ICS 01.040.35
F10/19
备案号：43660-43670

RR

中华人民共和国认证认可行业标准

RB/T 202—2013

信息安全保障人员认证准则

Certification requirements for information security assurance professional

2013-12-02 2014-06-15 实施

中华人民共和国国家质量监督检验检疫总局

中国国家认证认可监督管理委员会 发布

目　录

前　言

本标准按照GB/T 1.1—2009的给出规则起草。

本标准由国家认证认可监督管理委员会提出并归口。

本标准起草单位：中国信息安全认证中心、中华人民共和国国家质量监督检验检疫总局标准与技术法规研究中心。

本标准主要起草人：张剑、段静辉、宋志刚、徐然、郑莹、毛作奎、张斌。

信息安全保障人员认证准则

1 范围

本标准规定了信息安全保障人员认证的专业方向、级别和资格要求。

本标准适用于对信息安全保障人员进行认证考试和认证。

本标准不适用于对认证审核人员进行注册。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 27024 合格评定 人员认证机构通用要求

3 术语和定义

GB/T 27024 界定的以及下列术语和定义适用于本文件。

3.1

信息安全保障人员 information security assurance professional

从事信息安全相关工作的所有人员，如组织的管理人员（包括CIO、CSO、科技管理部门和风险控制管理部门的人员）、IT 相关的技术人员（包括运维、开发和集成人员），从事信息安全服务组织的技术人员（包括信息安全产品研发人员、信息安全咨询人员、信息安全服务实施人员和外派服务人员）。

3.2

认证专业方向 certified professional field

按照信息安全保障的技术方向划分的专业方向，并依据其对开展人员认证。

3.3

获证人员 certified applicant

通过信息安全保障人员认证考试和认证评价，获得或保持信息安全保障人员认证证书的人员。

3.4

工作经历 occupational history

取得相应学历后的所有工作历史，无论是有偿的还是无偿的，全职的还是兼职的，不包括实习经历。

4 认证专业方向与级别

信息安全保障人员认证专业方向和级别设置如表1所示。

信息安全保障人员认证分为预备认证、资格认证(基础级)和专业认证(专业级和专业高级)。信息安全保障人员级别从低到高依次分为预备级、Ⅰ级（基础级）、Ⅱ级（专业级）、Ⅲ级（专业高级）4个级别。其中Ⅱ级（专业级）、Ⅲ级（专业高级）设置认证专业方向，分别为：安全软件、安全集成、安全管理、安全运维、安全咨询、风险管理、应急服务、灾备服务、业务连续性（参见附录A）。

表1. 认证专业方向设置表

类型	级别	专业方向								
专业认证	Ⅲ级(专业高级) Ⅱ级（专业级）	安全软件	安全集成	安全管理	安全运维	安全咨询	风险管理	应急服务	灾备服务	业务连续性
资格认证	Ⅰ级（基础级）	保障基础								
预备认证	预备级	预备人员								

5 认证要求

5.1 基本要求

获证人员应满足如下基本要求：

a) 具有独立的民事行为能力，具备承担法律责任的能力；
b) 未受过刑事处罚；
c) 不存在法律法规禁止从业的情形；
d) 自愿遵守颁布的信息安全保障人员认证相关文件的有关规定，履行相关义务；
e) 符合有关法律法规的规定。

5.2 初次申请资格条件

5.2.1 教育及工作经历

5.2.1.1 预备人员认证资格要求

获证人员应满足下面要求：

a) 教育部发布的“具有普通高等学历教育招生资格的高等学校名单”中“普通本科院校”在校本科生或全国研究生招生计划中研究生招生单位在校研究生；
b) 通过 4 门以上经认定的考试课程(参见附录 B)考试。

5.2.1.2 基础级认证工作经历要求

获证人员应至少满足下面一项要求：

a) 本科（含）以上学历， 1 年以上从事信息安全有关工作经历；
b) 专科毕业，3 年以上从事信息安全有关的工作经历；
c) 5 年以上从事信息安全有关的工作经历；
d) 具有信息技术相关专业的初级技术职称,并且至少 1 年以上从事信息安全保障相关工作经历（表 1 中任意一个认证专业方向的工作经历均可）。

5.2.1.3 专业级认证工作经历要求

获证人员应至少满足下面一项要求：

a) 硕士研究生（含）以上学历，2 年以上从事信息安全有关工作经历，并且至少 1 年从事与申请认证专业方向相关的工作经历；
b) 本科毕业，4 年以上从事信息安全有关工作经历，并且至少 2 年以上从事与申请认证专业方向相关的工作经历；
c) 专科毕业，6 年以上从事信息安全有关工作经历，并且至少 2 年以上从事与申请认证专业方向相关的工作经历；
d) 7 年以上从事信息安全有关工作经历，并且至少 2 年以上从事与申请认证专业方向相关的工作经历；
e) 具有信息技术相关专业的中级技术职称，并且从事至少 2 年以上与申请认证专业方向相关的工作经历。

5.2.1.4 专业高级认证工作经历要求

获证人员应至少满足下面一项要求：
a) 硕士研究生（含）以上学历， 3 年以上从事信息安全有关工作经历，并且至少 2 年以上从事与申请认证专业方向相关的工作经历；
b) 本科毕业，5 年以上从事信息安全有关工作经历，并且至少 3 年以上从事与申请认证专业方向相关的工作经历；
c) 专科毕业，7 年以上从事信息安全有关工作经历，并且至少 3 年以上从事与申请认证专业方向相关的工作经历；
d) 8 年以上从事信息安全有关工作经历，并且至少 3 年以上从事与申请认证专业方向相关的工作经历；
e) 具有信息技术相关专业的高级技术职称，并且至少 3 年以上从事与申请认证专业方向相关的工作经历。

5.2.2 培训要求

获证人员应完成其申请的认证专业方向和相应级别认证考试要求的技术知识和应用能力培训。

5.2.3 考试要求

获证人员应满足下面要求：
a) 通过其申请的认证专业方向和相应级别的认证考试（要求参见附录 C），包括笔试和实验；
b) 必要时，通过由认证机构组织的专家面试；
c) 必要时，通过由认证机构组织的工作现场见证。

5.3 扩展认证专业方向资格要求

获证人员应满足下面要求：
a) 已通过信息安全保障人员认证其中一个认证专业方向认证；
b) 具有至少 1 年与所扩展认证专业方向相关的工作经历；
c) 完成其申请的认证专业方向和相应级别所要求的认证考试要求的技术知识和应用能力培训；
d) 通过相应认证专业方向和相应级别的认证考试。

5.4 再认证资格要求

获证人员应满足下面要求：

a) 已通过信息安全保障人员认证，且在认证有效期内；

b) 获证后 3 年内至少有 2 年的工作经历与获得认证的专业方向相关；

c) 每年不少于 16h 的信息安全相关专业的持续发展课程学习。

5.5 认证升级资格要求

获证人员应满足下面要求：

a) 已通过信息安全保障人员认证，且在认证有效期内；

b) 满足信息安全保障人员认证高一级别认证要求，包括工作经历、培训和考试要求。

5.6 预备人员转正资格要求

获证人员应满足下面要求：

a) 已通过信息安全保障人员认证预备级认证，且在认证有效期内；

b) 从事信息安全保障相关工作（表 1 中任意一个认证专业方向的工作经历均可）1 年。

注：转正时申请更换的信息安全保障人员认证证书为基础级证书。

附 录 A
（资料性附录）
信息安全保障人员认证分类分级

A.1 认证专业方向

信息安全保障人员按照信息安全保障的技术方向进行分类，依据能力要求进行分级。信息安全保障人员认证专业方向设置见表 1。

A.2 认证专业方向适合人员

认证专业方向适合人员说明见表 A.1。

表 A.1 认证专业适用人员

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

附 录 B
（资料性附录）
认定的预备人员考试课程

参考目前大专院校信息技术和信息安全相关专业的课程设置，采用表 B.1 中的 12 门课程作为认定的考试课程。此外，开展培训工作的院校可以推荐表 B.1 之外的相关课程，如通过评审，可以增补为认定的考试课程。

表 B.1 认定的考试课程表

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
注：预备人员至少从 01～04 号课程中选择 1 门和 05～12 号课程中选择 3 门进行考试。	

附 录 C
（资料性附录）
认证考试基本要求

C.1 认证考试科目

认证考试科目如表C.1 所示。

考试科目分为4类：基础类、通用类、专业类和附加类。其中，基础类和附加类不分级别。通用类分为两个级别:I 级和II级，专业类分为II级和III级，分别代表对相关内容掌握的程度，II级高于I级， III级高于II级。

表C.1 考试科目表

编号	考试科目名称	科目分类
B01	信息安全保障人员基本素质教育	基础类
B02	信息安全意识教育	基础类
B03	信息安全法律法规体系	基础类
B04	风险管理基础	基础类
G01	项目管理基础	通用类
G02	信息安全技术	通用类
G03	信息安全实验	通用类
P01	安全软件技术与测试	专业类
P02	信息系统安全集成	专业类
P03	信息安全管理	专业类
P04	安全运维技术与应用	专业类
P05	安全咨询	专业类
P06	风险管理	专业类
P07	应急服务技术与应用	专业类
P08	灾备服务技术与应用	专业类
P09	业务连续性管理	专业类

表 C.1（续）

序号	考试科目名称	科目分类
A01	通信技术基础	附加类
A02	管理体系审核	附加类
A03	渗透测试技术与应用	附加类

C.2 考试科目内容

各科目的考试内容如表 C.2 所示。

表 C.2　各考试科目内容

序号	科目名称	科目内容
B01	信息安全保障人员基本素质教育	1. 职业素养 2. 知识结构 3. 工作技能
B02	信息安全意识教育	1. 信息安全保障概念 2. 信息安全形势 3. 信息安全需求识别
B03	信息安全法律法规体系	1. 法律法规结构体系 2. 国内外信息安全法律法规建设概况 3. 国内外信息安全标准建设概况 4. 国内信息安全管理概况 5. 典型信息安全法律法规
B04	风险管理基础	1. 基本概念 2. 常见风险评估方法 3. 典型的风险评估方法 4. 风险处置方法 5. 风险管理相关标准
G01	项目管理基础	1. 项目管理基本概念 2. 项目管理的发展历史与现状 3. 九大项目管理知识领域 4. 开发类项目管理技巧 5. 集成类项目管理技巧
G02	信息安全技术	1. 信息安全技术发展 2. 密码学及其应用 3. 网络安全技术 4. 平台安全技术 5. 应用安全技术 6. 数据安全技术 7. 物理安全技术

表 C.2（续）

序号	考试科目名称	考试内容
G03	信息安全实验	1. 实验平台构建 2. 网络基础实验 3. 主机安全实验 4. 数据库安全实验 5. 密码学与加解密实验 6. 访问控制实验 7. 攻击技术实验 8. 主动防御技术实验 9. 安全管理实验
P01	安全软件技术与测试	1. 安全软件的业界标准与实践 2. 安全开发生命周期 3. 安全软件开发环境管理 4. 安全功能架构与设计 5. 安全漏洞分析 6. 安全编码 7. 密码安全模块 8. 安全测试与实验
P02	信息系统安全集成	1. 安全集成的业界标准与实践 2. 安全集成过程 3. 安全集成工具使用 4. 典型安全保障手段 5. 安全集成实例
P03	信息安全管理	1. 安全管理的业界标准与实践 2. 安全管理的实施过程 3. 安全管理工具使用 4. 典型安全保障手段 5. 安全管理实例 6. 风险管理
P04	安全运维技术与应用	1. 业界标准与实践 2. 安全运维结构与思想 3. 安全运维工具使用 4. 安全运维实例
P05	安全咨询	1. 安全相关标准 2. 咨询的过程管理 3. 安全方案设计 4. 安全咨询工具的使用 5. 安全咨询知识库管理 6. 典型咨询案例分析

表 C.2（续）

序号	考试科目名称	考试内容
P06	风险管理	1. 风险管理的业界标准与实践 2. 风险管理的实施过程 3. 风险管理工具使用 4. 典型风险处置措施 5. 风险管理实例
P07	应急服务技术与应用	1. 应急服务的相关规范 2. 应急服务过程管理 3. 安全技术工具的使用 4. 典型应急案例分析
P08	灾备服务技术与应用	1. 灾备服务的业界标准与实践 2. 灾备恢复技术 3. 灾备服务过程管理 4. 灾备工具使用与管理 5. 灾备实例分析
P09	业务连续性管理	1. 业务连续性的业界标准与实践 2. 业务连续性管理结构与思想 3. 业务连续性管理环节 4. 业务连续性管理程序与计划 5. 业务连续性管理实例
A01	通信技术基础	1. 通信的基本概念 2. 通信协议及应用 3. 安全通信协议
A02	管理体系审核	1. 审核的基本概念 2. 审核的基本流程 3. 审核的基本方法 4. 审核员的管理与能力要求
A03	渗透测试技术与应用	1. 渗透测试的基本概念 2. 渗透测试法律问题 3. 渗透测试方法论 4. 实施渗透测试与报告撰写 5. Unix 渗透测试方法与工具使用 6. Windows 系统渗透测试方法与工具使用 7. Web 应用系统渗透测试方法与工具使用 8. 数据库渗透测试与工具使用

C.3 各认证级别和专业方向的考试要求

各认证级别和专业方向的考试要求见表 C.3~C.21。

表 C.3　基础级要求

科目名称	科目内容考试范围
信息安全保障人员基本素质	全部
信息安全意识教育	全部
信息安全法律法规体系	全部
风险管理基础	全部
项目管理基础（Ⅰ级）	全部
信息安全技术（Ⅰ级）	1、3、7 必选， 2、4、5、6 任选 2 个以上

表 C.4 《安全软件专业级》要求

考试科目名称	选择范围
项目管理基础（Ⅱ级）	全部
信息安全技术（Ⅰ级）	2、5、6
安全软件技术与测试（Ⅱ级）	全部
信息安全实验（Ⅰ级）	任选 3 个以上

表 C.5 《安全软件专业高级》要求

考试科目名称	选择范围
信息安全技术（Ⅱ级）	2、5、6
安全软件技术与测试（Ⅲ级）	全部
信息安全实验（Ⅱ级）	任选 2 个以上

表 C.6 《安全集成专业级》要求

考试科目名称	选择范围
项目管理基础（Ⅱ级）	全部
信息安全技术（Ⅰ级）	全部
安全集成（Ⅱ级）	全部
通信技术基础	全部
信息安全实验（Ⅰ级）	任选 3 个以上

表 C.7 《安全集成专业高级》要求

考试科目名称	选择范围
信息安全技术（Ⅱ级）	全部
安全集成（Ⅲ级）	全部
通信技术基础	全部
信息安全实验（Ⅱ级）	任选 2 个以上

表 C.8 《安全管理专业级》要求

考试科目名称	选择范围
项目管理基础（Ⅱ级）	全部
信息安全技术（Ⅰ级）	1、3、4、7
安全管理（Ⅱ级）	全部
安全管理实验（Ⅰ级）	安全管理实验

表 C.9 《安全管理专业高级》要求

考试科目名称	选择范围
信息安全技术（Ⅱ级）	1、3、4、7
安全管理（Ⅲ级）	全部
管理体系审核	全部
安全管理实验（Ⅱ级）	安全管理实验

表 C.10 《安全运维专业级》要求

考试科目名称	选择范围
项目管理基础（Ⅱ级）	全部
信息安全技术（Ⅰ级）	1、3、4、7
安全运维技术与应用（Ⅱ级）	全部
信息安全实验（Ⅰ级）	任选 3 个以上

表 C.11 《安全运维专业高级》要求

考试科目名称	选择范围
信息安全技术（Ⅱ级）	1、3、4、7
安全运维技术与应用（Ⅲ级）	全部
信息安全实验（Ⅱ级）	任选 2 个以上

表 C.12 《安全咨询专业级》要求

考试科目名称	选择范围
项目管理基础（Ⅱ级）	全部
信息安全技术（Ⅰ级）	全部
安全咨询（Ⅱ级）	全部
通信技术基础	全部

表 C.13 《安全咨询专业高级》要求

考试科目名称	选择范围
信息安全技术（Ⅱ级）	全部
安全咨询（Ⅲ级）	全部
通信技术基础	全部

表 C.14 《风险管理专业级》要求

考试科目名称	选择范围
项目管理基础（Ⅱ级）	全部
信息安全技术（Ⅰ级）	3、4、5、6
风险管理（Ⅱ级）	全部
通信技术基础	全部
信息安全实验（Ⅰ级）	任选 3 个以上

表 C.15 《风险管理专业高级》要求

考试科目名称	选择范围
信息安全技术（Ⅱ级）	3、4、5、6
风险管理（Ⅲ级）	全部
通信技术基础	全部
信息安全实验（Ⅱ级）	任选 2 个以上

表 C.16 《应急服务专业级》要求

考试科目名称	选择范围
项目管理基础（Ⅱ级）	全部
信息安全技术（Ⅰ级）	3、4
应急服务技术与应用（Ⅱ级）	全部
通信技术基础	全部
渗透测试技术与应用	全部
信息安全实验（Ⅰ级）	任选 3 个以上

表 C.17 《应急服务专业高级》要求

考试科目名称	选择范围
信息安全技术（Ⅱ级）	3、4
应急服务技术与应用（Ⅲ级）	全部
通信技术基础	全部
渗透测试技术与应用	全部
信息安全实验（Ⅱ级）	任选 2 个以上

表 C.18 《灾备服务专业级》要求

考试科目名称	选择范围
项目管理基础（Ⅱ级）	全部
信息安全技术（Ⅰ级）	3、4、6、7
灾备服务技术与应用（Ⅱ级）	全部
信息安全实验（Ⅰ级）	任选 3 个以上

表 C.19 《灾备服务专业高级》要求

考试科目名称	选择范围
信息安全技术（Ⅱ级）	3、4、6、7
灾备服务技术与应用（Ⅲ级）	全部
信息安全实验（Ⅱ级）	任选 2 个以上

表 C.20 《业务连续性专业级》要求

考试科目名称	选择范围
项目管理基础（Ⅱ级）	全部
信息安全技术（Ⅰ级）	3、4、6、7
业务连续性管理（Ⅱ级）	全部
信息安全实验（Ⅰ级）	任选 3 个以上

表 C.21 《业务连续性专业高级》要求

考试科目名称	选择范围
信息安全技术（Ⅱ级）	3、4、6、7
业务连续性管理（Ⅲ级）	全部
信息安全实验（Ⅱ级）	任选 2 个以上