Information Systems Audit

Module 1

Mathew A Thomas
Grad. CWA, FCA, MCA, CDM, ISA, CISSP.

Introduction

- ✓ About the Course
- ✓ About the Module
  - ► Mod1 (7%) 14 Questions
- ✓ About the Material
  - ► Source, Organisation
  - ► Mod1: Chapters 1-4
- ✓ About this presentation
  - ► Chapter 1-4

Contents

- Audit Mission
  - Audit planning, Laws and Standards
- Risk Analysis
  - Risks and controls, Evaluation of business risks, Elements of risks
- Controls
  - Control objectives, General control procedures, Control types,
- Performing of I.S. Audit
  - Classification of Audits
  - Audit Methodology
    - Risk and materiality, Risk assessment, Audit Objectives, Compliance and substantive tests, Evidence, Sampling, CAAT, Evaluation and Judgment, Communication of Audit Findings, Management Action, Audit Documentation
  - Audit Resource Management
- Continuous Audit Approach
  - SCARF,EAM, Snap shot, Integrated test facility…

Audit Mission

- ✓ Audit Charter
  - State management's objectives
  - Delegation of authority
- ✓ Audit Planning
- ✓ Laws
  - Identify those government or other relevant external requirements
- ✓ Standards
  - ISACA Standards

Risk

- Risk: The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.
  - Assets
  - Threat
  - Probability of the threat

Risk Analysis I

- Vulnerability
  - The absence or weakness of a safeguard constitutes a vulnerability
- Safeguard
  - Is a control or countermeasure employed to reduce the risk associated with a specific threat.
- Exposure Factor/Impact
  - Represents the percentage of loss a a realized threat would have on a specific asset.

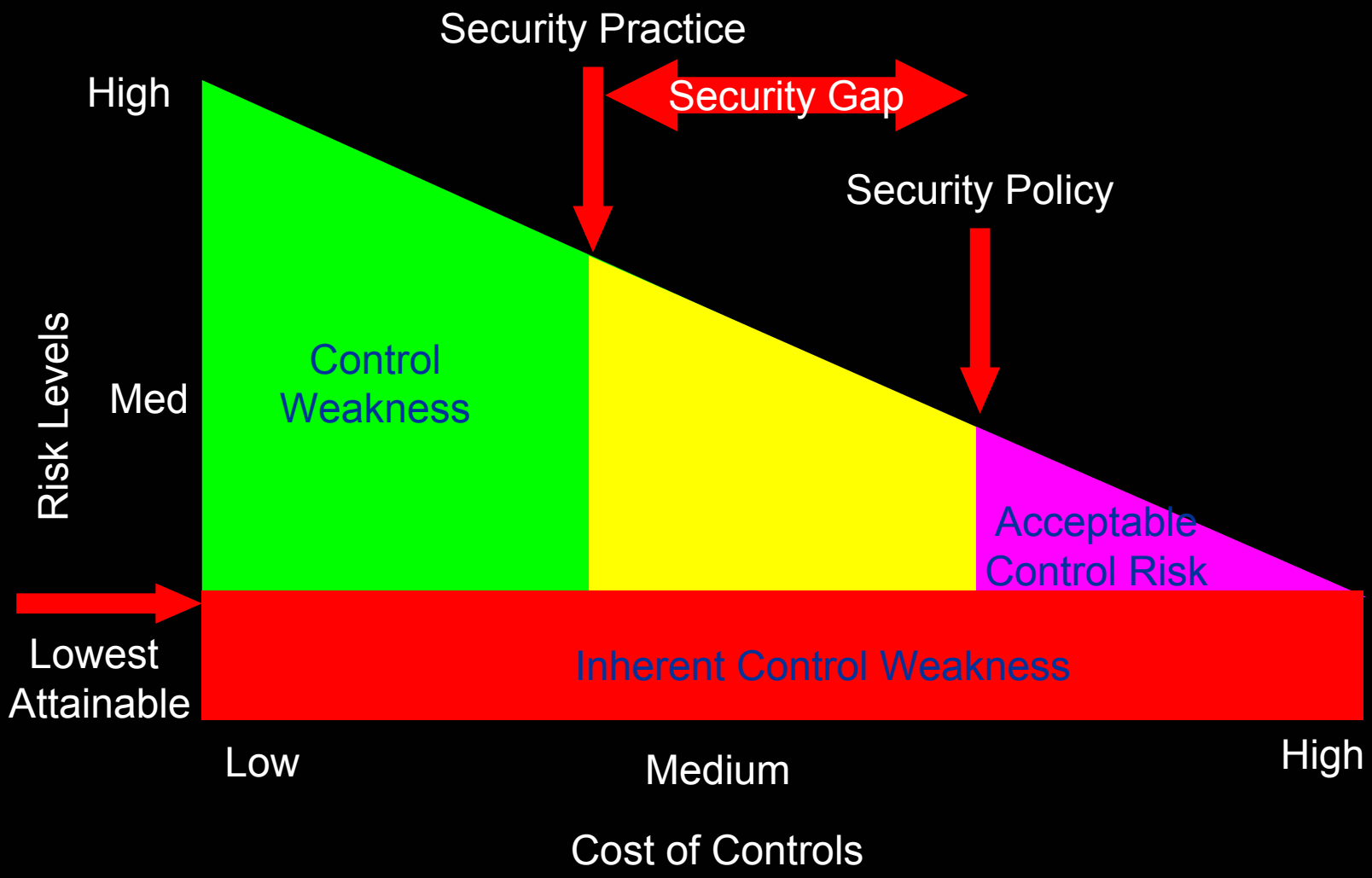
Risk Analysis II

- ✓ Single Loss Expectancy (SLE)
  - Asset Value x Exposure Factor
- ✓ Annualized Rate of Occurrence (ARO)
  - Estimated annual frequency of a threat
    - ► Meteorite strike : 1 in 10000 years
      - ★ ARO = 0.00001
    - ► Unauthorized access: six times a year x 100 employees
      - ★ ARO = 600

Risk Analysis III

- ✓ Annualized Loss Expectancy (ALE)
  - SLE x ARO
- ✓ Cost of Control < ALE

Control Weakness Vs Control Risk



SAP 6 I

- ✓ Audit risk
  - ► means the risk that the auditor gives an inappropriate audit opinion when the financial statements are materially misstated.
  - ► Audit risk =inherent risk x control risk x detection risk.
- ✓ Inherent risk
  - ► is the susceptibility of an account balance or class of transactions to misstatement that could be material, either individually or when aggregated with misstatements in other balances or classes, assuming that there were no related internal controls.

SAP 6 II

- ✓ Control risk
  - ► is the risk that a misstatement, that could occur in an account balance or class of transactions and that could be material, either individually or when aggregated with misstatements in other balances or classes, will not be prevented or detected and corrected on a timely basis by the accounting and internal control systems
- ✓ Detection risk
  - ► is the risk that an auditor's substantive procedures will not detect a misstatement that exists in an account balance or class of transactions that could be material, either individually or when aggregated with misstatements in other balances or classes.

Controls I

- Control is defined as
  - the policies, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.
- A control objective
  - is a statement of the desired result or purpose to be achieved by implementing control procedures in a particular activity.

Controls II

- Once risks have been identified,
  - Existing controls are evaluated
  - New controls can be designed to achieve an acceptable level of risk.

Internal Control Objectives

- Internal accounting controls
  - Primarily directed at accounting operations
    - Safeguarding of the assets
    - Reliability of financial records.
- Operational controls
  - Concerned with the day-to-day operations, functions and activities and ensure the operation is meeting the business objectives.
- Administrative controls
  - Concerned with operational efficiency' in a functional area and adherence to management policies.
  - Support the operational controls specifically concerned with operating efficiency.

Controls II

- ✓ Preventive
- ✓ Detective
- ✓ Corrective

Preventive Controls

- ✓ Deter problems before they arise
- ✓ Monitor both operation and inputs
- ✓ Attempt to predict potential problems before they occur and make adjustments
- ✓ Prevent an error, omission or malicious act from occurring

Detective Controls

- ✓ Controls that detect that an error, omission or malicious act has occurred and report the occurrence

Corrective Controls

- ✓ Minimize the impact of a threat
- ✓ Remedy problems discovered by detective controls
- ✓ Identify the cause of a problem
- ✓ Correct errors arising from a problem
- ✓ Modify the processing system (s) to minimize future occurrences of the problem

Classification of Audits

- ✓ Financial Audits
  - ► The purpose of a financial audit is to assess the correctness of financial statements or records. A financial audit will often involve detailed, substantive testing.
- ✓ Operational Audits
  - ► An operational audit is designed to evaluate the internal control structure in a given area. IS audits of application controls or of logical security systems, are examples of operational audits.
- ✓ Comprehensive Audits
  - ► A comprehensive audit combines both financial and operational audit steps. A comprehensive audit would include both compliance and substantive audit steps.

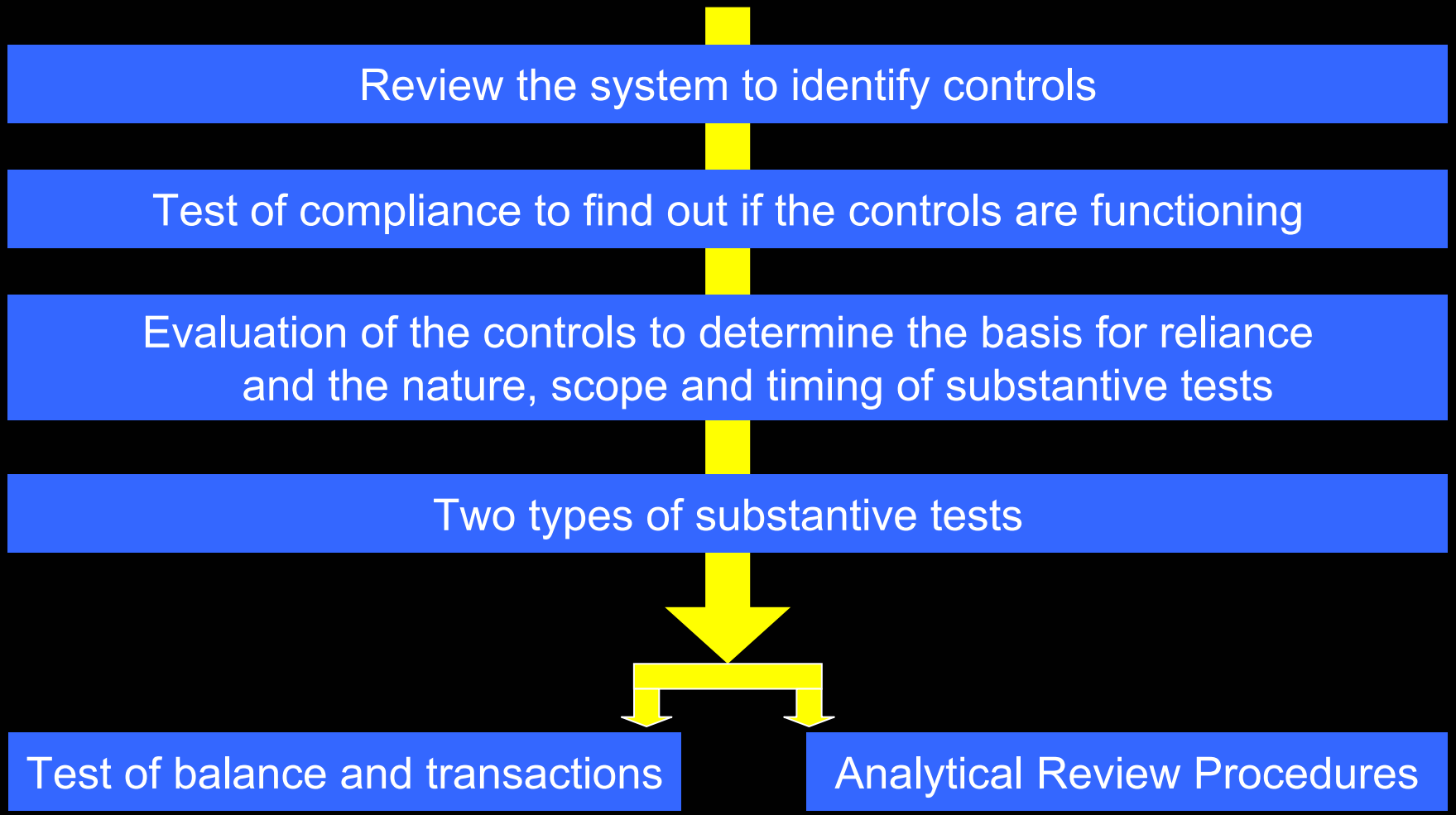
Compliance Vs. Substantive Testing

- Compliance Testing
  - evidence gathering for the purpose of testing an organization's compliance with control procedures
- Substantive Testing
  - evidence gathering to evaluate the integrity of individual transactions, data or other information

IS Audit Steps

1. Gather Information and plan
2. Obtain understanding of internal control
3. Perform compliance test
4. Perform substantive tests
5. Conclude the audit

IS Audit


Review the system to identify controls
Test of compliance to find out if the controls are functioning
Evaluation of the controls to determine the basis for reliance and the nature, scope and timing of substantive tests
Two types of substantive tests
Test of balance and transactions
Analytical Review Procedures

Phases of Audit I

- Audit Subject
  - Identify the area to be audited.
  - Identify the purpose of the audit.
- Audit Scope
  - Identify the specific systems, function or unit of the organization to be included in the review.
- Audit Planning
  - Identify technical skills and resources needed.
  - Identify the sources of information for test or review.
  - Identify locations or facilities to be audited.

Phases of Audit II

- Audit Procedures and Data Gathering
  - Identify and select the audit approach to verify and test the controls.
  - Identify a list of individuals to interview.
  - Identify and obtain departmental policies, standards and guidelines
  - Develop audit tools and methodology to test and verify control
- Procedures for Evaluating the Test
  - Organization specific

Phases of Audit III

- ✓ Procedures for Communication with Management
  - Organization specific
- ✓ Audit Report Preparation
  - Follow-up review procedures

Audit Evidence

- Evidence is any information used by the IS Auditor to determine whether the entity or data being audited follows the established audit criteria or objectives
- Examples
  - IS Auditor's observations
  - Notes taken from interviews
  - Material extracted from correspondence
  - Internal documentation
  - Results of audit test procedures

Reliability of Audit Evidence I

- ✓ Independence of the provider of the evidence
  - ► Evidence obtained from outside sources is more reliable than from within the organization
    - ★ Confirmation letters are used for verification of accounts receivable balances.
- ✓ Qualification of the individual providing the information or evidence
  - ► Whether the providers of information or evidence are inside or outside of the organization, the IS Auditor should always consider the qualifications of the persons providing the information.

Reliability of Audit Evidence II

- ✓ Objectivity of the evidence
  - ► Objective evidence is much better than evidence that requires considerable judgment or interpretation
    - ★ An IS Auditor's count of a cash fund is direct, objective evidence.
    - ★ IS Auditor's analysis of the efficiency of an application, based upon discussions with certain personnel, may not be objective audit evidence

Techniques for Gathering Evidence

- Reviewing IS Organization Structures
  - Ensure adequate separation or segregation of duties
  - Evaluate General organizational controls
- Reviewing IS Documentation Standards
  - Systems development initiating documents
  - Functional design specifications
  - Program change histories
  - User documentation manuals
- Interviewing Appropriate Personnel
- Observing Processes and Employee Performance

Sampling

- Statistical Sampling
  - Objective method of determining the sample size and selection criteria
- Non-Statistical Sampling (Judgment Sampling)
  - Subjective method of sampling
- Classification
  - Attribute Sampling
  - Variable Sampling

Attribute Sampling

- Attribute Sampling
  - Estimate the rate (percent) of occurrence of a specific quality (attribute) in a population
- Stop-or-Go Sampling
  - Prevent excessive sampling of an attribute by allowing an audit test to be stopped at the earliest possible moment.
- Discovery Sampling
  - When expected occurrence rate is extremely low

Variable Sampling

- Monetary Unit Sampling
  - Estimate of overstatement in an account balance.
- Stratified Mean per unit
  - Population is divided into groups and samples are drawn from the various groups.
- Unstratified mean per unit
  - Sample mean is calculated and projected as an estimated total.
- Difference estimation
  - Total difference between audited values and book (unaudited) values based on differences obtained from sample observations.

Statistical Terms I

- Confidence Coefficient/Level
  - Probability that the characteristics of the sample are a true representation of the population
  - The greater the confidence coefficient, the larger the sample size.
- Level of Risk
  - 1-CL
- Precision
  - Represents the acceptable range difference between the sample and the actual population
  - The higher the precision amount, the smaller the sample size.

Statistical Terms II

- Expected Error Rate
  - Estimate of the errors that may exist
  - More the expected error rate, greater the sample size.
- Tolerable Error Rate
  - Maximum misstatement or number of errors that can exist without an account being materially misstated.

Computer-Assisted Audit Techniques

- Advantages:
  - Reduced level of audit risk
  - Greater independence from the auditee
  - Broader and more consistent audit coverage
  - Faster availability of information
  - Improved exception identification
  - Greater flexibility of run times
  - Greater opportunity to quantify internal control weaknesses
  - Enhanced sampling

Examples I

- Test Data Generators
  - Prepare a computerized test data file for use in testing and verify the logic of application programs.
- Expert Systems
  - Software applications developed to hold a base of expert knowledge and logic provided by experts in a given field.
- Standard Utilities
  - Resident in software packages that specify the status of parameters used to install the package.

Examples II

- Software Library Packages
  - Verify the integrity and appropriateness of program changes.
- Specialized Audit Software
  - Used to perform specific audit steps for the IS Auditor, such as sampling, footing and matching.

Continuous Audit Techniques I

- Audit Hooks
  - Points in application programs ("exits") that can be used to call in routines to perform audit testing on a concurrent basis.
- Continuous and Intermittent simulation
  - During a process run of a transaction, simulates the instruction execution of the application. As each transaction is entered, the simulator decides whether the transaction meets certain predetermined criteria and if so, audits the transaction.
- Snapshot
  - This technique involves taking "pictures" of a transaction as it flows through the computer system. Audit software routines are embedded at different points in the processing logic to capture images of the transaction as it progresses through the various stages of processing.

Continuous Audit Techniques II

- Integrated Test Facilities (ITF)
  - Involves setting up dummy entities on an application system and processing test or production data against the entity as a means of verifying processing accuracy.
- System Control Audit Review File (SCARF)/ Embedded Audit Module (EAM)
  - Involves embedding audit software modules within an application system to provide continuous monitoring of the system's transactions. The information is collected into a special computer file that can be examined by the IS Auditors.

Communicating Audit Results I

- No specific format for an IS audit report
  - Introduction
  - Statement of audit objectives and scope
  - The period of audit coverage
- The IS Auditor's overall conclusion and opinion on the adequacy of controls and procedures examined during the audit.
- The IS Auditor should communicate any reservations or qualifications with respect to the audit. This may state that the controls or procedures examined were found to be adequate or inadequate.

Communicating Audit Results II

- ✓ Detailed audit findings and recommendations and the decision to include or not include findings in an audit report should be based on the materiality of the findings and the intended recipient of the audit report.
- ✓ An audit report may include a variety of findings, some of which may be quite material while others are minor in nature.
- ✓ Management evaluates responses to the findings, stating corrective actions to be taken and timing for implementing these anticipated corrective actions.

Examples II

- Audit Hooks
  - Points in application programs ("exits") that can be used to call in routines to perform audit testing on a concurrent basis.
- Integrated Test Facilities
  - Involves setting up dummy entities on an application system and processing test or production data against the entity as a means of verifying processing accuracy.
- Snapshot
  - This technique involves taking "pictures" of a transaction as it flows through the computer system. Audit software routines are embedded at different points in the processing logic to capture images of the transaction as it progresses through the various stages of processing.

Examples III

- System Control Audit Review File
  - Involves embedding audit software modules within an application system to provide continuous monitoring of the system's transactions. The information is collected into a special computer file that can be examined by the IS Auditors.
- Specialized Audit Software
  - Used to perform specific audit steps for the IS Auditor, such as sampling, footing and matching.

Thank You

Mathew A Thomas
mat@vsnl.com