IT Audit/Security Certifications

Kevin Savoy, CPA, CISA, CISSP
Director of Information Technology Audits

Brian Daniels, CISA, GCFA
Senior IT Auditor
Certs Anyone?

- There are many certifications out there for IT auditors.
- Some are very difficult…Some are very easy
- Some are very Technical…Some are very non-Technical
- Some are very applicable…Some not at all
Certs Anyone?

- What does it all mean?
- We will walk through several of the most popular audit certifications to help you figure out which will help you the most
  - CISA
  - CISM
  - CISSP
  - GCFA
  - CPA
  - CIA
  - Vendor Certifications (Cisco, Microsoft)
Certified Information Systems Auditor (CISA)

- CISA is administered by ISACA
- Considered a benchmark exam for IT/IS auditors
- Many employers now require it for job candidates
- Internationally recognized with more than 50,000 professionals earning this certification worldwide
## CISA – Areas of Focus

<table>
<thead>
<tr>
<th>CISA Job Practice Area</th>
<th>% of Exam</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  IS Audit Process</td>
<td>10</td>
</tr>
<tr>
<td>2  IT Governance</td>
<td>15</td>
</tr>
<tr>
<td>3  Systems and Infrastructure Lifecycle Management</td>
<td>16</td>
</tr>
<tr>
<td>4  IT Service Delivery and Support</td>
<td>14</td>
</tr>
<tr>
<td>5  Protection of Information Assets</td>
<td>31</td>
</tr>
<tr>
<td>6  Business Continuity and Disaster Recovery</td>
<td>14</td>
</tr>
</tbody>
</table>
Who is ISACA

- Information Systems Audit and Control Association

- Created in 1967

- International Organization with 170 chapters in over 70 countries

- Chapters provide their members with:
  - Education
  - Resource Sharing
  - Professional Networking
  - etc.
CISA Exam

- 4 hour time frame
- 200 Multiple choice questions
- Only offered 2 times per year, June and December
- Must take it at an ISACA approved testing center
  - In Virginia, Only Richmond and Roanoke
- No obvious order to the question sequence
- ISACA member $410, Nonmember $530
  - Save US $50 by registering online
CISA Experience Requirements

- A minimum of 5 years of professional Information System auditing, control or security experience

- Can substitute 1 year for previous information systems experience or financial audit experience

- Can substitute 1-2 years for 60-120 hours of college credit hours
  - Associates Degree = 1 year sub. credit
  - Bachelor Degree = 2 years sub. credit

- Do NOT have to meet experience requirements to sit for the exam, only to attain actual certification.
How do you keep the CISA?

- Adherence to Code of Professional Ethics

- Maintenance Fee:
  - $40-ISACA member
  - $70-non-member

- CPE requirements
  - At least 20 hours per year
  - At least 120 hours in a fixed 3 year period

- You may be audited for your CPE hours… Keep Records!
How hard is the CISA exam?

- Pretty challenging
- Only ~50% pass rate each exam.
- Must keep a decent pace of at least 50 questions per hour to get it done.
- Don’t let a question you don’t know set you back for a half an hour
What’s it worth?

FROM COMPUTERWORLD, July 2007:

• A report released last week by New Canaan, Conn.-based Foote Partners LLC shows that formally certified security professionals on average are still commanding about **10% to 15% higher salaries** than noncertified individuals in comparable roles…Among the certification programs commanding the highest premiums were Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM).

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9026624&intsrc=news_ts_head
Certified Information Security Manager (CISM)

- CISM is administered by ISACA
- Many employers now request it for supervisory information security job candidates
- Newer Certification but Internationally recognized for Information Security Management with more than 7,000 professionals earning this certification worldwide after only about 4 years of existence
## CISM – Areas of Focus

<table>
<thead>
<tr>
<th>2007 CISM Job Practice Areas</th>
<th>% of Exam</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Information Security Governance</td>
<td>23%</td>
</tr>
<tr>
<td>2. Information Risk Management</td>
<td>22%</td>
</tr>
<tr>
<td>3. Information Security Program Development</td>
<td>17%</td>
</tr>
<tr>
<td>4. Information Security Program Management</td>
<td>24%</td>
</tr>
<tr>
<td>5. Incident Management and Response</td>
<td>14%</td>
</tr>
</tbody>
</table>
CISM Exam

- 4 hour time frame
- 200 Multiple choice questions
- Only offered 2 times per year, June and December
- Must take it at an ISACA approved testing center
  - In Virginia, Only Richmond and Roanoke
- No obvious order to the question sequence
- ISACA member $410, Nonmember $530
  - Save US $50 by registering online
CISM Experience Requirements

- A minimum of 5 years of information security work experience

- Can substitute 2 years if you possess:
  - CISA in good standing
  - CISSP in good standing
  - Masters Degree in information security or a related field (MBA, MIS, etc.)

- Can substitute 1 year if you possess:
  - One full year of information systems management experience
  - Skill-based security certifications (GIAC, MCSE, CompTIA Security +, etc.)

- Total Substitution can only be 2 years though.

- Do NOT have to meet experience requirements to sit for the exam, only to attain actual certification.
How do you keep the CISM?

- Adherence to Code of Professional Ethics

- Maintenance Fee:
  - $40-ISACA member
  - $70-non-member

- CPE requirements
  - At least 20 hours per year
  - At least 120 hours in a fixed 3 year period

- You may be audited for your CPE hours….Keep Records!
How hard is the CISM exam?

- Pretty challenging
- Only ~50-60% pass rate each exam.
- Must keep a decent pace of at least 50 questions per hour to get it done.
- Don’t let a question you don’t know set you back for a half an hour.
What’s it worth? (Look Familiar?)

FROM COMPUTERWORLD, July 2007:

- A report released last week by New Canaan, Conn.-based Foote Partners LLC shows that formally certified security professionals on average are still commanding about **10% to 15% higher salaries** than noncertified individuals in comparable roles…Among the certification programs commanding the highest premiums were Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM).

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9026624&intsrc=news_ts_head
Certified Information Systems Security Professional (CISSP)

- CISSP is administered by ISC2
- Considered a benchmark exam for IT security professionals (ideal for mid- and senior-level managers)
- Many employers now require it for job candidates
- Internationally recognized with more than 49,000 professionals earning this certification worldwide
CISSP – Areas of Focus (Domains)

1. Access Control
2. Application Security
3. Business Continuity and Disaster Recovery Planning
4. Cryptography
5. Information Security and Risk Management
6. Legal, Regulations, Compliance and Investigations
7. Operations Security
8. Physical (environment) Security
9. Security Architecture and Design
10. Telecommunications and Network Security
Who is (ISC)²

- International Information Systems Security Certification Consortium (www.isc2.org)

- Non-profit organization based in the U.S that has certified security professionals in over 120 countries

- Certified members have access to:
  - Education
  - Resource Sharing
  - Professional Networking
  - Career job board
CISSP Exam

- 6 hour time frame
- 250 Multiple choice questions (vendor neutral)
- Offered many times per year at multiple sites around the country
- Cost $499 (early registration) or $599 (regular)
A minimum of 5 years of professional full time security work in order to **SIT** for the exam (practitioner, auditor, consultant, investigator, or instructor)

Can substitute 1 year for BS or BA or Masters in information security

Can substitute 1 year if hold approved certification (CISA, many of the GIAC’s such as GCFA, MSCA, MCSE and many more)

For those who pass exam you must be endorsed by a current (ISC)2 credential holder
How do you keep the CISSP?

- Adherence to Code of Professional Ethics

- CPE requirements
  - At least 120 hours in a fixed 3 year period
  - 40 hours may be non technical

- Maintenance fee of $85

- You may be audited for your CPE hours….Keep Records!

- You can become certified in concentrations once you have the CISSP
How hard is the CISSP exam?

- Pretty challenging (more technical than CISA)
- 60-65% pass rate each exam
- Must keep a decent pace of at least 42 questions per hour on average to get it done
- Don’t let a question you don’t know set you back for a half an hour
What’s it worth? The debate continues!

- CISA’s and CISSP’s are two of the highest paid certifications: usually averaging in the high $90’s depending on what study or who you talk to.

- The on going never ending debate on whether certs are worth it or not depends on vantage point you are looking from (your compensation viewpoint or from the hiring manager’s viewpoint)

- Many downplay certs as being unnecessary as there are many who may pass a test but may not be an expert.

- My take is that it at least shows that you are interested in continuing to learn about your profession. My comeback to the above criticism is that a BS or MS or PHd does not necessarily make you an expert either!

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9026624&intsrc=news_ts_head
GIAC Certified Forensic Analyst (GCFA)

- GCFA is administered by GIAC (Global Information Assurance Certification) and is given in conjunction with attending a six day SANS course on Computer Forensics.

- Targeted towards those responsible for forensic investigation/analysis, advanced incident handling, or formal incident investigation.

- Exam content is very technical, but also a good portion of legal and policy material as well.

- Rapidly growing in importance, currently only about 2,600 individuals with GCFA certification.
## GCFA – Areas of Focus

<table>
<thead>
<tr>
<th>GCFA Content Area</th>
<th>Exam #</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Forensic and Investigative Essentials</td>
<td>1</td>
</tr>
<tr>
<td>2 Forensics Methodology Illustrated Using Linux I</td>
<td>1</td>
</tr>
<tr>
<td>3 Forensics Methodology Illustrated Using Linux II</td>
<td>1</td>
</tr>
<tr>
<td>4 Windows File Systems Forensics</td>
<td>2</td>
</tr>
<tr>
<td>5 Incident Investigation &amp; Forensics Legal Issues</td>
<td>2</td>
</tr>
<tr>
<td>6 Advanced Forensics Techniques</td>
<td>2</td>
</tr>
</tbody>
</table>
Who is GIAC?

- Global Information Assurance Certification

- Created in 1999 to validate real world skills of IT Security Professionals

- Offer exams in various content areas including:
  - Systems Administration
  - Management
  - Audit
  - Software Security

- GIAC Exams are given based on related classes offered by SANS, which are among the best in the business for level of technicality and practicality.
GCFA Exam

- 2 Exams, 2 hour time limit for each exam
- 75 Multiple choice questions on each exam, must score a 70% on the exam
- Switching to Proctored Exams at approved locations
- Open Book and Open Notes, but you will no longer be able to use Google or jump out to a command line to answer questions or look them up
- You cannot just show up without having prepared – It is more challenging because of the open nature of the exam
- Exam Fee $499
GCFA Experience Requirements

- You must attend the SANS Security 508 course entitled System Forensics, Investigation, & Response and take the exams within 4 months of completion

- **BAD NEWS:**
  - This class is offered through SANS for $2,500 – 3,500

- **GOOD NEWS:**
  - SANS EDU offers the class for usually $600 – $1,000 for EDU and Local Law enforcement
  - additional $499 for the exam, usually discounted if you sign up at the class

- Virginia Tech offered it in the Spring of 2007, I took it at the University of Missouri in 2006

- Offered in Austin, Texas in Feb 2008 that may have EDU pricing…Still TBD
How do you keep the GCFA?

- Must retake the exam every 4 years
- The retake is not watered down, but the same exam new candidates take that year
- Recertification Fee:
  - $325 plus shipping for that years course books (for now…may change)
- You don’t have to take the SANS course again, but they give you the books from it
- They do this because they want to ensure GCFAs stay up to date since the technology involved changes so frequently.
How hard is the GCFA exam?

- Very technical in nature and your level of technical expertise will affect your impression of the exam.

- Take the Practice Exams Seriously, as they are great preparation.

- You can actually miss 22 out of 75 questions on each exam and still pass. Don’t dwell on a missed questions since they let you know as you go.
What’s it worth?

- Depends on your job

- The training alone is very productive and useful for someone who is responsible for the technical or the managerial side of forensics and incident response.

- Helps your credibility in court cases if you are a certified professional, but just like any certification, does not ensure that you always know what you are doing

- From eWeek in June 2007 –
  - "We've been reporting for more than a year that pay for IT certifications has been on a steady decline," remarks David Foote, Foote Partners CEO and chief research officer……..Several certifications, however, are holding their own. IT professionals with security certifications—including all versions of the CISSP, CISA, GSE, CISM, SSCP and GCFA—earned 10 percent to 14 percent premiums on their base pay over their non-certified counterparts.
Certified Public Accountant with Certified Information Technology Professional credential (CPA/CITP)

- **CPA/CITP** is administered by AICPA
- CPA considered benchmark for accountants/auditors run by each state board of accountancy while the CITP is an add on credential from AICPA
- CPA not required for most IT audit positions although it is often considered a desirable along with CIA or CISA or CISSP
- There are 650,000 CPA’s with only 1000 or so holding the CITP credential
Who is AICPA

- American Institute of Certified Public Accountants (www.aicpa.org)

- AICPA members have access to:
  - Education
  - Resource Sharing
  - Professional Networking
CPA and CITP – Areas of Focus

**CPA**
1. Auditing & Attestation
2. Financial Accounting & Reporting (business enterprises, not-for-profit organizations, and governmental entities)
3. Regulation (professional responsibilities, business law, and taxation)

**CITP**
1. IT Architecture
2. Business Process Enablement
4. Information Systems Management
5. Systems Security, Reliability, Audit and Control
6. IT Governance and Regulation
CPA Exam (new format)

- 2 day exam, 4 parts, can be taken individually
- Offered many times per year at multiple sites around the country at Prometric test centers or Board-operated sites. It is a computerized test.
- Cost: around $550
CITP exam

- **THERE IS NONE**

- You fill out and send in an application that details your other IT certs, IT related CPE, college degrees, and billable and non-billable hours you have worked in IT related jobs.

- Cost for initial application process is $550
CPA Requirements

- Must have in most states completed 150 semester hours of university level study. (Most are sitting with the 5 year BA/BS MS degree)

- Usually must have at least 36 semester hours in accounting and 40 or so in general business
How do you keep the CPA and CITP?

- Adherence to Code of Professional Ethics for CPA

- CPE requirements for CPA
  - At least 120 hours in a fixed 3 year period
  - 20 hours minimum per year

- AICPA dues and state license fee and $350 annual fee for CITP designation (must recertify CITP every 3 years as of now)

- You may be audited for your CPE hours….Keep Records!
How hard is the CPA exam?

- Extremely challenging
- Less than 20% pass all parts first time
- 40% pass rate each part
What’s it worth?

- CPA is the gold standard for accounting. Salaries reflect this. Often IT audit involves knowing the financial procedures so the CPA is a plus for most employers.

- CITP does not seem to be catching on. Most CPA’s who wish to be involved in technology sit for the CISA and/or CISSP
Certified Internal Auditor (CIA)

- CIA administered by IIA

- CIA considered benchmark for internal auditors

- CIA not required for most IT audit positions although it is often considered a desirable along with CPA or CISA or CISSP
Who is IIA

- Institute of Internal Auditors is the professional association of internal audit profession (www.theIIA.org)

- IIA members have access to:
  - Education
  - Resource Sharing
  - Professional Networking
CIA – Areas of Focus

1. Internal Audit Activity’s Role in Governance, Risk, and Control
2. Conducting the Internal Audit Engagement
3. Business Analysis and Information Technology
4. Business Management Skills
CIA Exam

- 2 day exam, 4 parts, can be taken individually, CPAs do not have to sit for fourth part.

- As of January 08 it will be offered many times per year at multiple sites around the country. It is now a computerized test starting in 08.

- Cost: around $400
CIA Requirements

- Must have completed a 4 year degree to sit for the exam

- Must have 2 years of audit experience to become certified. Can do this after the test has been passed.
How do you keep the CIA?

- Adherence to Code of Professional Ethics for CIA
- CPE requirements for CIA
  - At least 80 hours in a fixed 2 year period
- You may be audited for your CPE hours….Keep Records!
How hard is the CIA exam?

- Challenging
- 48% first time pass rate all parts
What’s it worth?

- CIA is the gold standard for internal accounting. Salaries reflect this. IT audit involves knowing the internal controls and procedures so the CIA is a plus for most employers.

- Is a good complementary cert to a more technical cert such as CISA or CISSP
Cisco Certified Network Associate (CCNA)

- Highly Technical and appropriate for auditors doing heavy network device audits of Firewalls, Routers, Switches, etc.

- Material mainly based on Router Configuration

- Exams redesigned after 11/6/07.

- Multiple ways to certify:
  - One composite exam of 50-60 questions and lasting 90 minutes
  - One 90 minute exam of 50-60 questions and a second 75 minute exam of 45-55 questions

- Recertification is required every 3 years. Tests given at a Testing Center.

- Usually held by networking professionals instead of auditors.
Microsoft Certified System Administrator (MCSA)

- Moderately challenging, requires some specialized knowledge of Operating Systems and Logical Networking

- Requires 3 core exams and an elective exam
  - 2 Networking exams
  - 1 Client Operating System exam
  - 1 more specialized elective exam

- Exams given at testing center.

- Exams considered valid as long as the exam taken remains valid. Once it is retired, you must update.

- Also a specialization called MCSA: Security, that requires the three core tests to be taken, plus 2 more security tests

- Exams taken for MCSA will count towards MCSE if so desired
Contact Info

- Kevin Savoy – savoy@virginia.edu
- Brian Daniels – bdaniels@virginia.edu