cyberm

Information Technology Risk Management "ITRM"

Course Title:

Information Technology
Risk Management (ITRM)

Duration:

5 days, 40 Hours

Class Format Options:

Instructor-led classroom

Who Should Attend:

- *Information Security Officers and Security Administrators interested in enhancing their security skills and becoming more familiar with methods and technics of conducting Risk Assessment and Mitigation.*
- *Graduate Students of CS, Engineering and MIS fields who are interested in getting hands-on experience in the field of computer and network security*
- *Anyone who is preparing for key industry security certifications such as ISO 27001.*

Prerequisites:

Information Security
Foundations

Course Overview

IT Risk Management is the identification, assessment, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives whether positive or negative) followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. IT Risk Management training is building the capabilities to identify, assess and propose the appropriate migration option in order to minimize the level of risk exposed to. During the training attendees shall be exposed to the methods and best practices to implement a sound risk management solution in the organization by following the appropriate risk approach which shall provide a systematic approach to manage the risks identified and be able to implement the right solution in all information assets lifecycle. This is a 5-day training with hands on and practical exercises that will enable the users to develop and implement the risk management solution on all the organization's information assets.

Upon Completion

Students will gain the following knowledge:

- IT Risks Framework
- Conducting BIA
- Develop a Risk Methodology
- Building Risk Library
- Identify Risk Calculation Methods

Contact: info@cyberm.co.za / +27 83 262 2025

Risk Assessment Introduction

- Risk Assessment Introduction
- Business and Financial Risk Definitions
- CIA
- Risk Frameworks
- Risk Assessment Types Roles and Responsibilities
- Risk Awareness
- Risk Assessment Methods
- Risk Assessment Plan

RA Requirements

- Introduction
- Risks Types
- Risk Analysis Requirements
- Risk Analysis Team
- Risk Analysis Questionnaire
- Root cause analysis

Building RM module

- ISO 27000 Series
- ISO 27001 Controls
- Applicable Controls Selection
- Cost Benefit Analysis Controls
- Gap Analysis
- Information Gathering
- Controls Level of Implementation
- Building Risk Assessment Module

Risk Calculation

- Information Security Risk
- Risk Factors
- Risk Models
- Risk Calculation Formula
- Risk Calculation Approach
- Risk Rating
- Acceptable Risk
- Residual Risk
- Risk Assessment Model
- Risk Assessment Template

Risk Assessment Elements

- Risk Assessment Documentation
- Scope Definition
- Asset Register
- Qualitative and Quantitative
- BIA

Risk Library

- Threats
- Threats valuation Vulnerabilities
- Vulnerabilities valuation
- Risk Library

Risk Implementation

- RA is a Security Program
- Risk Management Process
- Information Gathering
- BIA
- Threat Assessment
- Controls Selection
- Controls Implementation
- Risk Acceptance
- Risk Reporting
- Risk Follow up

Reporting

- RA Reports Types
- RA Reports Characteristics
- RA Reports Owners and Viewers
- RA Statistics