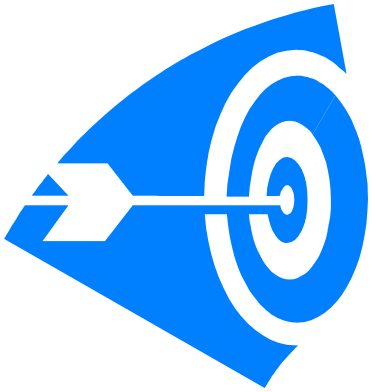
Course: Information Security Management in e-Governance

Day 1

Session 1: Introduction to the Course

Agenda



- Welcome to the training course
- Getting to know the participants - Personal introductions and objectives
- Introduction to the training course objectives
- Understanding the expectations from the participants

Welcome & Introduction

Sponsors, Facilitators and Participants

Expectations from the course

What are your expectations from the course?

Synopsis of training course

What does the training programme contain?

Business need for the course

Module 1:

The training course will equip the participants with a range of practices and standards in relation to information security management for e-Governance projects to:

- Secure critical information assets of government against loss, theft etc
- Ensure data confidentiality, integrity and non-repudiation
- Ensure availability and continuity of the IT services
- Ensure IT systems implementations inline with the security policies and standards defined by DIT/central/state governments…

Performance Objectives of the Course - Module 1

The training course performance objectives in terms of expected capabilities to be demonstrated by the participants in their respective departments post training completion includes the following:

- Support information security risk assessment and development of information security strategy, policy and procedures for e-Governance projects
- Ensure that e-Governance solutions are implemented to address information security risks and threats
- Support in implementation of security monitoring and evaluation mechanisms to ensure compliance to security policies, procedures
- Good practices and standards in information security
- Approach for managing information security
- Identification of information security risk categories in the organization
- Definition of broad level solutions for information security risk management
- Definition of scope of Information Systems Security Policy
- Introduction to Enterprise Applications

Knowledge – Skills – Attitudes (KSA) matrix for course – Module 1

Knowledge

- Information security risks and its impact on the government business
- Understand IT landscape in e-Governance and potential information security risks and threats across various levels
- Information Security Architecture for e-Governance projects
- Approach for development and implementation of security strategy, policies and procedures
- Policy and regulatory aspects related to information security in e-Governance

Knowledge – Skills – Attitudes (KSA) matrix for course – Module 1

Skills

- Define the scope of information security audit

Knowledge – Skills – Attitudes (KSA) matrix for course – Module 1

Attitude

- Recognize the information security risks in the business environment and its impact to the organization
- Appreciate the need for information security and its awareness in the organization
- Provide enough emphasis on information security management within the organization
- Align organization culture to implement best practices in information security

A Typical day during the training…

- Five sessions per day
  - Three sessions pre-lunch
  - Two sessions post -lunch
- Each session is for approximately 60 minutes
- Each session can be a:
  - Theoretical or conceptual discussion
  - Discussion on real life examples (successful e-Governance initiatives..)
  - Classroom exercise on application of concepts learned during the training…
  - Presentation or discussion on the findings from the classroom exercise
  - Or can include all the above…….

Course Outline

Day	Sessions
Day 1	Session 1: Welcome to the training course Session 2: Introduction to Information Security in e-Governance Session 3: Models and Frameworks for Information Security Management Session 4: Securing Business Applications Session 5: Securing Data and Operating Systems
Day 2	Session 1: Securing IT Infrastructure Session 2: Security in end user environment Session 3: Physical and Environmental Security Session 4: Security Policies Session 5: Disaster Recovery Planning

Course Outline – contd..

Day	Sessions
Day 3	Session 1: Information Security Audit – Concepts & Importance Session 2: Regulatory Framework of e-Governance Session 3: Introduction to ERP Applications Session 4: Introduction to Open Source Systems Session 5: Key Learnings, Feedback and training course wrap up

End of Session