Strategic Knowledge Areas in Security and Risk Management

INSTITUTE FOR PROFESSIONAL AND EXECUTIVE DEVELOPMENT

www.iped-uk.com

UNIT SPECIFICATION

EDUCATION FOR NOW & THE FUTURE

Designed in England,
United Kingdom

Unit Title

Strategic Knowledge Areas in Security and Risk Management

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.

>>>

Learning outcome Learner will:	Assessment criteria Learner can:
1.0 Understand the nature of, and strategic issues relating to security risk management.	1.1 Define security. 1.1.1 Explain the meaning and implication of breach of security. 1.1.2 Differentiate between security risk management and safety risk management. 1.2 Define risk and give examples. 1.2.1 Explain the meaning of security risk and give examples. 1.3 Define threat and describe who a threat actor is. 1.3.1 Group threat by source, motive and method of operation. 1.3.2 Group assets by risk and threat. 1.4 Give an account on security risk management. 1.4.1 Explain what a security risk management system is. 1.4.2 Describe a security system. 1.5 Explain what is meant by risk management. 1.6 Give an account on risk assessment methodologies. 1.6.1 Discuss the high level risk assessment process. 1.6.2 Examine the U.S Department of Homeland Security 10-Step Risk-Assessment Methodology. 1.7 Evaluate the risk management process. 1.7.1 Examine the basic risk management process. 1.7.2 Analyse the U.S Government Accountability Office (GAO) risk management process. 1.7.3 Explore the risk management process in more detail. This includes: o Terms of reference establishment o Communication and consultation o Context establishment o Risk identification

	- Use of risk registers o Risk evaluation o Risk treatment: - Principles of risk treatment - Use of security risk management plan - Principles of security risk management treatments o Monitoring and review: - Aspects of security risk management that require continual monitoring and review - Types of monitoring and review - Key elements of a monitor and review process - Benefits of conducting a post-event review following a security breach 1.8 Evaluate the nature of risk appetite and its significance in security risk management. o Explain the meaning of risk appetite. o Categorize attitude to risk. o Examine factors influencing risk appetite. o Explain risk aversion 1.9 Give an account on the role of security risk management enablers in successfully managing security risks. SRM enablers include: o Regulation and policy o Training and implementation o Operations and application o Governance and accountability o Sustainability and resilience 1.10 Examine the pillars of security risk management. 1.11 Discuss the role of security governance in security risk management. 1.12 Explain the duty of care obligation in security risk management.

	1.13 Give an account security culture and its implication in managing security risks. ○ Examine the main subcultures that must exist to assure an informed security culture.

>>>

>>>

Learning outcome Learner will:	Assessment criteria Learner can:
2.0 Understand the guiding principles to successful security risk management, resilience building and business continuity planning.	2.1 Give an account on the guiding principles to successful risk management. The principles include: o Leadership and management commitment o Having organization wide security and risk policies o Linking strategy, planning and delivery o Establishing and managing to an agreed risk threshold o People security o Physical and environmental security o Operational security management o Business continuity and resilience o Testing o Measuring and reviewing o Document control o Assurance 2.2 Give an account on resilience building in security risk management. o Explain the meaning of resilience. o Describe the characteristics of a resilient organization. 2.2.1 Discuss the requirements for building resilience. 2.3 Evaluate the use and benefits of business continuity plans. o Explain what a business continuity plan is. o Examine the purposes served by business continuity plans.

>>>

>>>

Learning outcome Learner will:	Assessment criteria Learner can:
3.0 Understand how to successfully assess exposure to risks, threats and vulnerability.	3.1 Discuss exposure assessment in security risk management. o Define exposure, and exposure assessment. o Examine the influences of exposure in security risk management. o Explain the meaning of exposure timeframe. 3.1.1 Examine the objective of exposure assessment. 3.2 Explore the causes of variations in risk ratings. 3.3 Give an account on collateral exposure assessment. 3.4 Discuss the factors that need to be identified and evaluated as part of exposure analysis. 3.5 Examine the elements that interact to form the building blocks involved in creating and assessing exposure. 3.6 Give an account on threat assessment. 3.6.1 Analyse the causes of absence of data or information during threat assessment. 3.6.2 Discuss how threat assessment can be successfully conducted in the absence of data or information. This includes: o Use of subject matter experts. o Use of admiralty scale. o Use of green and red teams. 3.6.3 Analyse the determinants of threat. These include: o Intent o Likelihood o Risk aversion o Risk tolerance o Target attractiveness

	3.6.4 Evaluate the use of warning signs and indicators in threat assessment. 3.7 Give an account on vulnerability analysis or assessment. 3.7.1 Categorize vulnerability assessment tools. 3.7.2 Examine vulnerability assessment techniques. These include: o The U.S Department of Justice Framework or approach to determining vulnerability and target attractiveness. o CARVER – U.S Department of Defence technique for prioritizing the relative attractiveness or vulnerabilities of targets. 3.7.3 Analyse the common features of vulnerability assessment models. 3.8 Give an account on criticality assessment.

>>>

>>>

Learning outcome Learner will:	Assessment criteria Learner can:
4.0 Understand resource, control and quality management issues relating to security risk management	4.1 Discuss the importance of resource management in achieving successful security risk management. o Define resource, and give examples. o Evaluate how resource management contributes to effective and successful management of security risks. 4.1.1 Examine the types of resources in managing security risks: - Security risk management resources which include [-] physical security, [-] people, [-] information, and [-] information and communications technologies. - Financial resources. 4.1.2 Explain how resources available to an organization to apply security risk management treatments can be analysed and configured based on their attributes. 4.2 Give an account on the role of quality management in achieving successful security risk management. o Define quality, and quality management in the context of security risk management. o Analyse the prisms through which security risk management can be evaluated. o Explore the benefits of quality management in security risk management. 4.2.1 Explain the concept of Security-In-Depth, and examine its significance. 4.2.2 Discuss the nature and importance Hierarchy of Controls, as used in security risk management. 4.2.3 Discuss the concept of As Low As Reasonably Practicable (ALARP). 4.2.4 Analyse the use of security specifications in security risk management. o Explain what a security specification is. o Examine the benefits associated with the establishment of security specifications. 4.2.5 Discuss the role of leadership in quality management, in the context of security risk

	management. 4.2.6 Evaluate the role of staff and stakeholder involvement in quality management, in the context of security risk management. 4.2.7 Discuss the role of continuous improvement in quality management, in the context of security risk management. 4.3 Give an account on the use of capability maturity models in security risk management. o Explain what a capability maturity model is. o Analyse relevant capability maturity model(s) that can be used in security risk management. 4.4 Give an account on change management in security risk management. 4.5 Give an account on assurance and audit in security risk management. o Define assurance and audit. o Explain how assurance and audit are used in successfully managing security risks. 4.5.1 Examine the principles of assurance and audit. 4.6 Discuss the contribution of performance management in security risk management. o Explain performance management in the context of security risk management. o Explore the benefits of performance management in security risk management. 4.6.1 Discuss the considerations that must be made in managing performance. These include: o Ensuring clear definition of roles o Performance planning o Delivery and monitoring o Formal assessment and reward.

>>>

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.