Internal Controls Framework

Arab Federation of Accountants & Auditors
3 November 2018
Cairo, Mariotte Hotel

Elie Abboud *Managing Partner – UHY Lebanon*
Former President - LACPA

The adopted Internal Control Framework

While Internal Control was not defined in the Act, the COSO definition has been accepted by the US government and its agencies, incorporated in US auditing standards , and is a generally accepted integrated framework for control infrastructure.

As defined in 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 following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

COSO identifies five components of control that need to be in place and integrated to ensure the achievement of each of the objectives.

Objectives Are A Prerequisite for Internal Control

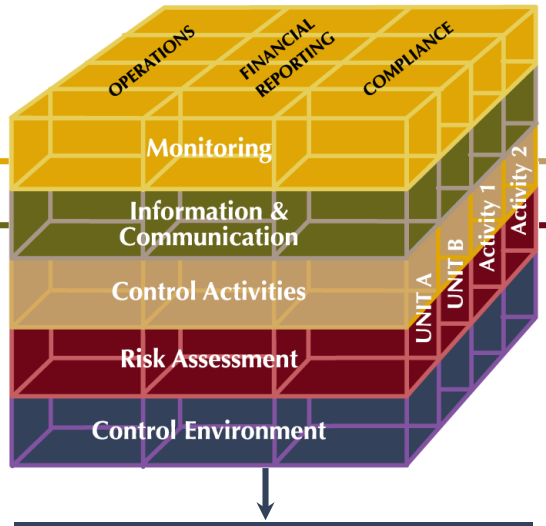
Effectiveness and Efficiency of Operations	**Relates to an entity's basic business objectives, including performance and profitability goals and safeguarding of Resources.**
Reliability of Financial Reporting	**Relates to the preparation of reliable published financial statements, including interim and condensed financial statements and selected financial data derived from such statements, such as earnings releases, reported publicly.**
Compliance with Laws and Regulations	**Relates to complying with those laws and regulations to which the entity is subject.**

Objective Categories Are Distinct, But Overlap

The Five Components under the COSO Framework

Monitoring

- Assessment of a control system's performance over time.
- Combination of ongoing and separate evaluation.
- Management and supervisory activities.
- Internal audit activities.



Control Activities

- Policies/procedures that ensure management directives are carried out.
- Range of activities including approvals, authorizations, verifications, recommendations, performance reviews, asset security and segregation of duties.

Information and Communication

- Pertinent information identified, captured and communicated in a timely manner.
- Access to internal and externally generated information.
- Flow of information that allows for successful control actions from instructions on responsibilities to summary of findings for management action.

Control Environment

- Sets tone of organization-influencing control consciousness of its people.
- Factors include integrity, ethical values, competence, authority, responsibility.
- Foundation for all other components of control.

Risk Assessment

- Risk assessment is the identification and analysis of relevant risks to achieving the entity's objectives-forming the basis for determining control activities.

All five components must be in place for a control to be effective.

Integrated Components Summary

There is a direct relationship between:

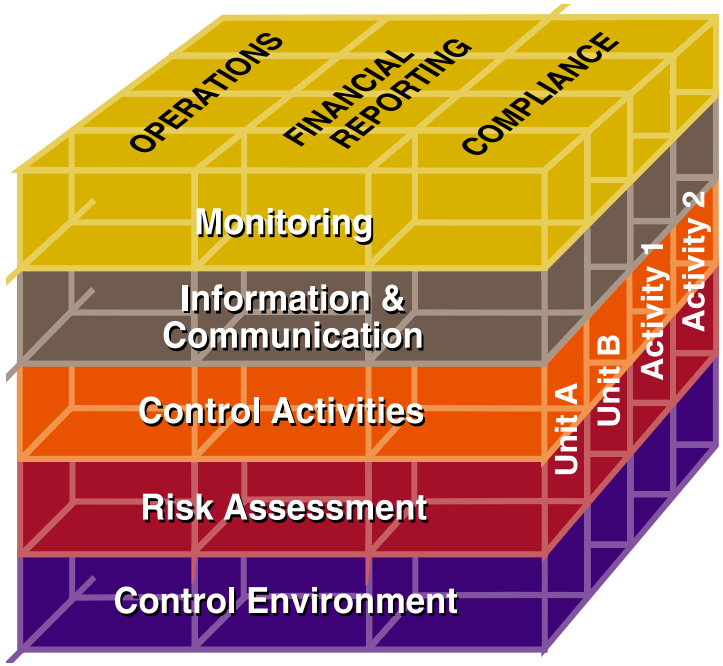
- Objectives ---- What an entity strives to achieve,
- Components--- What is needed to achieve the objectives.

All components are relevant to each objective category.

For Example:

- When looking at any one category - the reliability of financial reporting, for instance - all five components must be present and functioning effectively to conclude that internal control over reliable financial information is effective.

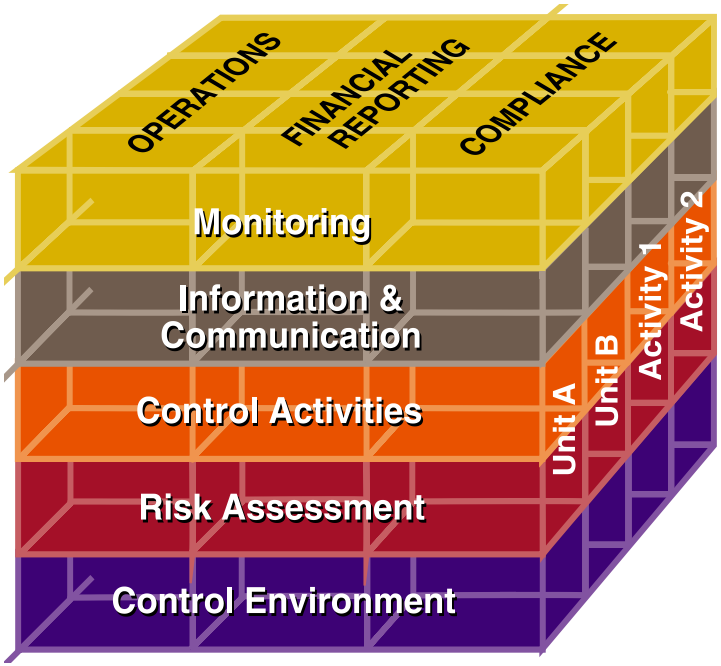
Control Environment



Control Environment

- Sets the tone of an organization, influencing the control consciousness of its people.
- Factors include:
  - Integrity and ethical values,
  - Competence of people,
  - HR practices,
  - Management's operating philosophy,
  - The way authority and responsibility are assigned, and
  - The attention and direction provided by the board.
- Foundation for all other components of control.

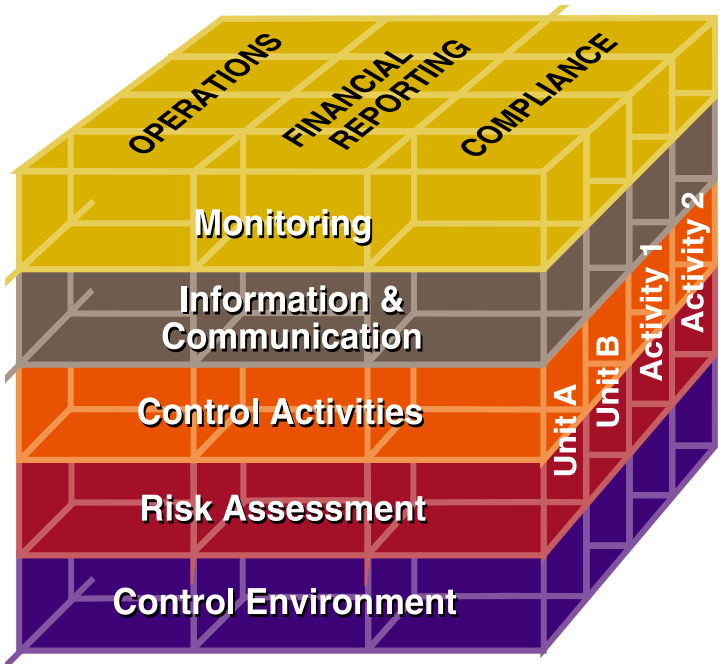
Risk Assessment



Risk Assessment

- A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent
- The identification and analysis of relevant risks to achievement of the objectives
- Forms a basis for determining how risks should be managed
- Mechanisms are needed to identify and deal with the special risks associated with change

Control Activities

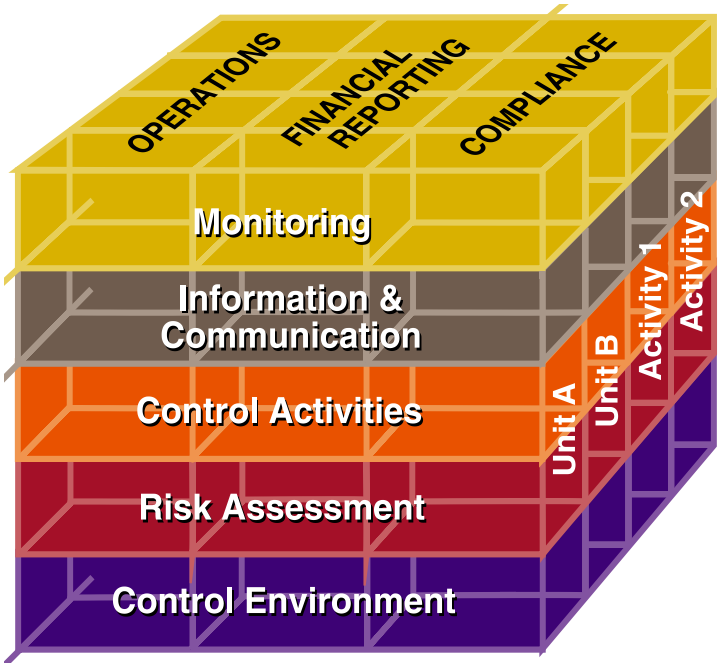


Control Activities

- Policies/procedures that ensure management directives are carried out.
- They help ensure that necessary actions are taken to address risks
- Control activities occur throughout the organization, at all levels and in all functions
- Range of activities including:

  Approvals, authorizations, verifications, recommendations, performance reviews, asset security and segregation of duties.

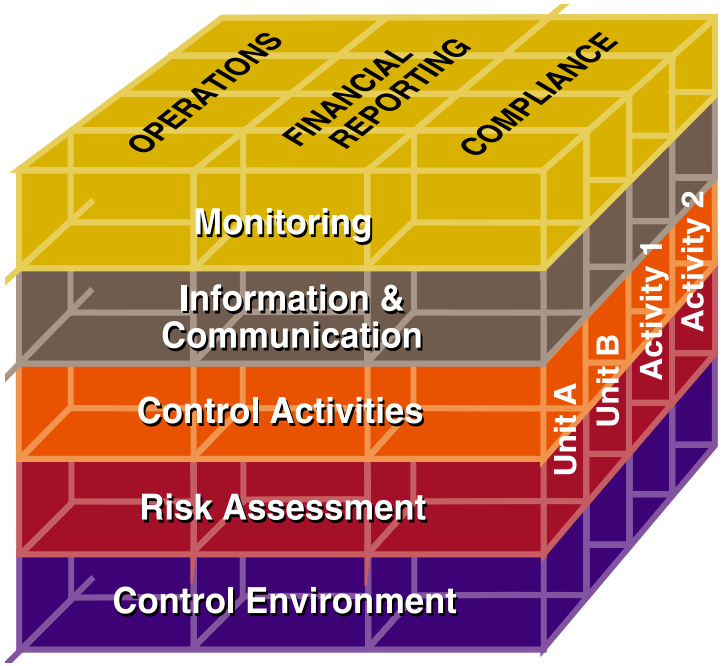
Information & Communication



Information and Communication

- Pertinent information is identified, captured and communicated in a timeframe that allows people to carryout their responsibilities.
- Includes internal and externally information about events, activities and conditions necessary for informed business decision-making and external reporting
- Flow of information that allows for successful control from instructions on responsibilities to summary of findings for management action.

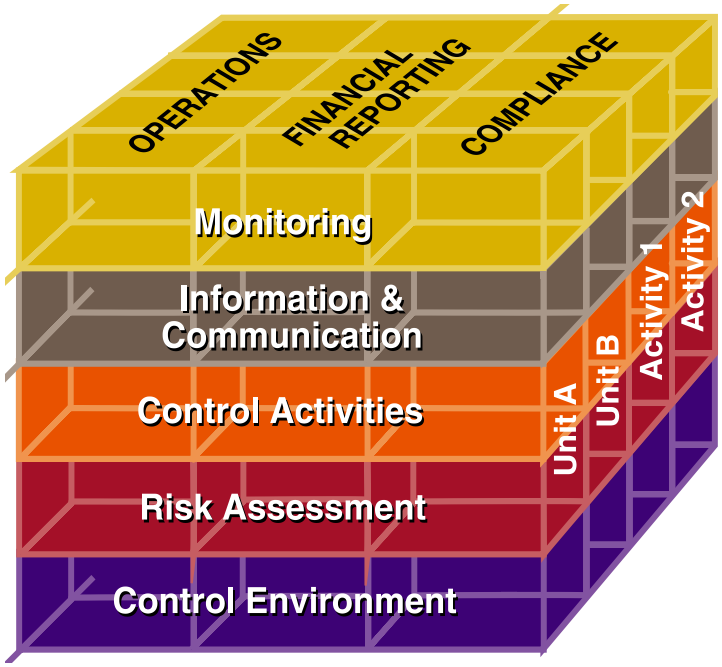
Monitoring



Monitoring

- Assessment of a control system's performance over time.
- Combination of ongoing and separate evaluation.
- Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board.
- The combination of ongoing and separate evaluations will ensure that the internal control system maintains effective over time.

Monitoring – A Deeper Look



Monitoring

- Ongoing monitoring includes regular management and supervisory activities, and other actions personnel take in performing their duties
- Separate evaluations provide independent feedback at a point in time.
  - The scope and frequency will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures.
  - Evaluation may be in the form of internal self-assessments, checklists and internal control reviews.
  - These reviews may be done by the internal auditor, external auditor (to the extent relevant for audit purposes) and external consultants.

Control Environment Evaluation Attributes

Integrity and Ethical Values

Existence and implementation of codes of conduct and other policies regarding acceptable business practice, conflicts of interest, or expected standards of ethical and moral behavior.

Dealings with employees, suppliers, customers, investors, creditors, insurers, competitors, and auditors, etc. (e.g., whether management conducts business on a high ethical plane, and insists that others do so, or pays little attention to ethical issues).

Pressure to meet unrealistic performance targets - particularly for short-term results - and extent to which compensation is based on achieving those performance targets.

Control Environment Evaluation Attributes

Commitment to Competence

Formal or informal job descriptions or other means of defining tasks that comprise particular jobs.

Analyses of the knowledge and skills needed to perform jobs adequately.

Organizational Structure

Appropriateness of the entity's organizational structure, and its ability to provide the necessary information flow to manage its activities.

Adequacy of definition of key managers' responsibilities, and their understanding of these responsibilities.

Adequacy of knowledge and experience of key managers in light of responsibilities.

Control Environment Evaluation Attributes

Board of Directors or Audit Committee

Independence from management, such that necessary, even if difficult and probing, questions are raised.

Frequency and timeliness with which meetings are held with chief financial an/or accounting officers, internal auditors and external auditors.

Sufficiency and timeliness with which information is provided to board or committee members, to allow monitoring of management's objectives and strategies, the entity's financial position and operating results, and terms of significant agreements.

Sufficiency and timeliness with which the board or audit committee is apprised of sensitive information, investigations and improper acts (e.g., travel expenses of senior officers, significant litigation, investigations of regulatory agencies, defalcations, embezzlement or misuse of corporate assets, violations of insider trading rules, political payments, illegal payments).

Control Environment Evaluation Attributes

Management's Philosophy and Operating Style

Nature of business risks accepted, e.g., whether management often enters into particularly high-risk ventures, or is extremely conservative in accepting risks.

Frequency of interaction between senior management and operating management, particularly when operating from geographically removed locations.

Attitudes and actions toward financial reporting, including disputes over application of accounting treatments (e.g., selection of conservative versus liberal accounting policies; whether accounting principles have been misapplied, important financial information not disclosed, or records manipulated or falsified).

Control Environment Evaluation Attributes

Assignment of Authority and Responsibility

Assignment of responsibility and delegation of authority to deal with organizational goals and objectives, operating functions and regulatory requirements, including responsibility for information systems and authorizations for changes.

Appropriateness of control-related standards and procedures, including employee job descriptions.

Appropriate numbers of people, particularly with respect to data processing and accounting functions, with the requisite skill levels relative to the size of the entity and nature and complexity of activities and systems.

Control Environment Evaluation Attributes

Human Resource Policies and Practices

Extent to which policies and procedures for hiring, training, promoting and compensating employees are in place.

Appropriateness of remedial action taken in response to departures from approved policies and procedures.

Adequacy of employee candidate background checks, particularly with regard to prior actions or activities considered to be unacceptable by the entity.

Adequacy of employee retention and promotion criteria and information-gathering techniques (e.g., performance evaluations) and relation to the code of conduct or other behavioral guidelines.

Risk Assessment Evaluation Attributes

Entity-Wide Objectives

Extent to which the entity-wide objectives provide sufficiently broad statements and guidance on what the entity desires to achieve, yet which are specific enough to relate directly to this entity.

Effectiveness with which the entity-wide objectives are communicated to employees and board of Directors.

Relation and consistency of strategies with entity-wide objectives.

Consistency of business plans and budgets with entity-wide objectives, strategic plans and current conditions.

Risk Assessment Evaluation Attributes

Activity-Level Objectives

Linkage of activity-level objectives with entity-wide objectives and strategic plans.

Consistency of activity-level objectives with each other.

Relevance of activity-level objectives to all significant business processes.

Specificity of activity-level objectives.

Adequacy of resources relative to objectives.

Identification of objectives that are important (critical success factors) to achievement of entity-wide objectives.

Involvement of all levels of management in objective setting and extent to which they are committed to the objectives.

Risk Assessment Evaluation Attributes

Risks

Adequacy of mechanisms to identify risks arising from external sources.

Adequacy of mechanisms to identify risks arising from internal sources.

Identification of significant risks for each significant activity-level objective.

Thoroughness and relevance of the risk analysis process, including estimating the significance of risks, assessing the likelihood of their occurring and determining needed actions.

Risk Assessment Evaluation Attributes

Managing Change

Existence of mechanisms to anticipate, identify and react to routine events or activities that affect achievement of entity or activity-level objectives (usually implemented by managers responsible for the activities that would be most affected by the changes).

Existence of mechanisms to identify and react to changes that can have a more dramatic and pervasive effect on the entity, and may demand the attention of top management.

Types of Control Activities

Control Activities generally consist of two elements: A policy establishing what should be done and procedures to effect the policy. Such activities can take a number of different forms, including:

Top Level Reviews - Reviews are made of actual performance versus budgets, forecasts, prior periods and competitors. Major initiatives are tracked - such as marketing thrusts, improved production processes, and cost containment or reduction programs - to measure the extent to which targets are being reached. Implementation of plans is monitored for new product development, joint ventures or financing. Management actions taken to analyze and follow up on such reporting represent control activities.

Direct Functional or Activity Management - Managers running functions or activities review performance reports. A manager responsible for a bank's consumer loans reviews reports by branch, region and loan (collateral) type, checking summarizations and identifying trends, and relating results to economic statistics and targets. In turn, branch managers receive data on new business by loan-officer and local-customer segment. Branch managers focus also on compliance issues, for example, reviewing reports required by regulators on new deposits over specified amounts. Reconciliations are made of daily cash flows with net positions reported centrally for overnight transfer and investment.

Types of Control Activities

Information Processing - A variety of controls are performed to check accuracy, completeness and authorization of transactions. Data entered are subject to edit checks or matching to approved control files. A customer's order, for example, is accepted only upon reference to an approved customer file and credit limit. Numerical sequences of transactions are accounted for. File totals are compared and reconciled with prior balances and with control accounts. Exceptions in need of follow-up are acted upon by clerical personnel, and reported to supervisors as necessary. Development of new systems and changes to existing ones are controlled, as is access to data, files and programs. Controls over information processing generally fall into two categories, general computer controls and application specific controls.

Physical Controls - Equipment, inventories, securities, cash and other assets are secured physically, and periodically counted and compared with amounts shown on control records.

Types of Control Activities

Performance Indicators - Relating different sets of data - operating or financial - to one another, together with analyses of the relationships and investigative and corrective actions, serve as control activities. Performance indicators include, for example, purchase price variances, the percentage of orders that are "rush orders" and the percentage of returns to total orders. By investigating unexpected results or unusual trends, management identifies circumstances where the underlying procurement activity objectives are in danger of not being achieved. Whether managers use this information only to make operating decisions, or also follow up on unexpected results reported by financial reporting systems, determines whether analysis of performance indicators serves operational purposes alone or financial reporting control purposes as well.

Segregation of Duties - Duties are divided, or segregated, among different people to reduce the risk of error or inappropriate actions. For instance, responsibilities for authorizing transactions, recording them and handling the related asset are divided. A manager authorizing credit sales would not be responsible for maintaining accounts receivable records or handling cash receipts. Similarly, salespersons would not have the ability to modify product price files or commission rates.

.

Discuss Sample Control Activities

- Original invoices are required for payment
- 3 way matching between PO, Receipt and Invoice
- Paid invoices are stamped and filed
- PO's and checks are consecutively numbered
- Electronic edit checks for system data entry
- System access controls preventing invoice entry and payment entry
- Check stock is locked with access restricted

Information and Communication Evaluation Attributes

Information

Obtaining external and internal information, and providing management with necessary reports on the entity's performance relative to established objectives.

Providing information to the right people in sufficient detail and on time to enable them to carry out their responsibilities efficiently and effectively.

Development or revision of information systems based on a strategic plan for information systems - linked to the entity's overall strategy - and responsive to achieving the entity- wide and activity-level objectives.

Management's support for the development of necessary information systems is demonstrated by the commitment of appropriate resources - human and financial.

Information and Communication Evaluation Attributes

Communication

Effectiveness with which employees' duties and control responsibilities are communicated.

Establishment of channels of communication for people to report suspected improprieties.

Receptivity of management to employee suggestions of ways to enhance productivity, quality or other similar improvements.

Adequacy of communication across the organization (for example, between procurement and production activities) and the completeness and timeliness of information and its sufficiency to enable people to discharge their responsibilities effectively.

Openness and effectiveness of channels with customers, suppliers and other external parties for communicating information on changing customer needs.

Extent to which outside parties have been made aware of the entity's ethical standards.

Timely and appropriate follow-up action by management resulting from communications received from customers, vendors, regulators or other external parties.

Discuss Example Information and Communication

- Daily purchase report by vendor
- Exception reports based on vendor analysis
- On-line communication of vendor payment policy
- Exception reports based on vendor analysis (duplicate invoice numbers)
- Feedback mechanisms for employees and vendors
- Investigation of vendor complaints of business practices

Monitoring Evaluation Attributes

Ongoing Monitoring

Extent to which personnel, in carrying out their regular activities, obtain evidence as to whether the system of internal control continues to function.

Extent to which communications from external parties corroborate internally generated information, or indicate problems.

Periodic comparison of amounts recorded by the accounting system with physical assets.

Responsiveness to internal and external auditor recommendations on means to strengthen internal controls.

Extent to which training seminars, planning sessions and other meetings provide feedback to management on whether controls operate effectively.

Whether personnel are asked periodically to state whether they understand and comply with the entity's code of conduct and regularly perform critical control activities.

Effectiveness of internal audit activities.

Monitoring Evaluation Attributes

Separate Evaluations

Scope and frequency of separate evaluations of the internal control system.

Appropriateness of the evaluation process.

Whether the methodology for evaluating a system is logical and appropriate.

Appropriateness of the level of documentation.

Reporting Deficiencies

Existence of mechanism for capturing and reporting identified internal control deficiencies.

Appropriateness of reporting protocols.

Appropriateness of follow-up actions.

Discuss Example Monitoring

- Supervisory review of purchase and payable process
- Periodic policy and procedure training
- Weekly review and analysis of material spend
- Periodic review of authority limits for purchasing
- Review of system controls for segregation of duties
- Internal audits of purchasing process

Internal Controls Maturity Framework

UNRELIABLE	INFORMAL	STANDARDIZED	MONITORED	OPTIMIZED
▪ Unpredictable environment where control activities are not designed or in place	▪ Control activities are designed and in place but are not adequately documented	▪ Control activities are designed, in place and are adequately documented	▪ Standardized controls with periodic testing for effective design and operation with reporting to management	▪ Integrated internal controls with real time monitoring by management and continuous improvement

- **Level 1 – Unreliable**
  - Unpredictable environment where control activities are not designed or in place
- **Level 2 – Informal**
  - Disclosure Activities and Controls are designed and in place but are not adequately documented
  - Controls mostly dependent on people
  - No formal training or communication of control activities
- **Level 3 – Standardized**
  - Control activities are designed and in place
  - Control activities have been documented and communicated to employees
  - Deviations from control activities will likely not be detected
- **Level 4 – Monitored**
  - Standardized controls with periodic testing for effective design and operation with reporting to management
  - Automation and tools may be used in a limited way to support control activities
- **Level 5 – Optimized**
  - An integrated internal control framework with real time monitoring by management with continuous improvement (Enterprise-Wide Risk Management)
  - Automation and tools are used to support controls activities and allow the organization to make rapid changes to the control activities if needed

Brainstorming

Think Like The Devil When Assessing the Risk of Fraud!

How would the Devil Manage this business unit or process?

- What would happen if The Devil were ABC Company customer or vendor

What if the Devil were hired as an employee?

External Auditors – Assessment of Control Risk

- Perform preliminary control risk assessments (CRA)

Audit Risk= Inherent risk (IR) * Control risk (CR) * Detection risk (DR)

- Lower
- Higher

- Min
- Mod
- Max

CRA

IR / CR	Minimum (Test)	Moderate (Walkthrough)	Maximum (Ineffective)
Lower	Minimal	Low	Moderate
Higher	Low	Moderate	High

External Auditors – Assessment of Control Risk

- Perform preliminary control risk assessments (CRA)

Minimal	Material errors are **unlikely** to occur.
Low	We **don't expect** material errors to occur but can't say there won't be any.
Moderate	We **expect few** errors, if any.
High	We **expect** material errors **or** we have not done enough to assess the likelihood.

External Auditors – Assessment of Control Risk

Develop the audit plan

- ❑ Develop test of controls work programs to assess the operating effectiveness of mega processes
- ❑ Develop substantive audit work programs for significant accounts

  - Determine the nature, extent and timing of audit procedures and tests of controls and substantive tests.
  - Design tests of controls based on our understanding of the control environment and conclusion on the design of controls to obtain sufficient evidence of operating effectiveness of the controls for Business Processes.
  - Design substantive tests of transactions and account balances to test assertions (completeness, existence and occurrence, recording, cut-off, valuation and presentation).

External Auditors – Assessment of Control Risk

Develop the audit plan

- ❑ Develop test of controls work programs to assess the operating effectiveness of mega processes
- ❑ Develop substantive audit work programs for significant accounts
  - Determine the nature, extent and timing of audit procedures and tests of controls and substantive tests.

- Nature – what **type** of tests?
- Extent – how **much** testing ?
- Timing – when are we going to do them?

Thank You