

SERVICE DESIGN - IT SECURITY MANAGEMENT

“Design secure IT services by aligning security controls with business objectives.”

Schedule

| Venue    | Fees                  |
|----------|-----------------------|
| In-House | ASK FOR THE QUOTATION |

► Available delivery methods: In-House Training

Introduction

This course provides a deep dive into IT Security Management as an essential process within the ITIL® Service Design phase. It explores how security policies, processes, and controls can be effectively embedded into service design and delivery to protect the confidentiality, integrity, and availability of information and IT services.

Objectives

- By the end of this course, participants will be able to:
- Understand the role of IT Security Management within the ITIL® Service Lifecycle
  - Define and implement an IT security policy framework
  - Identify key components of risk assessment and security controls
  - Integrate security measures into new or changed services
  - Monitor and manage compliance with security policies

## Why Attend

As cyber threats and data breaches rise, organizations must ensure that security is not an afterthought. This course empowers IT professionals and security managers to design services that are secure by default, minimizing risks while supporting business growth.

## Target Audience

- IT Security Managers and Officers
- ITIL® and Service Management Professionals
- IT Architects and Service Designers
- Risk Managers and Compliance Officers
- CIOs, CISOs, and Technical Leads

## Individual Benefits

- Gain a structured understanding of security within ITIL®
- Improve your ability to identify and mitigate IT security risks
- Enhance your role in designing secure IT systems and services
- Strengthen compliance with global IT security standards

## Organizational Benefits

- Reduce business risk from security breaches
- Strengthen alignment of IT services with governance frameworks
- Enhance resilience of digital services
- Ensure security is integrated early in the service lifecycle

## Instructional Methodology

- Expert-led discussions and best-practice demonstrations
- Interactive workshops and simulations
- Case studies of real-world security integration
- Group activities and scenario-based learning
- Pre- and post-assessment quizzes

## Course Outline

### DETAILED 5-DAY COURSE OUTLINE (CUSTOMIZABLE)

**Training Hours:** 7:30 AM – 3:30 PM **Daily Format:** 3–4 Learning Modules **Coffee Breaks:** 09:30 & 11:15 **Lunch Buffet:** 01:00 – 02:00

#### Day 1: Introduction to IT Security Management

- **Module 1:** The Role of Security Management in ITIL® Service Design (07:30 – 09:30)
- **Module 2:** IT Security Principles: CIA (Confidentiality, Integrity, Availability) (09:45 – 11:15)
- **Module 3:** Developing a Security Policy and Framework (11:30 – 01:00)
- **Module 4:** Organizational Roles, Responsibilities, and Governance (02:00 – 03:30)

#### Day 2: Risk Assessment & Control Design

- **Module 1:** Conducting IT Security Risk Assessments (07:30 – 09:30)
- **Module 2:** Identifying Threats, Vulnerabilities, and Impacts (09:45 – 11:15)
- **Module 3:** Designing and Selecting Security Controls (11:30 – 01:00)
- **Module 4:** Security Risk Treatment Planning (02:00 – 03:30)

#### Day 3: Security in Service Design

- **Module 1:** Embedding Security in the Service Lifecycle (07:30 – 09:30)
- **Module 2:** Integrating Security in SLA, OLA, and UC (09:45 – 11:15)
- **Module 3:** Identity and Access Management (IAM) Principles (11:30 – 01:00)
- **Module 4:** Case Study – Designing a Secure IT Service (02:00 – 03:30)

#### Day 4: Monitoring, Compliance & Incident Handling

- **Module 1:** IT Security Monitoring and Metrics (07:30 – 09:30)
- **Module 2:** Compliance with Standards (ISO 27001, GDPR, NIST) (09:45 – 11:15)
- **Module 3:** Handling Security Breaches and Incidents (11:30 – 01:00)
- **Module 4:** Security Event Management Tools and SIEM Overview (02:00 – 03:30)

#### Day 5: Security Strategy & Continuous Improvement

- **Module 1:** Aligning Security with Business Strategy (07:30 – 09:30)
- **Module 2:** Designing for Security Scalability and Agility (09:45 – 11:15)
- **Module 3:** Maturity Models and Continuous Security Improvement (11:30 – 01:00)
- **Module 4:** Capstone Exercise – Present a Secure Service Design Plan (02:00 – 03:30)

## Certification

Participants will receive a Certificate of Completion. This course supports continued professional development in ITIL®, cybersecurity, and IT service management best practices.

## Why Choose MAWA Events

- **Global Expertise:** More than 17 years of experience in professional training and consulting.
- **Industry-Leading Faculty:** Courses delivered by seasoned professionals with hands-on experience.
- **Practical Insights:** Learn to turn theory into actionable strategies for real-world business impact.
- **Client-Focused Solutions:** Customized programs designed to achieve your organisation's unique goals.

|                                                                                                                                |                                         |                                                 |
|--------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|-------------------------------------------------|
| <p><b>In-House / Customized Training</b></p> <p>Interested in running this course for your team?</p> <p>Please contact us:</p> | <p>TEL:</p> <p><b>+601116373203</b></p> | <p>EMAIL:</p> <p><b>info@mawaevents.net</b></p> |
|--------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|-------------------------------------------------|

© Material published by MAWA Events shown here is copyrighted. All rights reserved. Any unauthorized copying, distribution, use, dissemination, downloading, storing (in any medium), transmission, reproduction or reliance in whole or any part of this course outline is prohibited and will constitute an infringement of copyright.