CISSP®

Certified Information
Systems Security Professional

For the next generation of SECURITY LEADERS

Jim Molini, CISSP, CSSLP

(ISC)2北京分会第3次沙龙 2015-02-12 @北京花园饭店

文档密级：外部公开

(ISC)²

关于(ISC)²北京分会

- (ISC)²是推出信息安全领域金牌认证CISSP的美国非盈利教育组织，在中国的(ISC)²北京分会成立于2014年11月1日，专注信息安全，旨在建立北京及周边地区的一个安全技术交流的网络，促进分会会员之间的信息分享、经验交流、技术讨论和个人职业发展

- (ISC)²北京分会微信公众号：ISC2BJ
- 入会申请表
  - http://yunpan.cn/cJgzLuAUcbjx2
  - （提取码：871e）
- 联系邮件
  - info@isc2chapter-beijing.org

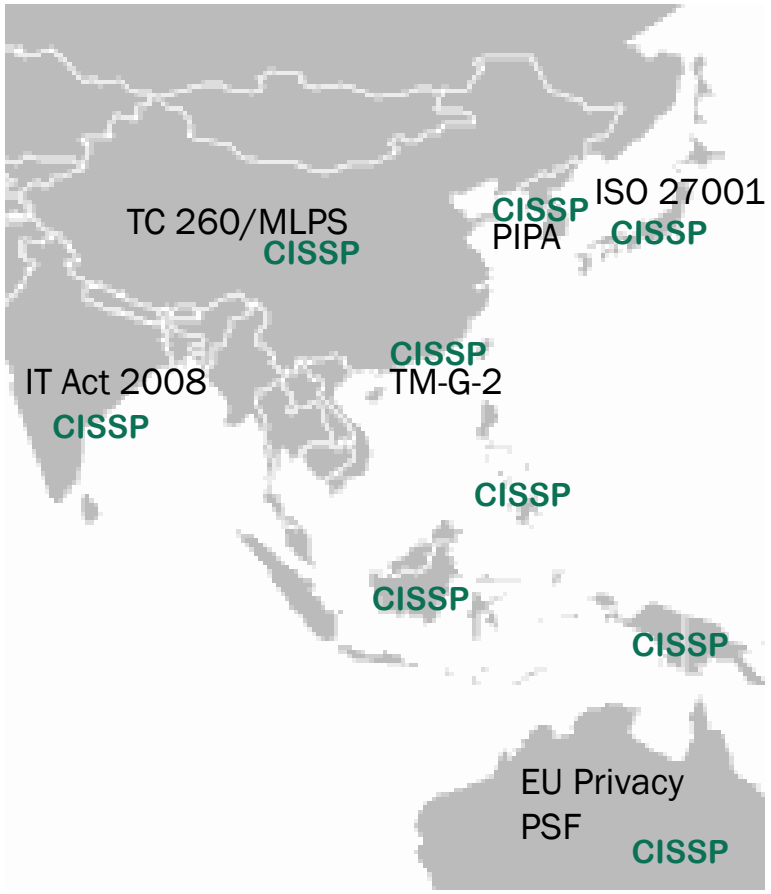
Agenda

- Overview
- CISSP Domain Enhancement
- Overview of New Domains
- Exams and Education Timeline
- Preparing for the new exam
- Q&A

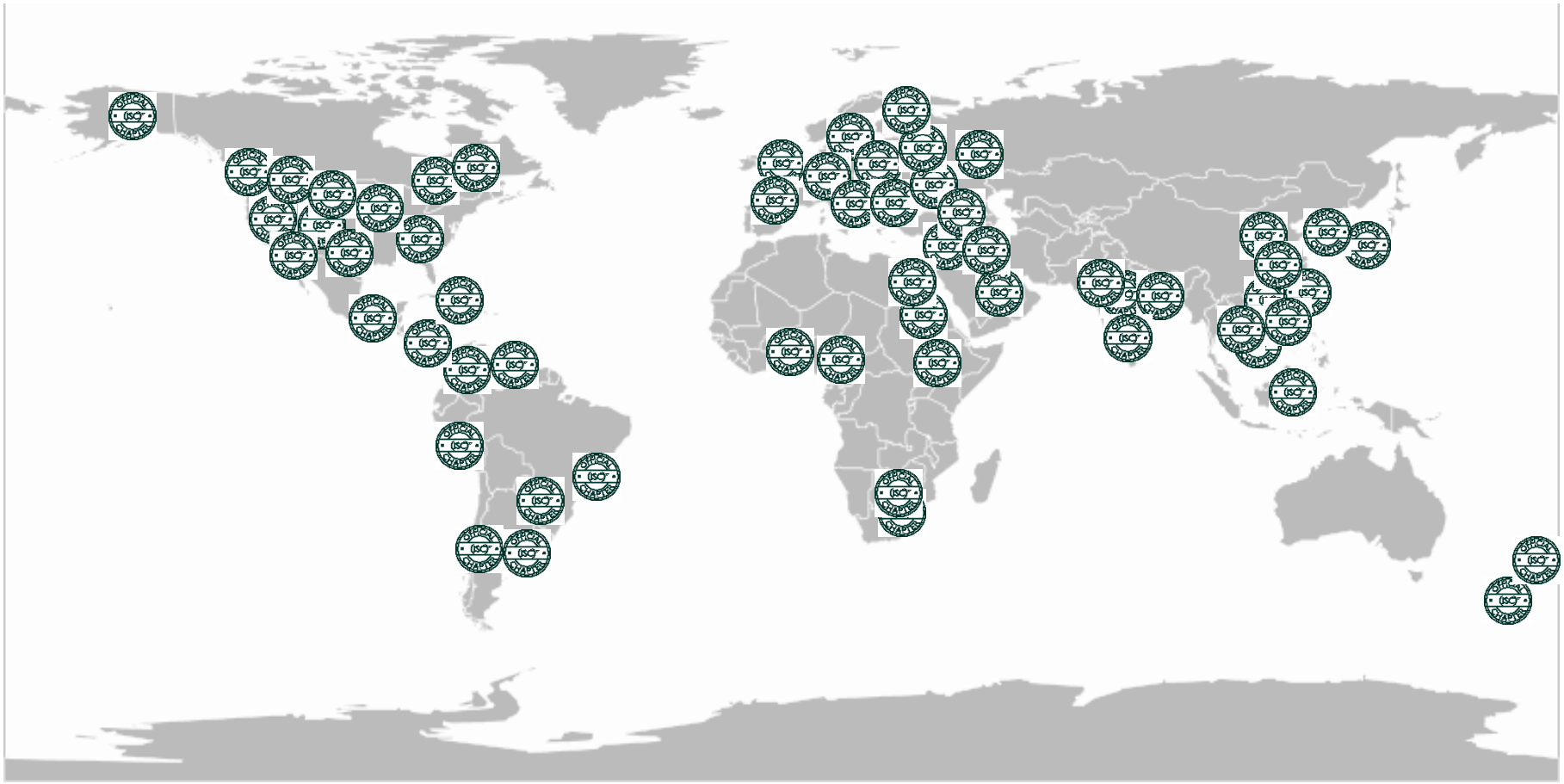
Comments in this presentation are the author's alone and are not endorsed by any organization or company. Please contact jimmolini@Hotmail.com with questions or comments.

Why support CISSP?

- Improves skills of people
- People improve security of machines
- Helps verify minimum skills in hiring
- Support best practices across multiple nations
- Common approach to controls
- Professional ethics requirement
- Over 90,000 CISSP's globally



Global Reach - Chapters



OVERVIEW OF NEW DOMAINS

A look into the 8 domains in the CISSP CBK

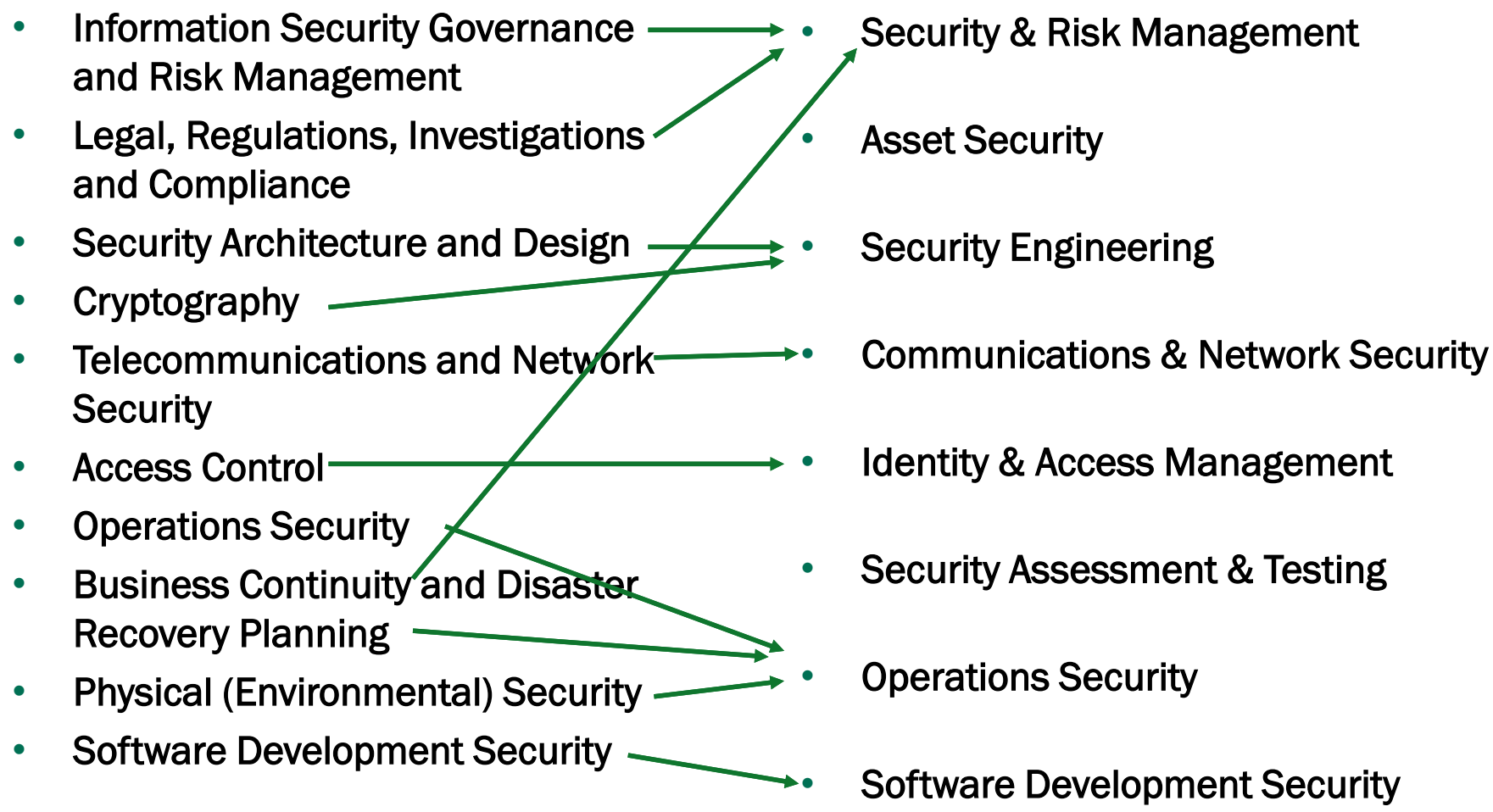
CISSP®
Certified
Information
Systems Security
Professional

CISSP Domain Enhancement

- Realign with new threats, technologies, regulations, standards, and practices
- Maintain the relevance of the credential
- Based on formal Job Task Analysis by information security experts

1993	2003	2013
Windows 3.1	Windows XP	Windows 8
Dial-up	Internet 2.0	IoT
Mainframes	Linux	Cloud

Jim's Domain Comparison



This comparison is not endorsed by (ISC)2.

CISSP Domain Enhancement

Effective April 15, 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)

CISSP® Certified Information Systems Security Professional

Security & Risk Management

- Concepts of confidentiality, integrity and availability
- Security governance
- Compliance
- Legal and regulatory issues
- Professional ethics
- Security policy, standards, procedures, and guidelines

CISSP® Certified Information Systems Security Professional

Security & Risk Management

- Business continuity
- Personnel security policies
- Risk management concepts
- Threat modeling
- Integrate security risk considerations into acquisition strategy and practice
- Information security training, and awareness

CISSP® Certified Information Systems Security Professional

Asset Security

- Classify information and assets
- Determine and maintain ownership
- Protect privacy
- Ensure appropriate retention
- Determine data security controls
- Establish handling requirements

Security Engineering

- Security Models & secure design principles
- Select security controls
- Understand security capabilities
- Assess and mitigate vulnerabilities in:
  - web-based systems
  - mobile systems
  - embedded devices and
  - cyber-physical systems
- Apply cryptography
- Physical security

CISSP® Certified Information Systems Security Professional

Communications & Network Security

- Network architecture security
- network component security
- Design and establish secure communication channels
- Respond to network attacks

CISSP® Certified Information Systems Security Professional

Identity and Access Management

The Identity and Access Management domain provides the basis for the understanding how access management works, why it is a key security discipline, and how each individual component to be discussed in this chapter relates to the overall access management universe. The most fundamental and significant concept to master is a precise definition of the term “access control”.

Identity and Access Management

- Physical and logical access control
- Identification and authentication
- Integrate identity as a service
- Integrate third-party identity services
- Implement and manage authorization mechanisms
- Prevent or mitigate access control attacks
- Manage the identity lifecycle

Security Assessment and Testing

- Design and validate test strategies
- Conduct security control testing
- Collect security process data
- Analyze and report test results
- Understand security vulnerabilities

Security Operations

- Understand and support investigations
- Understand investigation types
- Logging and monitoring
- Secure provisioning
- Foundational security operations concepts
- Resource protection techniques
- Incident management
- Preventative measures

Security Operations (cont.)

- Patch and vulnerability management
- Change management
- Disaster recovery
- Business continuity planning
- Physical security
- Personnel safety & security

Software Development Security

- Security in the software development lifecycle
- Security controls in development environments
- Assess the effectiveness of software security
- Assess security impact of acquired software

Updated CISSP Exam Availability

Language(s)	Date Available
English	April 15, 2015*
French, German, Portuguese, Spanish	May 15, 2015**
Japanese, Simplified Chinese, Korean	July 1, 2015

**Available globally with the exception of China, Japan and Korea. Available in Japan and Korea July 1, 2015.*
*** CISSP exams will not be available in French, German, Portuguese and Spanish from April 15 – May 14, 2015.*

CISSP® Certified Information Systems Security Professional

Exam Tips

- No questions on proprietary technology (e.g. Windows Server, Cisco IOS, or Huawei routers)
- Questions may ask about international standards (e.g. TCP/IP, ISO 27001, SAML)
- No answers that say: “None of the above” or “All of the above”
- Higher emphasis on Scenario Questions or matching exercises.

Sample Question

When should a Certificate Authority (CA) revoke a user's digital certificate?

A. If the certificate has not been used for 6 months
B. If the public key has been compromised
C. If the private key has been compromised
D. If the user upgrades the web browser

Preparing for the exam

- Practice Information Security
- Take a class from a professional training organization
- Form a study group
  - 2 hours every week for 9 weeks
  - Each member researches and presents training one domain
  - Work with a security expert to review material
  - Use sample questions for early testing

(ISC)² Education

Official (ISC)² Education Product	Launch Date
Official (ISC)² Training Seminar	March 16, 2015
Official (ISC)² Guide to the CISSP CBK Textbook (electronic version)	Early 2015
Official (ISC)² Practice Tests	Mid-2015

CISSP® Certified Information Systems Security Professional

How to Prepare

- Download the Exam Outline
  www.isc2.org/exam-outline
- Attend a Training S
  www.isc2.org/cissprevsem
- Read the Textbook
  www.isc2.org/store

QUESTIONS?

CISSP®
Certified Information
Systems Security Professional

(ISC)²®