



Careers, Credentials, Certifications and Associations

SENG460: Practice of Information Security & Privacy
Winter 2014

Andrew Hughes, CISM, CISSP

AndrewHughes3000@gmail.com

Lecture Theme

- Mechanisms and organizations available to help advance your career in information security

Lecture Contents

- Professional Associations
- Certifications
- Training & Professional Development
- Standards Development Organizations
- Careers



PROFESSIONAL ASSOCIATIONS

Description

- A professional association [...] is usually a nonprofit organization seeking to further a particular profession, the interests of individuals engaged in that profession, and the public interest.

Ref: en.wikipedia.org/wiki/Professional_association

Purpose

- Many professional bodies are involved in the development and monitoring of professional educational programs, and the updating of skills, and thus perform professional certification to indicate that a person possesses qualifications in the subject area.

Ref: en.wikipedia.org/wiki/Professional_association

Why join?

- To demonstrate dedication to best practices
- To demonstrate commitment to professional growth
- To help advance the profession
- To meet and network with peers
- To gain certification
(demonstration of ability or knowledge)
- To meet a job requirement
- To gain access to a body of knowledge and training

Pre-requisites for membership

- Membership fees
- Achieve a certification (some)
- Agree to terms and conditions
- Agree to adhere to standard of conduct or ethics
- Be referred (some)

Costs

- Wide range of membership fee levels
- Most have annual fees
- Professional Association fee structure
 - Can include ‘Head office’ amount
 - Can include ‘Local chapter’ amount
 - Can include ‘Certification maintenance’ amount
- Offering a student fee level is typical

Typical Membership Types

- Practicing
 - Active members meeting all requirements
- Student
 - Benefits, including scholarships
 - Reduced cost entry
- Academic
 - Faculty
- Retired
 - Inactive members wishing to retain partial association membership benefits



CERTIFICATION AND ACCREDITATION

Certification is...

- Certification refers to the confirmation of certain characteristics of an object, person, or organization. This confirmation is often, but not always, provided by some form of external review, education, assessment, or audit.

Ref: en.wikipedia.org/wiki/Certification

Accreditation is...

- The process a specific organization uses to conduct certification
- Includes
 - Definition of an authoritative reference or standard
 - Process used to verify candidate's qualifications or knowledge
 - Process used to maintain and audit the certification processes themselves
- Can be externally audited for higher value

Purposes of C&A

- To set practice standards
- To form the participation basis of professional association membership
- To provide independent proof of competency
- To differentiate from training
 - i.e. there is a formal, scored test

Benefits and Value

- Well designed and maintained accreditation programs are valuable
 - To you
 - To employers
 - To clients and customers

**“WHAT DISTINGUISHES ME
FROM MY COMPETITION?”**
**THE ISACA® CERTIFICATION
AT THE END OF MY NAME.”**

KETAN DHOLAKIA, CISM, CRISC
MANAGING PARTNER, MACLEAR
CHICAGO, ILLINOIS
ISACA MEMBER SINCE 2007

ACCOMPLISH | MORE

Benefits and Value 1/3

- You
 - To learn about a topic area, product, body of knowledge or common practices
 - To obtain proof of that learning
 - To align vocabulary, concepts, paradigm, with your colleagues or employers
 - Join a community of practice, gain networking connections locally and worldwide
 - Potential salary boost

Benefits and Value 2/3

- **Employers**
 - Independent confirmation that you know something
 - Ensure consistent paradigm and knowledge base among employees
 - Ensure consistent paradigm and knowledge base with clients/customers
 - For consulting firms credentials and certificates are marketable and increase value to clients

Benefits and Value 3/3

- Clients and customers
 - Independent confirmation that you know something
 - Credential assures that you are staying current in the field
 - Brand recognition
 - Alignment of vocabulary, concepts, paradigm, to increase understanding and reduce startup time
 - Access to a community of practice

Getting Certified

- Body of Knowledge
- Requirements
 - Testing
 - Experience
 - Attestation
 - Code of Ethics commitment
 - Fees
- Application process

Body of Knowledge

- The knowledge expected of practitioners
 - The knowledge base at the centre of the common practices
 - The reference standard for testing
- Regularly maintained and updated
- Sources
 - Individual contributors
 - Editors selecting external material
 - Research
- Format
 - Full text ‘textbook’
 - Subject lists

Testing Requirement

- Most certifications have a test of knowledge
- Variety of formats
 - Multiple choice (online, paper)
 - Case study
 - Hands-on lab test
- Highest value testing processes use strong testing methodology to prevent collusion, question theft, fraud

Experience Requirement

- Many certifications require it
- Knowledge is not enough to demonstrate competence and mastery
- Range
 - 1 year – 10 years
- Experience must be within the Body of Knowledge subject areas

Attestation Requirement

- Someone familiar with the Applicant's work vouches for them
- Independent confirmation of qualification
- Attester requirements (common)
 - Must hold the same certification
 - From same Professional Association
 - Bound by Professional Association ethics agreements
 - Employer
- Fraud could lead to disqualification of a certified attester

Code of Ethics Requirement

- Statement by the applicant to behave ethically & uphold the principles of the Professional Association
- Core feature of professional practice

Fees

- Exam fee
- Certification application fee
- Annual certification maintenance fee
- Annual membership fee
- Annual local Chapter fee
- Training costs
 - Not formally a fee, but might be a de facto requirement to pass the exam
- Wide range of amounts

Staying Certified

- Periodic expiry of certification
 - 3-5 year validity typical
- Requirements
 - CPE (annual and lifespan)
 - Annual requirements
 - Re-certify at end of validity period
- Fees

Recap quiz

- What are Professional Associations for?
- Why get certified?
- Describe some features of a Body of Knowledge

Professional Association Highlight



ISACA at a glance

- *Trust in, and value from, information systems*
- Focus
 - IT Audit, IT Security, IT Governance
- Most significant publication
 - COBIT
- Founded: 1967
- Size
 - ~110,000 members
 - 200+ chapters in 80+ countries
- www.isaca.org

ISACA Purpose & Mission

- To promote education and increase knowledge & skills of members in the fields of IT Systems audit and control
- To encourage a free exchange of techniques and approaches
- To keep members current with new developments in the field for their benefit and their employers benefit
- To communicate the importance of establishing controls to ensure effective use of IT systems

ISACA History

- ISACA was incorporated in 1969 by a small group of individuals who recognized a need for a centralized source of information and guidance in the growing field of auditing controls for computer systems.
- Now a world-wide organization
- Victoria is Chapter 100

Ref: www.isaca.org

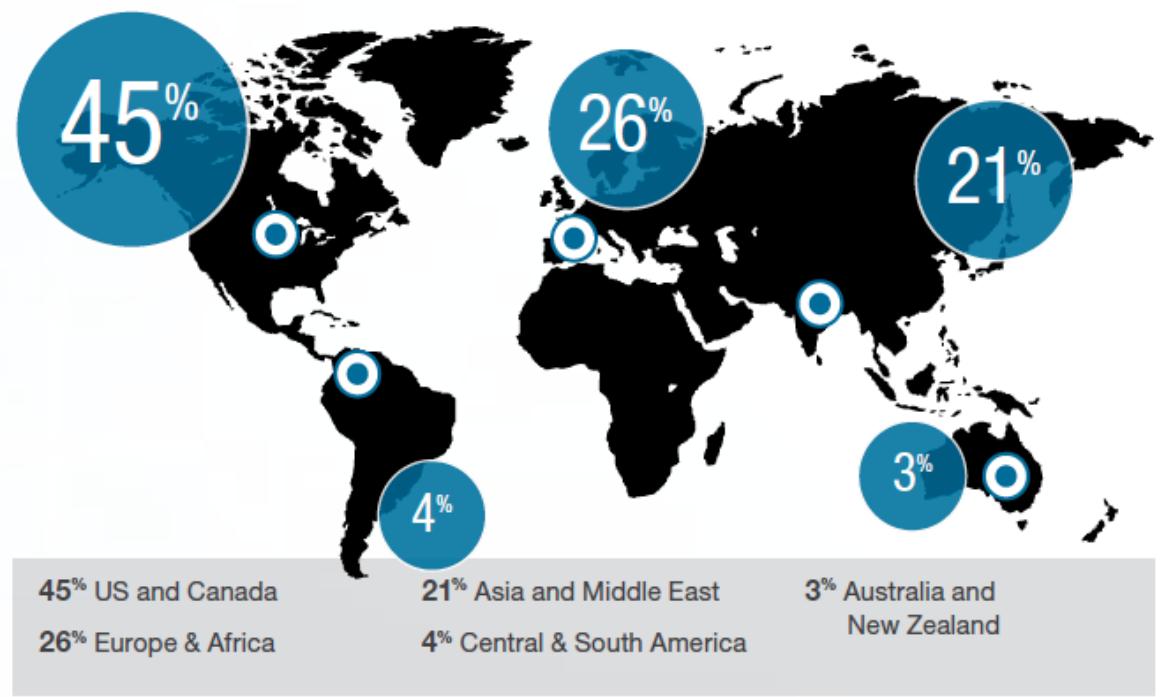
ISACA Structure

- International headquarters
 - President
 - Vice-Presidents
 - Directors
 - Support staff
- Five global regions
 - Asia, Central/South America, Europe/Africa, North America, Oceania
- Local chapters
 - Bylaws
 - Board of Directors
- Chapters have reporting requirements

ISACA Worldwide

ISACA Member Demographics

More than
110,000 IS & IT
professionals
worldwide



From ISACA 2014 Media Kit

ISACA Membership

- Professional membership
- Student membership
 - Full time student
 - Typical degree major:
 - Information systems, Business administration, Accounting, Information technology, Engineering, Computer science
- Academic membership
 - Faculty in specified disciplines

ISACA Member Profile

- IT and information systems professionals covering a range of titles and disciplines, many with a focus in IT assurance, control, security, governance and risk
- All organizational levels
- All industry categories

ISACA Member Profile

ISACA members
by job level/
position



ISACA members
by title

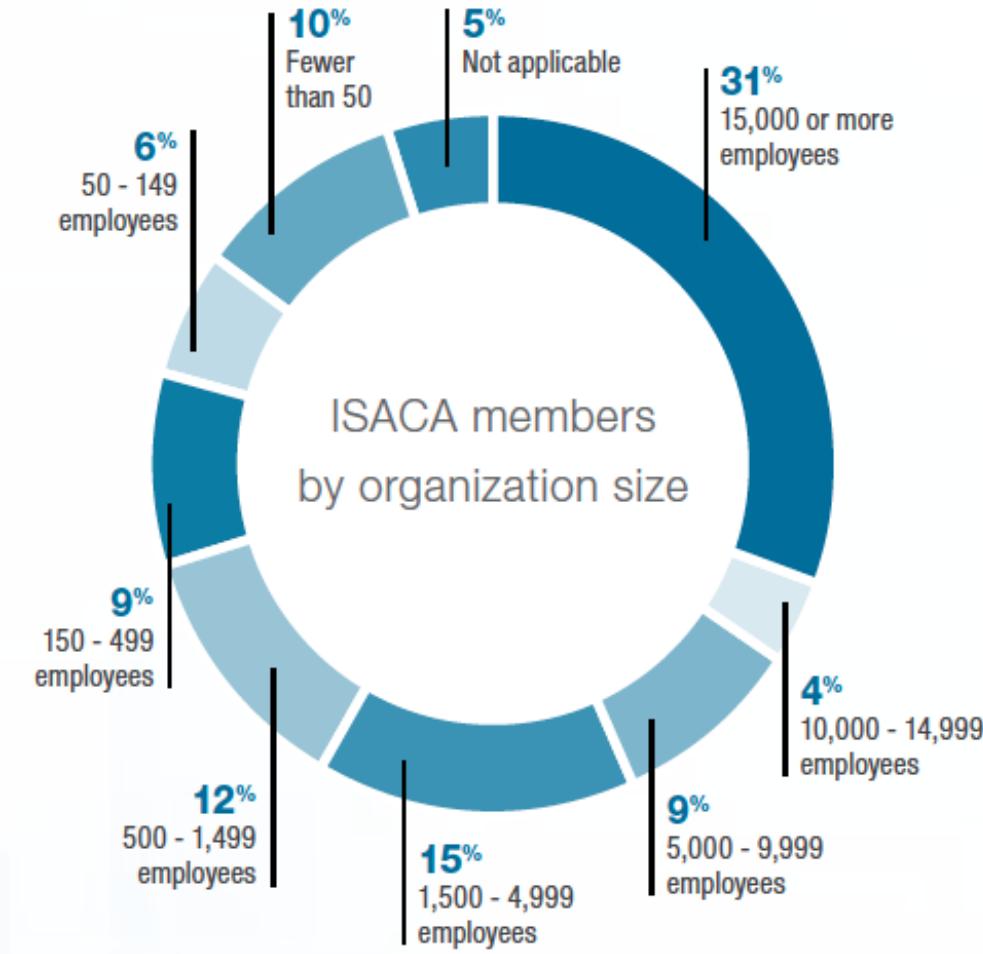


From ISACA 2014 Media Kit

ISACA Member Benefits

- **Professional Development**
 - Certification
 - eLearning (free online symposia)
 - Continuing Professional Education
 - Bookstore
- **Research and Knowledge**
 - Knowledge centre
 - COBIT
 - Journal (monthly publication)
- **Community and Leadership**
 - Networking
 - Leadership opportunities

ISACA Member Organizations



From ISACA 2014 Media Kit

ISACA Publications & Research



- **COBIT 5**
 - Global framework for governance and management of enterprise IT
 - Globally accepted principles, practices, analytical tools and models
 - “it helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use”
 - Used by IT Assessors to determine process maturity and controls

ISACA Training Programs

- “Training weeks”
 - 4 day courses held in a large number of cities
- Online courses
 - eLearning courses
 - Webinars
- Virtual conferences
 - Full day education programs
- On-site training
 - Instructor travels to your organization

ISACA Conferences

- Held in each global region
- CACS Conferences
 - Computer Audit, Control and Security
 - Workshops, courses and speakers
- ISRM Conferences
 - Information Security and Risk Management
 - Workshops, courses, speakers
- World Congress
 - Leadership forum, interviews, executive panels

ISACA Volunteering

- Many opportunities
 - Leadership & Boards of Directors
 - Boards and Committees
 - Exam development
 - COBIT development
 - Social media
 - Publications
- Share and gain knowledge
- Gain recognition
- Network and grow

ISACA for Students



Community and Leadership	Research and Knowledge	Professional Development
Local Benefits	ISACA eLibrary	Career Centre
ISACA Student Groups (ISG)	ISACA Journal	Local Education
Online Professional Networking	Knowledge Center	Conferences and Training
Knowledge Center	Free Publication Downloads	Webinars
	Discount on Publications	
	Free Download of COBIT	

Ref: www.isaca.org

ISACA Certification Programs



Certified Information
Systems Auditor®
An ISACA® Certification



Certified Information
Security Manager®
An ISACA® Certification



Certified in the
Governance of
Enterprise IT®
An ISACA® Certification



Certified in Risk
and Information
Systems Control™
An ISACA® Certification

Certification Program

ISACA CISA

CISA Overview



- Offered by ISACA
- Globally recognized certification for Information Systems Auditors
- Many salary surveys indicate that CISA confers a premium
- CISA certification is accredited by ANSI
- IT Auditors, IT Consultants, IT Audit Managers, Security Professionals, Non-IT Auditors
- Certification validity is 3 years

CISA Body of Knowledge

- Organized as a “Job Practice”
 - Domains of task and knowledge statements
 - Surveys of practitioners used to develop statements and weighting
- Domains
 - The Process of Auditing Information Systems
 - Governance and Management of IT
 - Information Systems Acquisition, Development and Implementation
 - Information Systems Operations, Maintenance and Support
 - Protection of Information Assets

CISA Job Practice Example

- Domain 3
 - Information Systems Acquisition, Development, and Implementation
- Task statement
 - 3.4 Evaluate controls for information systems during the requirements, acquisition, development and testing phases for compliance with the organization's policies, standards, procedures and applicable external requirements.
- Knowledge statement
 - 3.9 Knowledge of control objectives and techniques that ensure the completeness, accuracy, validity and authorization of transactions and data

CISA Testing Requirement

- Exams held 2 times per year, simultaneously in a very large number of locations worldwide
- Proctored, paper-based multiple choice
- 200 questions, 4 hours, pass-fail
- Scaled scoring
 - 200-800 points range
 - 450+ points to pass
- Fees
 - US\$470 (members); US\$650 (non-member)

CISA Experience Requirement

- Verified evidence of 5 years work experience in IT auditing, control, assurance or security
- Waivers for up to 3 years credit for
 - Non-IT auditing experience
 - 2 year or 4 year university degree
 - Degree from university using ISACA Model Curriculum
 - Masters degree in infosec or IT
- Can write exam before experience met

CISA Attestation Requirement

- CISA application form has section for employer to verify work experience by answering questions and marking a job practice checklist

CISA Ethics Requirement

- Support implementation of standards and procedures for effective governance/management of IT systems
- Perform duties with due diligence in accordance with professional standards
- Serve in the interests of stakeholders lawfully
- Maintain privacy and confidentiality
- Maintain competency
- Report significant findings that might affect results reporting
- Support stakeholders by increasing their understanding of governance/management of IT systems

CISA Fees

- US\$50 application fee
- Annual maintenance fee
 - US\$ 45 (members)
 - US\$ 85 (non-members)

CISA Certification Requirements

- Pass the exam
- Submit an Application for CISA Certification
 - Work experience
 - Experience verifier statement
- Adhere to Code of Professional Ethics
- Comply with the Information Systems Auditing Standards
- Adhere to the Continuing Professional Education Program
- Pay application fee

CISA CPE Requirement

- Objectives
 - Maintain individual competency
 - Identify non-compliant CISAs
 - Monitor CISAs maintenance of competency
- 120 hours required for the 3 year period
- 20 hours minimum per year
- Training, self study courses, chapter meetings
- Contribution to the profession
 - Teaching, publication, ISACA Boards, mentoring

Recap Quiz

- In what decade was ISACA founded?
- What is the name of ISACA's flagship product?
- What population is the CISA certification designed for?
- What are some of the ways you can get involved with ISACA?

Professional Association Highlight



(ISC)² at a glance

- International Information Systems Security Certification Consortium
- Focus
 - Education and certification of information security professionals throughout their careers
- Most significant publication
 - (ISC)² CBK – compendium of information security topics
 - Common Body of Knowledge
- Founded: 1988
- Size
 - 75,000+ members, 130+ countries
- www.isc2.org

(ISC)² Purpose & Mission

- “We make society safer by improving productivity, efficiency and resilience of information-dependent economies through information security education and certification.”

Ref: www.isc2.org

- Purpose
 - To be the Gold Standard for professional certification of information security professionals

(ISC)² History

- Consortium formed in 1988 to address the need for standardized curriculum
- CBK first finalized in 1992
- CISSP credential established 1994
- CISSP is ANSI accredited 2004

(ISC)² Structure

- **Structure:**
 - US HQ with offices in London, Hong Kong, Tokyo
 - Global non-profit
 - Local chapter program
 - Vancouver and Seattle closest to Victoria

(ISC)² Membership

- Regular membership
 - Receiving a credential confers membership
 - Credential must be maintained to retain membership
- Associate of (ISC)²
 - For exam passers lacking experience requirement

(ISC)² Member Profile

- **Members are**
 - Chief security officers, Chief technology officers, Chief information officers, Security managers, Systems engineers, Systems integrators, Chief risk officers, Systems and network administrators
- **Wide representation in industry and government sectors**

(ISC)² Member Benefits

- Free education events
- Discounts
- Magazine subscriptions
- Career tools
- Networking opportunities
- Global Information Security Workforce Study
- Chapter program

(ISC)² Publications

- (ISC)² Global Information Security Workforce Study
 - Pay scales, skills gaps, priorities, hiring practices
- The CBK 10 Domains
 - Cryptography
 - Security Architecture and Design
 - Security Operations
 - Business Continuity and Disaster Recovery Planning
 - Legal, Regulations, Investigations and Compliance
 - Physical (Environmental) Security
 - Access Control
 - Telecommunications and Network Security
 - Information Security Governance and Risk Management
 - Software Development

(ISC)² Training Programs

- Training programs directed towards certification exam subjects
 - eLearning – online self study
 - Official textbooks
 - Other Study materials
 - Review seminars
 - In person
 - Live online

(ISC)² Conferences

- Security Congress 2013
 - Training tracks
 - Wide range of speakers



(ISC)² Volunteering

- Range of volunteer opportunities
 - Many opportunities are focused on certification, exams, focus groups
 - Publication
 - Speaking engagements

(ISC)² for Students

- Associate of (ISC)²
 - Pass a certification exam
 - Code of Ethics
 - CPE
 - Annual Maintenance Fee

(ISC)² Certification Programs



Certified
Information
Systems Security
Professional



Certified
Authorization
Professional



Certified
Cyber
Forensics
Professional



Systems
Security
Certified
Practitioner



Certified
Secure
Software Lifecycle
Professional



HealthCare
Information
Security
and Privacy
Practitioner



Certified
Information
Systems Security
Professional

ISSAP[®] Architecture



Certified
Information
Systems Security
Professional

ISSEP[®] Engineering



Certified
Information
Systems Security
Professional

ISSMP[®] Management

Certification Program

• **(ISC)² CISSP**



CISSP Overview

- Offered by (ISC)²
- Globally recognized certification for Information Security professionals
- CISSP certification is accredited by ANSI
- Chief security officers, Chief technology officers, Chief information officers, Security managers, Systems engineers, Systems integrators, Chief risk officers, Systems and network administrators
- Certification validity is 3 years

CISSP Body of Knowledge

- The CBK 10 Domains
 - Cryptography
 - Security Architecture and Design
 - Security Operations
 - Business Continuity and Disaster Recovery Planning
 - Legal, Regulations, Investigations and Compliance
 - Physical (Environmental) Security
 - Access Control
 - Telecommunications and Network Security
 - Information Security Governance and Risk Management
 - Software Development

Domain example

- **Software Development Security Domain**
 - Refers to the controls that are included within systems and applications software and the steps used in their development.
- **Topics**
 - Systems development life cycle (SDLC)
 - Application environment and security controls
 - Effectiveness of application security

CISSP Testing Requirement

- In-person paper based or Computer Based Testing
- 250 multiple choice questions
- 6 hours
- Pass-fail
- Scaled scoring
 - 0 – 1000
 - 700 points to pass
- 5 day exam prep course
 - ~US\$2500

CISSP Experience Requirement

- 5 years in 2 or more of the 10 CBK Domains
- Experience credit for 4 year degree
- Experience credit for other recognized certification

CISSP Attestation Requirement

- Must be an (ISC)² certified, active member
- Must attest to your work experience

CISSP Ethics Requirement

- **Code of Ethics Canons:**
 - Protect society, the common good, necessary public trust and confidence, and the infrastructure.
 - Act honorably, honestly, justly, responsibly, and legally.
 - Provide diligent and competent service to principals.
 - Advance and protect the profession.

CISSP Fees

- Exam fees
 - US\$599
- Annual Maintenance Fees
 - US\$85

CISSP Certification Requirement

- Pass the exam
- Be endorsed by an (ISC)² certified
- Subscribe to the (ISC)² Code of Ethics
- Pay application fee

CISSP CPE Requirement

- **Objective**
 - Maintain individual competency
- 120 hours required for the 3 year period
- 20 hours minimum per year
- **Group A credits**
 - Directly related to Domain activities
- **Group B credits**
 - General enhancement of professional skills

Recap Quiz

- What are two primary benefits you enjoy by being a member of a Professional Association?
- Name one domain from the (ISC)2 CBK
- What is one pre-requisite of an applicant endorser?



TRAINING ORGANIZATIONS

Purpose

- To provide training and education in a range of subjects
- To be a source of continuing professional education
- To provide certification services similar to Professional Associations

Types of training options

- Training for certifications and exams offered by other organizations
 - Official course material
 - 3rd party course material
 - E.g. Microsoft courses, CISSP, etc
- Training for own certifications
 - Some training organizations are recognized as especially effective or high quality
 - The certification builds on the brand
 - E.g. SANS
- Training for current topics
 - Market research into hot topics, courses offered
 - E.g. MIS Training Institute, many others

Course material – from where?

- **Instructor-Author**
 - Many topical courses are authored by the instructor
- **Course vendor**
 - Several training companies invest in creating course material
- **Official Curriculum**
 - Certifying organization publishes course material
- **Based on BoK**
 - For certification, the course material normally follows and covers the Body of Knowledge
- **Advisory committee & exam question writers**
 - Typical for ANSI accredited – the examiners must be independent from the exam creators

Training modalities

- **Instructor-led**
 - Classic classroom training
- **Self-study**
 - Course material provided, no support
- **Self-study with mentor/instructor**
 - Course material provided with ability to contact instructor for assistance
- **On-line instructor-led**
 - Virtual classroom
 - Scheduled, group participation
- **Virtual conference**
 - Presentations and lectures around a central theme

Training Organization Highlight



SANS at a glance

- *The most trusted source for computer security training, certification and research*
- Large number of courses focused on ‘practical’ material instead of ‘theoretical’
- Frequent conferences
- Frequent course updates
- High quality instructors
- www.sans.org

SANS Purpose & Mission

- To provide in depth training for mastery of practical steps necessary for defending systems and networks
- To form the training basis that is tested by GIAC certification
- Stress on immediate value and utility

SANS Organization

- SANS Institute is a family of organizations
 - GIAC – Global Information Assurance Certification
 - SANS Technology Institute – Masters Degree in Information Security
 - Internet Storm Centre – ‘Internet early warning system’
- Many partnerships with other security organizations

SANS Publications & Research

- InfoSec Reading Room
 - Certification candidates must write paper for Gold status
- 20 Critical Security Controls
 - The most effective controls that block known attacks
www.sans.org/media/critical-security-controls/spring-2013-poster.pdf
- Top 25 Most Dangerous Software Errors
 - the most widespread and critical errors that can lead to serious vulnerabilities in software
- 20 Coolest Careers
- Career Roadmap
- Salary Surveys

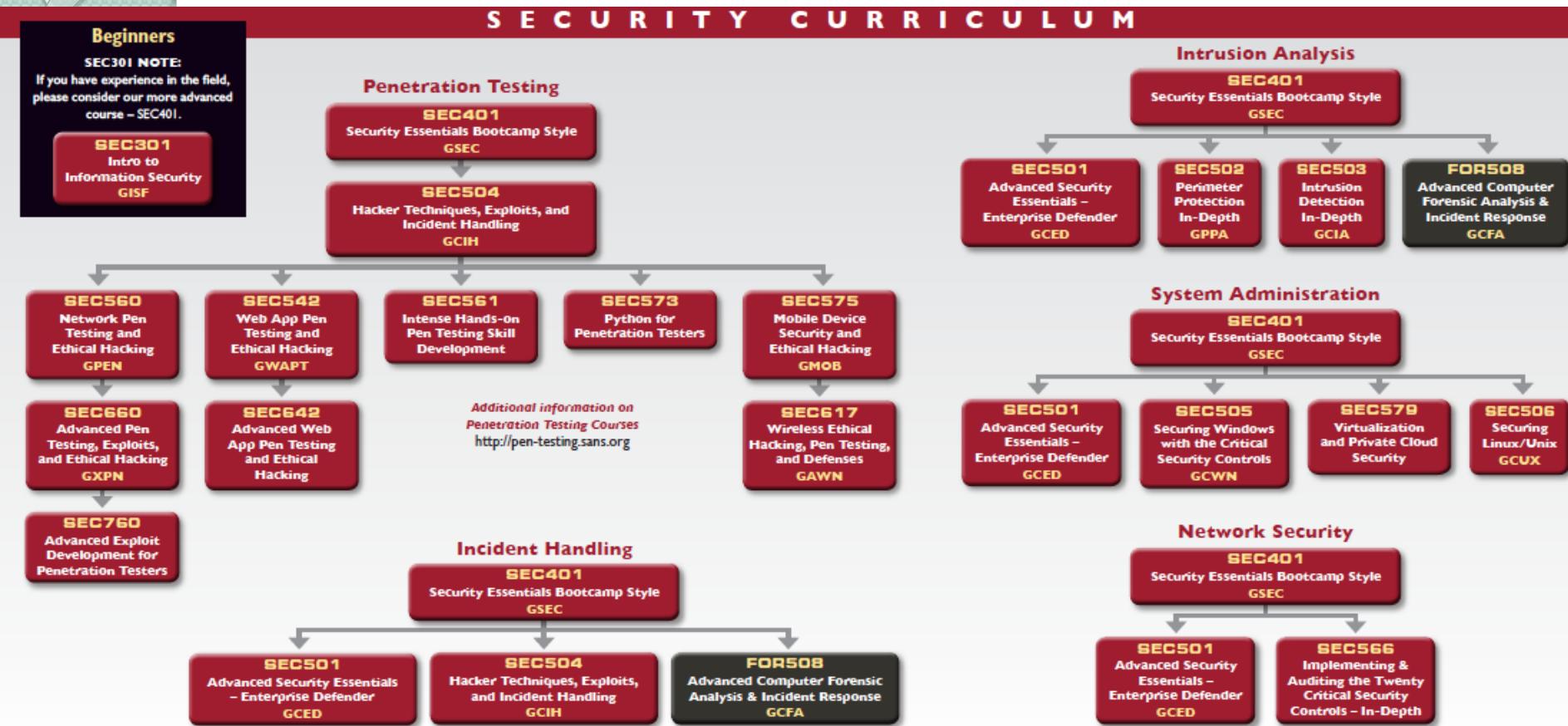
SANS Training Programs

- Targeted at 6 specializations
 - Security Curriculum
 - Management Curriculum
 - Forensics Curriculum
 - Audit Curriculum
 - Legal Curriculum
 - Software Security Curriculum
- Many courses associated with GIAC Certification

Security Curriculum

- Focus areas
 - Introductory level
 - Network Security
 - System Administration
 - Intrusion Analysis
 - Incident Handling
 - Penetration Testing

SANS Security Curriculum



www.sans.org/media/security-training/roadmap.pdf

Forensics Curriculum

Forensics Curriculum		
	Course	Certification
Level 1	<u>FOR408: Computer Forensic Investigations - Windows In-Depth</u>	<u>GCFE</u>
Level 2	<u>FOR508: Advanced Computer Forensic Analysis and Incident Response</u>	<u>GCFA</u>
Specialty Courses	<u>FOR526: Memory Forensics In-Depth</u>	
	<u>FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques</u>	<u>GREM</u>

Audit Curriculum

Audit Curriculum		
	Course	Certification
Level 2	<u>AUD507: Auditing Networks, Perimeters, and Systems</u>	<u>GSNA</u>
Specialty Courses	<u>SEC440: Critical Security Controls: Planning, Implementing and Auditing</u>	
	<u>SEC566: Implementing and Auditing the Critical Security Controls - In-Depth</u>	

Software Security Curriculum

Secure Software Development Curriculum		
	Course	Certification
Level 1	<u>DEV522: Defending Web Applications Security Essentials</u>	<u>GWEB</u>
	<u>SEC542: Web App Penetration Testing and Ethical Hacking</u>	<u>GWAPT</u>
Level 2	<u>DEV541: Secure Coding in Java/JEE: Developing Defensible Applications</u>	<u>GSSP-JAVA</u>
	<u>DEV544: Secure Coding in .NET: Developing Defensible Applications</u>	<u>GSSP-.NET</u>
Specialty Courses	<u>DEV536: Secure Coding: Developing Defensible Applications</u>	
	<u>DEV543: Secure Coding in C & C++</u>	

SANS Conferences

- Major conferences offering 20-40 courses
 - 4+ per year
- Smaller training events offering 1-10 courses
 - 1-2 per month
- Worldwide, wide selection of cities offered

Certification & Accreditation Program



GIAC Overview

- Affiliated with SANS
- Certification of ‘real world’ practical knowledge
- Large number of Certifications offered
- Certification fees ~US\$600

GIAC Body of Knowledge

- Each certification is associated with one or more SANS courses
- Courses built from input from real practitioners
- Input solicited from advisory councils – certifieds who attained ‘Honours’ exam scores

GIAC Testing Requirement

- Online proctored exams
- ANSI accredited
- Each exam has a different number of questions, time limits and passing scores
- For example, GIAC Penetration Tester exam is
 - 1 exam
 - 115 questions
 - 3 hours
 - 74% passing score

GIAC Experience Requirement

- None – Passing the exam confers Certification

GIAC Attestation Requirement

- None

GIAC Ethics Requirement

- **Code of Ethics**
 - Respect for the Public
 - Respect for the Certification
 - Respect for my Employer
 - Respect for Myself

GIAC Fees

- Certification fees ~US\$600
- Certification renewal US\$400

GIAC CMU Requirement

- GIAC Certifications are valid for 4 years
- To recertify, must gain 36 Certification Maintenance Units
 - Take the current exam -> 36 CMU
 - Teach courses
 - Publish research paper or book

Recap Quiz

- How are SANS activities and GIAC activities related?



VENDOR PROGRAMS

Purpose

- Product vendors offer training in their products
- Installers, operators and users of the products learn about features and techniques
- Consultants learn about products to serve their clients better

Types

- Training can be offered for single products or product families
- Some vendors offer certification based on passing exams or demonstrating product competence

Vendor Training & Certification



Microsoft Learning

- Comprehensive training and certification program for Microsoft technologies
- Covers all product lines
 - Server
 - Desktop
 - Database
 - Developer
- Multiple competence levels
 - Microsoft Certified Solutions Associate
 - Microsoft Certified Solutions Expert
 - Microsoft Certified Solutions Master

Microsoft Training Catalog

- There are extensive course, technology and certification offerings
 - The MS Training Catalog tool
 - Learning.microsoft.com/Manager/Catalog.aspx

The screenshot shows the Microsoft Training Catalog homepage. On the left, there is a sidebar with a blue header "Browse Catalog" containing three options: "By Product/Technology", "By Training Format", and "By Certification". The main content area has a green header "Search Catalog" with a dropdown menu "All Training Formats", a search bar "Enter search term here", a "Go" button, and a "Advanced Search" link. Below the header, a large green banner says "Welcome to the Microsoft Training Catalog". A sub-banner below it states: "The Training Catalog is a comprehensive collection of Microsoft Learning resources, including online training, books, classroom training, exams, and more." At the bottom, there is a section titled "Find Training" with three columns: "By Product or Technology" (with links to "Find training related to a specific product or technology" and "Browse through training by product"), "By Certification" (with links to "Find the exams and training that you need to get certified", "Browse through training by certification name", and "Discover the benefits of Microsoft Certification"), and "By Career" (with links to "Find training and career resources to help you meet your professional goals", "Professionals", "IT Managers", and "Students").

Microsoft Certification Example

- MCSD: SharePoint Applications
 - For SharePoint developers
- Recertification required every 2 years
- 4 exams required for certification



MCSM: Data Platform Requirements

Step	Title	Optional training	Required exam
1	Programming in HTML5 with JavaScript and CSS3	480	480
2	Developing ASP.NET MVC 4 Web Applications	486	486
3	Developing Microsoft SharePoint Server 2013 Core Solutions	488	488
4	Developing Microsoft SharePoint Server 2013 Advanced Solutions	489	489

Certification Fees

- Each 5 day classroom course up to \$2500
- Each exam ~US\$150
- For a fully instructor-led certification attempt, could be on the order of \$15,000 to \$20,000
- Using self-study and online options much cheaper
 - Courses in the hundreds of dollars range



STANDARDS DEVELOPMENT ORGANIZATIONS

Other organization types

- This section discusses a type of organization that can help with career growth
- These organizations are fundamental to the innovation and evolution in the online world
- These organizations need smart, innovative, passionate people to work on standardizing the tech that the world will be using next

SDO Description

- Wikipedia says
 - A standards organization, standards body, standards developing organization (SDO), or standards setting organization (SSO) is any organization whose primary activities are developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise producing technical standards that are intended to address the needs of some relatively wide base of affected adopters.
- Many types of Standards Development Organization
 - International, Treaty-Based, National, Industry/Sector

Industry- or Sector-Led SDO

- Often non-profit, volunteer powered
- Self-governing
- Can have formal liaison to national and international SDO
- Specific scope, structure and mandates
- ‘Safe’ forum for competitors to collaborate on common standards to advance the market

Basic structure

- Sector SDO have several typical characteristics
 - Clear intellectual property rights
 - Working groups or task forces to develop new standards material
 - Reporting/accountability structure up to a Board or Trustees
 - Formal standards adoption process including public review periods and ratification votes
 - Testing capabilities for conformance verification
 - Governance rules for counteracting commercial bias

Relevance?

- They define the cutting edge
- Leaders in the field actively contribute to the working groups
- Several key SDO create and establish internet security standards (and others)
- SDO are a great place to learn, grow careers and contribute

Some SDO

- OASIS
- IETF
- IEEE
- ISO
- ITU



Non-Profit Organization

INTERNET SOCIETY



ISOC at a glance

- *The Internet is for everyone.*
- The Internet Society is a cause-driven organization dedicated to an accessible, stable, open, trusted Internet
- Global approach, local collaboration and engagement
 - 55,000 members
 - 90 chapters worldwide
 - 130 Organization members
- www.internetsociety.org

ISOC Purpose & Mission

- The Internet Society engages in a wide spectrum of Internet issues, including policy, governance, technology, and development. We establish and promote principles that are intended to persuade governments to make decisions that are right for their citizens and each nation's future. Everything we do is based on ensuring that a healthy, sustainable Internet is available to everyone – today and for the next billion users.

Ref: www.internetsociety.org

ISOC History

- Founded in 1992
- The Internet Engineering Task Force (IETF) needed a home for continued support and funding of Internet Standards development
- As time went on, other core Internet sustainment bodies needed support as well
- ISOC was founded in part to do this

ISOC Membership

- **Organizational and Individual**
 - No charge options for individuals
- **Provides the opportunity to actively participate in ISOC activities**
 - Conferences, education events, briefings

ISOC Work Areas

- Public policy for open access
- Open development of standards, protocols, administration, technical infrastructure
- Organizing events for collaboration and information sharing
- Education and Leadership
- The IETF is an organized activity of ISOC

Standards Development Organization



IETF at a glance

- *The goal of the IETF is to make the Internet work better*
- The body that creates Internet-Drafts and RFC's which are often the de facto internet technical standards
- Formal process for ratifying documents, a goal is technical excellence
- www.ietf.org

IETF Purpose & Mission

- IETF is all about the engineering of the Internet
 - avoids policy and business concerns
- Cardinal principles (ref: www.ietf.org)
 - Open Process
 - Any interested person can participate
 - Technical Competence
 - Output is expected to follow sound network engineering principles
 - Volunteer Core
 - Participants come to “make the internet work better”
 - Rough Consensus and Running Code
 - Standards are based on real-world implementation experience
 - Protocol Ownership
 - IETF accepts responsibility for all aspects of its protocols

IETF Structure

- No members!
- Minimal formal structure
- No barriers to entry
- Only individuals participate, not their employers
- Standards work organized into 8 Areas
 - Multiple Working Groups within each Area

IETF Publications & Research

- The Working Groups produce Internet-Drafts (I-D)
- I-Ds often become Internet Standards in the form of Request For Comments (RFC)
- Documents are created by consensus
 - No members, so no way to vote
 - IETF structures architected to reflect the ever-changing nature of the internet

IETF Volunteering

- Participation is open
- All documents are freely available online
- Most work is conducted by mailing list
- Three in-person meetings a year
- Technical level is high

Standards Development Organization



OASIS at a glance

- Organization for the Advancement of Structured Information Standards
 - “not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society”
- Scale
 - 5000 participants, 600 organizations, 100 countries
- www.oasis-open.org

OASIS Purpose & Mission

- OASIS promotes industry consensus and produces worldwide standards for security, Cloud computing, SOA, Web services, the Smart Grid, electronic publishing, emergency management, and other areas.

Ref: www.oasis-open.org

OASIS Standards

- Over 80 standards developed
- The most adopted
 - BPEL, CAP, DITA, DocBook, ebXML (ISO 15000), EDXL, OpenDocument Format (ISO 26300), SAML, UDDI, WS-Security, and XACML
- Transparent process for development and ratification of work

Some Interesting Committees

- Biometrics
- Cloud Authorization (CloudAuthZ)
- Cross-Enterprise Security and Privacy Authorization (healthcare focus)
- Electronic Identity Credential Trust Elevation Methods
- XACML
- SOA Reference Model

OASIS Membership

- No minimum qualification requirement (except fees)
- Multiple membership levels
- Right to join in Committees (where the work is done)

Recap Quiz

- What value would you realize by participating in a Standards Development Organization?
- How does voting work for IETF RFC standards approval?



CAREERS

Careers

- What is a career?
 - An occupation or profession, especially one requiring special training, followed as one's lifework: *reference.com*
 - An occupation undertaken for a significant period of a person's life and with opportunities for progress: *google.com*

Career Path

- The trajectory of your career
 - A string of jobs, roles and experience
 - Typically start junior and increase responsibility
 - Starts with broad understanding, increase depth over time

SANS Top 20 Coolest Jobs

1. Information Security Crime Investigator/Forensics Expert
2. System, Network, and/or Web Penetration Tester
3. Forensic Analyst
4. Incident Responder
5. Security Architect
6. Malware Analyst
7. Network Security Engineer
8. Security Analyst
9. Computer Crime Investigator
10. CISO/ISO or Director of Security
11. Application Penetration Tester
12. Security Operations Center Analyst
13. Prosecutor Specializing in Information Security Crime
14. Technical Director and Deputy CISO
15. Intrusion Analyst
16. Vulnerability Researcher/ Exploit Developer
17. Security Auditor
18. Security-savvy Software Developer
19. Security Maven in an Application Developer Organization
20. Disaster Recovery/Business Continuity Analyst/Manager

Ref: www.sans.org/20coolestcareers/

Building your capabilities

- Knowledge
 - What you know & have learned
- Skills & Competencies
 - What you are able to do
 - employment.gov.bc.ca/sites/default/files/Competency_Definitions.pdf
- Experience
 - What have you done

BC Government Competencies

- Vision and Goal Setting
- Creating and Managing Change
- Analytical Thinking
- Business Acumen
- Conceptual Thinking
- Problem Solving / Judgment
- Negotiating / Conflict Management
- Listening, Understanding, and Responding
- Teamwork and Cooperation
- Solving Problems Creatively
- Commitment to Continuous Learning
- Expertise
- Innovation
- Motivating for Peak Performance
- Developing Others

Ref: employment.gov.bc.ca/sites/default/files/Competency_Definitions.pdf

Building a career

- How do you build one and where to start?
 - Find your subject
 - Excel!
 - Build a progression of responsibility and skills
 - Grow by experience and training
 - Be open to growth and change

Career maintenance

- Be an expert in your area
 - Watch for trends and new developments
 - Attain a broad base of experience and knowledge
- Some employers offer career growth programs
 - time and/or money for training, accreditation, mentor programs, performance management
- Bottom line: your career is yours – manage it and grow it to be what you want it to be

Assignment / Case Study

- Write your resume, as if you are applying for an intermediate level job in the field you are pursuing
 - 2 pages maximum
 - Keep in mind that you are trying to persuade the reader that you are competent in the field and have the right combination of skills, knowledge and experience
 - Search job sites if you need to see example job postings
- Create a real resume using these sections
 - Contact information and a one paragraph profile describing you in a professional way
 - Name, address, email and so on
 - Skills and Competencies
 - Use the BC Government Competencies document
 - Choose 3-6 competencies that apply to you and, in 2-3 sentences for each one, describe a real example which shows that you have that competency
 - Knowledge
 - Here's where the list of subjects, languages, methods, protocols, software, hardware, etc that you know about goes
 - Experience
 - For this exercise, do not worry about meeting any number of years requirements
 - This section is for job, co-op and volunteer experience. Highlight if possible how the job experience contributed to the competencies or knowledge listed above
 - Degrees, certificates, specialized courses
 - Title, date, subject, offering institution



END OF COURSE SLIDES