أكاديمية الزمالة العربية البريطانية

Arab British Academy Fellowship

A.B.A.F

Certificate in IT Disaster Recovery Planning

Why Attend

This course provides participants with concrete solutions, strategies and insights into the delivery of an effective IT infrastructure and disaster recovery plan with the goal of establishing resilience measures to protect their organizations' IT.

Using tested processes and procedures, participants will analyze the risks and impact to IT operations that threats might cause. A framework for building operational resilience will be provided to deliver an effective response for safeguarding the organizations technology interests and value-creating activities.

This practical course provides participants with a framework that considers ISO 27031, ISO 20000, ITIL and ISO 22301, aligned with the Business Continuity Institute (BCI) Good Practice Guidelines (GPG) 2013 and NCEMA 7000-2012.

Course Methodology

This course will be highly interactive and include group discussions, videos, case studies and syndicate work. Risk Evaluation, BIA and High Level IT DR Plan Templates will be applied during the course and given for use after the course. Supporting information, such as Steering Committee Terms of Reference (ToR's), Change Management, DR Test Strategy and testing processes and procedures will also be made available.

It includes specific templates for carrying-out a Business Impact Analysis (BIA) as well as completion of an IT DR Plan (DRP) that participants will be able to take away for use in their own organizations.

Course Objectives

By the end of the course, participants will be able to:

- Consider policies, objectives, targets, processes and procedures that are relevant to managing risk and improving IT Readiness for Business Continuity (IRBC)

- Apply best practice to build IT infrastructure and operational sustainability, including security of the environment
- Describe the processes and procedures to carry out a risk evaluation and identify risks, threats, hazards, vulnerabilities and weaknesses that could affect your organization
- Review the key components of asset, human, change and supply chain management that are specific to IT
- Discuss the components of a successful IT Disaster Recovery (DR) Program, including data management and the key components that are necessary to carry out a technology Business Impact Analysis (BIA)
- Estimate the Maximum Tolerable Period of Disruption (MTPD), to then identify the relationship with Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
- Produce a High Level IT Disaster Recovery

Target Audience

IT managers and professionals, including Disaster Recovery (DR) managers or anyone responsible for, or involved with, Disaster Recovery Plans (DRP), Business Continuity Plans (BCP) and/or technology and IT auditing.

Target Competencies

- Applying IT Readiness for Business Continuity (IRBC)
- Conducting Risk Evaluation
- Conducting Business Impact Analysis
- Incident and Change Management
- Disaster Recovery Planning
- IT Disaster Recovery Testing

Course Outline

- IT infrastructure

- The issue of resilience
- ISO 27031 Relationship with Information Security Management System (ISMS)
- Data center and IT infrastructure
- Operational sustainability
- Data center site infrastructure tier standard
- Elements of operational sustainability
- Infrastructure strategy and policy
- The strategy – how and depth

- The policy requirements
- Site and building protection
- Network and information systems protection

- Risk evaluation and Business Impact Analysis (BIA)

- Site and building risk assessment
- PESTEL analysis (Political, Economic, Sociological, Technological, Legal, Environmental)
- Types of BIA; strategic, tactical and operational
- Implementation methods for technology BIA

- Managing recovery plans

- Processes and procedures for supply chain management using a 3PQ (Third Party Questionnaire) approach, aligned with BSI PAS 7000
- On and off-site data and information storage, including emergency response arrangements
- Change management processes and procedures for day-to-day requirements
- Risk control measures for critical supporting equipment and systems

- Understanding IT disaster recovery (DR) and reviewing the main activities

- DR lifecycle, including resources and training
- IT DR as part of the ISMS
- Scope of IT elements and requirements

- IT disaster recovery plans

- Building technology recovery plans
- Plan ownership and structure, and roles and responsibilities of IT DR Team
- Data and information sources, and internal and external dependencies
- Best practice considerations using ISO 27301, as well as ISO 20000 and ITIL
- Managing and recovering end-user computing and communications technology and infrastructure
- Recovery options
- Developing, implementing and testing
- Ownership and plan structure
- Roles and responsibilities of BC Champion and Team Leaders
- Command, Coordination, Communications and Intelligence (C3i)
- Role of the command center and essentials
- Equipment and supporting information
- Producing Situation Reports (SITREPS)
- Types of testing/exercising
- Major incident response
- Defining an “incident” and the escalation process
- Establishing Command, Coordination and Communications (3C)
- Clarifying the role of the Network Operations Centre (NOC)
- Emergency response and plan invocation
- Consideration of the supporting information, equipment and systems required
- Production of Situation Reports (SITREPS), activity logging and tools
- Post incident review
- Learning from incidents

- The value of post-incident review
- Post-incident process

- Audit and maintenance

- What is the function of an IT audit?
- Steering Committee and Terms of Reference (ToR's)
- Overriding management review and continuous improvement
- Incorporating DR into the organization lifecycle processes and establishing virtual teams
- DR documentation and working with internal and external audit functions

أكاديمية الزمالة العربية البريطانية

Arab British Academy Fellowship

A.B.A.F