AMEDA

مسقط للمقاصة والإيداع
Muscat Clearing & Depository

MUSCAT 2019
30th AMEDA Meeting
5th Training
December 10-13 ,2019
W Muscat Hotel

IT RISK MANAGEMENT

IT Risk Management Strategy

Mr. S.M.QAMAR

AGENDA

- Introduction to IT Risk Management
- IT Risk Management Framework – based on ISACA Risk IT®
- RISK IT® - MCD Implementation & Planning

Introduction to IT Risk Management

General Risk Management Definition

Risk management is the identification, evaluation, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives) followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities –

- source : Wikipedia

Introduction to IT Risk Management

IT Risk Management Definition

IT Risk Management is the process of understanding and responding to factors that may lead to a failure in the confidentiality, integrity or availability of an information system. IT security risk is the harm to a process or the related information resulting from some purposeful or accidental event that negatively impacts the process or the related information – Source SANS Institute.

- Threat to Information System Operation
- Vulnerabilities in Information System

Introduction to IT Risk Management

Why Care About IT-related Risk?

- Enterprises are dependent on automation and integration
- Need to cross IT silos of risk management
- Important to integrate with existing levels of risk management practices

Introduction to IT Risk Management

Manage and Capitalize on Business Risk

- Enterprises achieve return by taking risks.
- Some try to eliminate the very risks that drive profit.
- Guidance was needed on how to manage risk effectively.

IT Risk Management Framework

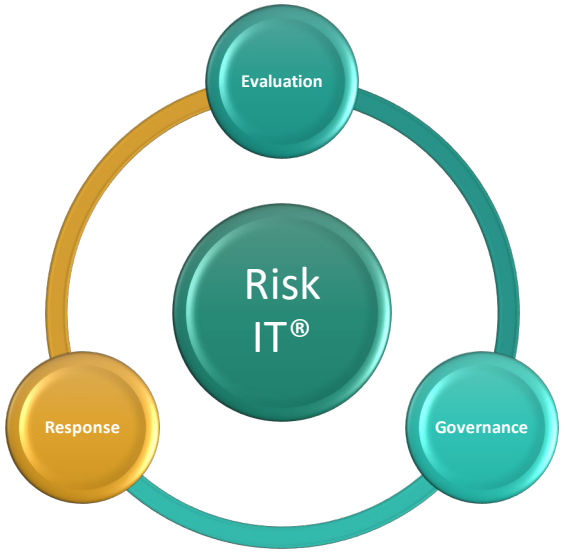
Based on ISACA® Risk IT

- **Governance**
  - Establish & Maintain Common IT Risk View
    - Perform Enterprise IT Risk Assessment
    - Promote IT Risk Aware Culture in the Organization
  - Integrate with Enterprise Risk Management (ERM)
    - Establish & Maintain Accountability for IT Risk Management
    - Provide Adequate Resources for IT Risk Management
  - Make Risk-aware Business Decisions
    - Embed IT risk consideration in strategic business decision making
    - Prioritise IT risk response activities

IT Risk Management Framework

Based on ISACA® Risk IT

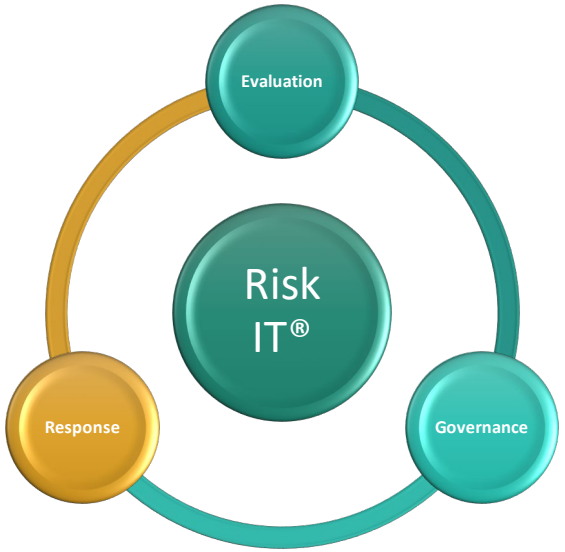
- **Evaluation**
  - Collect Data
    - Establish and maintain a model for data collection
    - Collect data on the operating environment
    - Collect data on risk events
  - Analyze Risk
    - Define IT risk analysis scope
    - Identify risk response options
    - Perform a peer review of IT risk analysis
  - Maintain Risk Profile
    - Map IT resources to business processes
    - Determines business criticality of IT resources
    - Understand IT capabilities
    - Update risk scenario components
    - Maintain the IT risk register and IT Risk map



IT Risk Management Framework

Based on ISACA® Risk IT

- **Response**
  - Articulate Risk
    - Communicate IT Risk Analysis Results
    - Report IT Risk Management Activities & State of Compliance
    - Identify IT Related Opportunities
  - Manage Risk
    - Inventory Controls
    - Monitor Operational Alignment with Risk tolerance thresholds
    - Respond to discovered risk exposure & opportunity
    - Implement Controls
  - React to Events
    - Maintain incident response plans
    - Monitor IT risk
    - Initiate incident response
    - Communicate lessons learned from risk events

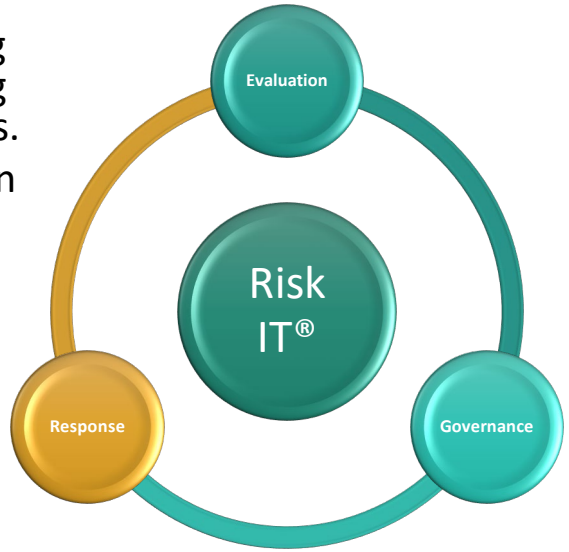


IT Risk Management Framework

Based on ISACA® Risk IT

Guiding Principles of Risk IT

- Always connect to enterprise objectives
- Align the management of IT-related business risk with overall enterprise risk management
- Balance the costs and benefits of managing risk
- Promote fair and open communication of IT risk
- Establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels.
- Understand that this is a continuous process and an important part of daily activities.



IT Risk Management Framework

Based on ISACA® Risk IT

- **RISK IT® Framework MCD Implementation - Governance**
- **RISK IT® Framework MCD Implementation - Evaluation**
- **RISK IT® Framework MCD Implementation - Response**

RISK IT® - Governance

- Risk appetite and tolerance, responsibilities and accountability for IT risk management, awareness and communication, and risk culture

  - Formation of Risk Management Committee to look after overall Enterprise risk profile that include IT Risk
  - IT Steering Committee with an additional agenda to focus on IT Risk Management & Mitigation Initiatives
  - Internal Audit to control & audit Risk Management activities
  - IT Risk Awareness Programs for all stakeholders & clients
  - Annual Mandatory Network & IT Audit by Eminent global Service Providers

RISK IT® - Evaluation

- **Describing business impact and risk scenarios**

  - Comprehensive Business Continuity Plan (BCP) that include IT Disaster Recovery Plan
  - Enterprise wide Business & IT Risk Register

RISK IT® - Response

- **Key risk indicators (KRI) and risk response definition and prioritization**

  - Formation Business Continuity & Planning Committee to manage business disruptions
  - Mandatory Quarterly Disaster Recovery Testing & Reporting with all Market stakeholders
  - Regular Internal & Annual External Audit by independent audit firms, State Audit & CMA
  - Auto Monitoring of Network Devices & Vulnerability Assessment

Questions

AMEDA

مسقط للمقاصة والإيداع
Muscat Clearing & Depository

MUSCAT 2019
30th AMEDA Meeting
5th Training
December 10-13 ,2019
W Muscat Hotel

THANK YOU!

S.M.Qamar

IT MANAGER

Phone: +968-24 82 22 99

Email: qamar@mcd.gov.om