

Course Aim:

This course aims to equip participants with the knowledge and capability to design, implement and manage a cost-effective security system that suits the unique requirements of their organization.

Essential For:

Security Executives, Investigators, Compliance Officers, Facility personnel (including in-house plain-clothes detectives), and Corporate Protection Managers

Certification:

Upon successful completion of the course, participants will be awarded:

Certificate of Attendance (co-awarded by STET Homeland Security Services and ASIS International, Singapore)

Course Duration: 4 days



FOR REGISTRATION/ ENQUIRIES, CONTACT:

Seah Fiona
Phone: 6477 6688
Fax: 6477 6677
(Attn: Seah Fiona)
E-mail: seahfiona@stet.com.sg

317 Outram Road #03-02
Holiday Inn Atrium Singapore
Singapore 169075

Corporate Security and Risk Management [HLST 017]

**10% Discount for
ASIS Members**

Providing Strategic Security Solutions

Risk is always present — the corporation needs to assess these threat conditions in relation to itself, and take measures to mitigate their impact. Corporate Security Practitioners need to know the tools that can be employed to create a security framework for their organizations, and the constraints and opportunities that can aid in structuring a foundation for corporate resilience and timely, effective response.

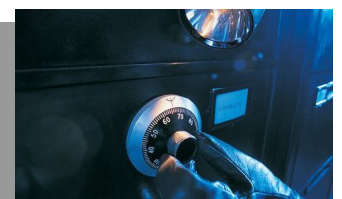
At the corporate level, security becomes more than individual manpower and technology considerations. With the emergence of organized crime involving a complex cocktail of physical, IT and chemical/ biological elements, corporations can no longer afford any slack in security. Increasingly, Corporate Security Practitioners need to be more thoroughly equipped to manage and augment security at their organization.

Course Synopsis:

This security training course is a professional course that is specially designed to meet the needs of the security practitioners. This course teaches the participants the methodology of managing security risks and formulating security mitigation plans. Towards the end of the course, participants will be taught with the technique of using appropriate technology to augment the facility existing security measures and they will also be imparted with the knowledge of introducing contingency management approach to mitigate security threats posed by criminals and terrorists.

Course Benefits:

- I. Acquire both the competencies and comfort level to manage corporate security and risk at a managerial level
- II. Gain the macro perspective of a Corporate Security Practitioner to apply to your own organization



Course Aim:

This course aims to equip participants with the knowledge and capability to design, implement and manage a cost-effective security system that suits the unique requirements of their organization.

Essential For:

Security Executives, Investigators, Compliance Officers, Facility personnel (including in-house plain-clothes detectives), and Corporate Protection Managers

Certification:

Upon successful completion of the course, participants will be awarded:

Certificate of Attendance (co-awarded by STET Homeland Security Services and ASIS International, Singapore)

Course Duration: 4 days



FOR REGISTRATION/ ENQUIRIES, CONTACT:

Seah Fiona
Phone: 6477 6688
Fax: 6477 6677
(Attn: Seah Fiona)
E-mail: seahfiona@stet.com.sg

317 Outram Road #03-02
Holiday Inn Atrium Singapore
Singapore 169075



STET Homeland Security Services Pte Ltd
A Company of ST Electronics



Corporate Security and Risk Management [HLST 017]

Topic Synopsis

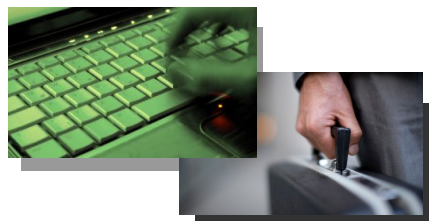
Providing Strategic Security Solutions

Introduction - Role of Corporate Security Practitioner

- ↘ Corporate security objectives
- ↘ Risk management philosophy and its methodology

Concept in Formulating the Security Mitigation Plan –Strategic, Operational & Tactical Planning Levels

- ↘ Analysing current corporate strengths and vulnerabilities
- ↘ Establishing Level 1 strategies for operational and technical solutions
- ↘ Determining Level 2 concepts for operational-technical security plans
- ↘ Developing Level 3 tactical operational interface procedures on asset protection encompassing:
 - *Concept of perpetrations*
 - *Technologies employed for barrier types*
 - *Loss prevention and control measures*
 - *Managing security guards*
 - *Means and methods for detection and screening*



Emergency and Business Continuity Management

- ↘ Introduction to targets & threat missions of perpetrators
- ↘ Considerations & need for contingency planning & procedure development
- ↘ Managing effects & recovery of attack on own corporate target(s)

Managing Security Risks

- ↘ Defining risks
- ↘ Causes and effects of risks
- ↘ Strategies in mitigating security risks
- ↘ Managing visitor access
- ↘ Means of response
- ↘ Maintaining security log

Use of Technology to Augment Security

- ↘ Introduction to electronic detection systems
 - *Intrusion Detection Systems (IDS)*
 - *Closed Circuit Television (CCTV) Systems*
 - *Electronic Access Control Systems*
- ↘ Control functions
 - *Integrated Security System (ISS)*
 - *Security Control Room (SCR)*

EX “En Garde”

(Exercise for security design and planning for the facility)

- ↘ Facilitator-led discussion on:
 - *Security protection concepts & facility design*
 - *Recap of security planning process*
 - *Design system based on risk management process*
 - *Analysis of site layout, operations characteristics & vital facilities, their security concerns and vulnerabilities*
 - *Security measures in place*
- ↘ Conduct risk analysis, design mitigation strategies & develop countermeasures including budgetary considerations
- ↘ Present security operational plans