The Hong Kong Institute for IT Professional Certification

LG1, 78 Tat Chee Avenue, Kowloon Tong, Hong Kong
Tel: 2834 2228 Fax: 2834 3003
URL: http://www.hkitpc.org Email: hkitpc@hkitpc.org

CPIT (InfoSec) Examination Scope

Introduction

CPIT (InfoSec), Information Security Officer, is a CPIT credential developed specifically for entry level information security officers and those IT professionals who have information security management responsibilities. **Information Security** refers to the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. It involves providing advices and counsel to senior management to establish information security requirements and appropriate corporate-wide policies as well as managing the execution of information security programs within an organization.

The Exam is to measure an individual's ability and knowledge as it pertains to the performance of his/her job. To ensure that the Exam is reflective of the work performed by information security practitioners, the questions are developed by professional writers, reviewed and endorsed by industry leaders, security experts and practitioners.

Practice Areas for the Examination

The Examination contains contents that originate in eight domains that have been highlighted in the corresponding Specifications of Competency Standards (SCS) of Information Security function for the Information and Communications Technology (ICT) Industry of the Hong Kong Qualifications Framework. (See http://www.hkqf.gov.hk/guie/SCS_list_ict.asp.) These eight domains are listed and briefly described in Table 1.

Examination Format

The examination is to be taken in a designated area, following a pre-set schedule. It will be a three-hour examination for 120 questions in multiple-choice format. Also,

- each question should only have one choice as the correct or the most correct answer.
- there will be no deduction for the question(s) left unanswered or incorrectly answered.
- questions that are answered with more than one choice are considered void.

Study Aids for the Examination

Reference materials that provide the corresponding Information Security competency coverage can be found either on the Web or any well published Information Security discipline and practice textbooks. A few suggestions are listed below:

- CISM Review Manual 2008 English Edition
  http://www.isaca.org/Template.cfm?Section=Browse_By_Category&Template=/Ecommerce/ProductDisplay.cfm&ProductID=812

- CISA Review Manual 2008 English Edition
  http://www.isaca.org/Template.cfm?Section=Browse_By_Category&Template=/Ecommerce/ProductDisplay.cfm&ProductID=821

- Official (ISC)² Guide to the SSCP® CBK®
  http://www.asestores.com/Merchant2/merchant.mvc?Screen=PROD&Product_Code=ISC-AU2774&Category_Code=ISC-BOOKS&Store_Code=ISC2

- Information Security Management Handbook, Sixth Edition by Harold F. Tipton and Micki Krause. Auerbach Publications © 2007 ISBN:9780849374951

- Journal published by the Professional Information Security Association (PISA)
  http://www.pisa.org.hk/publication/index.htm

- Computer Forensics Manual published by the Information Security and Forensics Society (ISFS)
  http://www.isfs.org.hk/publications/public.htm

Table 1

1. Business Continuity Planning • Establish a business continuity planning strategy • Prepare full set of business continuity planning documentation • Conduct drill test on business continuity planning • Provide awareness training program to staff dealing with business continuity planning
2. Forensics • Provide advice on computer forensics • Manage computer forensics evidence • Investigate an information security case • Prepare and present forensics investigation report
3. Information Security Governance • Establish reporting and communication channels • Maintain information security policies
4. Information Security Management • Develop information security practices and procedures • Evaluate and assess effectiveness of corporate information security practices • Ensure availability, integrity and confidentiality of information systems • Develop information security awareness programme
5. Information Security Programme Management • Develop methods to satisfy information security policy requirements • Promote accountability in managing information security risks • Minimize information security risks
6. Information System Audit • Enact information system security audit plan • Prepare and deliver information system security audit report • Evaluate and follow up on the recommendations in the information system security audit report
7. Response Management • Manage the execution of response and recovery plans • Establish procedures for documenting security incident
8. Risk Management • Ensure risk management related activities are integrated into life cycle processes • Define strategies and prioritize options to mitigate risk