PRACTITIONER CERTIFICATE IN INFORMATION ASSURANCE ARCHITECTURE

v2.3

A Security Architect (SA) is a senior-level enterprise architect role, either within a dedicated security team or as part of a more general Enterprise Architecture (EA) team.

SUMMARY

This course prepares the student to challenge either the British Computer Society's 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. PCiIAA explains what the role of a Security Architect is, covering responsibilities, as well as the business, technical, procedural and administrative requirements of the role. The role of the SA originates from a modern approach to IT in business, known as Enterprise Architecture, as explained by a variety of frameworks in use today, such as TOGAF, MODAF, DODAF and Zachman, all of which have their own views pertaining to security architecture.

WHO SHOULD ATTEND?

- Students who wish to gain the BCS PCiIAA or CREST's CRTSA certificate and qualify as a Practitioner, Senior Practitioner or Lead Practitioner in Security Architecture under the CESG Certified Professional (CCP) scheme.
- System administrators who wish to become security architects.
- Technical architects looking to move into the field of security architecture.
- Security professionals wanting to gain an appreciation of the technical and business aspects of their profession, or move into a more senior architecture role.

LEARNING OBJECTIVES

Students who have successfully completed the PCiIAA course will be able to:

- 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 practices.
- Provide consultancy and advice to explain Information Assurance and architectural problems.
- Securely configure ICT systems in compliance with their approved security architectures.

COURSE AGENDA

DURATION: 5 DAYS

MODULE 1

The Basics of Security Architecture

What is Security Architecture? This module lays down the foundation of understanding of what it means to be a security architect and what the basic principles of architecture are. It describes the relationship to Enterprise Architecture Frameworks and how some of these frameworks address security. Security architecture is at the heart of what it is to be a security architect.

- What is Security Architecture?
- The Role of a Security Architect.
- Security Design Principles.
- Conceptual Architectures.

MODULE 2

Advanced Security Architecture Concepts

This module lays down the next level of detail for a variety of architectural concepts. It starts by describing security mechanisms, such as cryptographic mechanisms. It then goes on to describe a wide range of security services. Finally the module describes how the security services can be applied within a system and how design patterns are an important tool for a SA.

- Core Security Mechanisms.
- Security Services, Part 1, Part 2 and Part 3.
- Security Design.

MODULE 3

Information Assurance Methodologies

This module goes into the various methodologies and techniques that can be used to assure the implementation of a system or a product. This includes the purpose of vulnerability and penetration testing.

- Information Assurance Frameworks.
- Product and Service Assurance.
- Cryptographic Assurance.
- Vulnerability and Penetration Testing.

MODULE 4

Innovation and Business Improvement

This module explains how security can drive change and improve business functions when done properly. Different business scenarios and sectors can drive a wide variety of security architecture innovations and changes and it’s important that the accomplished security architect has a good understanding of business practices, such as mergers, outsourcing and SaaS solutions.

- Business Change, Security Metrics and ROI.
- Risk, Security Postures and Security Culture.
- Security as a Business Enabler.
- IA Maturity Models.

COURSE AGENDA

MODULE 5

Security Across the Lifecycle

This module introduces the Solution Architect to the various security concerns and considerations when embarking on a new development project all the way to in-service support and decommissioning. It highlights the major areas of security work throughout a project that will be built upon in the following modules. This module looks at auditing and traceability of solutions, building systems using COTS or bespoke code (and the complications of each choice), some aspects related to the business matters needing consideration when embarking on a secure development programme, and how systems are accepted as fit for purpose and put into an operational capacity

- Security Across the Lifecycle

MODULE 6

Preparation for the PCiIAA and CRTSA Exams and Mock Exam

This final module will prepare the student for the PCiIAA or the CRTSA examinations.

- Format, structure and scoring of the PCiIAA examination
- Format, structure and scoring of the CRTSA examination
- Mock Examination, using the BCS sample paper

EDUCATIONAL APPROACH

- This training is based on both theory and practice:
  - Sessions of lectures illustrated with examples based on real cases
  - Review exercises to assist the exam preparation
  - Practical exercises
- To benefit from the practical exercises, the number of training participants is limited

ASSESSMENT, EXAMINATION AND CERTIFICATION

- At the end of each module the student is encouraged to undertake an assessment to assess their knowledge of the material provided in that module and to see if the objectives of the module have been met. Throughout the course quizzes are undertaken that enables a student to test their knowledge of the information covered in that topic.
- The Practitioner Certificate in Information Assurance Architecture (PCiIAA) course leads to either the BCS PCiIAA practitioner level certificate or the CREST Registered Technical Security Architect (CRTSA) senior practitioner level qualification.