ISACA Certifications- Strategy for New Computer-Based Exams

CISA, CISM, CRISC, CGEIT, CSXF

Instructor
Jay Ranade
CISA, CISM, CGEIT, CRISC, CBCP, CISSP, ISSAP, CIA, CRMA, HCISPP
Risk Management Professionals Intl.
jayranade@aol.com
New York City

Instructor Introduction

Jay, a certified CISA, CISM, CRISC, CGEIT, CISSP, ISSAP, HCISPP, CIA, CRMA, and CBCP, is an internationally renowned expert on computers, communications, disaster recovery, IT Security, and IT controls. He has written and published **more than 35 IT-related books** on various subjects ranging from networks, security, operating systems, languages, and systems. He also has an imprint with McGraw-Hill with more than **300 books called "Jay Ranade Series".** The New York Times critically acclaimed his book called the **"Best of Byte".** He is currently working on a number of books on various subjects such as IT Audit, IT Security, Business Continuity, and IT Risk Management.

Jay has consulted and worked for Global and Fortune 500 companies in the US and abroad including American International Group, Time Life, Merrill Lynch, Dreyfus/Mellon Bank, Johnson and Johnson, Unisys, McGraw-Hill, Mobiltel Bulgaria, and Credit Suisse. He was a member of the ISACA International's Publications Committee(2005-07).

He also teaches graduate-level classes on Information Security Management and Ethical Risk Management at New York University. Jay is also adjunct professor at St John's University and teaches Accounting Information Systems, IT Auditing, Internal Auditing, Security and Forensics, and Operational Risk Management.

Jay has been teaching ALL ISACA certification exams' prep classes for ISACA New York Metropolitan chapter since 2006. He also teaches these classes in London, Singapore, Cayman Islands, and other international chapters.

He was presented "Best Educator Award" by the president of ISACA NY Metropolitan Chapter in June 2013.

Instructor's Information

- Contact information for classes in USA New York City (jay Ranade)
  - JAYRANADE@AOL.COM
  - Risk Management Professionals International
- Contact information for classes in USA ISACA New Jersey chapter
  - mizbat@verizon.net, Joe.Nunes@crowehorwath.com, Jsjoseph2099@outlook.com
- Contact information for classes in Germany and Austria (Jutta Zilian)
  - jutta.zilian@rmpi-austria.co.at, jutta@zilian.co.at,
- Contact information for classes in Armenia, Russia, Ukraine, and Middle East (Komitas and Azat)
  - komitas@gmail.com
  - azatg101@gmail.com
- Contact information for classes in Singapore, Bangkok, Malaysia, Brunei (Lisa Thung)
  - lisa@adastra.com.sg
- Contact information for classes in London (Richard Nwanze)
  - richard@net-security-training.co.uk
- Contact information for classes in Cayman Islands, Bermuda, and Caribbean Islands (Polly Pickering)
  - polly.pickering@eshoreltd.com

Who this presentation is for?

- **This presentation is for early 2017. It will be little outdated after March, 2018. Things do change!!! Use due diligence……**
- IT Audit (CISA), IT Risk Management (CRISC), Information Security Management (CISM), IT Governance (CGEIT), Cyber Security Fundamentals (CSX-F)
- Have one or none of the ISACA's certifications and want to know how to prepare for certifications exams

ISACA Exam Registration Deadlines

- Used to be paper based exam before 1-1-2017
- Now, it is computer-based held three times a year
  - **May 1- June 30, August 1- September 30, November 1 – December 31**
  - Conducted by **PSI at 700+ locations worldwide**
  - 150 multiple choice questions for all exams
- Register for the exam
  - **Early Bird** for May 1-June 30 exam was February 28. Registration closes June 23
  - Check dates for August-September and November-December from www.isaca.org
  - Usually deadline extended by few days

CISA

- CISA
  - Certified Information Systems Auditor
- Is it only for auditors? No…..
  - Auditors, control professionals, Info Security, IT Professionals
- Domains changed wef 1-1-16
- 127,000 CISAs worldwide as of January, 2017

CISA Results

- Scaled Score System
  - 200 to 800
  - Need 450 to pass
  - What does it mean?
- Mostly results available right away
  - Official results come later
  - ISACA gives score for each domain

CISA - How to prepare for Exam

- Exam Languages- Chinese Traditional, Chinese Mandarin Simplified, English, French, German, Hebrew, Italian, Japanese, Korean, Spanish, Turkish
- CISA review Manual from ISACA (???)
- Practice QAE from ISACA
  - 1000 practice questions in hard copy format for 2016-17 **OR**
  - Subscription-based access to questions
- Books from other publishers (???)
- Sample Q/A from non-ISACA sources
- Study groups not recommended
- CISA training classes
  - Usually a 3-5 day class
  - Chapters, independent instructors, training schools
  - **Always know the instructor, Google the name**
  - Check references of school and instructor

CISA – After you pass the exam

- You file for certification
- Exam passing does not mean you are certified
- 5 years experience
  - One year IS experience or one year non-IS auditing can be substituted
  - Certain degrees can substitute for one year
  - Three years audit, controls, or security experience
- http://www.isaca.org

CISM

- CISM
  - Certified Information Security Manager
- Who is it for?
  - CISO, Info. Security professionals, Info Security Managers
- Approximately 23,000 CISMs worldwide
- Difference between CISSP and CISM
  - Knowledge vs. Wisdom
- Difference between CISM and ISSMP

CISM Exam

- Computer-based exam held three times a year in three 2 month windows
- Syllabus changed wef 1-1-2017
  - 150 multiple choice questions
- Register for the exam
  - June 23, 2017 deadline for May1 -June 30 window
  - Usually deadline extended by few days

CISM Results

- Scaled Score System
  - 200 to 800
  - Need 450 to pass
  - What does it mean?
- Results available as soon as you finish the exam
  - Official results thereafter
  - ISACA gives score for each domain

CISM - How to prepare for Exam

- Exam languages- **English, Japanese, Korean, Spanish**
- CISM review Manual from ISACA (???)
- Practice Q/A from ISACA
  - **1,000 questions** in hard copy format for 2017 **OR**
  - Online access license from ISACA
- Books from other publishers
- Sample Q/A from non-ISACA sources
- Study groups not recommended
- CISM training classes
  - Usually a 3-5 day class
  - Chapters, independent instructors, training schools
  - **Always know the instructor**
  - Check references of school and instructor

CISM – After you pass the exam

- You file for certification
- Exam passing does not mean you are certified
- 5 years experience
  - Two years substitution for CISA or CISSP or post-graduate degree in information security
  - Few other certifications qualify for substitution
  - A must- Three years as **information security manager** in 3 of the 4 practice areas (???)
- http://www.isaca.org

CRISC

- CRISC
  - Certified in Risk and Information Systems Controls
- Who is it for?
  - IT Risk professionals, Operational Risk Managers, auditors, security professionals,
- Approx. 19,000 CRISCs worldwide
  - Mostly grandfathered 5 years ago

CRISC Exam

- Held three times a year in 2 month windows
  - Syllabus changed wef 1-1-2015
  - Computer-based exam wef 1-1-2017
  - 150 multiple choice questions, **some are case study-based**
- Register for the exam
  - Deadline is June 23 for May 1 – June 30 exam window
  - Usually deadline extended by few days

CRISC Results

- Scaled Score System
  - 200 to 800
  - Need 450 to pass
  - What does it mean?
- Results available **right away**
  - Official results come later
  - ISACA gives score for each domain

CRISC - How to prepare for Exam

- Exam languages- **English, Spanish**
- CRISC review Manual from ISACA (???)
- Practice Q/A from ISACA
  - 500 practice questions in hard copy format for 2017 **OR**
  - Get online QAE access license from ISACA
- Books from publishers (???)
- Sample Q/A from non-ISACA sources
- Study groups not recommended
- CRISC training classes
  - Usually a 3-4 day class
  - Chapters, independent instructors, training schools
  - Always know the instructor
  - Check references of school and the instructor

CRISC – After you pass the exam

- You file for certification
- Exam passing does not mean you are certified
- 3 years experience
  - Minimum **three years work experience in 3 of the 4 CRISC domains (in the last 10 years)**
- http://www.isaca.org

CGEIT

- CGEIT
  - Certified in the Governance of Enterprise IT
- Who is it for?
  - CIOs, Big 4 partners, CAEs, senior Auditors, IT Risk Management Professionals, management consultants
  - How many CGEITs worldwide?
- How is CGEIT different from domain 2 of CISA (IT Governance)
  - IT Governance of IT vs. Enterprise Governance of IT

CGEIT Exam

- Three times a year in 2-month windows
  - Syllabus changed wef 1-1-2013
  - Computer based exam wef 1-1-2017
  - 150 multiple choice questions, **some are case study-based**
- Register for the exam
  - Deadline is June 23 for May1-June 30 window exam
  - Usually deadline extended by few days

CGEIT Results

- Scaled Score System
  - 200 to 800
  - Need 450 to pass
  - What does it mean?
- Results available right after the exam
  - Official results come by email later
  - ISACA gives score for each domain

CGEIT - How to prepare for Exam

- Exam language - **English**
- CGEIT review Manual from ISACA (???)
- Practice QAE from ISACA
  - 250 hardcopy format questions for 2017 edition
- Sample Q/A from non-ISACA sources (???)
- Study groups not recommended
- CGEIT training classes
  - Usually a **3-4 day class**
  - Chapters, independent instructors, training schools
  - **Always know the instructor**, very few instructors in the world can teach this class
  - Check references of school and instructor

CGEIT – After you pass the exam

- You file for certification
- Exam passing does not mean you are certified
- At least 5 years experience oversight or advisory role in IS Governance
  - **Out of 5 years, at least one year in IT Governance Framework**
  - One year substitution for **non-IT-Governance experience in assurance, security, consulting** etc
  - One year substitution for many other certifications including CISA, CISM, CIA, PMP etc
  - Two years full time university professor teaching IT Governance substitution for every year of experience
- http://www.isaca.org

CSX- Cybersecurity Fundamentals Certificate

- CSXF
  - Cybersecurity Fundamentals Certificate
- Who is it for?
  - Information Systems Security professionals, IT Auditors, IT Risk Management Professionals
- How many certified worldwide?
- There are 5 follow up hands-on certifications after this
  - You don't need 5 subsequent certifications unless you want to specialize in cybersecurity

CSX- Cybersecurity Fundamentals Certificate - Exam

- Exam can be taken at anytime
- **It is computer-based exam proctored over webcam**
- You can take it from home as well
  - 75 questions in 2 hours
  - Pass score 65 percent (50 correct answers needed)
  - You get score right away as you submit the exam
  - **You pass the exam and you get certificate**
- Register for the exam anytime at www.isaca.org

CSXF- Cybersecurity Fundamentals Certificate - Preparing

- Review Manual from ISACA is good
- Not many practice Q/A from ISACA
  - If you have appeared in any ISACA exam, you should be OK with the exam format
  - **25 sample questions from ISACA website give you the score but don't tell you where you were wrong**
- Sample Q/A from non-ISACA sources (???)
- Training classes
  - Usually a 2-3 day class
  - Chapters, independent instructors, training schools
  - **Always know the instructor**
  - Check references of school and instructor

Other Certifications Being Investigated

- CISSP from ISC2
- CFE from ACFE
- CIA from IIA
- CIPP/? from IAPP
- CCSK from CSA and CCSP from ISC2
- I plan to do this webinar every 6 months
  - So, you will know what is hot and what is not

So which one is right for you?

- IT Auditors
  - CISA is a must
  - + CIA if you are also Internal Auditor
  - + CISM if you audit information security
  - + CISSP if you audit **infrastructure or GCs**
  - + CGEIT if you also audit IT governance
  - + CSX Fundamentals for cybersecurity audits

So which one is right for you?

- Integrated Auditing
  - CIA is a must (operational auditing)
  - + CISA is a must (IT auditing)
  - + Financial systems auditing a must

So which one is right for you?

- CISO or Information Security Manager
  - CISM is a must
  - + CISSP will be very helpful since you will be dealing with technical people
  - + CSXF if you liaise with cybersecurity manager
  - + CRISC if you switch jobs between security management and information risk management (many do)
  - Advise: Do CISM and CRISC in the same 2 month exam window, there is knowledge overlap

So which one is right for you?

- Information Risk Manager
  - CRISC is a must
  - + CISM if you switch jobs between security and risk management (many do)
  - + CRMA from IIA if you liaise with CRO

So which one is right for you?

- IT Governance
  - CGEIT is a must
  - + CISA recommended
  - + CRISC recommended

So which one is right for you?

- IT Management Consultant or Big-4 partner
  - CGEIT is a must
  - + CISA helpful to understand controls
  - + CRISC helpful since world is becoming risk management oriented

So which one is right for you?

- CIO (chief information officer)
  - CGEIT a must since you are dealing with CEO and board
  - + CISA since you are dealing with IT professionals (and auditors)
  - + CISM since you are dealing with second line of defense in security (CISO)
  - + CRISC since you are dealing with second line of defense in risk management

So which one is right for you?

- Fraud Risk Managers or investigators
  - CFE is a must
  - CPA or CA since frauds involve accounts
  - + CISA to learn how criminals bypass IT controls
  - + CISSP (for digital forensic experts)

So which one is right for you?

- Healthcare Security, Privacy, Compliance
  - (USA only) HCISPP (from ISC2) is a must
  - + CISSP (if you are also CISO)
  - + CRISC (if you are healthcare risk manager)

So which one is right for you?

- CPO (Chief Privacy Officer)
  - CIPP/US (for USA)
  - CIPP/C (for Canada)
  - CIPP/E (for EU)
  - CIPP/G (for US Government)
  - CITP (for IT professionals)

Can you do 2 certifications in one exam window?

- CISM and CRISC can be done together – they have symbiotic relationship
  - There is overlap
- CSXF goes well with CISSP (very well in fact)
- CGEIT should be standalone

Thanks from

Jay Ranade (jayranade@aol.com)

Joe Nunes, Judith Jospeh (New Jersey)

Jutta Staudach Zilian (Germany)

Lisa Thung (Singapore)

Richard Nwanze, Daniel Nwanze (London)

Polly Pickering (Cayman Island)

Komitas Stepanyan (Armenia)

Azat Gabrielyan (Armenia)