Available as e-learning

Continuing Professional Development

Practitioner Certificate in Information Assurance Architecture

Our **five day** practitioner course prepares you for a career in security architecture. A Security Architect is a senior-level enterprise architect role, either within a dedicated security team or as part of a more general Enterprise Architecture team. The course prepares you to take either the BCS Practitioner Certificate in Information Assurance Architecture (PCIIAA) exam or the CREST Registered Technical Security Architect (CRTSA) exam for Senior or Lead Practitioners. It has been designed to cover all learning objectives required of all domains covered in both certifications. You will also receive access to an online resource that includes content, exercises, model answers, topical quizzes with feedback, module tests and a mock exam to prepare you for taking and successfully completing the BCS PCIIAA exam on the final day of the course or the CREST CRTSA exam at a later date.

Aim

Understand the business environments IT systems need to provide for, as well as the technical controls available that can be called upon to address the threats against confidentiality, integrity and availability.

Who Should Attend?

- Professionals who wish to gain the BCS PCIIAA or CREST's CRTSA certification
- Those who wish to qualify as a practitioner, senior practitioner or lead practitioner in security architecture under the CESG Certified Professional (CCP) scheme
- System administrators and technical architects who wish to become security architects
- Trainees who have taken the CISMP and wish to progress into a practitioner role.

Prerequisites

Trainees will require a broad understanding of all aspects of Information Security and Information Assurance equivalent to the BCS Certificate in Information Security Management Principles (CISMP).

Learning Objectives

- Describe the business environment and the information risks that apply to systems
- Describe and apply security design principles
- Identify information risks that arise from potential solution architectures
- Design alternate architectures or countermeasures to mitigate identified information risks
- Ensure that proposed architectures and countermeasures adequately mitigate identified information risks
- Apply “standard”' security techniques and architectures to mitigate security risks
- Develop new architectures that mitigate the risks posed by new technologies and business
- Provide consultancy and advice to explain Information Assurance and architectural problems
- Securely configure ICT systems in compliance with their approved security architectures.

PCIIAA

Cascades 1 | 1190 Park Avenue | Aztec West | Bristol | BS32 4FP | UK
Tel: +44 (0) 207 887 2699 Email: clientservices@pgitl.com Visit: www.pgitl.com

PGI