ISO 27031 IT Disaster Recovery & Business Continuity Management

Introduction

Because over the years more and more activities have become dependent upon information and communication technologies (ICT), and ICT failures are becoming more critical, it is natural to expect the spread of literature dealing specifically with this issue. In this context, the ISO 27031 standard approaches how to use the PDCA (Plan-Do-Check-Act) cycle to put into place a systematic process to prevent, predict, and manage ICT disruption incidents that have the potential to disrupt ICT services. By doing so, this standard helps to support both business continuity management (BCM) and information security management (ISM). By its nature, ISO 27031 is a perfect standard to resolve the control A.17.2.1 from ISO 27001. Many organizations struggle to define the best method to meet business expectations regarding information technology (IT) recovery. ISO 27031 provides guidance to business continuity and IT disaster recovery professionals on how to plan for IT continuity and recovery as part of a more comprehensive business continuity management system (BCMS). The standard helps IT personnel identify the requirements for Information and Communication Technology (ICT) and implement strategies to reduce the risk of disruption, as well as recognize, respond to and recover from a disruption to ICT.

ISO 27031 introduces a management systems approach to address ICT in support of a broader business continuity management system, as described in ISO 22301. ISO 27031 describes a management system for ICT readiness for business continuity (IRBC). An IRBC is a management system focused on IT disaster recovery. IRBC uses the same Plan-Do-Check-Act (PDCA) model as the business continuity management system described in ISO 22301. The objective of IRBC is to implement strategies that will reduce the risk of disruption to ICT services as well as respond to and recover from a disruption. Business continuity and IT professionals will find the use of the PDCA model very familiar but with necessary changes to support recoverability of ICT based on business requirements and expectations. ISO 27031 defines the information and communication technology (ICT) requirements for Business Continuity (BC) program that supports the mandate for an infrastructure that supports business operations when an event or incident with its related disruptions affects the

continuity of critical business functions. This includes security of crucial data as well as enterprise operations. This course focuses on the technical and procedural issues surrounding ICT Service Continuity & Disaster Recovery (DR).

Who Should Attend?

Managers, Team Leaders, Line Managers, Superintendents, OE Champions, Quality and Project Managers, Supervisors, Executives, Internal and External Auditors, Members of IT Team, Health & Safety Managers, Risk Managers, Business Process Owners, Business Finance Managers, Business Risk Managers, Regulatory Compliance Managers, Project Managers, Continuity, Risk, Quality, IT and Environmental Managers, Anyone involved in the system development, implementation and maintenance, Regulatory Affairs Managers, Consultants, Anyone who is involved in ISO standards, ICT Managers and technicians tasked with implementing technical continuity capability, Anyone involved in strategic or operational IT Service Management

Course Objectives:

By the end of this course, delegates will be able to:

- Understand the ICT requirements for business continuity
- Determine ICT continuity strategies
- Learn how to develop and implement ICT strategies
- Learn how to exercise and test the techniques
- Learn how to maintain, review and improve the system
- Learn how to integrate ICT continuity

Course Outline:

- Why do we need ICT continuity
- What is ICT continuity
- Disaster recovery
- Relationship with business continuity
- The concept of resilience
- The purpose and content of ISO 27031
- The purpose and content of ISO 27031
- What is business impact analysis (BIA)?
- BIA for ICT continuity
- How to conduct BIA?
- The concept of critical process
- Presenting BIA summary
- What is information risk?
- Identification of risks
- Risk assessment process
- Quantitative risks assessment
- Determining choices for risk treatment
- Strategies and determining/selection of appropriate ones
- Technical solutions for DR
- Strategies for data protection: backup, restoration and replication
- Telecommunications and networking issues related to DR
- ISO 27031 implementation issues
- How to integrate ISO 27031 with existing BCM?
- How to align IT service continuity program with ISO 27031?