Global Certification Institute
Professional Certification

InfoSec Skills®
Custom Courses Online or Onsite

Foundation Certificate in Information Security (FCIS)

Course Description

14th April 2015

Version 1.4

Course Overview

Overview

Duration: 1.5 days / 11.5 hours

The **Foundation Certificate in Information Security (FCIS)** course is designed to provide the foundation of knowledge necessary for individuals who have IT or information security responsibilities as part of their day-to-day role, or who are thinking of moving into an information security function. Every member of IT staff should have this knowledge. If your IT staff do not know what a BIA is or do not understand the significance of Risk Assessments then it may be time to baseline all your IT staff with this course.

The FCIS course introduces the concept of and disciplines within Information Assurance and how this can contribute to and form part of the overall business strategy for an organisation. It provides the opportunity for those exploring or moving into information security roles to enhance or refresh their knowledge and, in the process, gain a recognised industry qualification, regulated by the Global Certification Institute (GCI). This is useful to both the individual and employer in terms of attesting to the level of professional ability an individual has attained.

Based upon international standards and industry best practice, this course provides a great foundation for anyone starting a career in Information/Cyber Security or who are taking on extra Information Security responsibilities. 11.5 hours of condensed knowledge + a 1 hour exam proves your understanding of the top four disciplines of Information Security.

The InfoSec Skills FCIS course primes the student with all the knowledge needed to sit the Global Certification Institute (GCI) - Foundation Certificate in Information Security (FCIS) examination.

Why should you attend?

This course is intended for anyone who has an interest in information security, either for potential or existing security professionals, or as an additional part of his or her general business knowledge (for example, the material covered on this course would make good supporting material for network/system administrator who have or who are taking on additional security responsibilities, business managers, IT managers, security analysts and IT staff. When used as a baseline for all IT staff this course ensures that they speak the same language as your security team and that they understand why the security team do what they do.

Prerequisites

Knowledge of IT systems would be advantageous but not essential.

An understanding of the general principles of information technology security would be useful, but again, not essential.

Course Contents

The course consists of five modules:

- Module 1 – Introduction to Information Security Management
- Module 2 – Introduction to Information Risk Management
- Module 3 – Introduction to Business Continuity Management
- Module 4 – Introduction to Information Assurance Architecture
- Module 5 – Preparation for the FCIS exam

Assessment

Each topic contains a quiz that enables a student to test their knowledge of the information covered in that topic. At the end of each module the student must undertake a test to assess their understanding of the information provided in that module and to see if the objectives of the module have been met. At the end of the course, we provide an overview of the format, structure and scoring of the exam that prepares you for the Global Certification Institute (GCI) - Foundation Certificate in Information Security (FCIS) exam and professional certificate, which is bundled with this course.

Total Length of Course

The total time specified in this syllabus is a minimum of 11.5 hours of lecturing and practical work.

Course Materials

On attending this course students are provided with:

- Full colour, indexed, perfect bound, course book containing all course slides and notes
- Classroom exercises
- Sample exam questions

Course Outline

Module 1 – Introduction to Information Security Management

Overview

In this module the student will learn the basic concepts of information security along with the main terminology commonly in use. Students will gain an understanding of why information security is becoming increasingly important, not just in the IT community but also in the business community at large.

Topics

- Concepts and definitions
- Benefits and requirements of information security

Module Learning Outcomes

At the end of this module the student will:

- Be able to define and explain the key terms used in information security and use these terms correctly and appropriately
- Be able to explain and justify a number of the key concepts in information security and explain these concepts correctly and appropriately

Length of Module

2 hours.

Module 2 – Introduction to Information Risk Management

Overview

This module introduces the student to the basic concepts of business risk management, its rationale, core terminology and fundamental principles. It introduces the need for and application of international standards and regulatory frameworks and stresses the adoption of a strategic approach to information risk management.

Topics

- Information risk management terminology
- Risk management in the business context
- Information risk management fundamentals

Module Learning Outcomes

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

- Understand the significance of information risk management to business
- Understand and be able to apply basic information risk management terminology
- Understand basic information risk management principles

Length of Module

4 hours.

Module 3 – Introduction to Business Continuity Management

Overview

In this module the student will learn the basic concepts of business continuity management along with the main terminology commonly in use. Students will gain an understanding of why business continuity management is becoming increasingly important, not just in the IT community but also in the business community at large.

Topics

- The need for business continuity management
- The context of business continuity management in the business
- The business continuity lifecycle

Module Learning Outcomes

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

- Define and explain the key terms used in business continuity management in their appropriate context
- Explain and justify a number of the key concepts of business continuity management
- Explain the overall business continuity lifecycle

Length of Module

2 hours.

Module 4 – Introduction to Information Assurance Architecture

Overview

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.

Topics

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

Module Learning Outcomes

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

- Describe the role of the security architect and the concept of security architectures in context of enterprise architectures.
- Explain the skills, especially soft skills, an SA must possess.
- 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.

Length of Module

3 hours.

Module 5 – Preparation for the FCIS exam

Overview

The final module will prepare the student for the FCIS examination to be undertaken through an online proctored exam.

Topics

- Format, structure and scoring of the exam

Objectives

At the end of this module the student will:

- Understand the format and scoring of the examination
- Be prepared to take and pass the FCIS examination

Length of Module

30 minutes.