Global Certification Institute
Professional Certification

InfoSecSkills®
Custom Courses Online or Onsite

Solution Architecture Security Practitioner (SASP)

22nd January, 2014

v1.0

1. Course Introduction

1.1. Overview

It is rare for todays' IT systems to have no security facilities within them. Many organisations, or projects, cannot afford to have an assigned security architect. Yet many solutions or technical architects do not have a good understanding of Information Assurance (IA). This means that many systems are being designed and built that do not mitigate many of the current and emerging threats from today's interconnected IT world. The Solution Architecture Security Practitioner (SASP) course is targeted at Solution Architects wishing to know how to design secure systems and gain the knowledge of how to architect into a system a wide range of security controls.

This course is aimed at the following staff:

- Solution or Technical Architects who wish to build security into their projects.
- Security professionals wanting to gain an appreciation of the technical and business aspects of their profession, or move into a more senior architecture role.

1.2. Course Learning Outcomes

Students that have successfully completed the SASP course will be able to:

- 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.
- Securely configure ICT systems in compliance with their approved security architectures.

1.3. Prerequisites

There are no formal entry requirements for candidates taking the examination for the Solution Architecture Security Practitioner (SASP). However, candidates should be experienced solutions or technical architects.

Table 1 - Course Summary

Module	Number of Topics	Time in Hours
Module 1 – Security Across the Lifecycle	1	2
Module 2 – The Basics of Security Architecture	2	2
Module 3 – Advanced Security Architecture Concepts	3	8
Module 4 – Information Assurance Methodologies	2	4
Totals	**8**	16

1.4. Assessment

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.

At the end of the course students may challenge the Global Certification Institute (GCI) SASP exam.

2. Module 1 – Security Across the Lifecycle

This module takes 2 hours.

2.1. Introduction

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. It pulls together many of the previous points in the course. 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.

2.2. Module Learning Outcomes:

At the end of this module the student will be able to:

- Describe the typical Terms of Reference of a Solution Architect with security architecture responsibilities.
- Explain why it is important to brief engineering teams at the start of a development process.
- Describe the concepts of audit and traceability.
- Describe the different types of design artefacts at the conceptual, logical and physical layers.
- Recognise the security issues associated with commercial off-the-shelf / outsourced / off shore systems / applications / products.
- Describe the role of hardening and coding standards in the development of a system and sources of guidance.
- Discuss the importance of links with the whole business process.
- Identify the benefits of separation of development, test and support from operational systems.
- Describe the processes for authorising business systems for use.
- Recognise the benefits of independent certification that new or modified systems meet their security policy.
- Recognise the need for change control for systems under development to maintain software integrity.
- Describe procedures for the handling of security patches.
- Identify the reasons for escrow of source code.
- Identify common programming vulnerabilities.
- Discuss the need for development environment integrity.

2.3. Topics

- Security Across the Lifecycle.

3. Module 2 – The Basics of Security Architecture

This module takes 2 hours.

3.1. Introduction

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. However, unlike technical architecture work, where components are added together to create an end-solution based on technical know-how, security architecture adopts a framework approach for deploying patterns of risk-reducing technology that provide varying levels of assurance depending on the underlying security requirements.

Being an SA is a technical job, without doubt, but the key to success in these areas comes from detailed knowledge of what comprises security technology in terms of product assurance, network and technical design/development work (using secure development principles) and the trade off between physical, logical and procedural controls.

3.2. Module Learning Outcomes

At the end of this module the student will be able to:

- Explain the concepts and design principles used by security architects when designing systems. Design principles such as least privilege, segregation of duties are described.
- Describe security architectures at a high level using appropriate contextual terms and have enough knowledge to describe architectural concepts related to security concerns.
- Explain the importance of design patterns and conceptual architectures.
- Recognise separation of systems as a way to reduce risk.

3.3. Topics

- Security Design Principles.
- Conceptual Architectures.

4. Module 3 – Advanced Security Architecture Concepts

This module takes 8 hours.

4.1. Introduction

This module builds on the Module 2, laying 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.

4.2. Module Learning Outcomes:

At the end of this module the student will be able to:

- Describe common methods for identification and authentication.
- Describe common methods for access control.
- Describe requirements and methods for auditing and alerting.
- Describe common methods for content control, such as anti-virus and data loss prevention.
- Describe common cryptographic based services, such as a public key infrastructure.
- Describe intruder detection and prevention services and their placement in systems.
- Describe the role of directories in a system.
- Describe the functions of security management within a system.
- Describe a wide range of network security controls and the threats they counter. This includes layer 2 controls and the use of packet filtering and firewalls.
- Identify common methods for resilience and recognise different recovery capabilities and techniques, including back-up and audit trails.
- Identify security aspects of virtualisation.
- Appreciate practicality as an issue in the selection of security mechanisms.
- Appreciate the need for correctness of input and on-going correctness of all stored data including parameters for all generalised software.
- Distinguish between different cryptographic mechanisms and techniques.
- Appreciate the use of threat modelling techniques to establish where security services should be positioned within a system.
- Describe a number of design patterns being able to explain the threats and security controls used to counter the threats.

4.3. Topics

- Core Security Mechanisms.
- Security Services (parts 1 and 2).
- Security Design.

5. Module 4 – Information Assurance Methodologies

This module takes 4 hour.

5.1. Introduction

This final 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.

5.2. Module Learning Outcomes:

At the end of this module the student will be able to:

- Explain a wide range of Information Assurance methodologies.
- Compare the benefits of using different methodologies.
- Describe how Information Assurance methodologies can reduce risk.
- Employ methods, tools and techniques for identifying potential vulnerabilities.
- Apply different testing strategies depending on the risk profile of a system.
- Describe the OWASP top ten risks.
- Recognise that business processes need to be tested and not just the ICT elements.
- Explain the role of vulnerability and penetration testing.
- Plan and manage a penetration test.
- Explain the typical structure of a penetration test report.
- Describe the top 12 issues that should be addressed before a penetration test.
- Describe the typical findings of a penetration test report.

5.3. Topics

- Information Assurance Frameworks.
- Vulnerability and Penetration Testing.