Module Title : Course CDRP : Certified Data Centre Risk Professional
Duration : 2 days

Course Description

Data centres are at the core of many organizations. Downtime, of applications or the data centre itself, could lead to major direct and indirect losses to the business. This has led many organizations to build resilience at various levels such as at the data centre infrastructure and at the ICT layer. Fact is though that most companies are either over- or under spending due to the fact that many organizations have not been able to answer basic questions such as 'what is the cost of downtime' being it per application and/or the data centre itself.

Without knowing the cost of downtime it would be impossible to determine what level of investment is justified to mitigate the risks of downtime. This has led to the fact that many data centres have been built at potentially a Tier-4 level as per the ANSI/TIA-942, whereas from a business perspective a Tier-3 level would have been enough.

Risk management is the process to identify vulnerabilities and associated threats, to be followed by estimating the level of risk that they may face and how they might impact the organization if these risks were to emerge. Based on international standards (ISO/IEC27001:2005) and guidelines (ISO/IEC 27005:2011, NIST 800-30, ISO/IEC 31000/31010), CDRP (Certified Data Centre Risk Professional) is a course designed to expose attendants to the overall risk management process.

Focus is on both the data centre infrastructure and the physical data centre facility and equipment; the attendant will learn how to identify and quantify risk in their organization, creating the ability to reduce the risk to a level acceptable for the organization to allow them to make sound investment decisions based on facts rather than emotions. CDRP is a must for every organization that wants to manage their risk without over spending.

Audience

The primary audience for this two-day course is an IT, Facilities or Data Centre Operations professional working in and around the data centre (representing both end-customers and/or service provider/facilitators) and having responsibility to achieve and improve hi-availability and manageability of the Data Centre, such as: Data centre managers, Operations / Floor / Facility managers, IT managers, Information security managers, Security professionals, Auditors / Risk Managers / Professionals responsible for IT/corporate governance.

Prerequisites

While there are no specific requirements for this course, participants with at least three years of actual experience in data centre and/or IT infrastructures is recommended. This experience may come from a business or IT background but it is believed that the candidate has knowledge of both environments, understanding the mission of their organization. Having attended CITM and/or CDCP is recommended but not a requirement.

At Course Completion

After completing this course, you will be able to:

- Understand the different standards and methodologies for risk management and assessment
- Establish the required project team for risk management
- Perform the risk assessment identifying current threats, vulnerabilities and the potential impact based on customized threat catalogues
- Report on the current risk level of the data centre both quantitative and qualitative
- Anticipate and minimizing potential financial impacts
- Understand the options for handling risk
- Continuously monitor and review the status of data centre risk present
- Reduce the frequency and magnitude of incidents
- Detect and respond to events when they occur
- Meet regulatory and compliance requirements
- Support certification processes such as ISO/IEC 27001:2005
- Support overall corporate and IT governance

Course Outline

Introduction to Risk Management

- Risk management concepts
- Managements' concern
- Enterprise Risk Management (ERM)
- Information technology risk and the business
- Information security risk management
- Data centre risk
- Benefits of risk management

Standards, Guidelines and Methodologies

- ISO/IEC 27001:2005, ISO/IEC 27005:2011, ISO/IEC 27002:2007
- ISO/IEC 27005 in relation to ISO/IEC 27001 ISMS
- NIST SP 800-30

- ISO/IEC 31000:2009
- SS507:2008
- TIA/ANSI-942
- Other methodologies (CRAMM, EBIOS, OCTAVE, etc.)

Risk Management Definitions

- Asset
- Availability / Confidentiality / Integrity
- Control
- Information processing facility
- Information security
- Policy
- Risk
- Risk analysis / Risk assessment / Risk evaluation / Risk treatment
- Threat / Vulnerability
- Types of risk

Risk Assessment Software

- Risk assessment software
- Automation
- Considerations
- Vendor selection

Risk Management Process

- The risk management process
- Establishing the context
- Identification
- Analysis
- Evaluation
- Treatment
- Communicate and consultation
- Monitoring and review

Project Approach

- Project management principles
- Project management methods
- Scope
- Time
- Cost
- Roles and responsibilities

Context Establishment

- General considerations
- Basic criteria
- Risk appetite vs. risk tolerance
- Scope and boundaries
- Scope constraints
- Organization for risk management
- Training, awareness and competence

Risk Assessment - Identification

- The risk assessment process
- Identification of assets
- Identification of threats
- Identification of existing controls
- Identification of vulnerabilities
- Identification of consequences
- Hands-on exercise: Identification of assets, threats, existing controls, vulnerabilities and consequences

Risk Assessment - Analysis and Evaluation

- Risk estimation
- Risk estimation methodologies
- Assessment of consequences
- Assessment of incident likelihood
- Level of risk estimation
- Risk evaluation
- Hands-on exercise: Assessment of consequences, likelihood and estimating level of risk

Risk Treatment

- The risk treatment process
- Residual risk
- Risk reduction
- Constraints in risk reduction
- Risk retention
- Risk avoidance
- Risk transfer
- Control categories
- Cost-benefit analysis
- Control implementation

Communication

- Effective communication of risk management activities

Risk Monitoring and Review

- Ongoing monitoring and review
- Criteria for review

Risk scenario's

- Risk assessment approach
- Data centre site and facility
- Force majeure
- Organizational shortcomings
- Human failure
- Technical failure
- Deliberate acts

Exam

- Sample questions
- Self study (time permitted)
- Exam: Certi_ed Data Centre Risk Professional

Examination

Certification exam papers can be taken in paper based format at the end of the last day of the course, or online via an authorized training partner, depending on the country in which the course is delivered. The exam is a one hour, 40 questions, multiple choice and closed book exam. The attendee need to have 27 out of 40 questions correct in order to pass the exam. Results of the exam will be communicated to the attendee within four weeks following the examination.

Certification

Attendees who successfully pass the exam will receive the official 'Certified Data Centre Risk Professional' certificate. Certification is valid for a three years period after which the student needs to re-certify. More information on re-certification and verification of the current status of certification can be found on the EPI corporate website, http://www.epi-ap.com.