ICS 35.040

L 80

ZJXTJC

团　　体　　标　　准

T/ZJXTJC 002-2020

信息安全服务 人员能力评估标准

Information security service

— Assessment criteria for personnel capability

(正式稿)

2020－06－01 发布　　2020－07－01 实施

浙江省计算机信息系统集成行业协会　发布

目　录

前　言

本标准依据GB/T 1.1-2009给出的规则起草。

本标准由浙江省计算机信息系统集成行业协会提出并归口管理。

本标准由浙江省计算机信息系统集成行业协会牵头组织制定。

本标准主要起草单位：浙江省计算机信息系统集成行业协会、浙江省标准化协会、奇安信科技集团股份有限公司、深圳深信服科技股份有限公司、杭州安恒信息技术股份有限公司

本标准主要起草人： 金承钰、凌伟、廉清云、陈蕴韵、裘丹娜、张晓燕、潘金日、丁晓钟、陆新宁、毛祥根、钱高平、凌繁荣、卢文康、胡利军、刘蓝岭、张韵、向海涛、杨辉、曾希雯

本标准由浙江省计算机信息系统集成行业协会负责解释。

引　言

本标准是对提供信息安全服务的组织进行能力评估，在编制过程中考虑到省内环境与信息安全行业的实际情况，同时结合GB/T 32914-2016、GB/T 37696-2019等国家或行业标准制定而成。

信息安全服务 人员能力评估标准

1 范围

本标准规定了对信息安全服务提供方的从业人员服务能力通用等级要求。

本标准适用于评估组织和监管部门对信息安全服务提供方的服务人员能力进行评估，也为信息安全服务提供方对其自身从业人员的能力的改善提供指导，同样对信息安全服务需求方具有参考意义。

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 32914-2016 信息安全技术 信息安全服务提供方管理要求

GB_T 37696-2019 信息技术服务 从业人员能力评价要求

RB_T 202-2013 信息安全保障人员认证准则

SJ／T 11623-2016 信息技术服务从业人员能力规范

YD_T 1621-2007 网络与信息安全服务资质评估准则

3 术语和定义

GB/T 37696-2019所界定的以及下列术语和定义适用于本文件。

4 信息安全服务人员分类及等级

4.1 服务人员分类

信息安全服务人员基于信息安全服务行业的业务形态、发展及应用规律，结合《信息安全服务 人员能力评估标准》，分类见表1下：

表 1 信息安全服务人员类别

序号	信息安全服务人员类别
1	风险评估服务人员
2	系统集成服务人员
3	系统运维服务人员
4	应急处理服务人员

4.2 服务人员基本要求

信息安全服务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服务人员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。

4.3 服务人员资格等级及要求

在人员分类的基础上，根据信息安全服务行业发展的需求以及从业人员的职业发展客观规律，将从业人员资格分为技术及管理两个等级标准。其中技术等级划分为高级工程师、工程师、助理工程师、技术员四个资格级别，管理等级划分为高级项目经理及项目经理两个资格级别。具体要求见表2和表3：

表 2 技术等级资格要求

资格级别	技术等级资格要求
高级工程师	有运用服务类别所需的知识和技能，独立完成高度复杂的工作，精通关键的专业技能，并在专业方面有所创新，能够在专业领域内提供有效的专业技能指导，具有资深的工作经验。
工程师	能运用服务类别所需的知识和技能，独立完成较为复杂的工作，具备指导他人工作的能力，具有一定的工作经验。
助理工程师	能运用服务类别所需的知识和技能，在他人的指导下完成所承担的工作，并具有一定独立工作能力，具有一定的实践经历。
技术员	能运用服务类别所需的知识和技能，在他人的指导下完成所承担的工作。

表 3 管理等级资格要求

资格级别	管理等级资格要求
高级项目经理	有较全面的信息安全服务所需的知识和技能，有较强的沟通协调及团队管理能力，有丰富的项目管理工作经验，能够独立承担大、中型项目的管理工作。
项目经理	有信息安全服务所需的知识和技能，有一定的沟通协调及团队管理能力，有一定的参与项目管理工作经历。

5 人员能力技术等级资格评估要求

信息安全服务人员能力技术资格从知识、技能和经验三个方面进行评估。

5.1 高级工程师

5.1.1 知识要求

a) 掌握信息安全服务相关的通用知识，主要包括贯穿整个信息服务活动的基本理论和基本知识。
b) 精通服务类别相应工作所必备的知识，主要指与服务类别要求相适应的理论知识、技术要求和操作规程等。
c) 掌握服务人员应具备的职业道德常识，相关标准与规范知识，以及有关法律法规、安全和环境保护知识等。

5.1.2 技能要求

a) 熟练应用信息安全服务相关的通用知识及专业知识，能够针对服务类别相应工作给出专家级的意见，具备能够独立完成服务类别工作任务的能力，能带领其他人成功地完成工作任务。
b) 拥有独立完成信息安全服务所应具备的行为特征和综合素质等软技能，包括沟通、协调等，且能熟练应用。

5.1.3 经验要求

具有与服务类别一致的领导他人成功运作的经验，有咨询、改进或创新的经验，并将经验系统化，主导制度和体系的制定与推广。同时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 2 年以上从事与服务类别相关的工作经历；

b) 本科毕业，5 年以上从事信息安全有关工作经历，并且 3 年以上从事与服务类别相关的工作经历；
c) 专科毕业，7 年以上从事信息安全有关工作经历，并且 3 年以上从事与服务类别相关的工作经历；
d) 8 年以上从事信息安全有关工作经历，并且 3 年以上从事与服务类别相关的工作经历；
e) 具有信息技术相关专业的高级技术职称，并且 3 年以上从事与服务类别相关的工作经历。

5.2 工程师

5.2.1 知识要求

a) 掌握信息安全服务相关的通用知识，主要包括贯穿整个信息服务活动的基本理论和基本知识。
b) 掌握服务类别相应工作所必备的知识，主要指与服务类别要求相适应的理论知识、技术要求和操作规程等。
c) 理解服务人员应具备的职业道德常识，相关标准与规范知识，以及有关法律法规、安全和环境保护知识等。

5.2.2 技能要求

a) 熟练应用信息安全服务相关的通用知识及专业知识，具备能够独立完成服务类别工作任务的能力，能带领其他人有效地完成工作任务。
b) 拥有独立完成信息安全服务所应具备的行为特征和综合素质等软技能，包括沟通、协调等，且能较熟练应用。

5.2.3 经验要求

具有与服务类别一致的领导他人有效运作的经验，参与制度和体系的制定与推广。同时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 1 年以上从事与服务类别相关的工作经历；
b) 本科毕业，4 年以上从事信息安全有关工作经历，并且 2 年以上从事与服务类别相关的工作经历；
c) 专科毕业，6 年以上从事信息安全有关工作经历，并且 2 年以上从事与服务类别相关的工作经历；
d) 7 年以上从事信息安全有关工作经历，并且 2 年以上从事与服务类别相关的工作经历；
e) 具有信息技术相关专业的中级技术职称，并且 2 年以上从事与服务类别相关的工作经历。

5.3 助理工程师

5.3.1 知识要求

a) 理解信息安全服务相关的通用知识，主要包括贯穿整个信息服务活动的基本理论和基本知识。
b) 理解服务类别相应工作所必备的知识，主要指与服务类别要求相适应的理论知识、技术要求和操作规程等。
c) 理解服务人员应具备的职业道德常识，相关标准与规范知识，以及有关法律法规、安全和环境保护知识等。

5.3.2 技能要求

a) 能较熟练应用信息安全服务相关的通用知识及专业知识，具备能够独立工作的能力，且能完成成功地完成大部分工作任务。
b) 拥有一定的完成信息安全服务所应具备的行为特征和综合素质等软技能，包括沟通、协调等。

5.3.3 经验要求

具有与服务类别一致的成功完成工作任务的经历和案例。同时应至少满足下面一项要求：

a) 本科（含）以上学历，2 年以上从事信息安全有关工作经历，并且 1 年以上从事与服务类别相关的工作经历；

b) 专科毕业，3 年以上从事信息安全有关的工作经历，并且 1 年以上从事与服务类别相关的工作经历；

c) 5 年以上从事信息安全有关的工作经历，并且 1 年以上从事与服务类别相关的工作经历；

d) 具有信息技术相关专业的初级技术职称，并且 1 年以上从事与服务类别相关的工作经历。

5.4 技术员

5.4.1 知识要求

a) 理解信息安全服务相关的通用知识，主要包括贯穿整个信息服务活动的基本理论和基本知识。

b) 了解服务类别相应工作所必备的知识，主要指与服务类别要求相适应的理论知识、技术要求和操作规程等。

c) 了解服务人员应具备的职业道德常识，相关标准与规范知识，以及有关法律法规、安全和环境保护知识等。

5.4.2 技能要求

a) 能在他人指导下，应用信息安全服务相关的通用知识及专业知识，有效地完成工作任务。

5.4.3 经验要求

具有参与信息安全服务工作的经历。同时应至少满足下面一项要求：

a) 专科（含）以上学历，1 年以上从事信息安全有关工作经历；

b) 3 年以上从事信息安全有关工作经历，并且 1 年以上从事与服务类别相关的工作经历。

6 人员能力管理等级资格评估要求

信息安全服务人员能力管理资格从技术资格、知识及管理要求、经验等方面进行评估。

6.1 高级项目经理

6.1.1 信息安全服务高级项目经理需取得工程师及以上技术等级资格。

6.1.2 知识及管理要求

a) 熟悉国家和项目所在地的法律、法规和标准规范。

b) 严格执行企业财务制度，加强项目财务管理，严格控制项目成本。

c) 有丰富的项目管理能力，包括项目进度管理、质量控制、需求分析、测试、客户培训、问题反馈收集整理等；

d) 有丰富的资源整合能力，包括人力资源整合能力、行业资源整合能力、沟通协调能力等。

6.1.3 近两年作为项目负责人管理过的项目未发生较大的责任事故。

6.1.4 经验要求

近两年作为项目负责人管理过并已通过验收的项目，应满足下列要求之一。

a) 信息安全服务类别对应二级及以上项目不少于 1 个；

b) 信息安全服务类别对应三级及以上项目不少于 3 个。

6.2 项目经理

6.2.1 信息安全服务项目经理需取得助理工程师及以上技术等级资格。

6.2.2 知识及管理要求

a) 了解国家和项目所在地的法律、法规和标准规范。
b) 执行企业财务制度，加强项目财务管理。
c) 有较强的项目管理能力，包括项目进度管理、质量控制、需求分析、测试、客户培训、问题反馈收集整理等；
d) 有较强的资源整合能力，包括人力资源整合能力、行业资源整合能力、沟通协调能力等。

6.2.3 近两年作为项目负责人管理过的项目未发生较大的责任事故。

6.2.4 经验要求

近两年协助或负责管理并已通过验收的项目，应满足下列要求之一。

a) 信息安全服务类别对应三级及以上项目不少于 1 个；
b) 信息安全服务类别对应四级及以上项目不少于 2 个。

7 能力评估

7.1 能力等级资格评估过程

7.1.1 能力资格评估应按第 5 章、第 6 章要求，结合具体服务类别，建立评价指标体系；

7.1.2 过程要求

a) 应通过申请的服务类别和相应级别的考试，考试形式包括笔试、机试等；
b) 应通过职业履历鉴定；
c) 必要时，通过由评估机构组织的专家面试；
d) 必要时，通过由评估机构组织的工作现场见证。

7.2 扩展服务类别资格要求

a) 已通过信息安全服务人员能力其中一个资格评估；
b) 具有至少 1 年与所扩展服务类别相关的工作经历；
c) 通过相应服务类别和级别的考试。

7.3 能力等级资格再评估要求

a) 已通过信息安全服务人员资格评估，且在有效期内；
b) 获证后 3 年内至少有 2 年的工作经历与获得服务类别相关；
c) 每年不少于 20h 的信息安全相关专业的持续发展课程学习。

7.4 能力等级资格升级要求

a) 已通过信息安全服务人员资格评估，且在有效期内；
b) 满足信息安全服务人员资格高一级别要求。

7.5 能力等级资格的应用

对信息安全服务人员能力资格评估的结果，可作为其能力培养、职业发展以及信息安全服务企业能力评估等活动的依据。

附录 A
（资料性附录）
人员评估考试基本要求

1　人员能力技术等级资格评估考试科目及考试内容，见表 A.1、A.2 所示。

表 A.1　人员评估考试科目及考试内容（通用类）

序号	通用类知识	
	科目名称	考试内容
1	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
2	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
3	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
4	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
5	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
6	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
7	项目管理	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

表 A.2　人员评估考试科目及考试内容（专业类）

序号	信息安全服务类别	专业类知识	
		科目名称	考试内容
1	风险评估	1.1 风险管理	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
		1.2 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
		1.3 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
2	系统集成	2.1 信息安全系统集成	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
		2.2 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
3	系统运维	3.1 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
4	应急处理	4.1 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
		4.2 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
		4.3 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