Recommendation for Certifications and Organizations for IT Auditors

William F. Slater, III, MBA, M.S., PMP, CISSP, CISA

Week 3 Assignment

CYBR 615 – Cybersecurity Governance and Compliance

December 16, 2012

Agenda

- Trends that will shape the future of IT
- Recommendations for Professional IT Audit- Related Organizations
- Recommendations for Professional IT Audit-related Certifications
- Recommendations for IT Audit-related Training
- Conclusion
- Questions
- References

Key Trends That Will Shape the Future of IT

- Measuring and Managing **EVERYTHING**
- Controlling Costs of **EVERYTHING**
- Optimization of **EVERYTHING**
- Automation of **EVERYTHING** using smart applications and smart hardware
- Trying to be as “GREEN” as possible in **EVERYTHING**
- Trying to get **EVERYTHING** done with as few people as possible, even ZERO people
- **EVERYTHING** will be under Risk Management and Information Security management (i.e. ISO 27001)
- **EVERYTHING** will be under Service Management (i.e. ITIL and ISO 20000)
- Continuous Process Improvement in **EVERYTHING**
- Watch word: Save Your Company Money by optimizing **EVERYTHING**, continually improving **EVERYTHING** and adding business value
- The move to the Cloud to save money and increase efficiencies will continue to INCREASE
- **EVERYTHING** will be subject to compliance and **AUDITING**
- **EVERYTHING is “On the Table”**

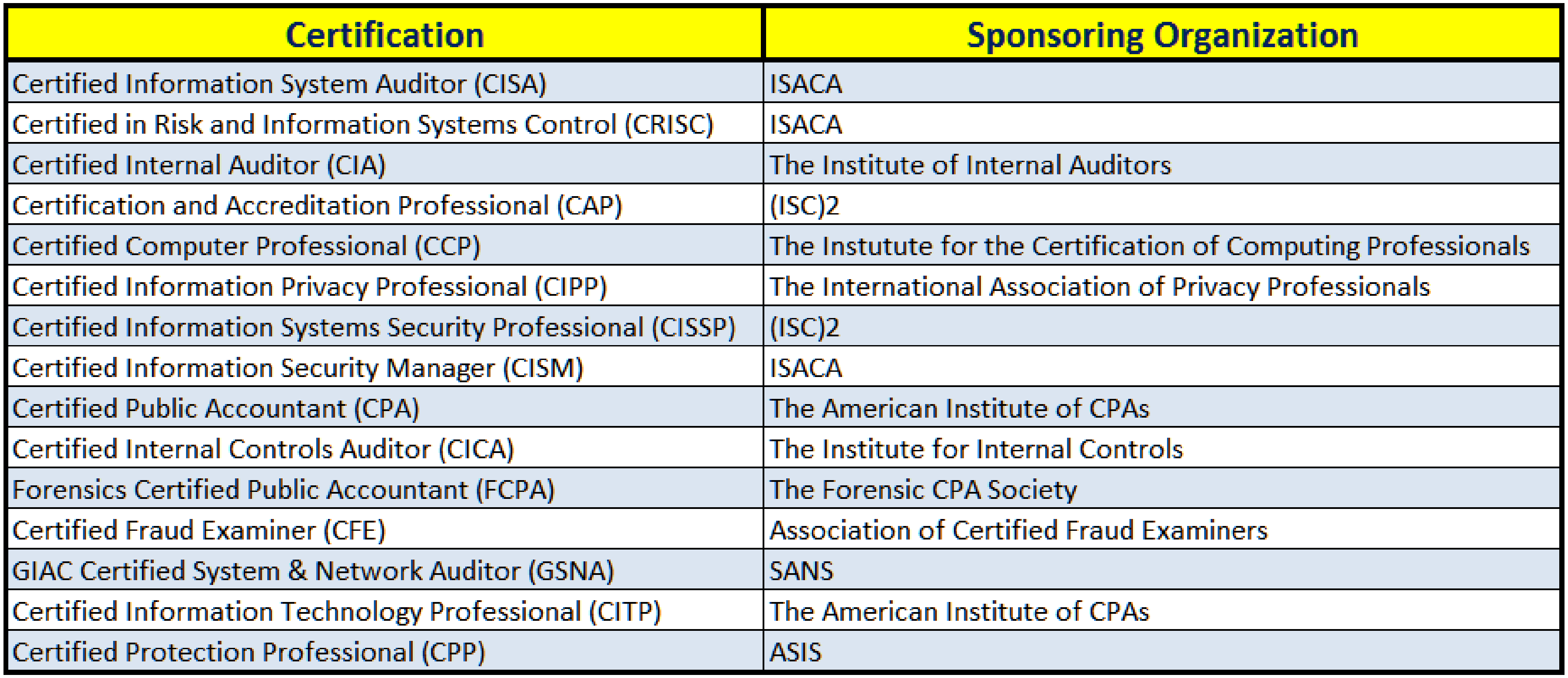
Professional IT Audit- Related Organizations

- American Society of Industrial Security International (ASIS)
- Federal IT Security Institute (FITSI)
- International Society for Auditing and Control Association (ISACA)
- International Information Systems Security Certification Consortium, Inc., (ISC)^2
- SANS Institute

Professional IT Audit-related Certifications

- These are some professional IT Audit-related certifications

(Wikipedia, 2012)

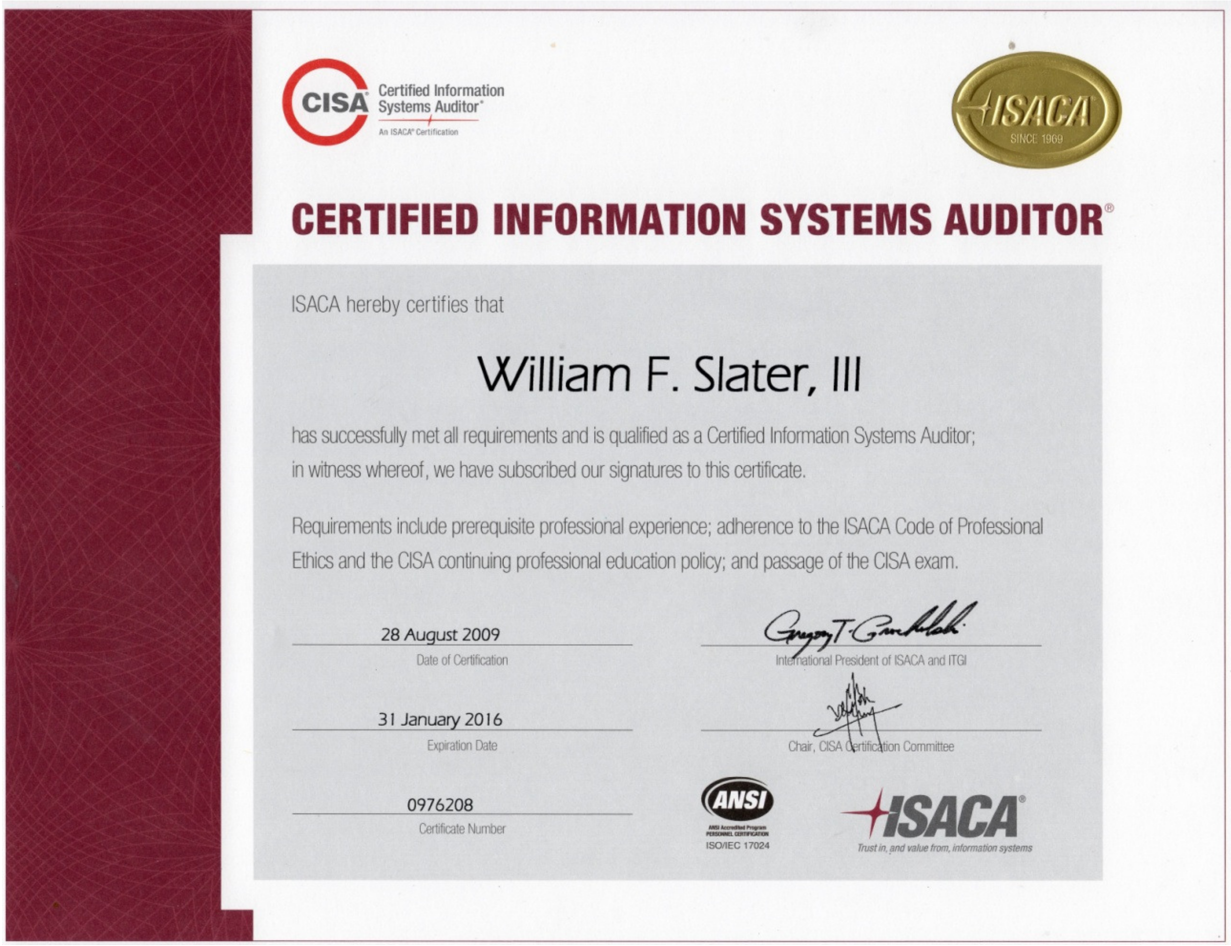


Certification	Sponsoring Organization
Certified Information System Auditor (CISA)	ISACA
Certified in Risk and Information Systems Control (CRISC)	ISACA
Certified Internal Auditor (CIA)	The Institute of Internal Auditors
Certification and Accreditation Professional (CAP)	(ISC)2
Certified Computer Professional (CCP)	The Instutute for the Certification of Computing Professionals
Certified Information Privacy Professional (CIPP)	The International Association of Privacy Professionals
Certified Information Systems Security Professional (CISSP)	(ISC)2
Certified Information Security Manager (CISM)	ISACA
Certified Public Accountant (CPA)	The American Institute of CPAs
Certified Internal Controls Auditor (CICA)	The Institute for Internal Controls
Forensics Certified Public Accountant (FCPA)	The Forensic CPA Society
Certified Fraud Examiner (CFE)	Association of Certified Fraud Examiners
GIAC Certified System & Network Auditor (GSNA)	SANS
Certified Information Technology Professional (CITP)	The American Institute of CPAs
Certified Protection Professional (CPP)	ASIS

IT Audit Related Training

- Some good sources for IT Audit-related training
  - ISO 19011 - Guidelines for auditing management systems (ISO, 2011)
  - ISO 17021 - Conformity assessment — Requirements for bodies providing audit and certification of management systems (ISO, 2006)
  - A Taxonomy of Information Systems Audits Assessments and Reviews (Wright, 2007)
  - ISO 27001 Lead Auditor Course (LaChapelle, 2011)
  - CYBR 515 – Cybersecurity Governance and Compliance, Bellevue University, Bellevue, NE
  - Small Business Information Security Workbook (Lincke, 2010)

What Does a CISA Look Like?



CISA Certified Information Systems Auditor®
An ISACA® Certification

ISACA
SINCE 1969

CERTIFIED INFORMATION SYSTEMS AUDITOR®

ISACA hereby certifies that

William F. Slater, III

has successfully met all requirements and is qualified as a Certified Information Systems Auditor; in witness whereof, we have subscribed our signatures to this certificate.

Requirements include prerequisite professional experience; adherence to the ISACA Code of Professional Ethics and the CISA continuing professional education policy; and passage of the CISA exam.

28 August 2009
Date of Certification

International President of ISACA and ITGI

31 January 2016
Expiration Date

Chair, CISA Certification Committee

0976208
Certificate Number

ANSI
ANSI Accredited Program
PERSONNEL CERTIFICATION
ISO/IEC 17024

ISACA®
Trust in, and value from, information systems

William F. Slater, III

Conclusion

- Certification maintenance usually requires that auditors attend and participate in continuing professional education, and these hours must be logged and reported at least annually
- These activities will greatly to the potential success of every IT Auditor:
  - Participation in professional organizations
  - Earning and maintaining professional certifications
  - Training and continual professional development

Questions

References

- AICPA. (2012). The American Institute of CPAs, sposnored of the CPA and CITP. Retrieved from http://www.aicpa.org/interestareas/informationtechnology/membership/pages/citpoverview.aspx on December 16, 2012.
- http://www.aicpa.org/BecomeACPA/Pages/BecomeaCPA.aspx December 16, 2012.
- Association of Certified Fraud Examiners. (2012). The Association of Certified Fraud Examiners website. Retrieved from http://www.acfe.com/ on December 16, 2012.
- Davis, C., et al. (2011). IT Auditing: Using Controls to Protect Information Assets. New York, NY: McGraw Hill.
- The Forensic CPA Society. (2012). The Forensic CPA Society website. Retreived from http://shopsite.fcpas.org/ on December 16, 2012.
- ISACA. (2012) The ISACA website. Retrieved from on http://ww.isaca.org on December 15, 2012.
- (ISC)2. (2012). The (ISC)2 website. Retrieved from http://www.isc2.org on December 14, 2012.
- IAPP. (2012). The International Association of Privacy Professionals website. Retrieved from https://www.privacyassociation.org/certification/cipp_it/ December 16, 2012.
- The Institute for Certification of Computing Professionals. The ICCP website. (2012). Retrieved from http://iccp.org/certification/designations/ccp on December 15, 2012.
- IIC. (2012). The Institute for Internal Controls website. Retrieved from http://www.theiic.org/certificationscpe/cica.html on December 16, 2012.
- isRisk.net (2012). IT Audit Careers Guide. Retrieved from http://www.isrisk.net/information-technology-it-audit-computer-audit-careers-guide/ on December 15, 2012.
- ISO. (2005) “Information technology – Security techniques – Information security management systems – Requirements”, ISO/IEC 27001:2005.

References

- ISO. (2006). ISO 17021 - Conformity assessment — Requirements for bodies providing audit and certification of management systems. Retrieved from http://isiri.org/portal/File/ShowFile.aspx?ID=746a125a-d702-477e-8e23-165d321dd57a on July 18, 2011.
- ISO. (2011). ISO 19011 - Guidelines for auditing management systems. Retrieved from http://www.cnis.gov.cn/wzgg/201202/P020120229378899282521.pdf on July 18, 2011.
- LaChapelle, E. (2011). ISO 27001 Lead Auditor Course Material from PECB (www.pecb.org). From a course delivered in Dallas, TX in July 2011.
- Lincke, S. (2011). The Small Business Information Security Workbook. Retrieved from http://itm.iit.edu/netsecure11/SusanLincke_SmallBizSecWorkbook.pdf on May 15, 2012.
- SANS. (2012. SANS IT Audit Courses. Retrieved from http:// it-audit.sans.org on December 14, 2012.
- Senft, S., et al. (2013). Information Technology Control and Audit, fourth edition.Boca Raton, FL: CRC Press.
- THEIIA. 2012. The Institute of Internal Auditors. Retrieved from https://na.theiia.org/certification/cia-certification/pages/cia-certification.aspx on December 16, 2012.
- Wikipedia. (2012). Information Technology Audit. Retrieved from http://en.wikipedia.org/wiki/Information_technology_audit on December 15, 2012.
- Wright, C. S. (2007). A Taxonomy of Information Systems Audits Assessments and Reviews. Retrieved from http://www.sans.org/reading_room/whitepapers/auditing/taxonomy-information-systems-audits-assessments-reviews_1801 July 23, 2007.