ACS-2821-001
Information Security in Business

Certification Programs and the Common Body of Knowledge

ACS-2821-001 – Slides Used In The Course

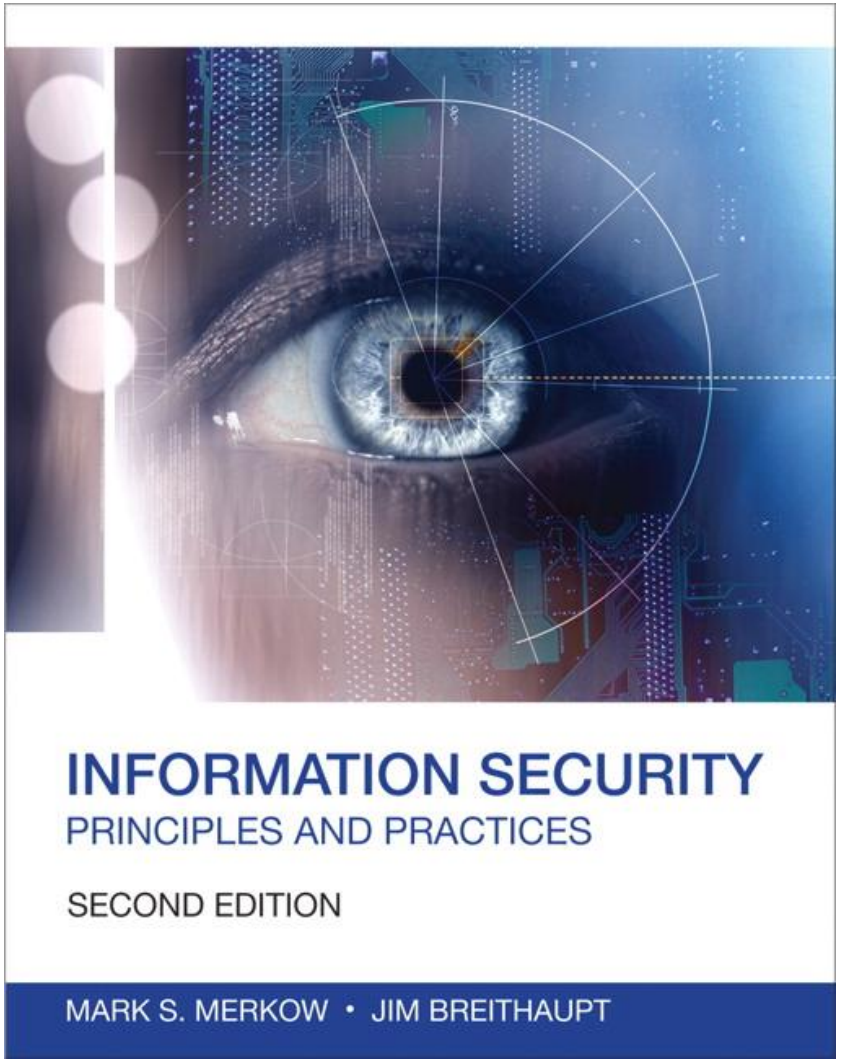
THE UNIVERSITY OF WINNIPEG

A note on the use of these slides:

These slides has been adopted and/or modified from the original for the use in this course. The author of the text have make these slides available to all (faculty, students, readers) and they obviously represent a *lot* of work on their part.

In return for use, please:

- If slides are being used (e.g., in a class) that the source be mentioned (after all, the author like people to use our book!)
- If any slides are being posted on a www site, note that they are adapted from (or perhaps identical to) the author original slides, and note their copyright of this material.



Objectives

- Analyze the Certified Information Systems Security Professional (CISSP) certificate program
- Define and describe the role of the International Information Systems Security Certifications Consortium
- Distinguish the contents of the 8 domains of the Common Body of Knowledge (CBK)
- Distinguish the CISSP from other security certifications programs

Certification and Information Security

- Industry standards, ethics, and certification of information systems professionals and practitioners are critical to ensuring that a high standard of security is achieved
- Certification benefits both the employer and the employee
- Oversight and governance of the professional certification process is needed
  - To help maintain its relevance and currency
  - To aid professionals in networking with other professionals

To meet that need, the (ISC)^2, ISACA, SANS organization was created

International Information Systems Security Certification Consortium $(ISC)^2$

- Global, non-profit organization with the following goals
  - Maintaining a CBK for information security
  - Certifying industry professionals and practitioners
  - Administering training and certification examinations
  - Ensuring credentials are maintained
- Two primary certifications
  - Certified Information Systems Security Professional (CISSP)
  - System Security Certified Practitioner (SSCP)
- To qualify for the CISSP certification:
  - Pass the CISSP exam
  - Have at least five years of cumulative, paid work experience in two or more of the eight domains
  - Agree to the $(ISC)^2$ Code of Ethics

The Information Security Common Book of Knowledge (CBK)

- The CBK is a compilation and distillation of all security information collected that is relevant to information security professionals
- CISSP certification includes a working knowledge of all 10 domains (before 2015) and currently 8 domains from the CBK
- The CBK is also a good source of reference in Information Security best practice and guidance

The Information Security CBK - 10 Domains (before 2015)

The 10 domains are as follows:

- Information Security Governance and Risk Management (Chap 4)
- Security Architecture and Design (Chap 5)
- Business Continuity and Disaster Recovery Planning (Chap 6)
- Legal Regulations, Investigations, and Compliance (Chap 7)
- Physical (Environmental) Security (Chap 8)
- Operations Security (Chap 9)
- Access Control (Chap 10)
- Cryptography (Chap 11)
- Telecommunications and Network Security (Chap 12)
- Software Development Security (Chap 13)

The Information Security CBK - 8 Domains (After 2015)

The University of Winnipeg

The 8 domains are as follows:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

Information Systems Audit and Control Association (ISACA)

- Provides practical guidance, benchmarks and other effective tools for all enterprises that use information systems
- Professional body that's defines the roles of information systems governance, security, audit and assurance professionals worldwide
- Developed and maintains internationally recognized framework
  - Control Objectives for Information and related Technology - COBIT®
  - Val IT™
  - Risk IT
  - Business Model for Information Security – BMIS
  - Information Technology Assurance Framework - ITAF
- Primary certifications related to Information Security
  - Certified Information System Auditor - CISA
  - Certified Information Security Manager – CISM
  - Certified in Risk and Information System Controls - CRISC

Certified Information Systems Auditor (CISA)

- Focuses more on business procedures than technology
- The 5 domains are:
  - Domain 1: Information System Auditing Process (21 percent)
  - Domain 2: Governance and Management of IT (17 percent)
  - Domain 3: Information Systems, Acquisition, Development and Implementation (12 percent)
  - Domain 4: Information Systems Operations and Business Resilience (23 percent)
  - Domain 5: Protection of Information Assets (27 percent)
- To qualify for the certification:
  - Passing the CISA exam
  - A minimum of 5 years of professional information systems auditing, control or security work experience
  - Agree to a Code of Professional Ethics to guide professional and personal conduct

Certified Information Security Manager (CISM)

- To ensure that the information security manager has the required knowledge and ability to provide effective security management and consulting
- The 5 domains are:
  - Domain 1—Information Security Governance: 23%
  - Domain 2—Information Risk Management: 22%
  - Domain 3—Information Security Program Development: 17%
  - Domain 4—Information Security Program Management: 24%
  - Domain 5—Incident Management and Response: 14%
- To qualify for the certification:
  - Passing the CISM exam
  - a minimum of five years of information security work experience, with a minimum of three years of information security management work experience in three or more of the job practice analysis areas
  - Agree to a Code of Professional Ethics to guide professional and personal conduct

Certified in Risk and Information Systems Control

- Certified individuals can help enterprises understand business risk
- The 5 domains are:
  - Domain 1—IT Risk Identification (27% of exam)
  - Domain 2—IT Risk Assessment (28% of exam)
  - Domain 3—Risk Response and Mitigation (23% of exam)
  - Domain 4—Risk and Control Monitoring and Reporting (22% of exam)
- To qualify for the certification:
  - Passing the CRISC exam
  - A minimum of at least three years of cumulative work experience performing the tasks across at least two (2) of the four (4) CRISC domains
  - These two (2) required domains, one (1) must be in either Domain 1 or 2
  - Agree to a Code of Professional Ethics to guide professional and personal conduct

SANS Institute - Global Information Assurance Certifications (GIAC)

- Provide assurance that a certified individual has the knowledge and skills necessary for a practitioner in key areas of computer, information and software security
- Intended primarily for practitioners or hands-on personnel such as system administrators and network engineers
- Address a range of skill sets including entry-level information security and broad-based security essentials
- Subject areas like:
  - Audit
  - Intrusion detection
  - Incident handling
  - Firewalls and perimeter protection
  - Forensics
  - Hacker techniques
  - Windows and Unix operating system security
  - Secure software and application coding

Other Certificate Programs

- (ISC)2 Specialization Certificates
  - Certified Cyber Forensics Professional $(ISC)^2$ – Retiring August 2020
  - HealthCare Information Security and Privacy Practitioner $(ISC)^2$
- ISACA Specialization Certificates
  - CSX Practitioner Certification (CSXP)
- Vendor-Specific Certification Programs
  - Cisco Security Tracks and Certificates
  - Certificate of Cloud Security Knowledge
  - Certified Ethical Hacker
- Entry-level certificates
  - Security + - CompTIA
  - CSX Cybersecurity Fundamentals Certificate – ISACA
  - Microsoft Technology Associate (MTA) Security Fundamentals – Microsoft
  - Information Security Fundamentals (GISF) - GIAC
  - Systems Security Certified Practitioner (SSCP) - $(ISC)^2$

Standards

Standards have been developed to cover management practices and the overall architecture of security mechanisms and services

- The most important of these organizations are:
  - **National Institute of Standards and Technology (NIST)**
    - NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private sector innovation
  - **Internet Society (ISOC)**
    - ISOC is a professional membership society that provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards
  - **International Telecommunication Union (ITU-T)**
    - ITU is a United Nations agency in which governments and the private sector coordinate global telecom networks and services
  - **International Organization for Standardization (ISO)**
    - ISO is a nongovernmental organization whose work results in international agreements that are published as International Standards

NIST Special Publication 800 Series of Standards on IT Security

SP	800-53 Rev. 4	Security and Privacy Controls for Federal Information Systems and Organizations
SP	800-50	Building an Information Technology Security Awareness and Training Program
SP	800-45 Version 2	Guidelines on Electronic Mail Security
SP	800-39	Managing Information Security Risk: Organization, Mission, and Information System View
SP	800-30 Rev. 1	Guide for Conducting Risk Assessments
SP	800-12 Rev. 1	An Introduction to Information Security
SP	800-94 Rev. 1	Guide to Intrusion Detection and Prevention Systems (IDPS)
SP	800-95	Guide to Secure Web Services
SP	800-100	Information Security Handbook: A Guide for Managers
SP	800-119	Guidelines for the Secure Deployment of IPv6
SP	800-121 Rev. 2	Guide to Bluetooth Security
SP	800-123	Guide to General Server Security
SP	800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

ISO/IEC 27000 Series of Standards on IT Security

THE UNIVERSITY OF WINNIPEG

27000:2016	"Information security management systems - Overview and vocabulary" provides an overview of information security management systems, and defines the vocabulary and definitions used in the 27000 family of standards.
27001:2013	"Information security management systems – Requirements" specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System.
27002:2013	"Code of practice for information security management" provides guidelines for information security management in an organization and contains a list of best-practice security controls. It was formerly known as ISO17799.
27003:2010	"Information security management system implementation guidance" details the process from inception to the production of implementation plans of an Information Security Management System specification and design.
27004:2009	"Information security management – Measurement" provides guidance to help organizations measure and report on the effectiveness of their information security management system processes and controls.
27005:2011	"Information security risk management" provides guidelines on the information security risk management process. It supersedes ISO13335-3/4.
27006:2007	"Requirements for bodies providing audit and certification of information security management systems" specifies requirements and provides guidance for these bodies.

Summary

- The benefits of certification and immersion into the CBK are clear to both employers and professionals who commit to life-long learning and to the betterment of themselves and their careers
- The benefits of standards a basis for mutual understanding, and are used as tools to facilitate communication, measurement, commerce and manufacturing. It disseminate knowledge and introduce new technologies and innovations that ensure these products, components and services supplied by different companies will be mutually compatible

ACS-2821-001 – Questions?