构建我国的网络安全从业人员能力评价与认证体系

中国信息安全认证中心
CHINA INFORMATION SECURITY CERTIFICATION CENTER

魏 昊

2015年8月

内容提纲

一、体系建设意义

二、目标、指导思想和原则

三、体系框架和主要内容

一、体系建设意义

1、建设强大的网络安全人才队伍是建设网络强国的战略要求

当前，网络空间已经成为人类不可或缺的生存空间，网络安全逐渐成为制约网络空间健康发展的瓶颈。世界各国已清晰地认识到，加强网络安全最关键的是人才，最匮乏的也是人才。

习总书记指出，建设网络强国，要把人才资源汇聚起来，建设一支政治强、业务精、作风好的强大队伍。“千军易得，一将难求”，要培养造就世界水平的科学家、网络科技领军人才、卓越工程师、高水平创新团队。

一、体系建设意义

2、建设强大的网络安全人才队伍是信息化社会发展的需求

随着我国信息化建设水平不断提高和应用不断深入，各行各业对网络安全从业人员的需求快速增加。据统计，2012年我国网络安全从业人员的缺口约为50万人，且每年以2-3万人的速度增长，而我国目前开设网络安全专业的高校只有100余家，每年毕业的学生不到1万人，累计不超过8万人，远不能满足需求。

一、体系建设意义

3、网络安全人才队伍建设面临的问题

（1）网络安全人才培养尚未体系化

网络安全是个内涵广泛的概念。网络安全人才从专业划分和职业设计的角度来讲，可以分为安全管理、安全运维、安全分析、安全防护等等不同领域。目前我们的学校教育和社会岗位需求之间有一定的脱节，课程体系、实践体系、岗位体系还不完善。建设强大的网络安全人才队伍，必须设计一个科学、完整、统一的人才培养体系，明确不同专业、岗位人员的职责和要求。

一、体系建设意义

3、网络安全人才队伍建设面临的问题

（2）网络安全人才培养尚未规范化、规模化

目前我国网络安全人才主要由高校、培训机构和用人单位内部培养等方式形成。由于各机构学科设置、重点方向、就业目标、工作内容不同等原因，对网络安全人才培养的内容、方式、要求也不尽相同，导致不同机构培养的人才在知识、技能、能力等方面存在显著差异。这种差异可能短期满足了不同用人单位的需求，但长期来看并不利于我国网络安全人才队伍的规范化、规模化建设培养。

一、体系建设意义

3、网络安全人才队伍建设面临的问题

（3）网络安全人才培养缺乏自主可控和统一监管

随着社会对网络安全从业人员需求的增加，国内外各类专业培训与认证也迅速增加，影响力较大的有：国际信息系统安全认证协会（(ISC)²)颁发的CISSP证书，美国信息安全研究机构SANS颁发的GIAC证书，相关企业颁发的MCSE,CCSP,STA，TCC等。我国相关机构颁发的CISAW，CISP，NCSE,INSPC等证书。但这些培训认证大部分没有纳入国家的统一监管，国外培训认证机构掌握我国网络安全人才信息的风险也没有得到有效控制。

一、体系建设意义

3、网络安全人才队伍建设面临的问题

（4）网络安全人才评价缺乏客观、统一的标准

网络安全是一个非常专业的领域，有些部门、行业对网络安全岗位人员的要求很高，有的部门则可能无法提出对网络安全人员的基本要求。缺乏客观统一的人才评价标准，不仅不利于用人单位选择合适的人才，也不利于网络安全人才的成长和流动。

一、体系建设意义

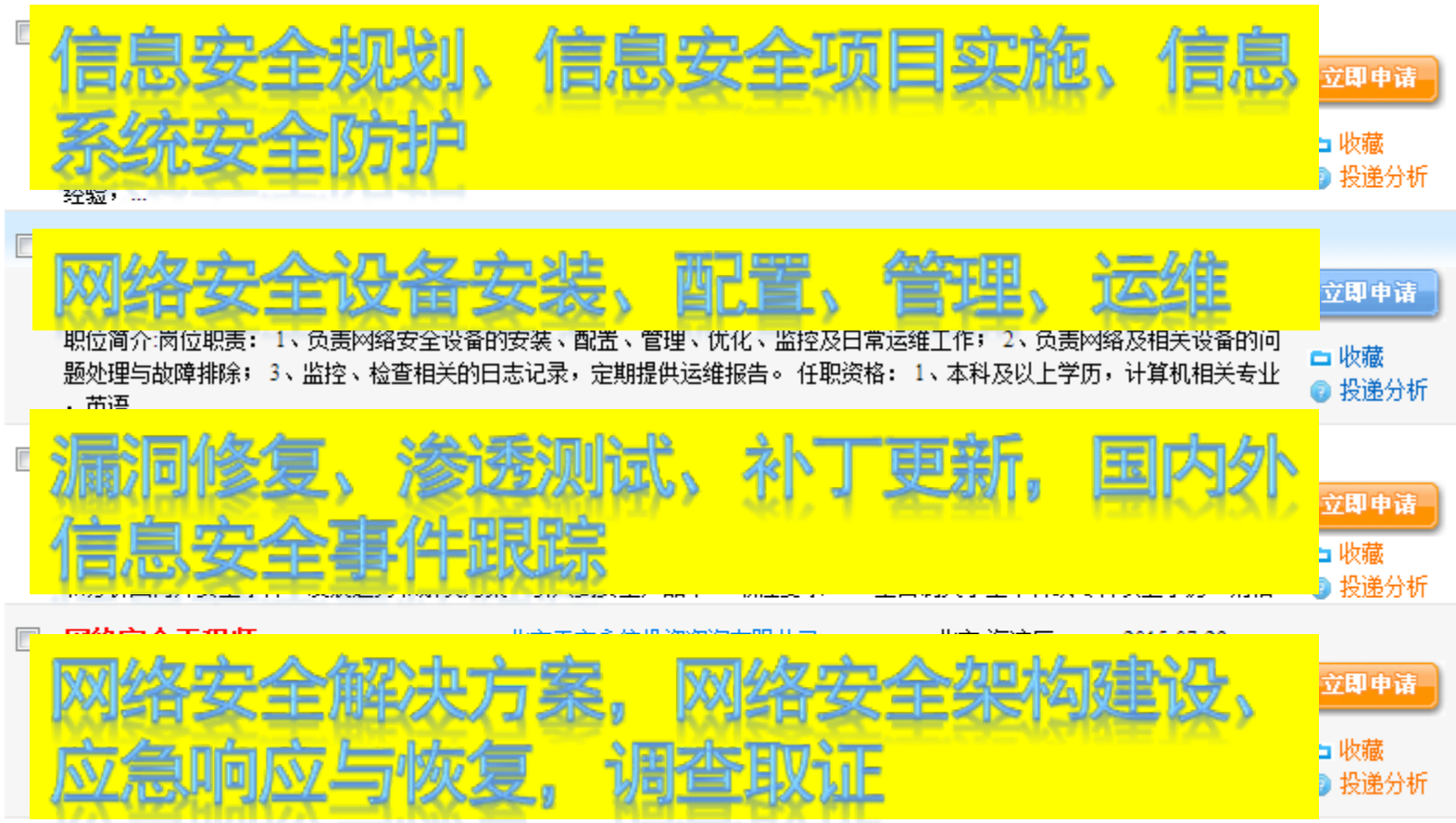
案例：用人单位眼中的网络安全人才

岗位	薪酬(w/m)	需求量
网络安全架构师、信息安全高级咨询顾问	4-5	6
网络安全总监	3-4	1
网络安全经理、网络安全专家	2.5-3	7
资深网络安全管理	2-2.5	11
网络安全工程师、网络安全分析员	1.5-2	28
网络安全工程师、咨询师、顾问	1-1.5	67
网络安全工程师、信息安全测试工程师	<1	150

数据来源：51job，7月30日查询结果。

一、体系建设意义

案例：用人单位眼中的网络安全工程师



一、体系建设意义

4、国外做法借鉴：

2011年9月，美国土安全部和人力资源办公室牵头提出《网络安全人才队伍框架（草案）》，明确了网络安全专业领域、岗位人员应具备的“知识、技能、能力”；2012年美国发布《网络安全教育战略计划》（NICE），明确提出了对普通公众、在校学生、网络安全专业人员三类群体进行教育和培训，以提高全民网络安全的风险意识、扩充网络安全人才储备、培养具有全球竞争力的网络安全专业队伍。

一、体系建设意义

4、国外做法借鉴

2013年，美国发布了网络空间安全人才队伍建设框架。该框架将网络安全从业人员分为7大类，31个专业领域。分别是：

安全提供，使用与维护，保护与防御，安全调查，收集与窃取，情报分析，发展与监管。

框架对31个专业领域及相关岗位的职责、知识、技能、能力进行了明确定义。

一、体系建设意义

4、国外做法借鉴

英国在2009年发布《网络安全战略》中强调：通过建立认证培训方案，提升从事信息保障和网络安全专业人员的技能水平；加强研究生教育，扩展具有深度网络知识的专家库。同时，英国政府还加强了高校硕士专业认证，以提升对网络安全专家的培养力度。

日本在2011年发布《保护国民网络安全》文件，采用通用人才评估和教育工具、大学与产业合作开发的实用型培养方法等来培养网络安全专家，并为这些专家规划可行的职业道路。

一、体系建设意义

4、国外做法借鉴小结：

1）明确的岗位职责，及对应的知识、技能、能力要求；

2）通用的人才评估工具；

3）通过建立认证培训方案，提高人员水平。

内容提纲

一、体系建设意义

二、目标、指导思想和原则

三、体系框架和主要内容

二、目标、指导思想和原则

1、体系建设目标

在中央网信办和相关部门的统筹领导下，通过3～5年的时间，综合教育、科研、培训、认证等各方力量，建立符合我国实际，以满足不同专业方向、岗位职责为目标，以知识考核、技能测验、能力评价为依据，符合国际人才评价标准程序的，科学、完整、统一的网络安全从业人员能力评价与认证体系。

二、目标、指导思想和原则

2、指导思想

以贯彻落实中央网信领导小组、习近平总书记“网络强国”建设要求为指导，以建设强大的网络安全人才队伍为出发点，充分发挥各方优势，全面深入研究制定网络安全从业人员能力评价要求准则，加大网络安全从业人员教育、培训、认证机构能力建设，构建我国网络安全从业人员能力评价与认证体系。

二、目标、指导思想和原则

3、建设原则

（1）统筹领导、加强协调

（2）统一规范、需求导向

（3）多方合作、充分衔接

（4）自主可控、保障安全

内容提纲

一、体系建设意义

二、目标、指导思想和原则

三、体系框架和主要内容

三、体系框架和主要内容

1、体系建设框架

网络安全从业人员能力评价与认证体系建设

标准体系建设：	组织体系建设：	能力体系建设：	运行体系建设：
1.学科标准体系	1.监管体系	1.人才培养能力	1.教育体系
2.技能培训标准	2.技术支撑体系	2.实训能力	2.培训体系
3.评价认证标准	3.运行体系	3.评价认证能力	3.评价认证体系
4.认证机构认可	4.评价体系	……	……
5.培训机构认可	……		
……			

三、体系框架和主要内容

2、标准体系

建立统一、规范的标准体系，是网络安全从业人员能力评价与认证体系建设的前提和基础。主要包括：

（1）网络空间安全学科建设标准体系；

（2）网络安全从业人员职业体系；

（3）网络安全从业人员技能培训标准体系；

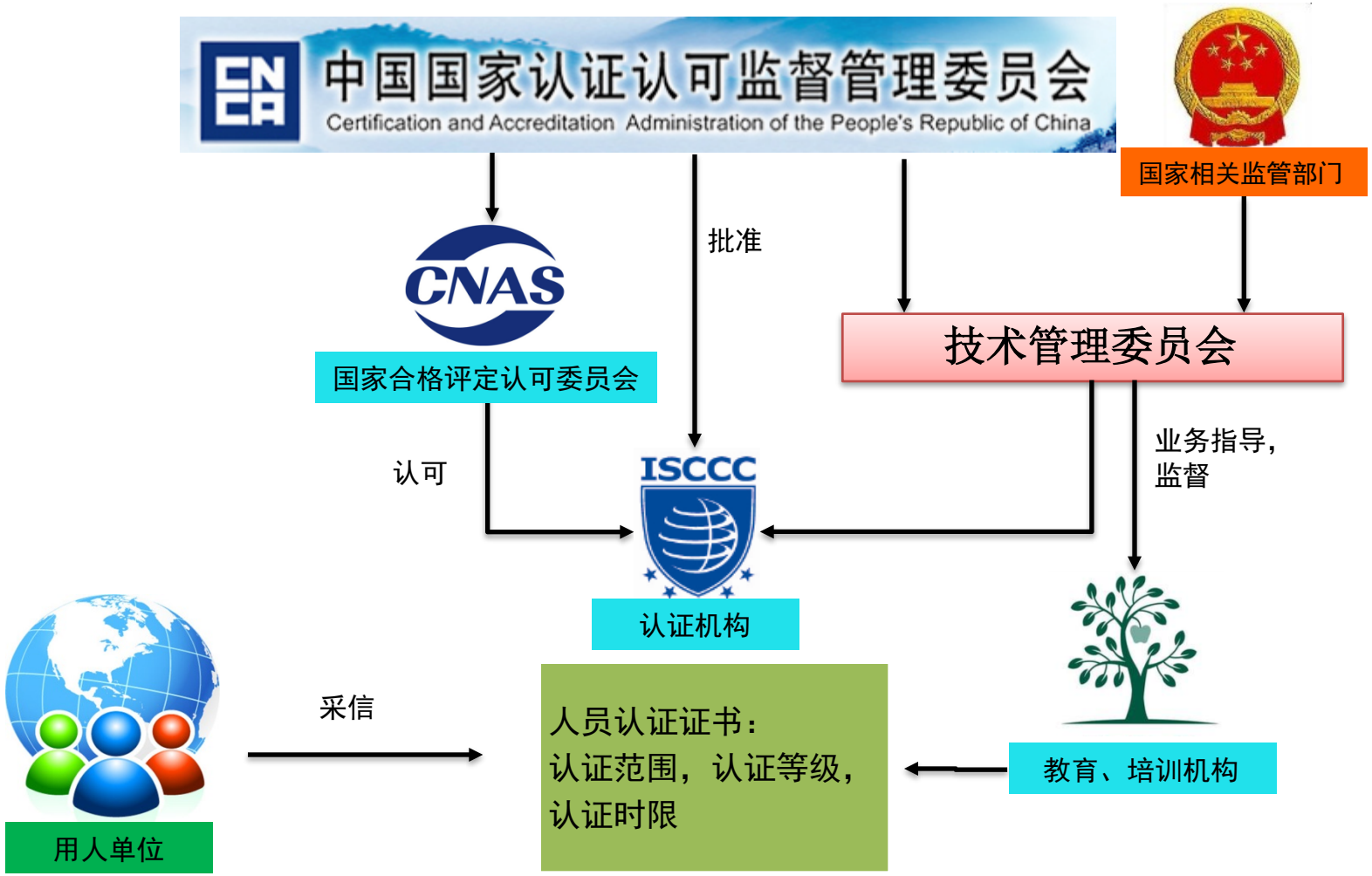
（4）网络安全从业人员能力评价与认证体系；

（5）网络安全从业人员认证机构认可标准；

（6）网络安全从业人员培训机构认可标准；等等

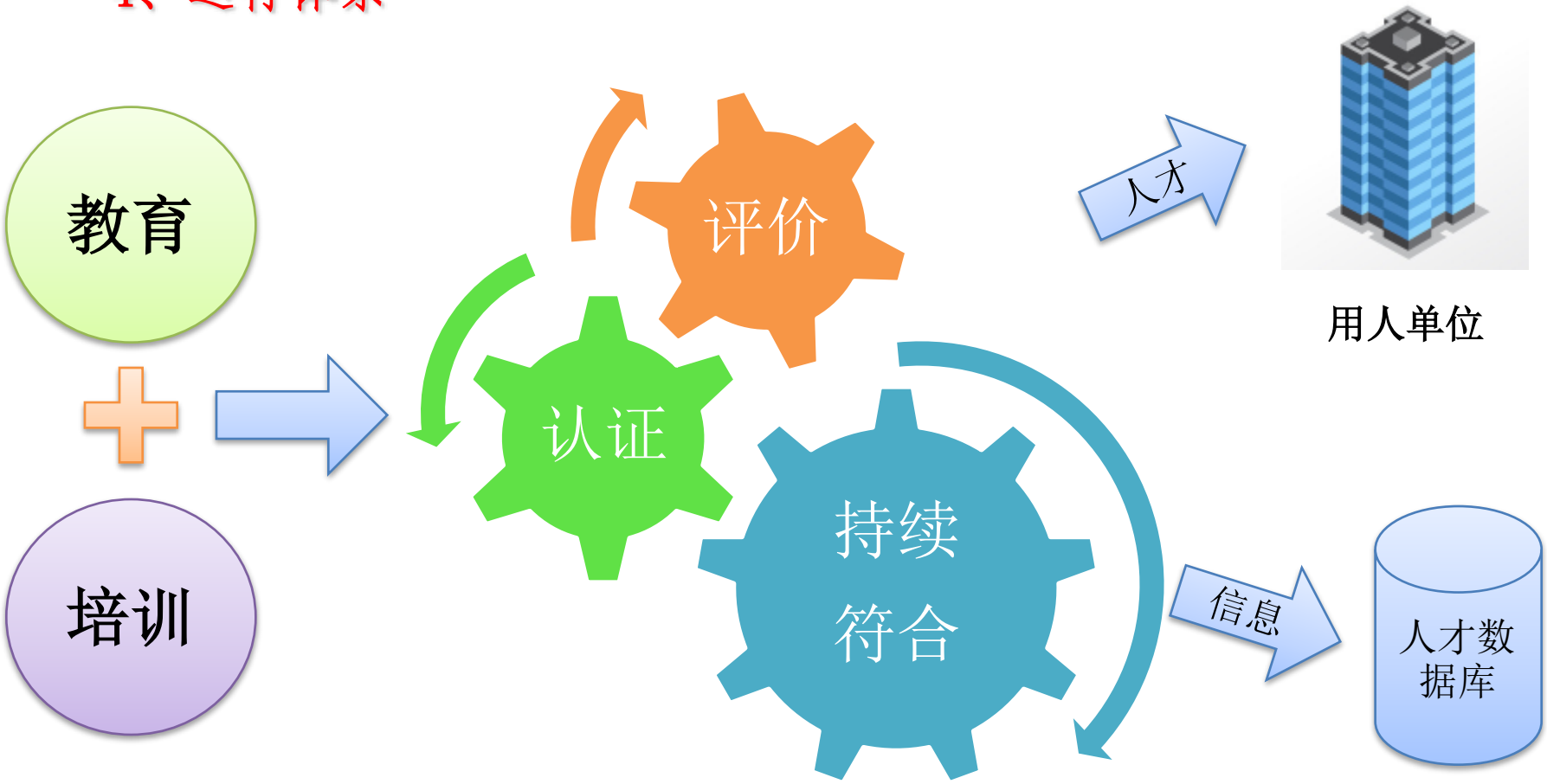
三、体系框架和主要内容

3、组织体系：多方合作、统一监管



三、体系框架和主要内容

4、运行体系



三、体系框架和主要内容

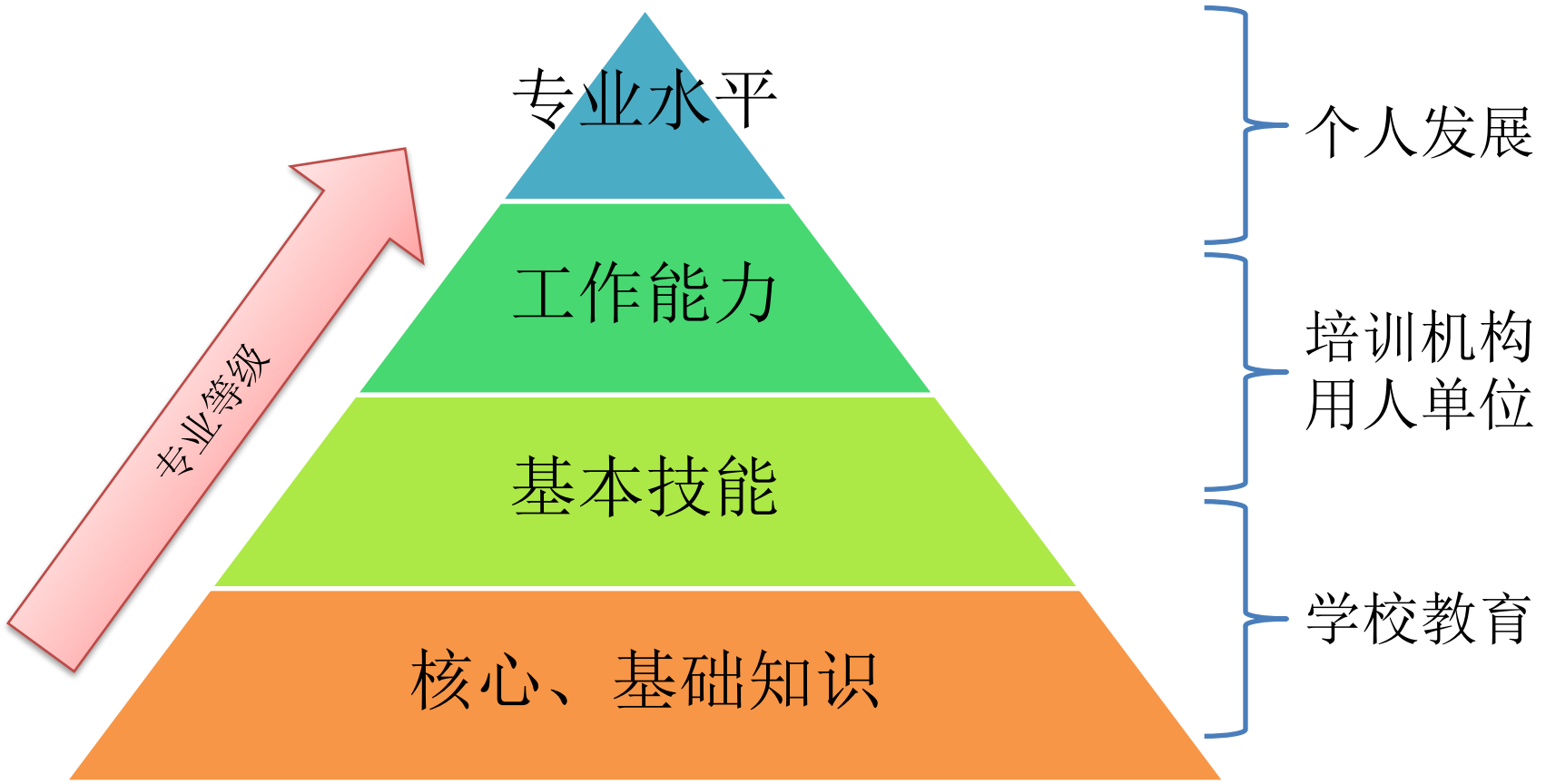
5、评价目标：满足岗位需求

工作岗位：网络安全工程师

工作职责：	知识要求：	技能要求：	能力要求：
网络配置与优化 网络备份与恢复 网络连接问题诊断 网络设备安全与维护 网络性能监测 网络补丁修复 网络故障恢复	网络通信基础 网络安全基础 网络通信协议 网络系统工程 ……	网络性能分析 路由表建立 网络性能优化 常用网络工具 ……	工作完成效果 工作完成水平

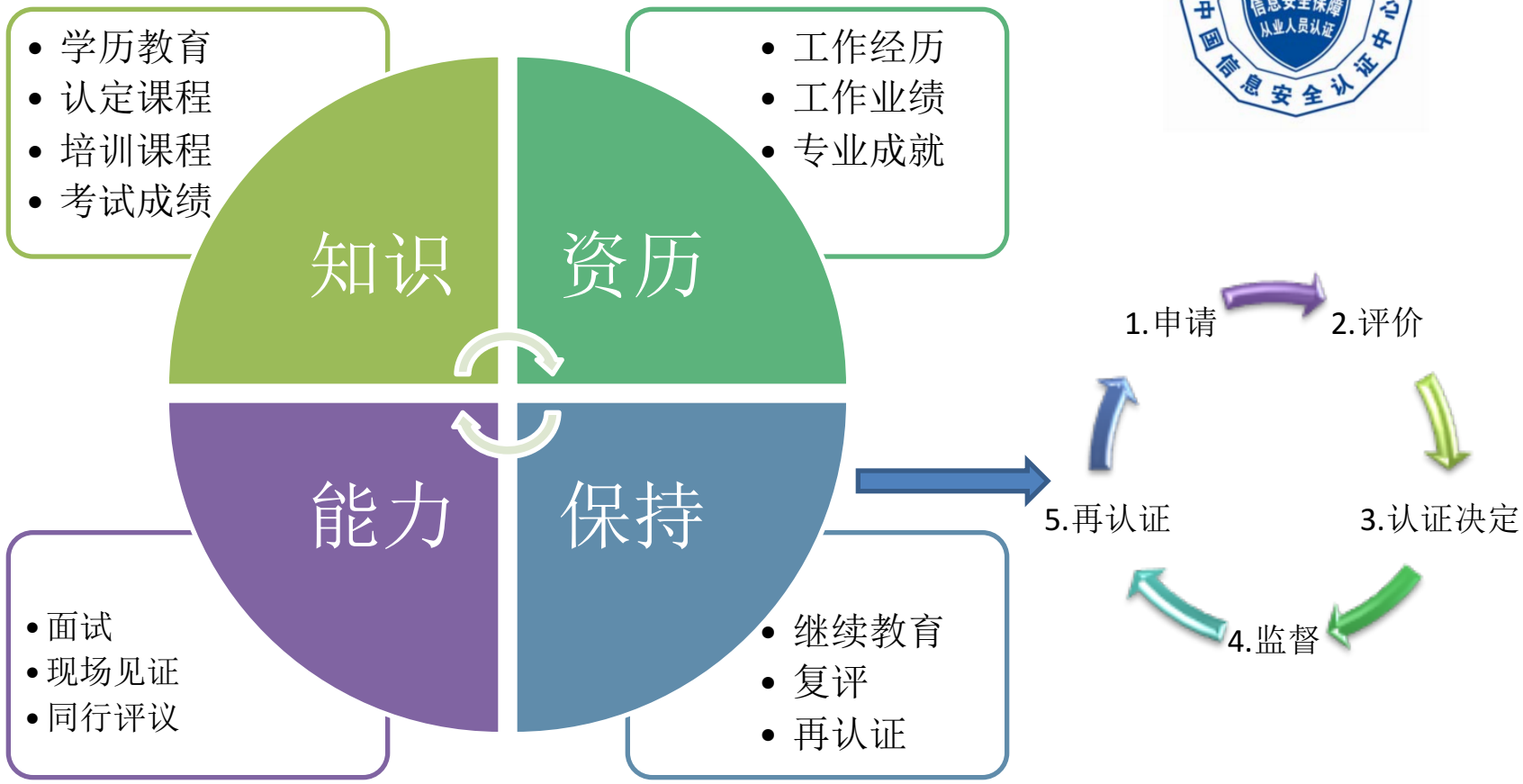
三、体系框架和主要内容

6、评价内容：涵盖知识、技能、能力



三、体系框架和主要内容

7、评价体系：符合人员评价国际标准



三、体系框架和主要内容

8、人员认证基本概念

人员认证：一种提供保证的方法，它通过对获得认证人员的能力进行评估、随后监督和定期复评这个全球承认的过程，表明获得认证的人员满足特定行业、岗位的标准要求。

人员认证与资格确认的区别：在技术创新不断加速、职业细分更趋专业和全球化程度日益提高的情况下，采用人员认证的方式可以有效弥补对人员教育和培训方面的差异，而对于与公共服务、官方或政府运作有关的职位，可能仍有必要采用资格确认的方式。

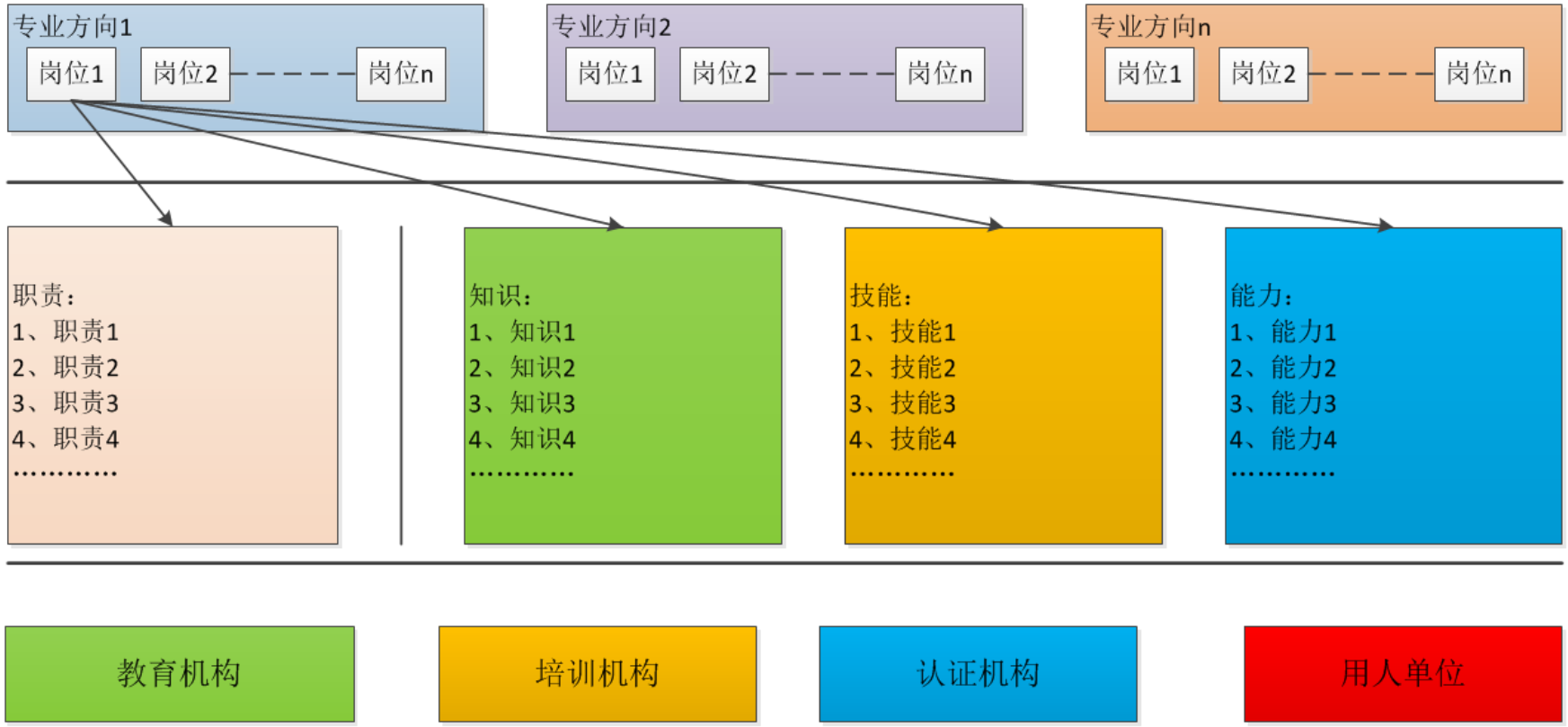
三、体系框架和主要内容

9、人员认证规范性、有效性的保证

- 认证机构需得到认监委批准，并接受监管；
- GB/T27024/ISO/IEC17024对人员认证机构有详细的要求：
  - 对认证机构的要求（包括组织机构要求，认证制度的开发和保持，管理体系要求，对分包、记录、保密、安全的要求）；
  - 对认证机构聘用人员的要求（特别是对考核员的要求）；
  - 对认证过程的要求（包括申请、评价、认证决定、监督、再认证，以及证书标志的使用）。

三、体系框架和主要内容

10、体系的核心内容：统一的话语体系



三、体系框架和主要内容

10.1、明确岗位需求和定义

三、体系框架和主要内容

10.2 根据岗位需求确定评价内容和方法

三、体系框架和主要内容

建设方案：

在“十三五”期间，逐步推进完成以下工作：

1、建立网络安全从业人员能力评价认证标准体系；

2、建设网络安全人才教育、培训、认证机构能力；

3、建设网络安全从业人员能力评价与认证组织体系；

4、开展网络安全从业人员能力评价与认证试点；

5、推广网络安全从业人员能力评价与认证，各部门采信。

三、体系框架和主要内容

工作基础：

- 2003年，《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发27号文）要求“规范和加强信息安全产品测评认证工作”。
- 2004年，原国信办、质检总局、认监委、公安部等8部委《关于建立国家信息安全产品认证认可体系的通知》（国认证联57号），要求建立统一的信息安全产品认证认可体系。
- 2006年6月，中编办批复设立中国信息安全认证中心。国家质检总局直属事业单位。

三、体系框架和主要内容

工作基础：我国信息安全认证认可制度与体系——产品认证

- 2008年1月，质检总局和认监委发布了《关于部分信息安全产品实施强制性认证的公告》（2008年第7号），宣布自2009年5月1日起，对部分信息安全产品实施强制性认证。
- 2009年4月27日，按照国务院领导的批示精神，质检总局、财政部和认监委联合发布了《关于调整信息安全产品强制性认证实施要求的公告》（2009年第33号），宣布将信息安全产品认证的实施时间延至2010年5月1日，在政府采购法规定的范围内强制实施。

三、体系框架和主要内容

工作基础：我国信息安全认证认可制度与体系——产品认证

➢ 国家信息安全产品认证目录（8类13种）

大类	小类
1、边界安全	1）防火墙
	2）网络安全隔离卡与线路选择器
	3）安全隔离与信息交换产品
2、通信安全	4）安全路由器
3、身份鉴别与访问控制	5）智能卡COS
4、数据安全	6）数据备份与恢复产品
5、基础平台	7）安全操作系统
	8）安全数据库系统
6、内容安全	9）反垃圾邮件产品
7、评估审计与监控	10）入侵检测系统（IDS）
	11）网络脆弱性扫描产品
	12）安全审计产品
8、应用安全	13）网站恢复产品

三、体系框架和主要内容

工作基础：我国信息安全认证认可制度与体系——管理体系认证

- 2010年8月12日，工业和信息化部、国家质量监督检验检疫总局、中国人民银行、国务院国有资产监督管理委员会、国家保密局、国家认证认可监督管理委员会联合发布《关于加强信息安全管理体系认证安全管理的通知》（工信部联协[2010]394号），加强对国有机构信息安全管理体系认证的监督管理。
- 中心作为主要单位参与业务连续性国际标准的转化工作，近期即将推出业务连续性管理体系认证。

三、体系框架和主要内容

工作基础：我国信息安全认证认可制度与体系——服务认证

- 2007年8月22日，国家认证认可监督管理委员会批准中国信息安全认证中心开展信息安全服务认证和培训试点工作。
- 制定供应链安全评价规范，并在华为等国内知名企业开展试点工作。

三、体系框架和主要内容

工作基础：信息安全认证业务体系

信息安全产品认证

- 国家信息安全产品认证
- 无线局域网产品认证
- IT产品信息安全认证
- 非金融机构支付业务设施认证
- 信息技术设备CCC认证
- XBRL可交换商业报表语言认证

信息安全管理体系认证

- 信息安全管理体系认证
- 信息技术服务管理体系认证
- 数据中心服务能力成熟度评价

1 2 3 4

信息安全服务资质认证

- 信息安全风险评估
- 信息安全应急处理
- 信息系统安全集成
- 灾难备份与恢复

信息安全培训和人员认证

- 审核员评审员检查员培训
- 信息安全意识公益培训
- 信息安全从业保障人员认证

三、体系框架和主要内容

信息安全人员认证方案

- 认证对象：正式人员+预备人员；
- 专业方向：覆盖技术和管理两方面，包括安全软件、安全集成、安全管理、安全运维、政务安全、服务管理、风险管理、网络攻防、业务连续性等9个专业方向。

认证类型	级别	认证要求
专业认证	III级（专业高级）	专业课程（二级）+附加课程
	II级（专业级）	通用课程（二级）+专业课程（一级）
资格认证	I级（基础级）	基础课程+通用课程（一级）
预备认证	预备级	大专院校认定课程+基础课程+通用课程（一级）

三、体系框架和主要内容

信息安全人员认证适用范围

序号	认证专业方向	适合人员
0	预备人员（CP）	在校大学生、研究生
1	保障基础(FP)	所有信息安全保障人员
2	安全软件(SS)	软件开发相关管理与技术人员
3	安全集成(SI)	系统集成相关管理与技术人员
4	安全管理(SM)	所有信息安全保障人员
5	安全运维(SO)	网络、系统、桌面等安全管理与技术人员
6	安全咨询(SC)	提供安全咨询服务相关的管理与技术人员
7	风险管理(RM)	集成、咨询和运维相关管理与技术人员
8	应急服务(ER)	网络、系统、风险等相关管理与技术人员
9	灾备服务(DR)	网络、系统、风险等相关管理与技术人员
10	业务连续性(BC)	集成、咨询、运维和风险相关管理与技术人员

三、体系框架和主要内容

信息安全人员认证认定课程

课程设计原则

1、考虑与学校课程的衔接；

2、面向实际应用场景；

3、面向工作岗位需求；

4、满足特定安全要求。

课程编号	课程名称
01	计算机原理
02	操作系统
03	计算机网络基础
04	数据通信原理
05	密码学
06	网络安全协议与标准
07	信息安全导论
08	计算机病毒理论与防治技术
09	防火墙技术
10	操作系统安全分析
11	数字鉴别及认证系统
12	网络安全检测与防范技术

三、体系框架和主要内容

信息安全人员认证培训课程

基础课程：

1. 《信息安全保障人员基本素质教育》
2. 《信息安全意识教育》
3. 《信息安全法律法规体系》
4. 《风险管理基础》

通用课程：

1. 《项目管理基础》
2. 《信息安全技术》
3. 《信息安全实验》

三、体系框架和主要内容

信息安全人员认证培训课程

专业课程：

1. 《安全软件技术与测试》
2. 《信息系统安全集成》
3. 《信息安全管理》
4. 《安全运维技术与应用》
5. 《安全咨询》
6. 《风险管理》
7. 《应急服务技术与应用》
8. 《灾难备份技术与应用》
9. 《业务连续性管理》

附加课程：

1. 《通信技术基础》
2. 《管理体系审核》
3. 《渗透测试技术与应用》

谢 谢！