ISOIEC 270312011 - Lead Implementer

INTRODUCTION

- The standard encompasses all events, risks and incidents that could have an impact on ICT infrastructure and systems. It extends the practices of information security incident handling and management, ICT readiness planning and services.
- ISO IEC 27031 guidance ensures continuous operations of business applications and supporting IT systems. The organization's business continuity plan is a number of processes and instructions to ensure the continuation of business in the event of an unplanned interruption (terrorism, pandemic outbreaks, fire, explosions, etc.)
- Continuity plans are based on risk understanding of business impacts and look to the requirements for resilience, alternative processes, and organizational recovery capability. Continuity plans also cover guidelines, roles and responsibilities, procedures, communication processes, and the testing approach.

This training course will highlight:

- Understanding ISO 27031 in relation to ISO 22301
- Processes for continuity of business
- Prevention, reaction, and recovery from disruptions
- Understanding of the concepts of MTPD, (Maximum Tolerable Period of Disruption), RTO (recovery time objective) and RPO (recovery time objective)
- Risk Mitigation methods

OBJECTIVES

At the end of this ISO/IEC 27031:2011 - Lead Implementer training course, you will learn to:

- Understand the implementation of a Business Continuity Management System (BCMS) in accordance with ISO 27031
- Gain a comprehensive understanding of concepts required for effective management
- Understand the relationship between the components of a BCM and the compliance with the requirements of different stakeholders of the organization
- Advise your organizations on best practices in the management of business continuity
- Improve the capacity for analysis and decision making in the context of ICT

ORGANISATIONAL IMPACT

- Delegates attending this training course will gain an understanding of the strong business reasons why organisations should effectively manage and plan all types of risk.
- A proper understanding of the security department's role
- Budget alignment
- Greater risk mitigation and risk prioritization
- More direct connection to the protection of company assets

PERSONAL IMPACT

- Delegates attending this ISO/IEC 27031:2011 - Lead Implementer training course will gain an improved personal knowledge of threats and risks to their organisation, they will learn skills to combat these threats and put into place standards, plans and strategies which if successfully implemented will increase their professional reputation and improve their ability to deal with serious security issues.
- Aligning BCM with the Organizational Mission
- Gain an intimate knowledge of your Organization
- Understand goals and objectives to the Organization
- Learn how to align risk objectives with business objectives
- Understand what ICT risks exist
- Provide objective perspective on risk
- Provide expertise in the area of risk mitigation and resilience

WHO SHOULD ATTEND?

This training course is suitable to a wide range of professionals but will greatly benefit:

- Information and communication technology managers
- Information technology managers
- Personnel involved with risk assessment and risk analysis
- Software engineers
- Network engineers and managers
- Managers
- Supervisors
- Executives
- ICT Managers and technicians tasked with implementing technical continuity capability
- Anyone involved in strategic or operational IT Service Management

Course Outline

Introduction to ICT Continuity

- Why do we need ICT Continuity in the organization?
- What is Information and communications technology (ICT) Continuity
- Understanding Disaster recovery
- Relationship with Business continuity
- The concept of performance and resilience

Introduction to ISO 27031

- The role of ICT Readiness for Business Continuity (IRBC) in BCM
- The Principles of the standard
- The Elements of the standard
- Outcomes and organizational Benefits
- Establishing the context of the standard
- Plan, Do, Check and Act
- Management Responsibility and accountability

Understanding ICT Requirements for BCM

- What is Business Impact Analysis (BIA)?
- BIA for ICT Continuity
- How to conduct BIA for your organization
- Critical' process concept
- Understanding concepts of MTPD, (Maximum Tolerable Period of Disruption), RTO (recovery time objective) and RPO (recovery time objective)
- Presenting the BIA Summary

Risk Assessment

- What is risk?
- Identification of continuity risks
- Risk assessment process
- Quantitative risks assessment
- Determining choices for risk treatment

Monitor, Review and Improvements for ISO 27031

- Maintaining ICT Readiness for Business Continuity (IRBC)
- IRBC Internal Audit
- Management Review
- Measurements
- Continual Improvement
- Corrective action