IS RISK AND FUNDAMENTAL IS AUDITING CONCEPTS

E.N.G.SARTORIO

Introduction

In today's digital environment, organizations rely heavily on information systems to support operations, decision-making, reporting, and regulatory compliance. While these systems improve efficiency and performance, they also introduce risks such as data inaccuracies, system failures, and security threats that may affect organizational objectives.

Purpose of the Report

- Explain computer risks and their effects
- Describe the different categories of IS risks
- Discuss the role of auditing in managing these risks
- Explain the elements of risk analysis and risk-based auditing
- Examine the reliability of audit evidence and audit procedures
- Highlight the importance of auditor independence and responsibilities related to fraud detection

UNDERSTANDING RISK

IN AN ORGANIZATION CONTEXT

Risk is essentially the **possibility that uncertainty may prevent an organization from achieving its objectives**. Every organization operates with goals such as: financial performance, operational efficiency, regulatory compliance, and customer satisfaction. *When uncertainties threaten those goals, risk arises.*

UNDERSTANDING RISK

IN AN ORGANIZATION CONTEXT

OBJECTIVES DURING A MAJOR SALE EVENT:

- GENERATE SALES
- MAINTAIN CUSTOMER SATISFACTION

RISK:

- WEBSITE CRASH DUE TO SYSTEM OVERLOAD
- SYSTEM FAILURE PREVENTS THE COMPANY FROM ACHIEVING ITS OBJECTIVES

COMPUTER RISK AND EFFECT

"**Risk**" is the possibility that one or more individuals or organizations will experience adverse consequences from those choices. Risk is the error of image of opportunity.

Is the likelihood of a significant loss occuring before taking into account any risk-reducing factors.

Control effectiveness is strongly impacted by the quality of work and control supervision.

Audit risk is the risk that the audit coverage will not address significant business exposures.

Visual Analogy

INHERENT RISK

NATURAL EXPOSURE

CONTROL RISK

SAFEGUARDS MAY FAIL

AUDIT RISK

AUDITOR FAILS TO DETECT THE PROBLEM

IS RISK CATEGORIES

STRATEGIC

The risk that IS either developed in-house or purchased are not aligned with the organization's goals and do not support the achievement of its mission.

OPERATIONS

The risk that the information systems in used by the organization impose unacceptable overheads on the organization or result in sub-optimal service levels.

REPORTING

This risk that IS cannot be relied on to produce information in an accurate, complete and timely manner.

COMPLIANCE

The risk that IS, in themselves, lead to a breaches of laws and regulations with a result of losses to the organization, either financial or in reputation.

AUDIT

Is an examination of the management controls within an information technology infrastructure and business applications.

INTERNAL

Audits are conducted by employees **within an organization**, they have first-hand knowledge of the systems and processes.

EXTERNAL

Bring a **fresh perspective to the audit process** and are not biased by internal politics or relationships.

RISK

Risk is the probability of an outcome having a negative effect on people, systems or assets.

RISK ANALYSIS

Is a multi-step process aimed at mitigating the impact of risks on business operations.

Components

Risk Assessment

IT risk assessment is the process of identifying an organization's critical IT assets, potential threats that could damage or compromise those assets, and vulnerabilities in the IT infrastructure.

Risk Communication

Risk communication is an interactive process of exchanging information and opinion among individuals, groups, and institutions.

Risk Management

Is the application of risk management methods to manage IT threats. IT risk management involves procedures, policies, and tools to identify and assess potential threats and vulnerabilities in IT infrastructure.

RISK ANALYSIS METHOD

QUALITATIVE

- Easier and more convenient.
- Rates risks based on perceived severity and likelihood.

QUANTITATIVE

- Calculates risk using available data.

RISK-BASED AUDITING AND RISK ASSESSMENT METHOD

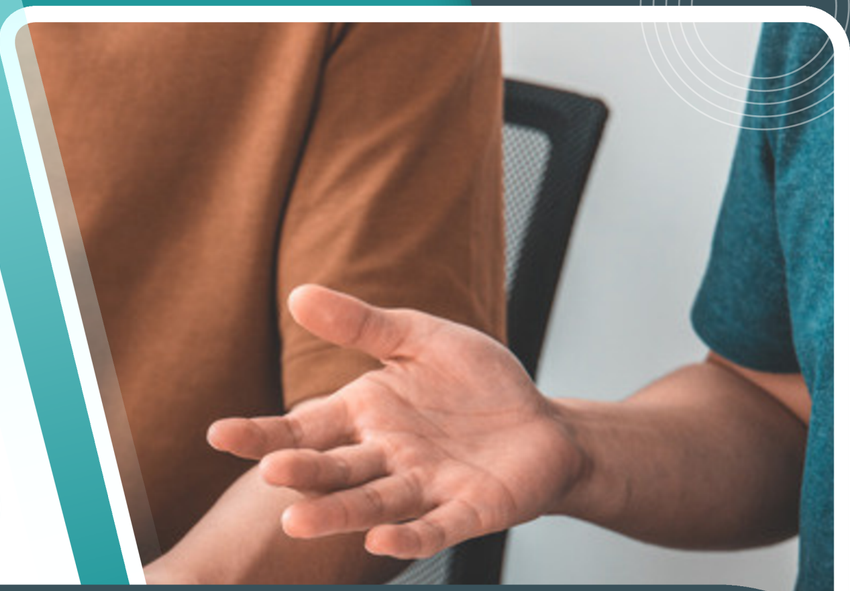
Risk-based auditing ensures that the internal audit activity is focusing its efforts on providing assurance and advisory services related to the organization’s top risks.

TYPES OF AUDIT APPROACHES

- Balance sheet approach
- Systems-based approach
- Substantive procedures approach
- Risk-based approach

RELIABILITY OF AUDIT EVIDENCE

The reliability of evidence depends on the nature and source of the evidence and the circumstances under which it is obtained.



VARIOUS FACTORS THAT INFLUENCE RELIABILITY OF AUDIT EVIDENCE

- Source of Evidence
- Objectivity and Independence
- Timeliness
- Internal Controls
- Documentary Evidence
- Auditor’s Direct Knowledge
- Consistency and Corroboration

The reliability of audit evidence is enhanced when it is consistent with other evidence obtained and when different sources of evidence support the same assertion. Consistency and corroboration provide a higher level of confidence in the reliability of the evidence.

AUDIT EVIDENCE PROCEDURES

Audit procedures can be classified into the following categories:

Risk assessment procedures and further audit procedures which consist of:
Tests of controls, and Substantive procedures, including tests of details and substantive analytical procedures.

The purpose of an audit procedure determines whether it is a risk assessment procedure, test of controls, or substantive procedure.

Below is the standard describing specific audit procedures:

- INSPECTION
- OBSERVATION
- INQUIRY
- CONFIRMATION
- RECALCULATION
- REPERFORMANCE
- ANALYTICAL PROCEDURES

AUDIT INDEPENDENCE

- Determine audit need
- Assess audit requirements
- Identify & select auditor
- prepare evidence & staff
- Undergo audit process
- Receive & review findings
- Accept(or appeal) results
- Sign off on report(if required
- Address findings as needed

Auditor independence refers to the freedom from bias, external control, or influence that ensures internal auditors are impartial, make judgments based on evidence, and are free from conflicts of interest while conducting audits.

RESPONSIBLE FOR FRAUD PREVENTION AND DETECTION

The International Standard on Auditing (ISA) 240 The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements defines fraud as an intentional act, by one or more individuals among management, those charged with governance, employees or third parties, involving the use of deception to obtain an unjust or illegal advantage.

In accordance with the ISA 240, the objectives of the auditor are:

- **To identify and assess the risk of material misstatement of the financial statements due to fraud**
- **To obtain sufficient appropriate audit evidence regarding the assessed risks of material misstatement due to fraud through designing and implementing appropriate responses, and**
- **To respond appropriately to fraud or suspected fraud during the audit.**
- **Risk Identification and Assessment**

THANK YOU