CISSP® 2015

Introduction

Biography

- William Wong

- CISSP, CISA, CISM, CGEIT, CRISC, PMP, PRINCE2, CobiT…..

- > 25 years in Financial Industry

- Working in IT of an international bank, responsible for Asset Management

- Part Time Lecturer

Domain 0 - Becoming a CISSP

- **Organization:**
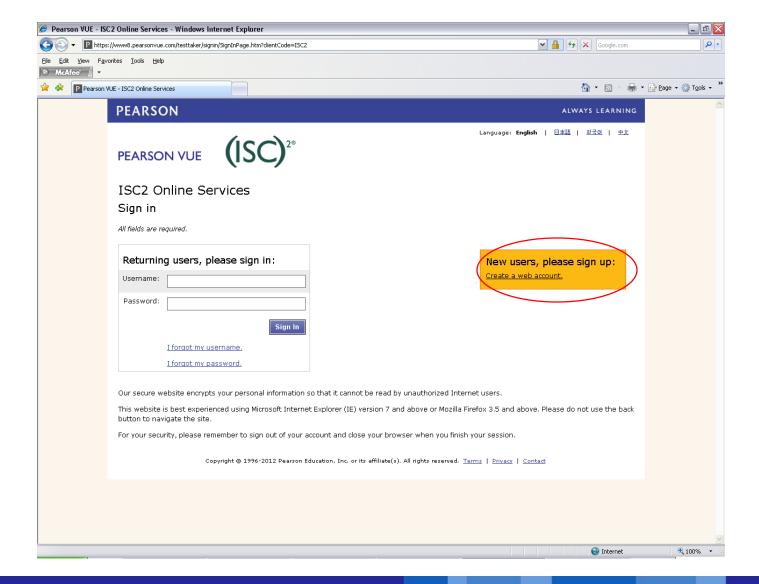 - International Information System Security Certification Consortium (ISC)^2
- **Why?**
  - Increasing needs, increase knowledge, increase salary
- **Book CISSP exam:**
  - **Link:** **https://www8.pearsonvue.com/testtaker/signin/SignInPage.htm?clientCode=ISC2**
  - **Step:** Create Account > Sign in > Select CISSP > Schedule Exam > Language: English > Select Test Center > Select dates
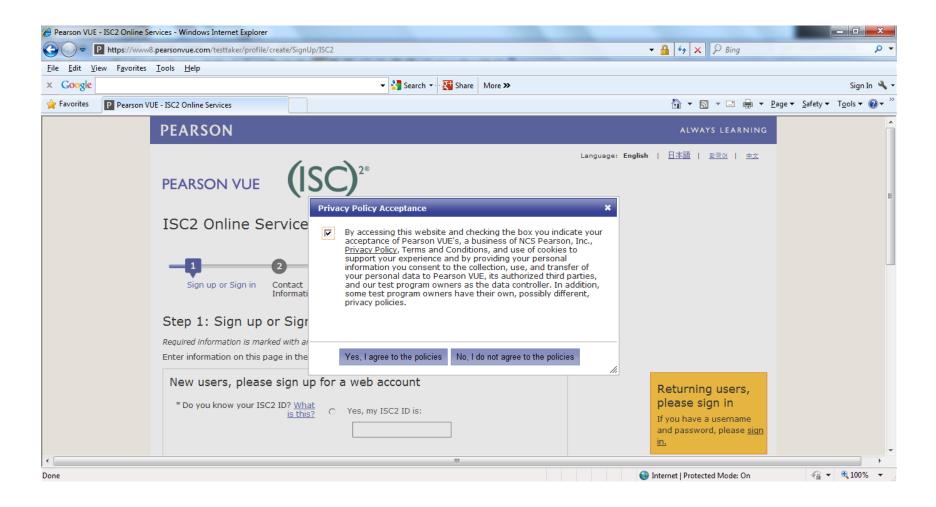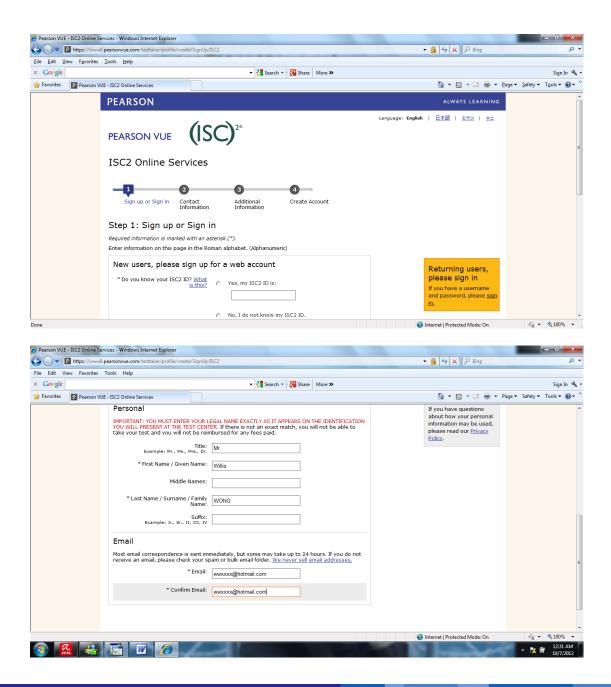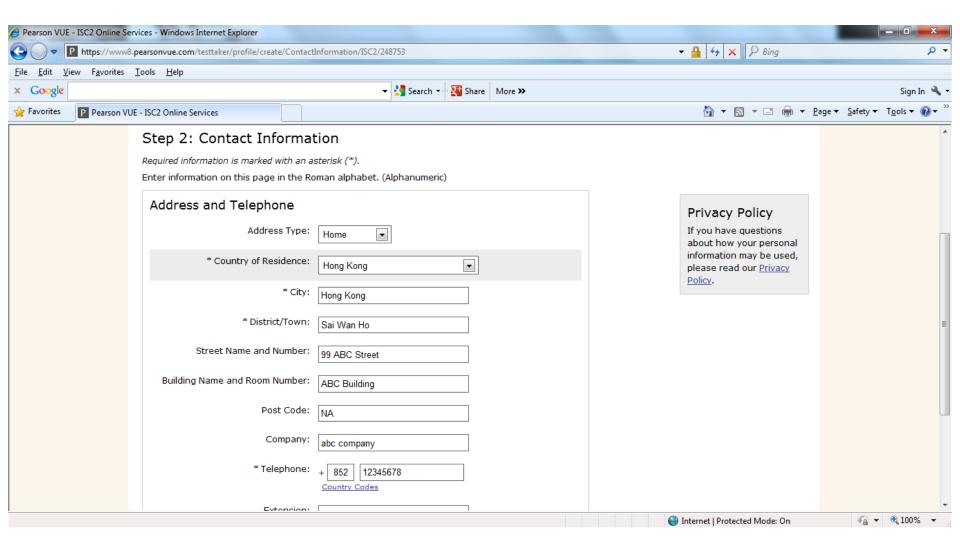 - Can book the exam within one year
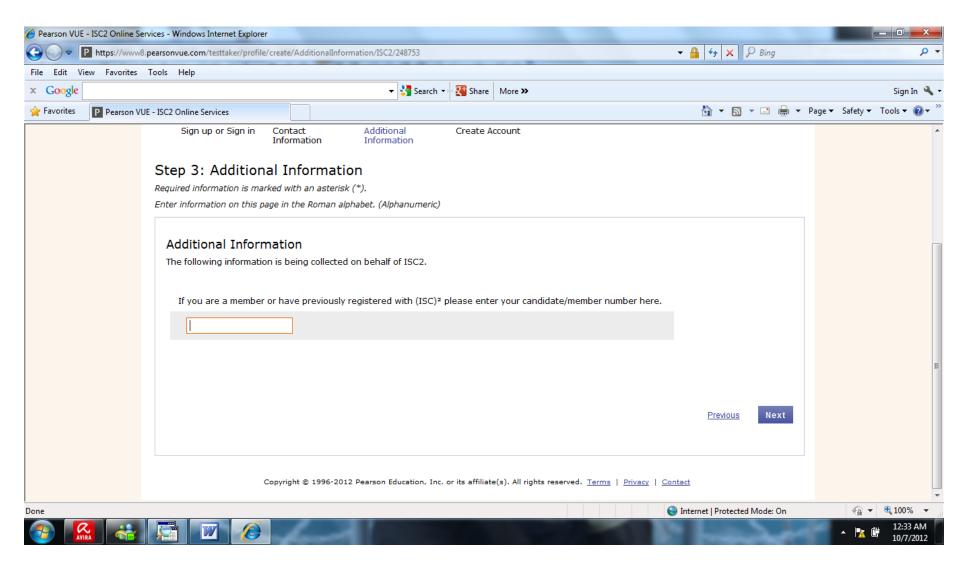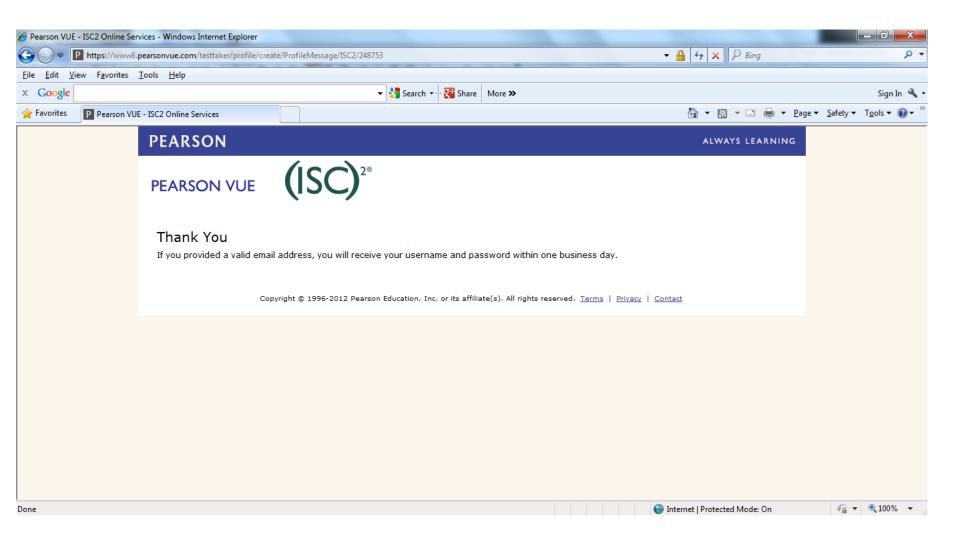 - **Cost:** US $599

Choose yes

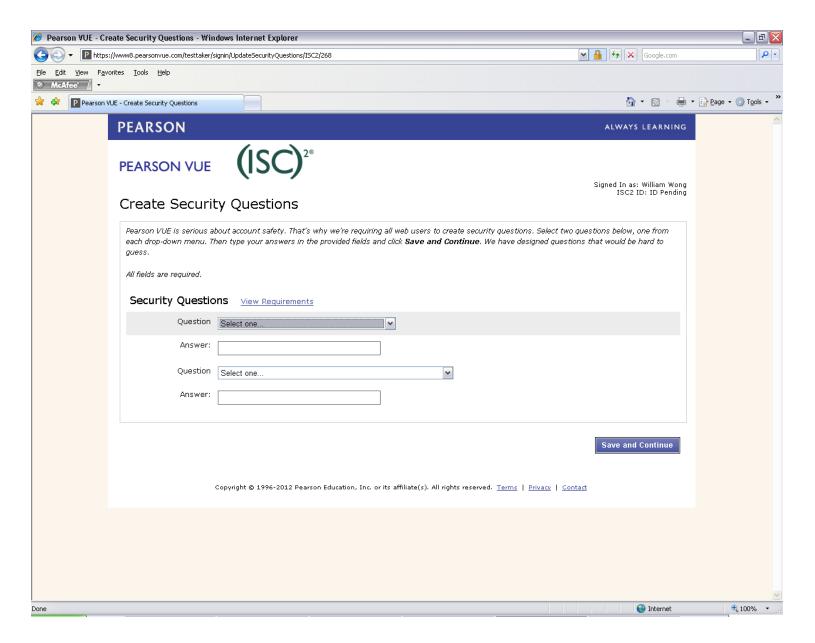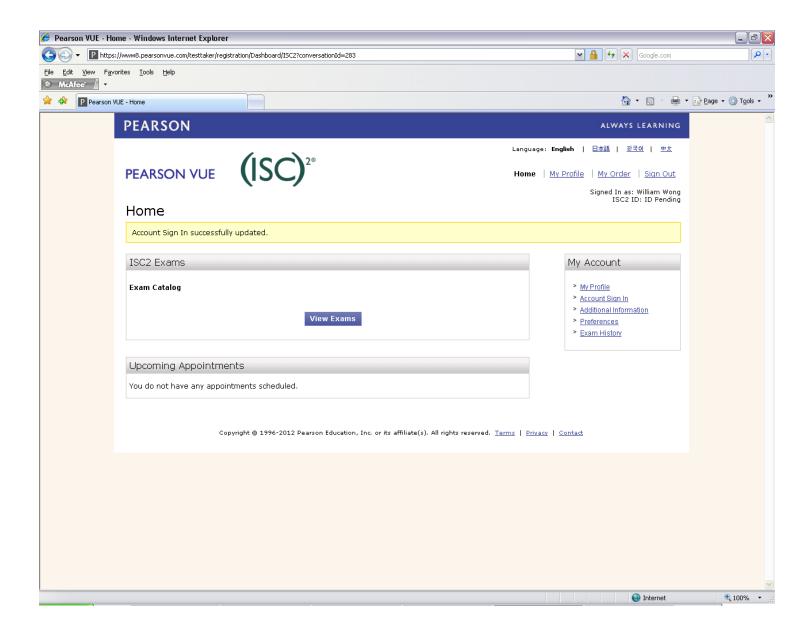# Contact Information

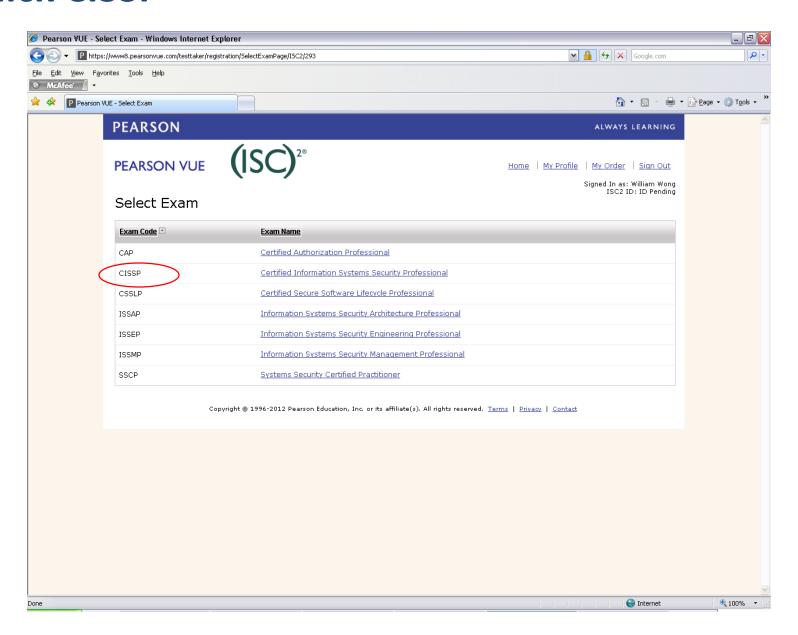# Additional Information

Thank You

Security Question after sign in

View Exam

Click CISSP

Schedule the exam

English

Proceed to Scheduling

Select Test Centre

Select a date

Examination

- **Passing the exam**
  - 250 questions in **6 hours**
  - Mostly MC, but a very few Drag & Drop, Hotspot
  - 4 answers only and only one is correct
  - 25 research questions, but don't know which
  - 700 points out of 1000, weighed, difficulty count, not product or vendor oriented
  - tested on security models and methodologies
  - scenario or situation questions
  - Passed: no score; Failed: score in each domain
  - Hardcopy of language **dictionary** is allowed
  - **Retest**: 1st failed 30 days; 2nd failed 90 days; 3rd failed 180 days; max 3 times per year
  - After exam passed, have to get one holds ISC2 certification, such as CISSP, SSCP or CAP. The sponsor will vouch for your years of experience.

Certification

- **Certification**
  - 5 years experience in 2 or more domains
  - 4 years experience in 2 or more domains + 4 years college degree
  - 3 years experience in 2 or more domains + 4 years college degree + other certificate
- **Recertification 3 years later**
  - 120 Continuing professional education (CPE)

8 Domains (effective from April 2015)

1. **Security and Risk Management** (Security, Risk, Compliance, Law, Regulations, Business Continuity)

2. **Asset Security** (Protecting Security of Assets)

3. **Security Engineering** (Engineering and Management of Security)

4. **Communications and Network Security** (Designing and Protecting Network Security)

5. **Identity and Access Management** (Controlling Access and Managing Identity)

6. **Security Assessment and Testing** (Designing, Performing, and Analyzing Security Testing)

7. **Security Operations** (Foundational Concepts, Investigations, Incident Management, Disaster Recovery)

8. **Software Development Security** (Understanding, Applying, and Enforcing Software Security)

History

- **History**:
  - 1980 needs
  - 1988 forming security certification program
  - 1989 nonprofit corporation ISC^2 in North America: includes code of ethics, test specification, study guide and exam.
  - Conflict of interest: set up course and exam, now you can learn in any training centres

ISACA
Trust in, and value from, information systems

UPCOMING EXAM: 12 SEPTEMBER 2015*
Early Registration Deadline: 17 June 2015
Final Registration Deadline: 24 July 2015

Register early and save US $50

REGISTER NOW

CISA & CISM

- ISACA **membership**: US$135.00 membership + US$55 HK Chapter
- **Exam. Schedule**: The second Saturday in Jun/Sep/Dec
- http://www.isaca.org/CERTIFICATION/CISA-CERTIFIED-INFORMATION-SYSTEMS-AUDITOR/REGISTER-FOR-THE-EXAM/Pages/default.aspx OR
- http://www.isaca.org > Certification > Register for the exam
- **Exam Registration Fees**
  - **Early** registration: US440 / $625 (Member / Non-Member)
  - **Final** registration: US490 / $675 (Member / Non-Member)
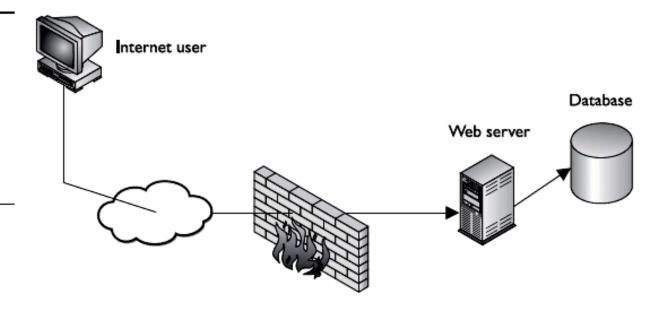- 200 multiple-choice questions in 4 hours in paper format

Security Trend

- **History:** mainframe, dump terminal, closed environment, complicated

- **Now**, *internet*, IT knowledge, open system, powerful PC, *highly rely* on system to process information

- **Nation**: War; Cryptographic

- **Companies**: Sarbanes-Oxley (SOX), Regulation, Security Requirement

- **Hacking & Attacking**

  - trend to profit and commerce

  - Hacker danger: homework, easy to use tools, proliferation, GUI, quiet mode (IDS), population, continuous challenge

  - Product continue to grow in functionality, but not necessarily in Security

  - Selfish, but push security industry

Trend to more security

Generation 1: Internet & web activities

Figure 2-5
Attackers have easy access if databases are directly connected to web servers with no protection mechanisms.

Trend to more security

Generation 2: Two-tier architecture

Internet user

DMZ = Demilitarized zone
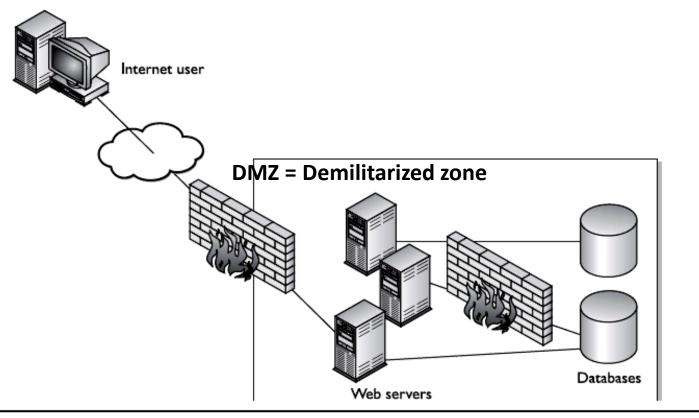
Web servers

Databases

Figure 2-6 A two-tier architecture consists of a server farm and back-end databases.

Trend to more security
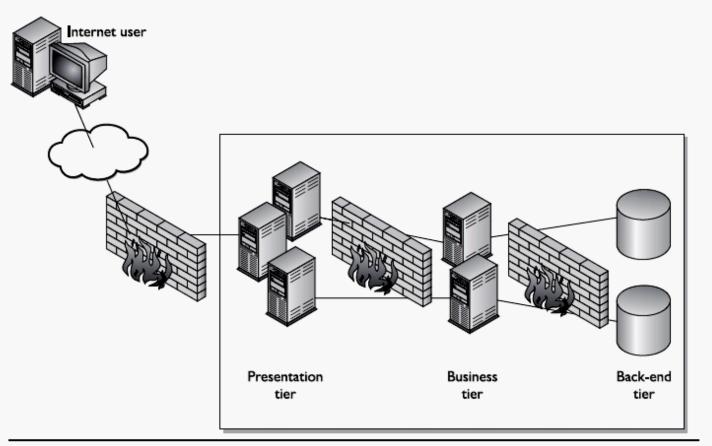
Generation 3: Three-tier architecture

Figure 2-7 A three-tier architecture is comprised of a front-end server farm, middle servers running middleware software, and back-end databases.

Layered approach

- **A Layered Approach**
    - diff vulnerabilities in diff layer
    - involve all parties, vendor, developer….
    - implementing solution at different spectrum
    - Spectrum can be coding, protocol, O/S, configuration, user activity, security program
    - Create layers of barriers to attacker
    - Example: antivirus on workstation, file server, mail server, proxy server etc
    - Example: ACL, configure application, file, registry, os, login credential policy
- **A Layer Missed**
    - If a layer missed (eg IDS), may cause problem, as business keeps changing.

Politics and Laws

- Transborder issue about <u>cryptography</u>
- US: Trusted Computer System Evaluation Criteria (TCSEC)
- Europe: Information Technology Security Evaluation criteria (ITSEC)
- <u>Law is behind</u> the development of computer crime
- Organization for Economic Co-operation and Development (OECD):
  - 30 members, 70 others actively involved,
  - principle of free market, democracy, economic growth, ..
  - provides intergovernmental discussion, collecting and publishing information and short-term economic forecasts
  - not governing body, but provide guidelines, documentation, advice and statistics to help work together
  - many countries use information to shape their laws

Trends

- In 2013, US President Obama issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity.
  - the National Institute of Standards and Technology (NIST) starts drafting a Cybersecurity Framework (CSF)
  - ISACA actively involved in the CSF development
  - Associated qualifications are announced by ISACA
    - Cybersecurity Fundamentals Certificate
    - Implementing the NIST Cybersecurity Framework using COBIT 5
    - CYBERSECURITY NEXUS (CSX) programs
      - Under developments

Education

- Many ways to learn and to certify

- No uniform, standardized way

- Different approaches: integrate with other IT component?