



Additional Security Courses

Identifying the Risks to Security

When it comes to the security of your organisation and its assets, there can be no half measures. You'll want to be totally confident that every precaution has been taken to protect your interests and your future investments, this module will enable you to identify the risks and consider a variety of security systems to enable you to implement a tangible security framework.

Key Sections:

- ISO27001 and risk management policy development.
- The Agenda Security Model.
- What are the risks?
- Risk Assessment and Business Continuity.
- Self Assessment, Perimeter.
- Outer Shell of Building.
- Building Internal.
- Web info.
- Signage.
- Trade info.
- Non-shredded waste.

Reducing Internal Risks via Security Based Recruitment Practices

What you see is not always what you get and so Agenda Security Services have designed a comprehensive course to improve the effectiveness of security screening during the recruitment process. This is the vital first step prior to undertaking the security screening of the candidate. Having effective recruitment processes can help to screen out undesirable individuals, fraudsters, saboteurs, infiltrators and thieves.

Key Sections:

- Three stage process.
- Security in the Recruitment.
- Screening, Awareness.
- What to look for.
- Body language.
- Questioning techniques.
- CV analysis.
- Power Googling.



Additional Security Courses

Security Screening Systems

In these days of heightened security awareness organisations need to assess the risks to their business continuity from security breaches. Employees are often cited as an organisations biggest asset but they are often also the biggest threat too. Whether the concern is about theft, industrial espionage, infiltration or terrorism we describe the systems to enable organisations to effectively screen individuals. In our experience there are increasing numbers of people using forged birth certificates, visas, qualifications and other documents to gain entry to organisations and with large fines being imposed for employing illegal workers effective screening can provide you with additional reassurance.

Key Sections:

- What to screen for.
- Why screen.
- Methods of screening.
- How to develop levels if screening required.
- Issues (timing, information required).
- Legal aspects.
- Data subject consent forms.

Traditional Security Disciplines

Traditional security principles are often overlooked these days due to the high tech threats that we face, but the fundamental physical security issues are still the same, this module offer advice on options to improve physical security and in particular the Secured by Design standard.

Key Sections:

- Secured by Design.
- Bolts, locks, bars, bollards, lighting, barbed wire, timed lighting.
- Site security.
- Alarms (types of).
- Access control.
- CCTV and sound,
- Telecoms, telephone systems, fax security, voice mail, automatic re-direction.
- Access to names/positions.
- Training of staff.
- Responsibilities.
- Communication policies.
- Equipment marking.
- Check insurances.
- Guards or not.



Additional Security Courses

Computer Security

There have been numerous widely publicised threats to computer system integrity. The Millennium bug passed without major problems but the same cannot be said for the large number of serious computer viruses that are attacking your networks every day. What can you do to improve the integrity of your systems and software? This module aims to offer some solutions to address the key threats.

Key Sections:

- Mobile platform policies.
- Shared network directories.
- Wireless LANs (protection of).
- VPN.
- Virus protection.
- Internet.
- Intranet.
- Extranet security awareness.
- Password complexity.
- Timeouts.
- User account protection.
- Security auditing software.

Desktop Defences

With computer fraud, illegal internet access and data theft being committed at increasing levels what can be done to protect the access points to your network or the internet. Many organisations have fantastic fire walls but cannot stop an employee or intruder either simply carrying out the base unit or downloading information onto a portable recording device. This module explains how bona fide staff can protect their desk top from such attacks.

Key Sections:

- Traditional ID Vs Two Factor: choosing passwords, Guest/User Accounts, Screen Savers, E-mail Encryption, back up options.
- Protection technologies.
- Biometrics.
- Tokens.
- Wireless connectivity.
- Security profiles and audits.
- Physical security thin client.
- Cable ties, security screws and plates.
- Dongle and token protection.
- Cabinets.
- Alarms movement and proximity sensors.
- Portable data recording devices.



Additional Security Courses

Identification Theft Defences

With more and more cases of identity fraud coming to light there is enormous potential for serious personal and business damage to be inflicted. This is not just financial as organisations can suffer loss of reputation and even legal problems where they and their employee identifications are being used for nefarious purposes. This module outlines the key threats and how organisations and individuals can limit the opportunity for somebody to steal their identities.

Key Sections:

- Improve your own personal security.
- Limit the possibility of ID theft.
- Power Google credit card details to show threat.
- Internet scams.
- Identification information available via networks/e-mails etc.

Dealing with Incidents

Whatever your business or organisation there is always somebody that will want to take advantage of any opportunities that you may present. Whether this is internal theft or any other type of incident such as a robbery this module provides advice on how to prevent or handle such situations.

Key Sections:

- What kinds of incidents.
- Theft (reducing the risks, why it happens and prevention).
- Robbery (types of robbers).
- What to do in the event of a robbery.
- Demonstration.
- Relationships with local community, police, neighbours.
- Incident reporting and evaluation.
- Offender description forms, guards (training, licensing and screening).
- Legally what you can and cannot do (reasonable force).

Site Security

Site security often means protecting the perimeters and building within the site against unauthorised entry. Access control is a major consideration but to manage site security effectively there are many other considerations. This module specifically looks at site security management and offers practical advice on how the risks can be managed effectively.

Key Sections:

- Fencing, Cameras, Guarding.
- Access, Barriers, Booking systems, Vehicular access.
- 24 hour protection.
- Legal issues.
- Landscaping.
- Vehicles, emergency service access.
- The use social engineering to test systems.