



المركز العالمي للتدريب والتطوير
International Centre For Training & Development



BEST MANAGEMENT Practices in IT Security



INTERNATIONAL ASSOCIATION FOR
HEALTH AND OCCUPATIONAL
SAFETY AND THE ENVIRONMENT



Course Introduction:

Delegates will have a blue print for building an effective security program leading to eventual accreditation to ISO17799. Delegates will also gain skills to get agreement from disparate interest groups on security issues. In addition they will receive a security audit questionnaire and be taught how to use it to produce a low risk installation.

Course Objectives:

Delegates will learn how to:

- Establish and maintain a workable information security program.
- Plan and administer the program
- What the implications of ISO17799 are to the corporation
- Getting continuing support from the user departments and IT staff
- How to work to advantage with the Security Manager
- How to analyze and reduce security threats
- How to creatively co-operate in an IT crime investigation
- How to write the corporate security manual
- Convincingly present the results of project studies

Who Should Attend?

Data security professionals as well as IT staff who wish to increase their understanding of security issues.

Course Outline:

IT Systems Security

- Role of the Systems Security Manager in 2003
 - Working with the Security Manager
 - Working with Departmental Managers
 - Investigations
- Job description
- International law and corporate liability
- Privacy laws
- 1995 UK Act
- US Patriot Act
- ISO 17799

Computer Crime

- Growing crimes of fraud, extortion and espionage
- Internet crime
- Employee crime

Information security

- Why information security is needed
- How to establish security requirements
- Information security starting points
- Critical success factors

How to implement a security program

- Designing an information security policy
 - Developing a strategy
 - Strategy framework
 - Strategy bed rocks
- Taking the lead and gaining management and organizational support
- Selecting an effective risk management methodology

Change and the organization

- **Managing change**
- Culture
- The project manager and change
- Launching a project
- End user education
- After commissioning
- Projects that fail

Requirements of ISO 17799

- Security standards for databases
- Security standards for personnel
- Security standards for encryption
- Communication standards

Environmental Security and Working with the Security Manager

- Physical security, what it is and who is responsible
- Security of file servers, firewalls, routers and Webs
- Secure perimeters

- Responsible persons

Investigations

- Role of security on the CIRT
- Investigating principles
- Investigative techniques for Windows and UNIX
- Investigating Web sites

Working with Departmental Managers to meet ISO17799

- The legal department and investigations
 - Outsourcing
 - Investigations
 - Surveillance
 - AUP
 - Anton Pillar Orders
- Line Managers, Continuity and Disaster Recovery Plans
 - Line managers and the test
- ISO17799 and legal requirements
- Getting agreement on security objectives
- Managing time
- The power of collaboration
- Persuasion as a tool

Conducting a Security Audit

- How an audit is conducted
- Linking with internal audit on:
 - Accounts to be examined
 - Procedures to be tested
 - Transactions to be analyzed
 - Policies to be reviewed
- The use of structured questionnaires
- Developing work sheets and writing reports
- Writing the Security Manual

Management basics

- The perceived system security manager's job
- Analysis of leadership styles
- The relationship between management and leading
- The proactive system security manager

- Goals and goal setting
- Building vision in the IT and user departments

The importance of listening, reading and remembering in security management

- Essentials of the listening environment
- Recognition devices
 - Informal recognition
 - Essentials of successful recognition programmers
- Creative listening
 - Ten keys to effective listening
 - Verifying comprehension by feed-back
- Reading
 - Speed reading
 - Reference, technical and study reading
 - Compartmentalizing the reading task
 - Further improvement
- Memory and recall
 - Retention and recall
 - Special memory systems
 - Remembering names and faces
 - *Associations
 - * Features
 - Increasing memory
 - Exercises

Communicating effectively

- Dress
- Body language
- AIDA
- ABC
- Mirroring
- Establishing immediate rapport

Controlling meetings for results

- Other people's meetings and hostile chairs
- Focusing on emerging goals and targets
- Meetings that go wrong
- Skills and techniques to achieve goals

Selling deliverables

- Presenting at board level
- Keeping on track
- Objectives in presentations
- Audiences
- Group behavior
- Dress rehearsals
- Ending the meeting
- Check lists

Grey areas in information security

- E-mail security and privacy
- Acceptable use policies
- Employee monitoring
- Cryptography and the international community
- Negligence issues

Course Methodology:

A variety of methodologies will be used during the course that includes:

- (30%) Based on Case Studies
- (30%) Techniques
- (30%) Role Play
- (10%) Concepts
- Pre-test and Post-test
- Variety of Learning Methods
- Lectures
- Case Studies and Self Questionnaires
- Group Work
- Discussion
- Presentation

Course Fees:

To be advice as per course location. This rate includes participant's manual, Hands-Outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Course Certificate:

International Center for Training & Development (ICTD) will award an internationally recognized certificate(s) for each delegate on completion of training.

Course Timings:

Daily Course Timings:

08:00 - 08:20	Morning Coffee / Tea
08:20 - 10:00	First Session
10:00 - 10:20	Coffee / Tea / Snacks
10:20 - 12:20	Second Session
12:20 - 13:30	Lunch Break & Prayer Break
13:30 - 15:00	Last Session

