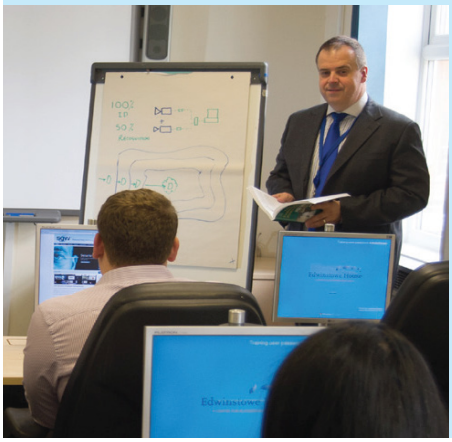
Threat, Risk and Vulnerability Assessment (TRVA) Course

Overview

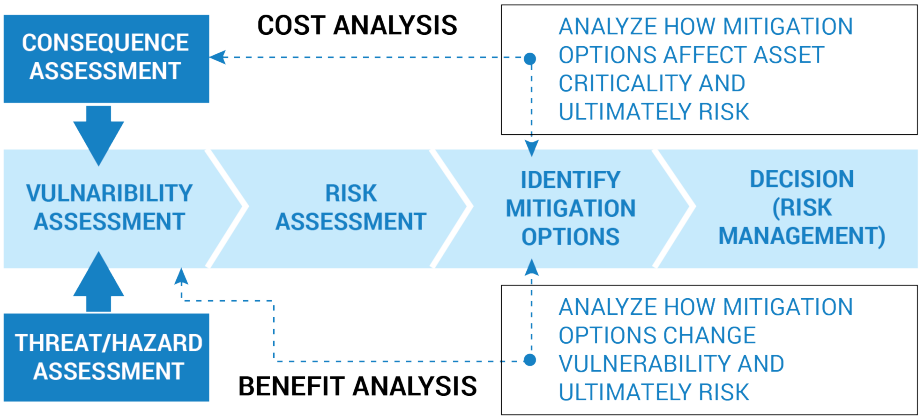


The Threat, Risk and Vulnerability Assessment (TRVA) has become one of the most integral elements of security risk management. Too often, security decisions are made without a clear understanding of the threat, and, vulnerabilities that impact a business and its assets. This course has been developed to allow delegates to gain an insight and a better understanding of the latest security planning and assessment concepts and solutions. The course will address and define Threat and Risk; what they are and how they affect security operations and assessment. It will define and assess Vulnerability, and how Risk, Threat and Vulnerabilities are intrinsically linked when mitigating risk. By constructing an integrated security approach; physical, technological and human elements of security, the course will provide tools and methodologies for understanding critical Threat, Risk and Vulnerability aspects, allowing delegates to take an effective approach towards security.

Module 1 - Introduction to the Risk Management Process (ISO31000)
Module 2 - Threat and Risk Methodology; Context,Threat and Risk distinction, interaction
Module 3 - Threat Assessment; threat capability, threat intent, threat source
Module 4 - Vulnerability Identification and Analysis; weaknesses in physical, technical or human security,'Soft' vs 'Hard' targets, CPTED
Module 5 - Risk Assessment; asset identification, context of risk to business, Likelihood and Impact
Module 6 - Practical and Group Exercises; Red vs Blue Team, Devils' Advocacy, Threat Scenario planning; Integrated security

Course Benefits

- Robust understanding of Threat, Risk, and Vulnerability methodologies
- Thorough grasp of Threat and Risk Identifi cation, Assessment and Evaluation in context – different threats, risks and treatment options
- Understanding of Asset identification, protection and criticality
- Ability to understand Risk Management Process when liaising with stakeholders
- Insight into Scenario Planning; categorising threats, methods of attack, likelihood and impact
- Appreciation of integrated security systems
- Insight into innovative security practices



Suitable For:

- Security managers and practitioners
- Physical protection professionals
- Security consultants
- Aviation security
- Critical infrastructure team
- Hotel secrity
- Public installations
- Event security
- Building managers
- Individuals who are looking to develop their security skills and professional knowledge.

Pre-Requisites:

There are no formal entry requirement for this course, and individual applications are assessed based on the candidate's experience and educational background.

Duration:
4 days

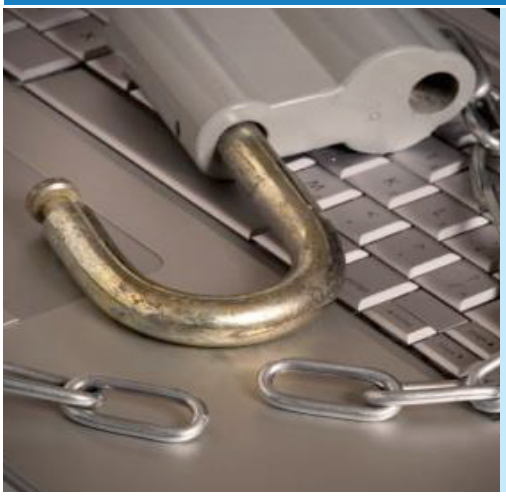
Venues:
This course is held frequently at regular intervals in Nottinghamshire, UK, Dubai, UAE & Riyadh, KSA ('see published dates')

Course Fee:
UAE Course Cost: AED 6,000
Saudi Arabia Course Cost: SAR 6,000
UK Course Cost: £1,100
('Includes lunch and refreshments')

Edwinstowe House, High Street, Edwinstowe, NG21 9PR, United Kingdom
info@sgw-consulting.co.uk

Security Risk Management Training Course

TRAINING COURSE MODULES



Risk Management (Security)

The training course will be delivered at SGW training course venues ('specified on our website'), over a five-day period (40 guided learning hours), with constant mentoring by the course tutors.

Assessment will be a combination of a case study response document and an evidence based portfolio will be produced by individual learners during the course of the training period.

This course is aimed at security managers and practitioners / individuals who are looking to develop their skills and professional knowledge.

Edwinstowe House, High Street, Edwinstowe, NG21 9PR, United Kingdom info@sgw-consulting.co.uk

Security Risk Management Training Course

Module 1

- Course Introduction
- ISO 31000
- Identify and evaluate clients' assets

Performance Criteria

Delegates will be trained to: –

a. gather relevant information from different sources sufficient to identify and evaluate clients' assets
b. collate and take account of all relevant information to support the evaluation of assets
c. use logical and systematic analysis of information to evaluate clients' assets
d. determine the potential impact to your clients through the loss of identified assets
e. take account of critical requirements that could impact on the security of your clients' assets
f. prioritise the value of identified assets in accordance with criteria agreed with your clients
g. evaluate relevant information according to its usefulness
h. maintain the security and confidentiality of information relevant to your clients' assets

Knowledge Criteria

Delegates must know and understand: –

1. current relevant legislation, regulations,codes of practice and guidelines relating to gathering, storing and maintaining information
2. how to find information to evaluate clients' assets
3. why you need to have sufficient information regarding clients' assets and what to do if there are any gaps in this information
4. how and why it is important to evaluate information according to its relevance and significance to the security of clients' assets
5. how and why it is important to use systematic analysis methods when identifying and evaluating clients' assets
6. how to determine the potential impact to clients if an asset was to be lost, damaged or interrupted
7. how and why it is important to take account of critical requirements that may impact on the security of clients' assets
8. how and why you should maintain the security and confidentiality of information

Range Statement

Delegates must be competent to deal with the following types of: -

1. Information about assets: nature, value, cost of replacement, potential impact to client
2. sources of information: internal to the client, external to the client, publicly available, confidential, official or restricted
3. assets: people, property, premises, information, reputation, brand,
4. impact: financial, commerce, reputation, operational, business interruption
5. critical requirements: commercial, contractual, regulatory, insurance

Security Risk Management Training Course

Module 2

- Identify and evaluate threats to clients' assets

Performance Criteria

Delegates will be trained to: –

a. gather relevant information from different sources sufficient to identify and evaluate threats to clients' assets
b. collate and take account of all relevant information to support the evaluation of threats, including the sources of threats
c. use logical and systematic analysis of information to evaluate threats to the security of clients' assets
d. categorise threats and possible methods of attack on assets and potential security measures
e. evaluate relevant information to determine its usefulness
f. maintain the security and confidentiality of information relevant to threats to your clients' assets

Knowledge Criteria

Delegates must know and understand: –

1. current relevant legislation, regulations, codes of practice and guidelines relating to gathering information
2. how to find information to identify and evaluate threats to the security of clients' assets
3. why you need to have all the relevant information regarding the threat to the security of clients' assets and what to do if there are any gaps in this information
4. how and why it is important to evaluate information according to its relevance and significance to the security of clients' assets
5. how and why it is important to use systematic analysis methods when identifying and evaluating threats to clients' assets
6. how and why you should maintain the security and confidentiality of information

Range Statement

Delegates must be competent to deal with the following types of: -

1. information about threats: sources, possibility and probability of attack, capability of source
2. sources of information: internal to the client, external to the client, publicly available, confidential, official or restricted
3. sources of threats: external to the client, internal to the client
4. threats: commercial, financial, criminal, natural disaster or hazard, political, actual, potential, accidental, deliberate

Security Risk Management Training Course

Module 3

- Identify and evaluate vulnerabilities in clients' current security arrangements

Performance Criteria

Delegates will be trained to: –

a. gather relevant information from different sources sufficient to identify and evaluate vulnerabilities in clients' security arrangements
b. collate and take account of all relevant information to support the evaluation of vulnerabilities
c. use logical and systematic analysis of information to identify and evaluate vulnerabilities in clients' security arrangements
d. evaluate relevant information according to its usefulness
e. identify actual and potential vulnerabilities in clients' security arrangements
f. maintain the security and confidentiality of information relevant to the vulnerabilities in your clients' security arrangements

Knowledge Criteria

Delegates must know and understand: –

1. current relevant legislation, regulations, codes of practice and guidelines relating to providing security of assets
2. how to identify and evaluate threats to clients' assets
3. why it is essential to have all the relevant information regarding the vulnerabilities in security arrangements and what to do if there are any gaps in this information
4. how and why it is important to evaluate information according to its relevance and significance to the security of clients' assets
5. how and why it is important to use systematic analysis methods when identifying and evaluating vulnerabilities in security arrangements
6. how and why you should maintain the security and confidentiality of information

Range Statement

Delegates must be competent to deal with the following types of: -

1. vulnerabilities: unauthorised access, theft (of property or information), damage, interference to operations (by internal or external parties), kidnapping of or harm to staff, contractors
2. security arrangements: permanent, temporary, staff security awareness

Security Risk Management Training Course

Module 4

- Determine the risks to the protection of clients' assets

Performance Criteria

Delegates will be trained to: –

a. take account of sufficient valid information to determine the risk to clients' assets
b. determine the level of risk to clients' assets, based on systematic analysis and evaluation of threats and vulnerabilities
c. inform clients promptly of situations where there are imminent risks to assets
d. produce reports that contain accurate and complete details of risk and security measure options, where applicable
e. record information in a suitable and retrievable format
f. maintain the security and confidentiality of information relevant to risks to clients' assets

Knowledge Criteria

Delegates must know and understand: –

1. current relevant legislation, regulations, codes of practice and guidelines relating to providing security of assets
2. how to take account of all relevant information to determine the risks to the protection of clients' assets
3. how and why it is important to use systematic analysis methods when determining risks to clients' assets
4. how and why it is important to produce accurate and complete details of analysis
5. the reason for recording information in a suitable and retrievable format
6. how and why you should maintain the security and confidentiality of information

Range Statement

Delegates must be competent to deal with the following types of: -

1. information about: assets, threats, vulnerabilities, other relevant factors
2. risk to assets: very high, high, medium, low
3. assets: people, property, premises, information, reputation, brand

Security Risk Management Training Course

Module 5 & 6

- Practical Group Training Exercises

Practical Group Training Exercises

The exercise can be presented as:

a. Three teams with each team being allocated a subject to research cumulating in members of that team having to present their finding to the other two teams. At the end of each presentation constructive feedback is given to team members by both the trainer and those acting as observers. The trainer should decide the size of the team(s) based on those attending and levels of experience.

b. Total class participation cumulating with a presentation and instructional debrief on each subject before moving onto the next objective

('see separate enclosed document – SGW-TRA-Practical Group Training Exercises')