University of Dar es Salaam

Lecture 8 – Risk Management

Aron Kondoro

Introduction

- Enables organization to focus on areas with highest impact
- Examples of impact
  - Financial loss
  - Decrease in shareholder value
  - Damage to organization reputation
  - Dismissal of senior management
  - Dissolution of the business

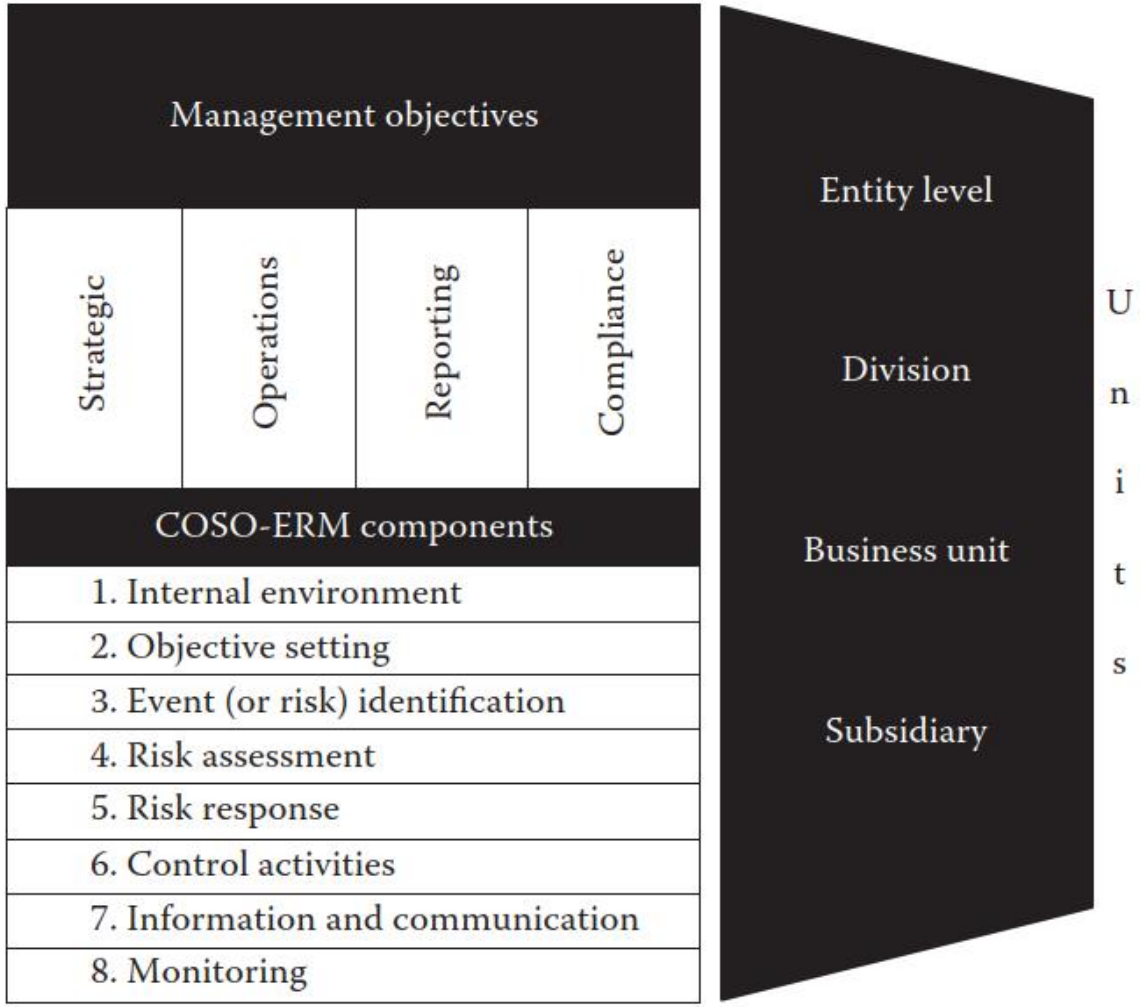
Introduction

- NIST defines risk management as
  - *Process of **identifying** and **assessing** risk, followed by **implementing the necessary procedures to reduce** such risk to acceptable levels*
- IT-related threats
  - Fraud
  - Erroneous decisions
  - Loss of productive time
  - Data inaccuracy
  - Unauthorized data disclosure
  - Loss of public confidence

Introduction

- COSO Enterprise Risk Management (ERM) Framework defines risk management as
  - *A process, **effected by an entity's board of directors**, management and other personnel, **applied in strategy setting** and across the enterprise, designed to **identify potential events** that may affect the entity, and **manage risks** to be within its risk appetite, to **provide reasonable assurance** regarding the achievement of entity objectives.*
- ERM has become widely accepted standard
  - 90% believe it will be part of their business process

Enterprise Risk Management Framework



- Effective tool for management to
  - Set goals and strategies
  - Identify, evaluate, and manage risk areas
  - Select and implement controls
  - Ensure organization meets goals

Internal Environment

- Refers to an organization's culture, behavior, actions, policies, procedures, tone, heart
- It is fundamental for all other ERM components. Consists of
  - Management's beliefs, operating style, risk appetite
  - Management's commitment to integrity, ethics, and competence
  - Management's oversight over internal control and structure
  - Human resource policies

Objective Setting

- Goals the company wants to achieve
- Types of objectives
  - Strategic – guide direction of business
    - E.g., become best seller in the market, acquire separate business
  - Operational – improve existing operations
    - E.g., hiring quality personnel, maintain certain levels of production
  - Reporting – ensure reliability, completeness, and accuracy of reports
    - E.g., financial statements
  - Compliance – ensure laws and regulations are followed

Event/Risk Identification

- Key questions
  - What could go wrong?
  - How can it go wrong?
  - What is the potential harm?
  - What can be done about it?
- Risk classification
  - Inherent – exist before control plans
  - Residual – left over after control plans
- Risk identification methods
  - Audits
  - Operations/process flowcharts
  - Risk analysis questionnaires
  - Financial statements
  - Insurance policy checklists

Risk Assessment

- Risks can come from **traditional sources** i.e., natural disasters, accidents, vandalism or **electronic sources** i.e., computer viruses, information theft, electronic sabotage
- Risk assessment resources
  - NIST.gov
  - GAO.gov – U.S. Government Accountability Office
  - Expected loss approach – assesses probable loss and frequency
    - Accidental/deliberate disclosure, modification, or destruction
  - Scoring approach – identifies and weighs IT systems properties
- Risk perspectives – **likelihood** and **impact**
- Risk categories – **critical**, **important**, and **unimportant**

Risk Response

- Four ways of risk response
  - Avoid – eliminate the risk
    - E.g., remove app feature that slows down critical process
  - Prevent – implementing IT controls
    - E.g., input validity checks, configuring logical security controls
  - Reduce – taking mitigating actions
    - E.g., user access reviews, reconciliations
  - Transfer – all/part of risk to third party
    - E.g., insurance, outsourcing
- Risk can also be assumed or retained
  - E.g., risk of bankruptcy in investments

Control Activities

- Procedures management implement to **safeguard assets**, **keep accurate and complete information**, and **achieve business goals** and objectives.
- Control types
  - Preventive – deter problems from occurring
    - E.g., hiring qualified personnel, controlling physical access
  - Detective – discover problems that cannot be prevented
    - E.g., bank account reconciliation
  - Corrective - correct, and recover from identified problems
    - E.g., maintaining backup copies

Information and Communication

- **Information** is organized and processed data necessary for decision making
- Characteristics of useful information
  - Relevant, Reliable, Complete, Timely, Understandable, Verifiable, Accessible
- **Communication** is the process of providing sharing, and obtaining necessary information in a continuing and frequent basis

Monitoring

- Ensure information and communication system is implemented effectively and operates as designed
- Examples
  - Internal audits
  - Budget monitoring
  - Periodic network security audits
  - Implementing fraud detection software

Risk Assessment

- Used by organizations to determine the **extent of potential threats** and **evaluate** the risks associated with IT systems
  - Allows efficient allocation of resources
- Can be part of yearly strategic plan, internal audit
- Standard guidelines
  - COBIT, NIST, ISO/IEC
- Includes risk identification and review of controls

Risk Assessment Guidelines

- **COBIT** - Standard set of IT practices/control objectives in managing IT risks, implementing adequate levels of control
- **ISO/IEC** - Guidelines for management of information security risks ISO/IEC 27005:2011
- **NIST** - FIPS standards
- **Government Accountability Office (GAO)** - reports on IT vulnerabilities
- **American Institute of Certified Public Accountants (AICPA)**
- **ISACA** - Information System Audit Guidelines
- **Institute of Internal Auditors (IIA)**
- **Committee of Sponsoring Organizations of the Treadway Commission (COSO)** – ERM framework

Insurance

- A way for an organization to protect and recover from losses
  - Reduces the risk
- Common risks handed by insurance
  - Damage to computer equipment
  - Business effects of the loss of computer functions
- Insurance policies
  - Coverage of hardware and equipment; media and stored information; replacement or reconstruction costs
- Cyber Insurance
  - designed to protect organizations from risks related to IT infrastructure and activities i.e., cyber-related security breaches, Internet-based risks
  - Coverage includes losses from data destruction, extortion, theft, hacking, DoS

Further Reading

- Chapter 6: Information Technology Control and Audit – Otero, Angel