Security and Risk Management in Practice

INSTITUTE FOR PROFESSIONAL AND EXECUTIVE DEVELOPMENT

www.iped-uk.com

UNIT SPECIFICATION

EDUCATION
FOR
NOW & THE
FUTURE

Designed in England,
United Kingdom

iPED

Unit Title

Security and Risk Management in Practice

Credit value

The credit value for this unit is 30 30 credits equivalent to 300 hours of teaching and learning (10 hours is equivalent to 1 credit) Guided learning hours (GLH) = 50 hours GLH includes lectures, tutorials and supervised study. This may vary to suit the needs and requirements of the learner and/or the approved centre of study. Directed learning = 50 hours: This includes advance reading and preparation, group study, and undertaking research tasks. Self-managed learning = 200 hours: This includes completing assignments and working through the core and additional reading texts. It also includes personal research reading via other physical and/or electronic resources.

iPED

>>>

Learning outcome Learner will:	Assessment criteria Learner can:

1.0 Understand the nature and purpose of security management.	1.1 Give an account on security management.
	1.1.1 Explain the meaning of protective security.
	1.1.2 Examine the roles of the security manager.
	1.1.3 Examine the roles of the security officer or guard.
	1.1.4 Explore the elements of security management. These include:
	   o Security risk management frameworks.
	   o Performance management and benchmarking.
	   o Policy, procedures and standards.
	   o Threat identification and use of intelligence.
	   o Threat assessment.
	   o Investigations.
	   o Root cause analysis.
	   o Design base threat.
	   o Asset and business impact identification.
	   o Security training
	   o Etc.

>>>

iPED

>>>

Learning outcome Learner will:	Assessment criteria Learner can:

2.0 Understand the nature and purpose of the private security industry, and the roles played by security operatives therein.	2.1 Evaluate the purpose of the private security industry.
	2.2 Examine the roles played by security operatives in the private security industry.
	2.2.1 Explore standards of behaviour for security operatives. These include:
	   o Code of behaviour.
	   o Personal appearance.
	   o Professional attitude and skills.
	   o General conduct.
	   o Organization or company values and standard.
	2.3 Describe the main private security sectors. These include:
	   o Door supervisors.
	   o Security officers (guarding).
	   o Security officers (key holding).
	   o Cash and valuables in transit operatives.
	   o CCTV operators.
	   o Close protection operatives.
	2.4 Explore the main ways through which security is provided to clients. These include:
	   o Manned security.
	   o Physical security.
	   o Systems.
	2.5 Give an account on security operatives' knowledge of existing relevant legislation.
	2.5.1 Explain why security operatives should have knowledge of existing legislation.
	2.5.2 Differentiate between civil law and criminal law, giving examples respectively.
	2.5.3 Discuss equality and diversity in the context of the security industry. This includes the following:

iPED

	o Definition of equality and diversity.
	o How security operatives should go about their duties, in relation to equality and diversity.
	o Explanation of discrimination, prejudice and stereotyping; and their implications in security management.
	o Types of discrimination.
	o Explanation of vicarious liability.
	2.5.4 Discuss key considerations in security operatives' use of force. These include:
	o Description of use of force.
	o The rule of self-defence.
	o Preventing a breach of peace and saving life.
	o What to consider when using force.
	2.6 Give an account on arrest procedures. This include:
	o Definition of arrest.
	o The common law power of arrest for breach of the peace.
	o Examination of offences for which security operatives have powers of arrest.
	2.6.1 Examine justifiable reasons for arrest.
	2.6.2 Explain things to do and/or consider during an arrest.
	2.6.2.1 Explore safety considerations during an arrest.
	2.6.2.2 Explore the nature and consequences of unlawful arrest.
	2.6.3 Discuss things to do and/or consider after an arrest.
	2.7 Give an account on conducting searches. This includes:
	o Potential consequences of searching someone without the necessary consent.
	o Types of searches.
	o Searching people and their property.
	o Searching rooms and buildings.
	o Document searching.

iPED

	o Guidance on undertaking successful searches.
	
	2.8 Give an account on reporting health and safety accidents and incidents. This includes:
	
	    o Reasons for the need to report health and safety accidents, and incidents.
	
	    o Reporting procedures.
	
	    o First aid situations.
	
	2.9 Give an account on reporting incidents and crime scene prevention. This includes:
	
	    o Definition of evidence.
	
	    o Types of evidence.
	
	    o Evidence preservation.
	
	    o Reporting procedures.

>>>

iPED

>>

Learning outcome Learner will:	Assessment criteria Learner can:
3.0 Understand how physical security can be successfully managed.	3.1 Give an account on the nature and purpose of physical security.
	3.2 Evaluate physical security considerations in protective security planning.
	3.3 Discuss the asset identification process in physical security risk management.
	3.4 Evaluate the use of controls and protective barriers.
	3.5 Give an account on how to ensure visibility and sustainability of physical security measures.
	3.6 Discuss how mixed access areas can be controlled. This includes:
	o Explanation of mixed access areas.
	o Use of Restricted Access Group (RAG) Modelling.

>>>

>>>

Learning outcome Learner will:	Assessment criteria Learner can:
4.0 Understand how to successfully manage people security.	4.1 Give an account on people security. This includes: - Definition of people security. - Components of people security. 4.1.1 Explore the important subgroups within people security. Discuss how they can be successfully managed. These include: - Human security. - Personnel security. - Identity management. - Personal protective practices. - Human factors and behaviours.

>>>

iPED

>>>

Learning outcome Learner will:	Assessment criteria Learner can:
5.0 Understand the significance of ICT (Information and Communications Technologies) and information security management.	5.1 Explain what Information and Communications Technologies (ICT) are. 5.1.1 Examine the vulnerability of information systems. 5.2 Explore the nature and significance of ICT security. 5.3 Evaluate potential threats to ICT systems. 5.4 Give an account on the nature and significance of information security. This includes: - Definition of information. - Definition of information system. 5.4.1 Discuss the purpose of information security. 5.4.2 Explore the elements of information security. 5.4.3 Examine the information security life cycle. 5.4.4 Discuss vulnerability of information.

>>>

iPED

Learning outcome Learner will:	Assessment criteria Learner can:
6.0 Understand how to successfully respond to and manage emergencies.	6.0 Explain the meaning of emergency. 6.1.1 Examine types of emergencies. 6.2 Discuss security operatives' role in dealing with emergencies on their sites. 6.3 Give an account on fire safety and procedures. This includes: - The fire triangle (i.e., elements needed for a fire to exist). - Classes of fire. - Basic fire prevention measures. - What to consider when attempting to fight a fire. - Firefighting equipment. - Fire evacuation procedures. 6.4 Give an account on the roles security operatives play in counter-terrorism. 6.4.1 Discuss security operative's awareness of potential terrorist activities. 6.4.2 Examine threat level definitions. 6.4.3 Discuss the role of managers and security operatives in counter-terrorism. 6.4.3.1 Explore behaviours that could indicate unusual or suspicious activity. 6.5 Give an account on the nature and significance of emergency management. 6.5.1 Examine the aims of emergency management plans. 6.5.2 Discuss the comprehensive approach to emergency management. 6.6 Evaluate how to effect emergency management planning. This includes: - Emergency management plan. - Mitigation. - Preparedness. - Decision flow.

	o Communications.
	o Response.
	o Recovery.
	6.7 Give an account on business continuity management.
	6.7.1 Discuss the benefits of business continuity management.
	6.8 Discuss the nature and significance of incidence management and reporting.

>>>

iPED

Recommended learning resources

Indicative reading	Risk and Security Management: Protecting People and Sites Worldwide 1st Edition by Michael Blyth; 2008. ISBN: 978-0470373057 • **For a full list of textbooks and publications relevant to this unit, please contact IPED - UK.**
Study manual	• A comprehensive IPED study material is available to aid in learning and research of this unit. • We supply IPED course materials free of charge. Our study materials, which offer quick learning start, are comprehensive, use simple English, and are easy to read and understand. The contents are so sufficient and self-explanatory; that in majority of cases readers do not require further support; although support is always available when you need it.

iPED