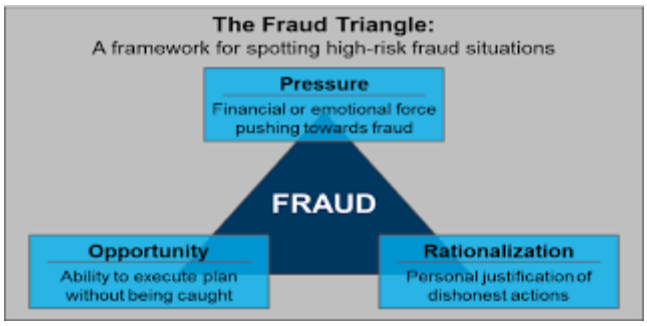
3. Integration of technology into governance, risk management and compliance projects
4. Design of the internal control system monitoring process
5. Preparation of documentation and the selection of software for controls procedures monitoring
6. Compliance of Section 404 of The Sarbanes-Oxley Act of 2002
7. Establishing Internal Control for safe guarding of asset
8. Being part of Internal Control Committee
9. Assist Internal Auditor in assessment of effectiveness of internal control

Brief History of Internal Control

Internal controls have existed from ancient times. They have long been a part of human affairs. Evidence of it can be found in **Ptolemaic** Kingdom of Egypt which was founded in 305 BC as there was a dual administration, with one set of bureaucrats charged with collecting taxes and another with supervising them. Also in the Republic of China, there was a Supervising Authority which investigates the other branches of government.

However, internal control issomewhat similar to as is perceived today, was first defined by the American Institute of Accountants in 1949, followed by further clarifications in 1958 and 1972.

Cadbury Committee in UK on Corporate Governance released a report in Dec 1992 for Financial Reporting Council of London Stock Exchange, recommending that single person should not be vested with the decision making power i.e. the role of chairman and chief executive should be clearly separate. It also recommended that a majority of Directors must be independent non-executive directors i.e. not having financial interests in the co. and should act independently while giving their judgment on issue of strategy, performance, allocation of resources and designing code of conduct.



Thereafter, in 1992, the Committee of Sponsoring Organizations of the Tread way Commission (COSO) issued *Internal Control – Integrated Framework* to help businesses and other entities assess and enhance their internal control systems It defined Internal Control consisted of 5 interrelated components: Control Environment, Risk Assessment, Control Activities, Information and Communication, Monitoring. In 2013, the framework was updated to address changes in business and operating environments since the original framework.

Besides, owing to accounting scandals in America, Sarbanes Oxley Act 2002 also emphasized on the importance of Internal control as Section 404 requires auditors to attest and report on the assessment on the effectiveness of the internal control structure and procedures for financial reporting and Sec 302 require the Principal Officers to certify quarterly and annual statements responsibility for establishing and maintaining Internal Controls over financial reporting.

In India, even though the concept of internal audit was present in the Companies Act, 1956 in the form of Section 581ZF which stipulated that 'Every Producer Company shall have internal audit of its accounts carried out, at such interval and in such manner as may be specified in articles, by a chartered accountant', the area of internal control was rather assumed and not prescribed in any regulatory framework till turn of this century. **Companies (Auditor's Report) Order, 2003** (referred to as "**CARO, 2003**) prescribed by Central Government, required auditors to state if there is an adequate internal control system commensurate with the size of the company and the nature of its business, for the purchase of inventory and fixed assets and for the sale of goods and services. Whether there is a continuing failure to correct major weaknesses in internal control system. The scope of it was increased in CARO 2015 to include reporting on adequate internal control procedure for sale of services also. CARO, 2015 also required auditors to comment onthe company has an internal audit system commensurate with its size and nature of its business. Internal Control also found its place in erstwhile Clause 49 of the Listing

Agreementby SEBI in 2005 which required Certification of internal controls and internal control systems by CEO/ CFO for the purpose for financial reporting. Thereafter, the requirements were more comprehensively dealt with in the Companies Act, 2013 and Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, which are mostly in line with SOX requirement in America**.** (Discussed in details later in the article).

Related Terms

Internal Financial Control

Internal controls are set to cover a variety of areas from operational to financial control. Controls over financial reporting have received the most attention from the regulatory and oversight communities.Especially after Satyam Scandal of 2009, the inability of the audit process to find the financial fraud committed by the management bought to focus various loopholes in the regulatory and legal framework dealing with board of directors and auditors of the company. Consequently, Indian legislators began search for best practices across the world like Sarbanes Oxley regulations in United States (US), Turnbull Guidance in United Kingdom (UK) and JSOX in Japan to raise the bar of corporate governance in India and the result was the introduction of Internal Financial Control regulations in Companies Act -2013. Explanation to section 134(5)(e) of the Companies Act, 2013 defines Internal financial Control as : the term "internal financial controls" means the policies and procedures adopted by the company for ensuring the orderly and efficient conduct of its business, including adherence to company's policies, the safeguarding of its assets, the prevention and detection of frauds and errors, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information.

Internal Control over Financial Reporting (ICFR)

From this definition, it is evident that the extent of the Internal Financial Control is not limited to financial reporting controls. However, the auditor of the company cannot be expected to comment on operational conduct/ operational efficiencies of the business. Therefore, it led to devising of new term Internal Controls over Financial Reporting (ICFR) which would mean the auditors would be required to report on the internal financial controls on financial reporting aspect only.

ICAI has issued a "Guidance Note on Audit of Internal Financial Controls over Financial Reporting" which defines internal financial controls over Financial Reporting quite narrowly as follows: "A process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with Generally Accepted Accounting Principles. A company's internal financial control over financial reporting includes those policies and procedures that

(i) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company;

(ii) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with Generally Accepted Accounting Principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and

(iii) Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements."

Therefore, Internal Control over Financial Reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles.

Internal Audit

Internal audit is an independent service to access an organization's internal controls, its corporate practices, its processes, and its methods. It helps in ensuring compliance with the various laws applicable to an organization, safeguarding of assets, prevention of fraud and errors thereby securing attainment of organizations mission. Internal audit is instrumental in checking the effectiveness of internal control function and its operational standards framed by the organization.

Institute of Internal Auditors (IIA) has prescribed *International Standards for the Professional Practice of Internal Auditing (Standards)*which is essential in meeting the responsibilities of internal auditors and the internal audit activity in diverse legal and cultural environments for organizations that vary in purpose, size, complexity, and structure; and by persons within or outside the organization.

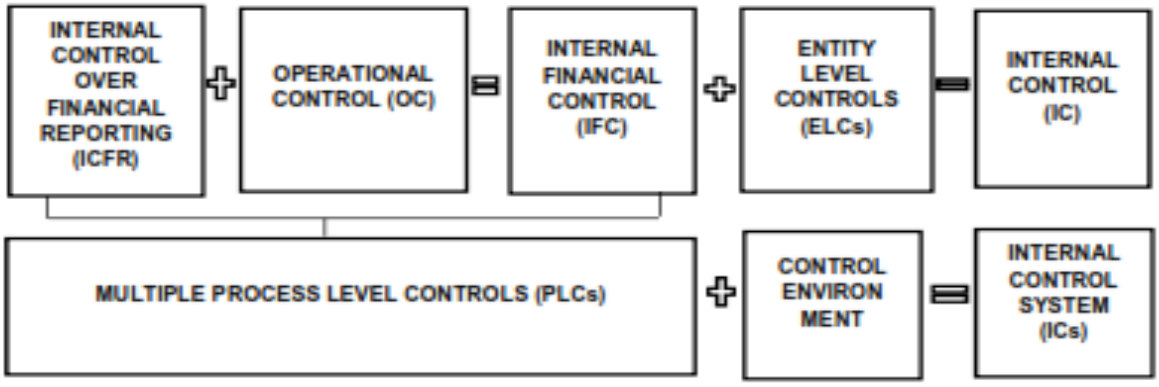
In India, The Internal Audit Standard Board of the ICAI pronounces*Standards on Internal Audit (SIAs)*, establish uniform evaluation criteria, methods, processes and practices. The Standards are pronouncements which form the basis for conducting all internal audit activity. These pronouncements are designed to help the internal auditor to discharge his responsibilities.

Internal Check

Internal check is an arrangement of duties of members of staff in such a manner than the work performed by one person is automatically and independently checked by the others. It is a kind of continuous internal audit carried on by the staff itself. It is introduced with defined instructions given to staff as to their arena of work with a view to control their work and maintenance of accurate records of the same.

Internal Control System

The term "Internal Controls System" is an all-encompassing term generally used to refer all types of controls put together, covering Control Environment or Entity Level Control, Operational Control and Internal Financial Controls?



Statutory Requirement for Internal Control in India

For All Companies

Section 143 (3) (i) of Companies Act, 2013 requires Auditor's report for all companies (listed or not) to state the adequacy and operating effectiveness of the Company's internal financial controls. Besides, Rule 8 (5) (viii) of Companies (Accounts) Rules, 2014 require Board of Directors to report on adequacy of internal financial controls with reference to financial statement. However, Ministry of Corporate Affairs (MCA) by **Notification No *G.S.R. 583(E) dated 13th June, 2017*** has notified that this provisionshall not be applicable for those audit reports of private limited companies /**One-person companies (OPC)** which has Annual turnover of less than Rest 50 Cores or has aggregate borrowings of less than 25 Cores from banks, Financial institutions or body corporate at any time during the financial year issued after 13th June 2017.

Additional Requirements for Listed Entities

Section 134 (5) (e) of Companies Act, 2013 requires that Directors' Responsibility statement shall state that: The directors, in the case of a listed company, had laid down internal financial controls to be followed by the company and that such internal financial controls are adequate and were operating effectively. Section 134 (8) states that If a company is in default in complying with the provisions relating of this section, the company shall be liable to a penalty of three lakh rupees and every officer of the company who is in default shall be liable to a penalty of fifty thousand rupees

Section 177 (4) (vii) of Companies Act, 2013 requires Every Audit Committee to act in accordance with the terms of reference specified in writing by the Board which shall inter alia include evaluation of internal financial controls and risk management systems. It also applies to Companies that has borrowed public money.

Section 177 (5) of Companies Act, 2013 states thatThe Audit Committee may call for the comments of the auditors about internal control systems, the scope of audit, including observations of the auditors and review of financial statement before their submission to the Board and may also discuss any related issues with the internal and statutory auditors and the management of the company. It also applies to Companies that has borrowed public money.

Schedule IV – II (4) of Companies Act, 2013 that deals with the Code for Independent Director requires that the independent directors of listed entity that has borrowed public money must satisfy themselves on the integrity of financial information and ensure that financial controls and the systems of risk management are robust and defensible.

Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 (LODR) on Internal Control

Compliance certificate be furnished by chief executive officer and chief financial officer to Board of Directors under ***Regulation 17(8)*** of LODR must state that

- They accept responsibility for establishing and maintaining internal controls for financial reporting and that they have evaluated the effectiveness of internal control systems of the listed entity pertaining to financial reporting and they have disclosed to the auditors and the audit committee, deficiencies in the design or operation of such internal controls, if any, of which they are aware and the steps they have taken or propose to take to rectify these deficiencies;
- they have indicated to the auditors and the Audit committee significant changes in internal control over financial reporting during the year and instances of significant fraud of which they have become aware and the involvement therein, if any, of the management or an employee having a significant role in the listed entity's internal control system over financial reporting

Part C of Schedule II which covers role of the audit committee and the information to be reviewed by the audit committee under ***Regulation 18(3)*** of LODR, requires Audit committee to:

- review, with the management, performance of statutory and internal auditors, adequacy of the internal control systems;
- review the findings of any internal investigations by the internal auditors into matters where there is suspected fraud or irregularity or a failure of internal control systems of a material nature and report the matter to the board

- mandatorily review the information management letters / letters of internal control weaknesses issued by the statutory auditors and) internal audit reports relating to internal control weaknesses;

Regulation 21(4) of LODR requires the board of directors to define the role and responsibility of the Risk Management Committee which should mandatorily include responsibility to formulate a detailed risk management policy including measures for risk mitigation including systems and processes for internal control of identified risks

Schedule V of LODR specifies additional disclosures in Annual Accounts of listed entity. It requires entities to disclose discussion on the internal control systems and their adequacy within the limits set by the listed entity's competitive position besides other things.

Standards on Auditing Pronounced by the Auditing and Assurance Standards Board (AASB) of ICAI on Internal Control

Standard on Auditing (*SA*) 315, "Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment" deals with the auditor's responsibility to identify and assess the risks of material misstatement in the financial statements, through understanding the entity and its environment, including the entity's internal control. It defines the term Business Risk, Internal Control, Risk assessment procedures and significant risk a follows:

- Business risk as a risk resulting from significant conditions, events, circumstances, actions or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies.
- Internal control as the process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, safeguarding of assets, and compliance with applicable laws and regulations. The term "controls" refers to any aspects of one or more of the components of internal control.

- Risk assessment procedures as the audit procedures performed to obtain an understanding of the entity and its environment, including the entity's internal control, to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels.
- Significant risk as an identified and assessed risk of material misstatement that, in the auditor's judgment, requires special audit consideration.

The standard requires the auditor to perform risk assessment procedures to provide a basis for the identification and assessment of risks of material misstatement at the financial statement and assertion levels including inquiries of management, of appropriate individuals within the internal audit function and of others within the entity who in the auditor's judgment may have information that is likely to assist in identifying risks of material misstatement due to fraud or error, Analytical procedures and observation and inspection.

***Standard on Auditing (*SA) 265, *"Communicating Deficiencies in Internal Control to Those Charged with Governance and Management"*,**deals with the auditor's responsibility to communicate appropriately to those charged with governance and management deficiencies in internal control that the auditor has identified in an audit of financial statements. The standard also sets norms for identification of deficiencies in internal control. Accordingly, deficiency in internal control is said to exist when:

- A control is designed, implemented or operated in such a way that it is unable to prevent, or detect and correct, misstatements in the financial statements on a timely basis; or
- A control necessary to prevent, or detect and correct, misstatements in the financial statements on a timely basis is missing.

The standard also gives guidance as to when such deficiency can be regarded as significant. Accordingly, the deficiency in internal control is significant if such deficiency or combination of deficiencies in internal control that, in the auditor's professional judgment, is of sufficient importance to merit the attention of those charged with governance. The standard requires auditor to communicate in writing significant deficiencies in internal control identified during the audit to those charged with governance on a timely basis, giving description of the deficiencies

and an explanation of their potential effects and sufficient information to enable those charged with governance and management to understand the context of the communication.

Standard on Auditing (SA) 610: Using the Work of Internal Auditors deals with the external auditor's responsibilities if using the work of internal auditors. The SA defines Internal audit function as a function of an entity that performs assurance and consulting activities designed to evaluate and improve the effectiveness of the entity's governance, risk management and internal control processes. It requires the external auditor to use the work of the internal audit function to modify the nature or timing, or reduce the extent, of audit procedures to be performed directly by the external auditor; it remains a decision of the external auditor in establishing the overall audit strategy.

Standard on Internal Audit (SIA) 120: Internal Controls seeks to clarify the concept and the responsibility of the Internal Auditor, Management and other stakeholders, with respect to Internal Controls, keeping in mind their legal, regulatory and professional obligations. It identifies financial accounting and reporting, operational processing and compliance with laws and regulations as three primary areas for internal control.

PCAOB on Internal Control

The Public Company Accounting Oversight Board (PCAOB) is a non-profit organization that regulates audits of publicly traded companies to minimize audit risk. It was established at the same time as the Sarbanes-Oxley Act of 2002 to address the accounting scandals of the late 1990s in North America. The PCAOB enforces the professional standards and other related laws and rules governing the audits of public companies and broker-dealers. PCAOB staff investigates potential violations by public accounting firms and individuals of these standards, laws, and rules. It prescribes Auditing Standards to regulate audits of public companies and SEC-registered brokers and dealers in order to protect investors and further the public interest in the preparation of informative, accurate, and independent audit reports. In 2007 PCAOB, released *AS 2201: An Audit of Internal Control over Financial Reporting That Is Integrated with An Audit of Financial Statements.*

AS 2201 requires an auditor to express an opinion on the effectiveness of the company's internal control over financial reporting. A company's internal control cannot be considered effective if one or more material weaknesses exist. To form a basis for expressing an opinion, the auditor must plan and perform the audit to obtain appropriate evidence that is sufficient to obtain reasonable assurance about whether material weaknesses exist as of the date specified in management's assessment. A material weakness in internal control over financial reporting may exist even when financial statements are not materially misstated.

Internal Control Framework

Internal Controls Framework" is a pre-defined benchmark Internal Control System, based on suitable criteria, which can be used by management or auditors to assess the design, adequacy and operating effectiveness of the overall internal control system.

Internal Control—Integrated Framework that was published in 1992 by the Committee of Sponsoring Organizations of the Tread way Commission (COSO), COSO is a voluntary private sector initiative dedicated to improving organizational performance and governance through effective internal control, enterprise risk management, and fraud deterrence. On May 14, 2013, COSO released an updated version of its Internal Control—Integrated Framework

The Framework was developed to address the effectiveness and efficiency of the entity's ***operations***, the financial and non-financial reporting's reliability, timeliness, transparency or other terms as set forth by regulators, recognized standard setters or the entity's policies, and the entity's ***compliance*** to the laws and regulations it is subject to.

Five elements of internal controls

The COSO Framework consists of five integrated components that are expected to assist the organization in achieving the objective of enterprise. These 5 components are *Control environment*, Risk assessment, Control activities, Information & communication, and Monitoring. These five components have a total of seventeen principles that represent the

fundamental concepts of the components to which they are associated. These principles in turn have defined approaches which serve as guides in accomplishing them. However, the Framework does not restrict entities from application of approaches of their own especially when not specifically addressed by the Framework.

Element 1: Control environment

The foundation of internal controls is the tone of your business at management level. Control Environment is foundation on which an effective system of internal control is built and operated in an organization. It is a set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. Those at helm of affairs like board of directors and senior management establish the tone at the top regarding the importance of internal control including expected standards of conduct. The Control environment strives to

- achieve its strategic objectives of the enterprise
- provide reliable financial reporting to internal and external stakeholders,
- operate its business efficiently and effectively,
- comply with all applicable laws and regulations, and
- safeguard its assets

There are 5 principles associated with control environment viz.

- The organization demonstrates a commitment to integrity and ethical values.

- The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
- Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
- The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
- The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Element 2: Risk Assessment

Every entity faces a variety of risks from external and internal sources. Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. A risk assessment is a process to identify potential hazards (hazard identification), analyze what could happen if a hazard occurs (Risk analysis, and risk evaluation) and Determine appropriate ways to eliminate the hazard, or control the risk when the hazard cannot be eliminated (risk control).In other words, it is a thorough look at the workplace to identify those things, situations, processes, etc. that may cause harm. Post identification management must analyze and evaluate how likely and severe the risk is. When this determination is made, it must decide what measures should be in place to effectively eliminate or control the harm from happening.

The following factors can assist in Risk Assessment:

• The industry in which your company operates

• General economic conditions

• The size and complexity of your organization

• Regulatory changes

• Company's operational strategies and objectives

• A potential exit strategy

Of the 17 principles stated in COSO framework, there are 4 principles linked with Risk Management viz.

- The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
- The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
- The organization considers the potential for fraud in assessing risks to the achievement of objectives.
- The organization identifies and assesses changes that could significantly impact the system of internal control.

Control Activities

Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are all encompassing and are performed at all levels of the entity and at various stages within business processes and technological environment. They may be preventive or detective in nature. They may also involve manual and automated activities. Example of control activities include:

- Authorizations and approvals,
- Verifications,
- Reconciliations,
- Business performance reviews.
- Segregation of duties, etc.

Of the 17 principles stated in COSO framework, there are 3 principles linked with Control Activities viz.

- The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

- The organization selects and develops general control activities over technology to support the achievement of objectives.
- The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Information and Communication

Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives. Information is obtained or generated by management from both internal and external sources in order to support internal control components. *Communication* based on internal and external sources is used to disseminate important information throughout and outside of the organization, as needed to respond to and support meeting requirements and expectations. It is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication of information is essential as it allows senior management to demonstrate to employees that control activities should be taken seriously. Communication is all pervasive as it flows up, down and across the entity.

Of the 17 principles stated in COSO framework, there are 3 principles linked with Control Activities via

- Uses relevant information
- Communicates internally
- Communicates externally

Monitoring Activity

Monitoring activities are periodic or ongoing evaluations to verify that each of the five components of internal control, including the controls that affect the principles within each component, are present and functioning. Ongoing or continuous evaluations are built into business processes at different levels of the entity and enables timely information. Separate or periodically evaluations vary in scope and frequency depending on size of the entity, assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings during the monitoring are evaluated against criteria established by top management and the

board of directors while setting control environment, and deficiencies are communicated to management and the board of directors as appropriate.

Of the 17 principles stated in COSO framework, there are 2 principles linked with Control Activities via

- Conducts ongoing and/or separate evaluations
- Evaluates and communicates deficiencies

INFORMATION TECHNOLOGY CONTROLS

With increasing importance of information technology on our lives and business environment, the need to protect and the IT systems from internal and external threats have also increased many fold. I**nformation technology controls** (or **IT controls**) are specific activities performed by persons or systems designed to ensure that business objectives are met. They indispensable part of an enterprise's internal control. IT control objectives relate to the confidentiality, integrity, and availability of data and the overall management of the IT function of the business enterprise. There are to categories of IT Controls: IT general controls (ITGC) and IT application controls. ITGC include controls over the Information Technology (IT) environment, computer operations, access to programs and data, program development and program changes. IT application controls refer to transaction processing controls, sometimes called "input-processing-output" controls. The COBIT Framework (Control Objectives for Information Technology) is a widely used framework promulgated by the IT Governance Institute, which defines a variety of ITGC and application control objectives and recommended evaluation approaches.

COBIT 2019 by IASACA

COBIT is an **Information Technology [IT] Management Framework** developed by the ISACA (Information Systems Audit and Control Association), to help businesses develop, organize and implement various strategies around and for information management and effective governance. It is expected to be a supportive tool for managers allowing them to bridge the crucial gap between technical issues, business risks, and control requirements.

Released in 1996 1st, COBIT (Control Objectives for Information and Related Technologies) was in its initial phase, designed as a set of IT control objectives, to help the financial audit

community, to better navigate with the growing IT environments around. In 1998, version 2 was brought, expanding the same, to apply outside the auditing community. Further after the year 2000, version 3 was developed, which brought in the IT management & information governance techniques, which are the further aspects, found in the framework today. **COBIT 5**, the latest iteration of the framework, was released in 2012

An updated version of COBIT was announced in 2018, doing away with the version number and naming it COBIT 2019 this time. This updated version of COBIT is designed to constantly evolve with "more frequent & fluid updates**,**" as per ISACA.

COBIT 2019 came in with an aim to build governance strategies; that are more flexible, collaborative and address the new plus changing technologies.COBIT 2019 update the set-up for advanced modern enterprises, by addressing & catering to the many new trends, evolving technologies & deeper security needs, in complex and connected environment/s.

The performance management systems now permit more flexibility, when using maturity plus capability measurements. Overall, the framework is designed to give businesses more flexibility, when customizing it's IT governance strategy and Policy overall.

Like other IT management frameworks, COBIT 2019 helps align business goals with IT goals by establishing and aligning the links between the two and creating a process that can help bridge a gap between IT silos/hubs and outside departments.

The main difference between COBIT 2019 and various other IT Management frameworks is that COBIT 2019 focuses specifically on security, risk management and information governance. This is emphatically clarified in COBIT 2019, with clearer definitions & outlines, of what COBIT is and what it is not. For example, as per ISACA COBIT 2019 is not a framework for organizing business processes, for managing technology, making IT-related decisions, architecture or strategies. COBIT 2019 focuses mainly & principally on security & risk aspects, over any other aspects, which may seem to overlap, but usually are not allowed to overlap, in the interests of clarity and effectiveness of security and risk aspects, combined with aligned information governance.

Rather, it's designed strictly as a framework, for governance and management of Enterprise IT only, across the organization, encompassing the risk & security aspects primarily, as above-said. This is better clarified & stated for businesses in the updated version, so that there is less confusion & ambiguity, about how COBIT 2019 should be used and implemented.

According to ISACA, COBIT 2019 was updated to include:

- Focus areas and design factors that give more clarity on creating a safe governance system, for business needs
- A better tool to measure performance of IT
- More support for decision making including new online collaborative features
- Better alignment with any global standards, frameworks and best practices, to boost the framework's relevance
- An open-source model that allows for feedback from the global governance community to encourage faster updates and enhancements
- Regular updates released on a rolling basis

COBIT 2019 also lays down "focus area" concepts, which describes specific governance topics, issues & allied matters, which can be addressed by the management or governance objectives. Some examples of these focus areas include small and medium enterprises, cyber-security, digital transformation and cloud computing. Focus areas keep being added and changed, as needed, based on trends, research and feedback. Most interestingly, that there is no limit for the number of focus areas, includable in COBIT 2019.

Components of COBIT 2019

- **COBIT 2019 Framework: Introduction and methodology**: The main guide that introduces the basic COBIT principles alongside the structure of the overall framework.
- **COBIT 2019 Framework: Governance and management objectives:** A companion guide that dives into the COBIT Core Model and 40 governance and management objectives. Each objective is described including its purpose, how it connects with the enterprise and how it aligns goals.
- **COBIT 2019 Design Guide**: A companion guide that offers in-depth guidance for developing a uniquely tailored governance system for your organization.

- **COBIT 2019 Implementation Guide**: The fourth companion guide in the framework, which guides businesses through implementing the governance strategy once it's developed. This includes best practices, ways to avoid pitfalls and how to integrate your COBIT 2019 strategy with other parts.

Note: One major change to COBIT 2019 is that it now encourages feedback from the practitioner or user community. In early 2019 the ISACA released a crowd-sourced version of COBIT 2019, where practitioners & users could leave comments, suggest improvements or innovatively propose new concepts and ideas, based on their experiences and what they have gone through.

COBIT principles and benefits

COBIT 2019 is designed to be more prescriptive to guide companies in developing a governance strategy, including Risk & Security aspects primarily, while also allowing organizations to more comfortably tailor, a unique best-fits, governance strategy as said here. It defines the "components to build and sustain a governance system: processes, policies and procedures, organizational structures, information flows, skills, infrastructure, and culture and behaviors," according to the ISACA. Formerly referred to as "enablers" in COBIT 5, these components better define, what businesses need for a strong governance system, with emphasis on Higher Security and lowering of Risks overall.

According to the ISACA, COBIT 2019 best suits clients that use multiple frameworks and well suited for those organizations that are required to follow specific regulatory guidelines from government, local and such other similar authorities/bodies.

The COBIT 2019 framework helps businesses align existing frameworks in the organization and understand how each framework, will fit into the overall strategy. It can also help businesses monitor the performance of these other frameworks, especially in terms of security compliance, information security and risk management.

It's also designed to give senior management, more insight into how technology can align with organizational goals. You can directly map pain points in the business to certain aspects of the framework, emphasizing the need for "control-driven IT," according to the ISACA.

BENEFITS AND WEAKNESSES OF INTERNAL CONTROLS

Robust internal control systems are beneficial to organizations because not only they provide a measure of security and assurance to management that policies are being followed and assets are not being misused but are also an organized means of achieving organizational goals and objectives. Therefore, in an organization where controls are weak or non-existent, a number of problems can result, such as:

- reduced quality of services or product,
- unauthorized transactions
- inaccurate or incomplete information
- untimely reports
- assets are not safeguarded
- misappropriation of funds
- regulatory non-compliances

These can become grave over a period of time and lead to organizational failure leading to loss of employment and economic losses to various stake holders like creditors, shareholders, government, bankers and employees,

TYPES OF INTERNAL CONTROL

Entity Level Controls and Process Level Controls

Entity Level Controls (ELCs): These are e broad-based internal control covering the whole entity e.g., Code of Conduct in an Organization. They are part of control environment.

Process Level Controls (PLCs): These are controls that are focused to a specific process or area e.g., Order processing or Payroll, etc. They are designed under the broad framework of entity level controls.

Internal Financial Controls and Operational Controls

As Internal Financial Controls (IFCs): When Internal Controls mitigate the risk of financial exposure, they are also referred to as Internal Financial Controls.

Operational Controls (OCs): When they mitigate operational risks, they are also referred to as Operational Controls.

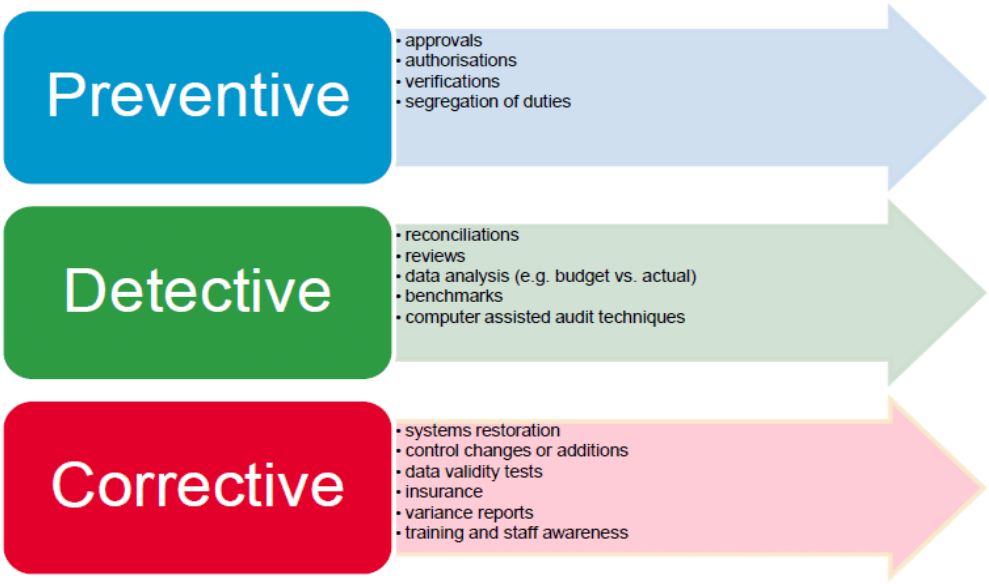
Manual Controls and Automated Control

Manual Control: Internal Control that generally operates with human intervention and requires continuous human effort is called Manual Controls.

Automated Control: When computer controls are used to mitigate risk of system failure/mal-functioning or application is called automated controls. Automated controls may be of two types IT General controls or Application Controls. When computer controls are deployed to secure the systems they are called IT General Controls (e.g., access controls) or check transaction processing at an application level and called Application Controls (e.g., sequential numbering of invoices, etc.).

Preventive, Detective and Corrective Internal Controls

Internal controls are detective, corrective, or preventive by nature. . Preventive controls are designed to keep errors and irregularities from occurring in the first place Detective controls on the other hand are designed to detect errors or irregularities that may have occurred. Corrective controls are designed to correct errors or irregularities that have been detected.



Conclusion

As we read through the importance of robust internal control system in an organization cannot be overstated. However, internal control has certain inherent limitations too. In the performance of the control procedures, errors can result from misunderstanding instructions, mistakes of judgment, carelessness, or other personal factors. Control procedures which require a segregation of duties can be circumvented by collusion. At times, control procedures can be circumvented intentionally by management and over a period of time control procedures may become inadequate or irrelevant due to changing circumstances and technology. Thus, monitoring and reviewing internal control system is as important as designing one. A need is therefore being felt, to have internal control committee in large organizations like audit committee with defined roles.

Important Link

https://www.pcaobus.org/

https://www.sarbanes-oxley-101.com/

https://www.isaca.org/resources/cobit

https://www.icai.org/post/standards-on-internal-audits

https://www.icai.org/post/auditing-review-and-other-standards-formerly-known-as-aas-complete-text

https://www.coso.org/Pages/default.aspx