



*This is to certify that  
Chris FitzGerald  
has completed the course  
Information Security and Risk Management - 243962\_eng  
on  
1/31/08*



Association for  
Computing Machinery

*Advancing Computing as a Science & Profession*



# Information Security and Risk Management

## About This Course

### Overview/Description

To identify the security requirements associated with identifying and protecting organizational information assets, perform the analysis techniques used in risk management, and recognize the responsibilities associated with different roles in an organization.

### Target Audience:

Mid-level and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers.

Requires a minimum of four years of professional experience in the information security field or three years plus a college degree.

### Certification:

No Certifications for this Course.

### Expected Duration:

2 Hours 55 Minutes

### First publication date:

This course was released June 11, 2007.

### Last revision:

This course was last updated September 17, 2007.

### Course Number:

243962\_eng

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

# Information Security and Risk Management

## Course Objectives

Topic Name	When you have completed this topic, you should be able to
Security Management and Change Control	recognize the goals of security management and change control.
Change Control Mechanisms	identify the change control mechanisms used to secure the operational environment.
Classifying Data	recognize the objectives and criteria associated with data classification, and distinguish between information classification roles.
Policies, Standards, and Guidelines	distinguish between policies, standards, baselines, and guidelines.
Employment Policies and Practices	recognize best practices and procedures for dealing with different aspects of employee relations.
Hiring a New Staff Member	determine the appropriate security procedures for hiring a new employee in a given scenario.
Risk Management	identify the principles of risk management, distinguish between planning types, and recognize what's involved in the analysis of different threats and vulnerabilities.
Risk Analysis and Evaluation	calculate the potential loss expectancy and the cost of countermeasures used for risk reduction in a given scenario.
Calculating Risk	calculate the loss expectancy associated with an information asset, perform a cost-benefit analysis, and determine how to handle the risk depending on the outcome of the countermeasure.
Roles and Responsibilities	identify the security-related responsibilities associated with different roles within an organization.

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

# Information Security and Risk Management

## References

### Books

#### **Official (ISC)2 Guide to the CISSP CBK**

2006, Harold F. Tipton (Editor), Kevin Henry (Editor), AUERBACH (2006), 0849382319

Copyright © 2007 SkillSoft. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.



*This is to certify that  
Chris FitzGerald  
has completed the course  
Security Architecture and Design - 243975\_eng  
on  
2/3/08*



Association for  
Computing Machinery

*Advancing Computing as a Science & Profession*



# Security Architecture and Design

## About This Course

### Overview/Description

To understand the principles of common computer architectures, distinguish between machine types and memory storage types, and recognize the logistics of common security models.

### Target Audience:

Mid-level and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers.  
Requires a minimum of four years of professional experience in the information security field or three years plus a college degree.

### Certification:

No Certifications for this Course.

### Expected Duration:

2 Hours 20 Minutes

### First publication date:

This course was released June 06, 2007.

### Last revision:

This course was last updated June 06, 2007.

### Course Number:

243975\_eng

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

## Security Architecture and Design

### Course Objectives

Topic Name	When you have completed this topic, you should be able to
Architecture, Addressing, and States	recognize the components of the basic information system architecture and their functionality, and differentiate between hardware, software, and firmware.
Machine Types and Functions	differentiate between machine types and recognize the functions of network protocols and the resource manager.
Storage Types	distinguish between types of storage device and how they are used.
Protection Rings	determine which system resources can be found at the different rings and how the rings control subject access to objects.
Certification, Accreditation, and OS Protection	differentiate between key security concepts, recognize the role of TCB, reference monitor, and security kernel in protecting the operating system, and recognize the two basic access control types.
Security Evaluation Standards	differentiate between the various criteria and standards used to evaluate security in a networking environment.
Security Standards	specify the security level that should be assigned to various objects and determine how to implement the standards.
Security Models	recognize the logistics of various security models used to enforce rules and protection mechanisms.

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

# Security Architecture and Design

## References

### Books

#### **Official (ISC)2 Guide to the CISSP CBK**

2006, Harold F. Tipton (Editor), Kevin Henry (Editor), AUERBACH (2006), 0849382319

Copyright © 2007 SkillSoft. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.



*This is to certify that  
Chris FitzGerald  
has completed the course  
Access Control - 243986\_eng  
on  
2/4/08*



Association for  
Computing Machinery

*Advancing Computing as a Science & Profession*



## Access Control

### About This Course

#### Overview/Description

To introduce access control concepts and methodologies and explain how they're implemented and administered in a centralized or decentralized environment.

#### Target Audience:

Mid-level and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers.  
Requires a minimum of four years of professional experience in the information security field or three years plus a college degree.

#### Certification:

No Certifications for this Course.

#### Expected Duration:

2 Hours 40 Minutes

#### First publication date:

This course was released June 13, 2007.

#### Last revision:

This course was last updated December 07, 2007.

#### Course Number:

243986\_eng

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

## Access Control

### Course Objectives

Topic Name	When you have completed this topic, you should be able to
Access Control Overview	identify the types of access control technologies used in a networking environment.
Knowledge-based and Biometric Authentication	identify knowledge-based and characteristics-based authentication technologies.
SSO, OTP, and Smart Card Authentication	recognize how single sign-on systems (SSOs), one-time passwords (OTPs), and smart cards are used for authentication.
Authentication Factors	determine the appropriate type of authentication to implement in a given enterprise scenario.
Passwords	recognize ways of securing passwords and identify different types of attack against passwords and password files.
Types of Access Control	select the appropriate access control model for a scenario.
Access Control Models	determine the most appropriate access control model to implement in a given scenario.
Access Control and Administration	recognize how different types of access control technique control access to resources, and distinguish between centralized and decentralized access control administration mechanisms.
Intrusion Detection and Monitoring	identify information detection system (IDS) mechanisms and implementation methods, and recognize various intrusion detection and prevention techniques.

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

## Access Control

### References

#### Books

##### **Official (ISC)2 Guide to the CISSP CBK**

2006, Harold F. Tipton (Editor), Kevin Henry (Editor), AUERBACH (2006), 0849382319

Copyright © 2007 SkillSoft. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.



*This is to certify that  
Chris FitzGerald  
has completed the course  
Application Security - 243998\_eng  
on  
2/4/08*



Association for  
Computing Machinery

*Advancing Computing as a Science & Profession*



# Application Security

## About This Course

### Overview/Description

To understand different threats to the enterprise environment and recognize different ways of increasing the security of application development.

### Target Audience:

Mid-level and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers.  
Requires a minimum of four years of professional experience in the information security field or three years plus a college degree.

### Certification:

No Certifications for this Course.

### Expected Duration:

2Hours 00 Minutes

### First publication date:

This course was released June 14, 2007.

### Last revision:

This course was last updated December 20, 2007.

### Course Number:

243998\_eng

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

## Application Security

### Course Objectives

Topic Name	When you have completed this topic, you should be able to
Application Development Fundamentals	distinguish between open and closed source code and recognize the functionality of different program types.
Attack Methods	distinguish between the types of attacks used in the enterprise environment and identify the appropriate methods to counteract them.
Malicious Code	recognize the different types of malicious code that can affect a system or network and identify the methods that can be used to mitigate them.
Identifying and Dealing with Attacks	identify the type of attack being perpetrated in a given scenario and determine the appropriate steps to counteract it.
Knowledge-Based Systems and the Development Life Cycle	recognize the characteristics of various knowledge-based systems and identify the activities involved in the different phases of the information systems development life cycle.
Databases and Data Warehousing	distinguish between various database models and technologies, and define basic concepts associated with databases and data warehousing.
Selecting a Database Model	select the appropriate database model for a given set of criteria.

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

## Access Control

### References

#### Books

##### Official (ISC)2 Guide to the CISSP CBK

2006, Harold F. Tipton (Editor), Kevin Henry (Editor), AUERBACH (2006), 0849382319

Copyright © 2007 SkillSoft. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.



*This is to certify that  
Chris FitzGerald  
has completed the course  
Operations Security - 244020\_eng  
on  
2/4/08*



Association for  
Computing Machinery

*Advancing Computing as a Science & Profession*



# Operations Security

## About This Course

### Overview/Description

To understand the different mechanisms used to identify different types of attack and their effects, and protect system resources, e-mail and Internet communication to ensure operations security.

### Target Audience:

Mid-level and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers.  
Requires a minimum of four years of professional experience in the information security field or three years plus a college degree.

### Certification:

No Certifications for this Course.

### Expected Duration:

2 Hours 20 Minutes

### First publication date:

This course was released June 06, 2007.

### Last revision:

This course was last updated December 20, 2007.

### Course Number:

244020\_eng

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

## Operations Security

### Course Objectives

Topic Name	When you have completed this topic, you should be able to
Operations Security Overview	recognize the activities involved in securing the operations of an enterprise and identify the technologies used to maintain network and resource availability.
Network Violations	identify the effects of various hardware and software violations on the system, and recognize how different types of operational and life-cycle assurance are used to secure operations.
Analyzing Violations	determine the effects of different attacks on the network and identify the consequences of those effects.
Auditing and Monitoring	recognize how different auditing and monitoring techniques are used to identify and protect against system and network attacks.
Protecting Resources and Securing E-mail	recognize the need for resource protection, distinguish between e-mail protocols, and identify different types of e-mail vulnerability.
The World Wide Web and File Transfer Protection	identify basic mechanisms and security issues associated with the Web, and recognize different technologies for transferring and sharing files over the Internet.
Attack Framework and Separation of Duties	recognize key reconnaissance attack methods and identify different types of administrative management and media storage control.
Separation of Duties and Responsibilities	identify the appropriate security measures and controls for creating a more secure workspace in given scenarios.

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

# Security Architecture and Design

## References

### Books

#### Official (ISC)2 Guide to the CISSP CBK

2006, Harold F. Tipton (Editor), Kevin Henry (Editor), AUERBACH (2006), 0849382319

Copyright © 2007 SkillSoft. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.



*This is to certify that  
Chris FitzGerald  
has completed the course  
Cryptography - 244031\_eng  
on  
2/5/08*



Association for  
Computing Machinery

*Advancing Computing as a Science & Profession*



# Cryptography

## About This Course

### Overview/Description

To recognize how different cryptographic technologies are used to provide confidentiality, integrity, and authentication for data being transferred across untrusted networks.

### Target Audience:

Mid-level and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers.  
Requires a minimum of four years of professional experience in the information security field or three years plus a college degree.

### Certification:

No Certifications for this Course.

### Expected Duration:

2Hours 00 Minutes

### First publication date:

This course was released July 11, 2007.

### Last revision:

This course was last updated July 11, 2007.

### Course Number:

244031\_eng

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

# Cryptography

## Course Objectives

Topic Name	When you have completed this topic, you should be able to
Cryptographic Terminology and Symmetric Algorithms	define key cryptographic terms and distinguish between types of symmetric key algorithms.
Asymmetric Algorithms	distinguish between types of asymmetric algorithms.
Using Symmetric and Asymmetric Algorithms	determine the appropriate cryptography implementation for a given scenario.
Cipher Types and Cryptanalytic Attacks	distinguish between types of cipher and identify different categories of cryptanalytic attack.
Message Authentication	distinguish between the various algorithms used for message authentication.
Using Hashing Algorithms	determine the appropriate hashing algorithm to use in a given scenario.
Certificate Authority and Digital Signatures	recognize how certificate authorities (CAs), digital signatures, and the Public Key Infrastructure (PKI) are used to provide confidentiality, integrity, and authentication.

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

# Cryptography

## References

### Books

#### Official (ISC)2 Guide to the CISSP CBK

2006, Harold F. Tipton (Editor), Kevin Henry (Editor), AUERBACH (2006), 0849382319

Copyright © 2007 SkillSoft. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.



*This is to certify that  
Chris FitzGerald  
has completed the course  
Physical (Environmental) Security - 244059\_eng  
on  
2/5/08*



Association for  
Computing Machinery

*Advancing Computing as a Science & Profession*



# Physical (Environmental) Security

## About This Course

### Overview/Description

To understand the considerations and mechanisms involved in implementing the physical security of an enterprise.

### Target Audience:

Mid-level and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers.  
Requires a minimum of four years of professional experience in the information security field or three years plus a college degree.

### Certification:

No Certifications for this Course.

### Expected Duration:

2Hours 00 Minutes

### First publication date:

This course was released July 23, 2007.

### Last revision:

This course was last updated July 23, 2007.

### Course Number:

244059\_eng

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

## Physical (Environmental) Security

### Course Objectives

Topic Name	When you have completed this topic, you should be able to
Physical Security Fundamentals	recognize basic threats to an organization's physical security and identify the security mechanisms used in securing an enterprise environment.
Perimeter Security	identify the security mechanisms and strategies used to protect the perimeter of a facility.
Securing the Perimeter	identify the appropriate physical security mechanisms to implement in a given scenario.
Internal Protection	identify the appropriate mechanisms and controls for securing the inside of a building or facility.
Intrusion Detection Systems	select the most appropriate intrusion detection technology for a scenario.
Implementing an Intrusion Detection System	determine the appropriate intrusion detection system to implement, given a specific scenario.
Compartmentalization	select the appropriate strategy for securing compartmentalized areas in a given scenario.

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

## Physical (Environmental) Security References

### Books

#### Official (ISC)2 Guide to the CISSP CBK

2006, Harold F. Tipton (Editor), Kevin Henry (Editor), AUERBACH (2006), 0849382319

Copyright © 2007 SkillSoft. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.



*This is to certify that  
Chris FitzGerald  
has completed the course  
Telecommunications and Network Security - 244069\_eng  
on  
2/6/08*



Association for  
Computing Machinery

*Advancing Computing as a Science & Profession*



# Telecommunications and Network Security

## About This Course

### Overview/Description

To understand the structures, transmission methods, transport formats, and security technologies used in providing telecommunications and network security.

### Target Audience:

Mid-level and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers.  
Requires a minimum of four years of professional experience in the information security field or three years plus a college degree.

### Certification:

No Certifications for this Course.

### Expected Duration:

3 Hours 40 Minutes

### First publication date:

This course was released July 31, 2007.

### Last revision:

This course was last updated July 31, 2007.

### Course Number:

244069\_eng

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

## Telecommunications and Network Security

### Course Objectives

Topic Name	When you have completed this topic, you should be able to
Telecommunications and Network Security Overview	identify security issues associated with e-mail, facsimile, and PBX systems, and recognize how the LPC algorithm is used to secure voice communications.
Internet, Intranet, and Extranet Security	identify the characteristics and functionality of the different technologies used to protect an organization at the network edge.
TCP/IP	identify the characteristics of TCP and IP, and recognize the functionality of the OSI reference model.
The OSI Model	distinguish between the layers of the OSI reference model and their associated functionality and technologies.
Data Topologies, Physical Media, and LAN Technologies	distinguish between types of data topology and physical media, and recognize the functionality of different LAN technologies.
Networks, Access Methods, Transmissions, and Devices	recognize the network topologies, media access methods, data transmission types, and devices used by LANs and WANs.
Switching, Remote Access, Ethernet, and Token Ring	identify the characteristics of the switching, remote access, and authentication methods used by LANs and WANs, and recognize the functionality of Ethernet and Token Ring technologies.
Network Communication and VPNs	recognize the characteristics of the various network communications mechanisms and technologies used in an enterprise environment, and identify the protocols used by VPNs.
Protocols at the Network Layer	recognize the characteristics and functionality of the protocols used to secure data in transit in an enterprise environment.
Security at the Transport Layer	recognize how different transport layer mechanisms secure network data.
Security at the Application Layer	recognize how different technologies are used to protect data at the Application layer.
Securing the Application Layer	determine the most appropriate methods and mechanisms for securing information at the Application layer, given a scenario.

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

# Telecommunications and Network Security

## References

### Books

#### Official (ISC)2 Guide to the CISSP CBK

2006, Harold F. Tipton (Editor), Kevin Henry (Editor), AUERBACH (2006), 0849382319

Copyright © 2007 SkillSoft. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.



*This is to certify that  
Chris FitzGerald  
has completed the course  
Business Continuity and Disaster Recovery Planning - 244085\_eng  
on  
2/6/08*



Association for  
Computing Machinery

*Advancing Computing as a Science & Profession*



# Business Continuity and Disaster Recovery Planning

## About This Course

### Overview/Description

To recognize how to plan for business continuity and disaster recovery in the event of unforeseen and critical loss.

### Target Audience:

Mid-level and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers.  
Requires a minimum of four years of professional experience in the information security field or three years plus a college degree.

### Certification:

No Certifications for this Course.

### Expected Duration:

2 Hours 20 Minutes

### First publication date:

This course was released July 27, 2007.

### Last revision:

This course was last updated August 04, 2007.

### Course Number:

244085\_eng

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

## Business Continuity and Disaster Recovery Planning

### Course Objectives

Topic Name	When you have completed this topic, you should be able to
Creating a Business Continuity Plan	recognize the phases involved in creating a business continuity plan (BCP).
Project Initiation and Management	recognize what's involved in the project initiation and management phase of the business continuity planning process.
Business Impact Analysis	identify the steps for conducting a business impact analysis (BIA) in a given scenario.
Conducting a BIA	determine the appropriate strategy for performing a business impact analysis (BIA) in a given scenario.
Recovery Strategies	identify the appropriate strategies for recovering critical business systems and resources, and maintaining business continuity in the event of a disaster.
Plan Design and Development	identify the factors that need to be reviewed and documented in a business continuity plan, given a scenario.
Awareness Training, Maintenance, and Testing	identify the objectives and functions associated with testing and maintaining a business continuity plan.
Designing a BCP	determine the appropriate strategy for designing a business continuity plan (BCP) in a given scenario.

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

# Business Continuity and Disaster Recovery Planning

## References

### Books

#### Official (ISC)2 Guide to the CISSP CBK

2006, Harold F. Tipton (Editor), Kevin Henry (Editor), AUERBACH (2006), 0849382319

Copyright © 2007 SkillSoft. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.



*This is to certify that  
Chris FitzGerald  
has completed the course  
Legal, Regulations, Compliance, and Investigations - 244096\_eng  
on  
2/7/08*



Association for  
Computing Machinery

*Advancing Computing as a Science & Profession*



# Legal, Regulations, Compliance, and Investigations

## About This Course

### Overview/Description

To identify the types and characteristics of computer crime, distinguish between the laws relating to information technology, and recognize the investigative and ethical considerations involved in dealing with computer crime.

### Target Audience:

Mid-level and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers.

Requires a minimum of four years of professional experience in the information security field or three years plus a college degree.

### Certification:

No Certifications for this Course.

### Expected Duration:

2 Hours 15 Minutes

### First publication date:

This course was released July 31, 2007.

### Last revision:

This course was last updated July 31, 2007.

### Course Number:

244096\_eng

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

# Legal, Regulations, Compliance, and Investigations

## Course Objectives

Topic Name	When you have completed this topic, you should be able to
Types of Computer Crime	distinguish between the major categories of computer crime and recognize examples of them.
Computer Crimes and Intellectual Property	recognize the characteristics of various computer-related crimes and identify the type of intellectual property law that applies in a given scenario.
Protecting Intellectual Property	determine the type of intellectual property that should be put in place in a given scenario.
Types of Law	recognize the characteristics of various law systems and categories of law, and identify laws related to information security and privacy.
Computer Crime-Related Laws	distinguish between the laws that have been created to deal with different types of computer crime.
Due Care and Evidence Control	recognize the definition of the principles of due care and due diligence, and identify the phases and types of evidence involved in computer crime.
Securing Evidence	determine the appropriate process for controlling evidence when investigating a computer-related crime in a given scenario.
Investigation and Ethics	recognize the investigative and ethical considerations involved in dealing with computer crime.

Copyright © 2007 SkillSoft PLC. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft PLC in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.

## Legal, Regulations, Compliance, and Investigations References

### Books

#### Official (ISC)2 Guide to the CISSP CBK

2006, Harold F. Tipton (Editor), Kevin Henry (Editor), AUERBACH (2006), 0849382319

Copyright © 2007 SkillSoft. All rights reserved.  
SkillSoft and the SkillSoft logo are trademarks or registered trademarks  
of SkillSoft in the United States and certain other countries.  
All other logos or trademarks are the property of their respective owners.