

中华人民共和国通信行业标准

YD/T 2669-2013

电信网和互联网 第三方安全服务能力评定准则

Evaluation criteria for competence of third party security service
provider in telecon network and internet

2013-10-17 发布

2014-01-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
3.1 术语和定义	1
3.2 缩略语	2
4 电信网和互联网第三方安全服务概述	2
4.1 类型	2
4.2 电信网和互联网第三方安全服务能力等级的评判原则	2
4.3 电信网和互联网安全防护对第三方安全服务能力的要求	3
5 电信网和互联网第三方安全服务能力评定通用性要求	3
6 电信网和互联网第三方安全风险评估服务能力评定要求	3
6.1 丙级能力评定要求	3
6.2 乙级能力评定要求	5
6.3 甲级能力评定要求	7
7 电信网和互联网第三方安全设计与集成服务能力评定要求	8
7.1 丙级能力评定要求	8
7.2 乙级能力评定要求	10
7.3 甲级能力评定要求	11
参考文献	14

前 言

本标准是“电信网和互联网安全防护体系”系列标准之一。该系列标准预计结构及名称如下：

1. 《电信网和互联网安全防护管理指南》
2. 《电信网和互联网安全等级保护实施指南》
3. 《电信网和互联网安全风险评估实施指南》
4. 《电信网和互联网灾难备份及恢复实施指南》
5. 《固定通信网安全防护要求》
6. 《移动通信网安全防护要求》
7. 《互联网安全防护要求》
8. 《增值业务网—消息网安全防护要求》
9. 《增值业务网—智能网安全防护要求》
10. 《接入网安全防护要求》
11. 《传送网安全防护要求》
12. 《IP 承载网安全防护要求》
13. 《信令网安全防护要求》
14. 《同步网安全防护要求》
15. 《支撑网安全防护要求》
16. 《非核心生产单元安全防护要求》
17. 《电信网和互联网物理环境安全等级保护要求》
18. 《电信网和互联网管理安全等级保护要求》
19. 《固定通信网安全防护检测要求》
20. 《移动通信网安全防护检测要求》
21. 《互联网安全防护检测要求》
22. 《增值业务网—消息网安全防护检测要求》
23. 《增值业务网—智能网安全防护检测要求》
24. 《接入网安全防护检测要求》

25. 《传送网安全防护检测要求》
26. 《IP 承载网安全防护检测要求》
27. 《信令网安全防护检测要求》
28. 《同步网安全防护检测要求》
29. 《支撑网安全防护检测要求》
30. 《非核心生产单元安全防护检测要求》
31. 《电信网和互联网物理环境安全等级保护检测要求》
32. 《电信网和互联网管理安全等级保护检测要求》
33. 《域名系统安全防护要求》
34. 《域名系统安全防护检测要求》
35. 《网上营业厅安全防护要求》
36. 《网上营业厅安全防护检测要求》
37. 《WAP 网关系统安全防护要求》
38. 《WAP 网关系统安全防护检测要求》
39. 《电信网和互联网信息服务业务系统安全防护要求》
40. 《电信网和互联网信息服务业务系统安全防护检测要求》
41. 《增值业务网 即时消息业务系统安全防护要求》
42. 《增值业务网 即时消息业务系统安全防护检测要求》
43. 《域名注册系统安全防护要求》
44. 《域名注册系统安全防护检测要求》
45. 《移动互联网应用商店安全防护要求》
46. 《移动互联网应用商店安全防护检测要求》
47. 《互联网内容分发网络安全防护要求》（本标准）
48. 《互联网内容分发网络安全防护检测要求》
49. 《互联网数据中心安全防护要求》
50. 《互联网数据中心安全防护检测要求》
51. 《电信网和互联网第三方安全服务能力评估准则》（本标准）

随着电信网和互联网的发展，将不断补充和完善电信网和互联网安全防护体系的相关标准。

本标准按照 GB/T1.1-2009 给出的规则起草。

YD/T 2669-2013

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院、中国电信集团公司、中国移动通信集团公司、中国联合网络通信集团有限公司。

本标准主要起草人：江浩洁、侯继江、冯运波、陈利军、祝 卓、李晶晶、黄 晨。

电信网和互联网第三方安全服务能力评定准则

1 范围

本标准规定了为电信网和互联网提供第三方安全服务的组织应具备的安全服务能力。

本标准适用于第三方评定和认证机构对提供电信网和互联网第三方安全服务的组织进行电信网和互联网第三方安全服务能力的评定，可作为电信运营企业对提供第三方安全服务的组织进行选择的依据，可作为国家有关主管部门对为电信网和互联网提供安全服务的第三方安全服务组织进行管理、检查的管理性规范，也可以作为第三方安全服务提供商改进自身能力的指导。

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，仅所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 5271.8-2001 信息技术 词汇 第8部分：安全

3 术语、定义和缩略语

3.1 术语和定义

GB/T 5271.8-2001中界定的以及下列术语和定义适用于本文件。

3.1.1

电信网 Telecom Network

利用有线和/或无线的电磁、光电系统，进行文字、声音、数据、图像或其他任何媒体的信息传递的网络，包括固定通信网、移动通信网等。

3.1.2

互联网 Internet

广域网、局域网及终端（包括计算机、手机等）通过交换机、路由器、网络接入设备等基于一定的通讯协议连接形成的，功能和逻辑上的大型网络。

3.1.3

电信网和互联网安全防护体系 Security Protection Architecture of Telecom Network and Internet

电信网和互联网的安全等级保护、安全风险评估、灾难备份及恢复三项工作互为依托、互为补充、相互配合，共同构成了电信网和互联网安全防护体系。

3.1.4

电信网和互联网相关系统 Systems of Telecom Network and Internet

包括接入网、传送网、IP承载网、信令网、同步网、支撑网等。其中，接入网包括各种有线、无线和卫星接入网等，传送网包括光缆、波分、SDH、卫星等，而支撑网包括业务支撑和网管系统。

3.1.5

电信网和互联网安全等级 Security Classification of Telecom Network and Internet

电信网和互联网及相关系统安全重要程度的表征。重要程度可从电信网和互联网及相关系统受到破坏后,对国家安全、社会秩序、经济运行、公共利益、网络和业务运营商造成的损害来衡量。

3.1.6

电信网和互联网安全等级保护 Classified Security Protection of Telecom Network and Internet
对电信网和互联网及相关系统分等级实施安全保护。

3.1.7

电信网和互联网第三方安全服务能力等级 Qualification Level of the Third Party Security Service for Telecom Network and Internet

一个组织提供电信网和互联网安全服务的综合能力等级,包括法律资格、组织与管理能力、技术能力、人员构成与素质、规模与资产、项目管理能力等多个方面。

依据电信网和互联网安全等级保护要求提供电信网和互联网安全服务的第三方具备相应的能力等级(具体见本标准第4章)。

3.1.8

电信网和互联网第三方安全服务 the Third Party Security Service for Telecom Network and Internet

为了适应电信网和互联网安全管理的需要,一个组织按照一定的合同或协议,运用科学的方法和手段,通过有效的措施来保障电信网和互联网的正常运行,为企业提供全面或部分安全评估、评测或解决方案的服务,包含从安全体系到具体的技术解决措施。这里的“第三方”是相对于自评估提出的概念。

3.2 缩略语

下列缩略语适用于本文件。

ISO	International Organization for Standardization	国际标准化组织
PMP	Project Management Professional	项目管理专业人士认证

4 电信网和互联网第三方安全服务概述

4.1 类型

本标准涉及到的电信网和互联网第三方安全服务分为两类,第一类是风险评估,第二类是安全设计与集成。

4.1.1 风险评估

运用科学的方法和手段,系统地分析电信网和互联网及相关系统所面临的威胁及其存在的脆弱性,评估安全事件一旦发生可能造成的危害程度,并提出有针对性的抵御威胁的防护对策和安全措施,防范和化解电信网和互联网及相关系统安全风险,将风险控制在可接受的水平,为最大限度地保障电信网和互联网及相关系统的安全提供科学依据。

4.1.2 安全设计与集成

对组织的安全框架进行设计,形成安全建设规划,并对计划实施的安全策略细化,在安全解决方案的基础上,实施安全产品集成、安全软件定制开发、安全加固与整改或其它的安全技术和咨询服务。

4.2 电信网和互联网第三方安全服务能力等级的评判原则

电信网和互联网第三方安全服务能力评定是对电信网和互联网安全服务提供组织的客观评价,直接反应了电信网和互联网安全服务提供组织的服务资格、水平和能力。

针对电信网和互联网第三方安全服务能力的评定要求则是对电信网和互联网安全服务提供组织的资格状况、经济实力、技术能力、服务队伍、服务过程能力等方面的具体衡量和评价。本标准中能力评定要求分别针对每一类服务提供组织分为通用性要求和不同服务类型区别要求，通用性要求是指所有电信网和互联网安全服务提供组织都必须达到的安全能力要求（具体指标要求见本标准第5章）；不同服务类型区别要求是指对不同类型的电信网和互联网安全服务提供组织提出了不同的能力要求（具体指标要求见本标准第6、7章）。

每类安全服务(风险评估和安全设计与集成)均提出了三级能力要求，由高到低依次是甲级、乙级、丙级能力。在本标准中，高等级能力的要求涵盖了低等级能力要求的所有方面。

4.3 电信网和互联网安全防护对第三方安全服务能力的要求

4.3.1 第1级

不作要求。

4.3.2 第2级

获得电信网和互联网第三方安全服务能力丙级及丙级以上能力评定的组织。

4.3.3 第3.1级

获得电信网和互联网第三方安全服务能力乙级及乙级以上能力评定的组织。

4.3.4 第3.2级

获得电信网和互联网第三方安全服务能力甲级能力评定的组织。

4.3.5 第4级

同3.2级要求。

4.3.6 第5级

同3.2级要求。

5 电信网和互联网第三方安全服务能力评定通用性要求

通用要求包括以下四项：

1) 从事电信网和互联网第三方安全服务的组织必须是在中华人民共和国境内注册成立（港澳台地区除外），由中国公民投资或者国家投资的，具有独立法人资格及相关部门颁发的合法经营资格的企事业单位（港澳台地区除外）；

2) 从事涉密的电信网和互联网第三方安全服务的组织必须满足国家保密机关的相关要求；

3) 从事电信网和互联网第三方安全服务的组织应具备电信网络安全保障服务工作经验一年以上，无违法记录；

4) 从事电信网和互联网第三方安全服务的组织其法人及主要业务、技术人员需无犯罪记录。

6 电信网和互联网第三方安全风险评估服务能力评定要求

从事电信网和互联网第三方安全风险评估服务的组织应符合本标准第5章通用性要求的所有条款。

6.1 丙级能力评定要求

6.1.1 资格要求

进行涉密集成的组织必须获得国家保密部门的能力证书。

6.1.2 规模与资产

组织的规模和资产应满足:

- 1) 正式编制员工应不少于15人;
- 2) 注册资金应不少于100万元人民币。

6.1.3 人员构成和素质要求

组织的人员构成和素质应符合:

- 1) 直接从事风险评估服务的人员不低于8人, 大学本科以上学历不少于80%;
- 2) 从事风险评估的组织内至少应有2名具备2年以上电信网和互联网领域风险评估项目经验的安全工程师。

6.1.4 业绩要求

组织的从业业绩应符合:

- 1) 应具备1年以上的安全行业从业时间;
- 2) 至少有2个项目中涉及风险评估服务的金额超过10万元人民币;
- 3) 近3年内至少成功完成2个风险评估项目, 且终验通过;
- 4) 近1年没有出现因各阶段验收未通过或企业自身原因而废止的风险评估服务项目。

6.1.5 组织与管理要求

组织应具备如下管理要求:

- 1) 应拥有健全的组织与管理体系;
- 2) 应制定符合国家保密部门要求的保密制度;
- 3) 应落实保密规章制度和执行保密技术标准;
- 4) 应建立人员管理程序, 明确保密岗位与职责, 定期对安全服务人员进行安全保密教育与培训, 并签订保密责任书, 规定应当履行的安全保密义务和承担的法律責任。

6.1.6 质量保证要求

组织应满足如下质量保证要求:

- 1) 应建立并落实质量管理体系;
- 2) 应能够自行评估服务质量的状况, 并能对服务质量进行持续改进;
- 3) 从事风险评估服务的组织应建立相关投诉、应急响应服务机制。

6.1.7 项目管理要求

组织应满足如下项目管理要求:

- 1) 应具有成文的项目管理制度, 并符合相关项目管理标准;
- 2) 应具有系统地对员工进行安全技术、项目管理、保密规章制度的培训机制和计划, 并能有效组织实施与考核;
- 3) 应能提供项目管理制度可有效运行的证据。

6.1.8 技术能力要求

组织应具备如下技术能力:

- 1) 应对电信网和互联网的整体概念有一定了解;
- 2) 应能够独立完成电信网和互联网网络单元IP层面安全渗透测试;
- 3) 应具有确定网络的安全需求的能力;

4) 应具有对网络安全系统有效维护的能力。

6.1.9 服务队伍要求

组织内从事风险评估的服务队伍的人员应符合:

1) 从事风险评估的队伍中的相关人员应是中国公民;

2) 从事风险评估的队伍内至少应有1名经过电信网和互联网安全防护技术和标准的系统培训的安全工程师;

3) 从事风险评估的队伍内应至少有2名经过国家和相关机构认可、针对安全风险评估服务能力的安全工程师(有相关的能力证书,如:CIW、CISP、CISSP、CISA等)。

6.1.10 设备、设施与环境要求

组织的设备、设施和环境应满足如下要求:

1) 应具有固定的办公场所;

2) 应具有专门从事电信网和互联网安全风险评估服务的相关工具或软件,如漏洞扫描工具、安全基线核查、网站安全检测工具等。

6.1.11 服务过程能力要求

组织应具有以下基本能力:

- 1) 评估系统安全威胁的能力;
- 2) 评估系统脆弱性的能力;
- 3) 评估安全对系统的影响的能力;
- 4) 评估系统安全风险的能力;
- 5) 确定系统的安全需求的能力;
- 6) 确定系统的安全输入的能力;
- 7) 进行管理安全控制的能力;
- 8) 进行监测系统安全状况的能力;
- 9) 进行安全协调的能力;
- 10) 进行检测和证实系统安全性的能力;
- 11) 进行建立系统安全的保证证据的能力;
- 12) 根据风险评估结果进行系统整改的能力。

6.2 乙级能力评定要求

从事电信网和互联网第三方安全风险评估服务的组织应达到本标准6.1风险评估服务丙级能力要求的所有条款,并在以下方面增强或增加要求:

6.2.1 规模与资产

组织的规模和资产应满足:

- 1) 正式编制员工应不少于50人;
- 2) 注册资金应不少于500万元人民币。

6.2.2 人员构成和素质要求

组织的人员构成和素质应符合:

- 1) 直接从事风险评估服务的人员不低于20人,大学本科以上学历不少于80%;

- 2) 从事风险评估的组织内至少应有5名具备2年以上通信领域风险评估项目经验的安全工程师。

6.2.3 业绩要求

组织的从业业绩应符合：

- 1) 应具备2年以上的安全行业从业时间；
- 2) 至少有4个项目中涉及风险评估服务的金额超过10万元人民币；
- 3) 近3年内至少成功完成10个风险评估项目，且终验通过；
- 4) 近2年没有出现因各阶段验收未通过或企业自身原因而废止的风险评估服务项目。

6.2.4 组织与管理要求

组织应具备如下管理要求：

- 1) 应具有专门从事电信网和互联网安全风险服务的部门或团队；
- 2) 对项目实施过程中获取、保存、传播和销毁与安全事件处理服务有关商业秘密信息等方面作出明确规定；
- 3) 应具有专门制定和宣贯保密制度的部门或团队。

6.2.5 质量保证要求

组织应满足如下质量保证要求：

- 1) 应有专门的部门或人员制定完整的质量体系，并具有健全的制度宣传和培训机制；
- 2) 质量体系应针对项目开始至项目结束各个环节有比较完善和细致的控制手段。

6.2.6 项目管理要求

组织应满足如下项目管理要求：

- 1) 应有专门的部门或人员制定总体的项目管理体系，并具有健全的制度宣传和培训机制；
- 2) 项目管理体系应针对人和项目有明确的责权利分工，有比较明确和完善的项目过程控制记录；
- 3) 至少有1名安全服务人员接受过系统的项目管理培训，获得过相关权威机构的认证（如PMP等）。

6.2.7 技术能力要求

组织应具备如下技术能力：

- 1) 应了解电信网和互联网安全防护系列标准，应对电信网和互联网的整体概念和传统网和非传统网的若干网络单元有一定了解；
- 2) 应具有国家或行业权威机构对组织能力的认可证明（如国家信息安全服务资质证书、信息安全风险评估资质证书、信息安全应急服务资质证书等）；
- 3) 应具有专门研究电信网和互联网技术和业务的部门或团队；
- 4) 应依据电信网和互联网安全防护体系系列标准进行安全风险服务；
- 5) 应能够评估电信网和互联网安全风险、脆弱性、管控能力及安全对电信网和互联网的影响力；
- 6) 应具有确定电信网和互联网的安全需求的能力；
- 7) 应具有对电信网和互联网安全系统有效维护的能力；
- 8) 应具备切实可行的应急服务方案。

6.2.8 服务队伍要求

组织内从事风险评估的服务队伍的人员应符合：

1) 从事风险评估的队伍内至少应有2名经过电信网和互联网安全防护技术和标准的系统培训的安全工程师;

2) 从事风险评估的队伍内应至少有4名经过国家和相关机构认可, 针对安全风险评估服务能力的安全工程师(有相关的能力证书如: CIW、CISP、CISSP、CISA等)。

6.2.9 设备、设施与环境要求

组织的设备、设施和环境应满足如下要求:

- 1) 应具有针对网络安全问题研究的实验环境;
- 2) 应具有成熟的工具、软件体系。

6.3 甲级能力评定要求

从事电信网和互联网第三方安全风险评估服务的组织应达到本标准6.2风险评估服务乙级能力要求的所有条款, 并在以下方面增强或增加要求:

6.3.1 规模与资产

组织的规模和资产应满足:

- 1) 正式编制员工应不少于100人;
- 2) 注册资金应不少于3000万元人民币。

6.3.2 人员构成和素质要求

组织的人员构成和素质应符合:

- 1) 直接从事风险评估服务的人员不低于30人, 大学本科以上学历不少于80%;
- 2) 从事风险评估的组织内至少应有12名具备3年以上通信领域风险评估项目经验的安全工程师。

6.3.3 业绩要求

组织的从业业绩应符合:

- 1) 企业应具备3年以上的安全行业从业时间;
- 2) 至少有6个项目中涉及风险评估服务的金额超过10万元人民币;
- 3) 企业风险评估服务年业绩中电信网和互联网行业比重大于或等于30%;
- 4) 近3年内至少成功完成20个风险评估项目, 且终验通过;
- 5) 近5年没有出现因各阶段验收未通过或企业自身原因而废止的风险评估服务项目。

6.3.4 组织与管理要求

组织应具备如下管理要求:

- 1) 从事电信网和互联网安全风险评估服务的部门或团队应为企业二级部门;
- 2) 对项目实施过程中获取、保存、传播和销毁与安全事件处理服务有关商业秘密信息等方面有明确的行之有效的控制手段。

6.3.5 质量保证要求

组织应满足如下质量保证要求:

- 1) 应依据ISO 9001质量体系标准制定完善的质量体系;
- 2) 应依据ISO 27001制定完善的信息安全管理体系规范(ISMS)。

6.3.6 项目管理要求

组织应满足如下项目管理要求:

- 1) 项目管理制度应对项目立项、审批过程有明晰表述;
- 2) 项目管理制度应对项目过程有控制方法或有依据标准, 应有对过程中发生的项目变更或变化进行管理的手段;
- 3) 项目管理制度应对项目完成后的审计、验证、考核等内容有管理办法;
- 4) 应具备项目管理制度落实的证据, 可以但不限于电子文档、会议记录、过程管理表格等。

6.3.7 技术能力要求

组织应具备如下技术能力:

- 1) 深入了解电信网和互联网安全防护系列标准, 并参与起草制定国家或行业标准, 对电信网和互联网的整体概念和传统网和非传统网的若干网络单元有深入了解;
- 2) 参与支撑国家或行业重大项目。

6.3.8 服务队伍要求

组织内从事风险评估的服务队伍的人员应符合:

- 1) 从事风险评估的队伍内至少应有5名经过电信网和互联网安全防护技术和标准的系统培训的安全工程师;
- 2) 从事风险评估服务的队伍内应至少有10名经过国家和相关机构认可, 针对安全风险评估服务能力的安全工程师;
- 3) 应具有产品研发团队, 其中大学本科以上学历人员占90%以上;
- 4) 具有专业的安全攻防队伍, 有能力对各类主流操作系统、主流数据库及为完成特定功能所开发的系统进行黑盒测试, 并对代码进行白盒检查。

6.3.9 设备、设施与环境要求

组织的设备、设施和环境应满足如下要求:

- 1) 应具有专业的攻防实验室, 支撑国家相关部门;
- 2) 应具有自主研发的检测工具(硬件或软件), 并获得国家相关部门的认可;
- 3) 安全产品应在国家和行业领域占据领先地位, 应获得国家或行业权威认可证明。

7 电信网和互联网第三方安全设计与集成服务能力评定要求

7.1 丙级能力评定要求

应达到本标准第6章电信网和互联网第三方安全服务能力评定通用性要求的所有条款。

7.1.1 资格要求

进行涉密集成的组织必须获得国家保密部门的能力证书。

7.1.2 规模与资产

组织的规模和资产应满足:

- 1) 正式编制员工应不少于20人;
- 2) 注册资金不少于500万元人民币。

7.1.3 人员构成和素质要求

组织的人员构成和素质应符合:

- 1) 直接从事安全设计与集成服务的人员不低于10人, 大学本科以上学历不少于80%;

2) 至少有5人具有3年以上的安全设计与集成服务行业从业经验,并具有深度参与的安全设计与集成服务成功案例。

7.1.4 业绩要求

组织的从业业绩应符合:

- 1) 应具备1年以上的安全行业从业时间;
- 2) 至少有2个项目中涉及安全设计与集成服务的金额超过100万元人民币;
- 3) 近3年内至少成功完成2个安全设计与集成项目,且终验通过;
- 4) 近1年没有出现因各阶段验收未通过或企业自身原因而废止的安全设计与集成服务项目。

7.1.5 组织与管理要求

组织应具备如下管理要求:

- 1) 应拥有健全的组织与管理体系;
- 2) 应制定符合国家保密部门要求的保密制度;
- 3) 应落实保密规章制度和执行保密技术标准;
- 4) 应建立人员管理程序,明确保密岗位与职责,定期对安全服务人员进行安全保密教育与培训,并签订保密责任书,规定应当履行的安全保密义务和承担的法律責任。

7.1.6 质量保证要求

组织应满足如下质量保证要求:

- 1) 应建立并落实质量管理体系;
- 2) 应能够自行评估服务质量的状况,并能对服务质量进行持续改进;
- 3) 从事安全设计与集成服务的组织应建立相关投诉、应急响应服务机制,例如应该具备7×24小时服务电话。

7.1.7 项目管理要求

组织应满足如下项目管理要求:

- 1) 应具有成文的项目管理制度,并符合相关项目管理标准;
- 2) 应具有系统地对员工进行安全技术、项目管理、保密规章制度的培训机制和计划,并能有效组织实施与考核;
- 3) 应能提供项目管理制度可有效运行的证据。

7.1.8 技术能力要求

组织应具备如下技术能力:

- 1) 应对电信网和互联网的整体概念有一定了解;
- 2) 应能对市场上的主流网络安全产品进行功能分析,在具体项目中应能针对具体的网络架构和网络单元中存在的安全事件设计安全策略和安全解决方案,具有安全产品的系统集成能力;
- 3) 应具有对集成的系统进行安全性检测和验证的能力;
- 4) 应具有对集成的系统有效维护的能力。

7.1.9 服务队伍要求

组织内从事安全设计与集成的服务队伍的人员应符合:

- 1) 从事安全设计与集成的队伍中的相关人员应是中国公民;

2) 从事安全设计与集成的队伍内至少应有1名经过电信网和互联网安全防护技术和标准的系统培训的安全工程师;

3) 从事安全设计与集成服务的队伍内至少应有2名经过国际、国家和相关机构认可的,与安全设计与集成能力相关的安全工程师。

7.1.10 设备、设施与环境要求

组织的设备、设施和环境应满足如下要求:

- 1) 应具有固定的办公场所;
- 2) 应具有自主研发的安全产品,具有比较完善的研发和实验环境。

7.2 乙级能力评定要求

从事电信网和互联网第三方安全设计与集成服务的组织应达到本标准7.1安全设计与集成服务丙级能力要求的所有条款,并在以下方面增强或者增加要求:

7.2.1 规模与资产

组织的规模和资产应满足:

- 1) 公司正式编制员工应不少于100人;
- 2) 注册资金应不少于1000万元人民币。

7.2.2 人员构成和素质要求

组织的人员构成和素质应符合:

- 1) 直接从事安全建设与整改服务的人员不低于20人,大学本科以上学历不少于80%;
- 2) 至少有8人具有3年以上的安全设计与集成服务行业从业经验,并具有深度参与的安全设计与集成服务成功案例。

7.2.3 业绩要求

组织的从业业绩应符合:

- 1) 企业应具备3年以上的安全行业从业时间;
- 2) 应至少有3个项目中涉及安全设计与集成服务的金额超过100万元人民币。
- 3) 近三年内应至少成功完成5个安全设计与集成项目,且终验通过;
- 4) 近两年应没有出现因各阶段验收未通过或企业自身原因而废止的安全设计与集成服务项目。

7.2.4 组织与管理要求

组织应具备如下管理要求:

- 1) 应具有专门从事电信网和互联网安全设计与集成服务的部门或团队;
- 2) 对项目实施过程中获取、保存、传播和销毁与安全事件处理服务有关商业秘密信息等方面作出明确规定;
- 3) 应具有专门制定和宣贯保密制度的部门或团队;
- 4) 应建立人员管理程序,明确保密岗位与职责,定期对安全服务人员进行安全保密教育与培训,并签订保密责任书,规定应当履行的安全保密义务和承担的法律法律责任。

7.2.5 质量保证要求

组织应满足如下质量保证要求:

- 1) 应有专门的部门或人员制定完整的质量体系,并具有健全的制度宣传和培训机制;

2) 质量体系应针对项目开始至项目结束各个环节有比较完善和细致的控制手段;

3) 从事安全设计与集成服务的组织应建立相关投诉、应急响应服务机制,例如应该具备7×24小时服务电话。

7.2.6 项目管理要求

组织应满足如下项目管理要求:

1) 应有专门的部门或人员制定总体的项目管理体系,并具有健全的制度宣传和培训机制;

2) 应具有系统地对员工进行安全技术、项目管理、保密规章制度的培训机制和计划,并能有效组织实施与考核;

3) 项目管理体系应针对人和项目有明确的责权利分工,有比较明确和完善的项目过程控制记录;

4) 至少有2名安全服务人员接受过系统的项目管理培训,获得过相关权威机构的认证(如PMP等)。

7.2.7 技术能力要求

组织应具备如下技术能力:

1) 应了解电信网和互联网安全防护系列标准,应对电信网和互联网的整体概念和传统网和非传统网的若干网络单元有一定了解;

2) 应具有国家或行业权威机构对组织安全设计与集成能力的认可证明(如国家信息安全服务资质证书、信息安全集成类资质证书等);

3) 应具有专门研究电信网和互联网技术和业务的部门或团队;

4) 应依据电信网和互联网安全防护体系系列标准进行安全设计与集成服务;

5) 应具有较完善的安全产品集,同时应能对市场上的主流网络安全产品有很深入的了解,在具体项目中可以针对网络架构和网络单元存在的安全问题进行功能分析、提出整体的安全框架设计、安全策略和安全解决方案,应具有较强的安全产品系统集成能力。

7.2.8 服务队伍要求

组织内从事安全设计与集成的服务队伍的人员应符合:

1) 从事安全设计与集成服务的队伍内至少应有2名经过电信网和互联网安全防护技术和标准的系统培训的安全工程师;

2) 从事安全设计与集成服务的队伍内应至少有4名经过国际、国家或相关机构认可,针对安全设计与集成服务能力的安全工程师。

7.2.9 设备、设施与环境要求

组织的设备、设施和环境应满足如下要求:

应具有针对安全设计与集成产品的开发、测试和实验环境,安全产品研发团队具有较高的技术水平和确实有效服务行业的研发成果。

7.3 甲级能力评定要求

从事电信网和互联网第三方安全设计与集成服务的组织应达到本标准7.2安全设计与集成服务乙级能力要求的所有条款,并在以下方面增强或者增加要求:

7.3.1 规模与资产

组织的规模和资产应满足:

- 1) 公司正规编制员工应不少于200人;
- 2) 注册资金应不少于3000万元人民币。

7.3.2 人员构成和素质要求

组织的人员构成和素质应符合:

- 1) 直接从事安全设计与集成服务的人员不低于30人,大学本科以上学历不少于80%;
- 2) 至少有15人具有3年以上的安全设计与集成服务行业从业经验,并具有深度参与的安全设计与集成服务成功案例。

7.3.3 业绩要求

组织的从业业绩应符合:

- 1) 企业应具备5年以上的安全行业从业时间;
- 2) 应至少有10个项目中涉及安全设计与集成服务的金额超过100万元人民币;
- 3) 近三年内应至少成功完成10个安全设计与集成项目,且终验通过;
- 4) 近五年应没有出现因各阶段验收未通过或企业自身原因而废止的安全建设或整改服务项目。

7.3.4 组织与管理要求

组织应具备如下管理要求:

- 1) 从事电信网和互联网安全设计与集成服务的部门或团队应为企业二级部门;
- 2) 对项目实施过程中获取、保存、传播和销毁与安全事件处理服务有关商业秘密信息等方面有明确的行之有效的控制手段。

7.3.5 质量保证要求

组织应满足如下质量保证要求:

- 1) 应依据ISO 9001质量体系标准制定完善的质量体系;
- 2) 应依据ISO 27001制定完善的信息安全管理体系规范(ISMS)。

7.3.6 项目管理要求

组织应满足如下项目管理要求:

- 1) 项目管理制度应对项目立项、审批过程有明晰表述;
- 2) 项目管理制度应对项目过程有控制方法或有依据标准,应有对过程中发生的项目变更或变化进行管理的手段;
- 3) 项目管理制度应对项目完成后的审计、验证、考核等内容有管理办法;
- 4) 应具备项目管理制度落实的证据,可以但不限于电子文档、会议记录、过程管理表格等。

7.3.7 技术能力要求

组织应具备如下技术能力:

- 1) 深入了解电信网和互联网安全防护系列标准,并参与起草制定国家或行业标准,对电信网和互联网的整体概念和传统网和非传统网的若干网络单元有深入了解;
- 2) 应参与过支撑国家或行业重大项目;
- 3) 应具有完善的安全产品体系,可以在项目中有针对性的提出最优化的安全设计框架、安全策略和安全解决方案,具有很强的安全产品系统集成能力。

7.3.8 服务队伍要求

组织内从事安全设计与集成的服务队伍的人员应符合：

- 1) 从事安全设计与集成的队伍内至少应有5名经过电信网和互联网安全防护技术和标准的系统培训的安全工程师；
- 2) 从事安全设计与集成服务的队伍内应至少有10名经过国家和相关机构认可，针对安全设计与集成服务能力的安全工程师；
- 3) 应具有产品研发团队，其中大学本科以上学历人员占90%以上。

7.3.9 设备、设施与环境要求

组织的设备、设施和环境应满足如下要求：

- 1) 应具有专业的针对安全产品研发、测试环境，获得过国家或相关权威机构的认可；
- 2) 安全产品开发生产环境满足国家权威机构的要求；
- 3) 安全产品应在国家和行业领域占据领先地位，应获得国家或行业权威认可证明。

参 考 文 献

- [1]GB/T 19000.3-2001 质量管理和质量保证标准 第3部分:GB/T 19001在计算机软件开发、供应、安装和维护中的使用指南
- [2]GB/T 19001-2000 质量管理体系
- [3]GB/T 19004.2-1994 质量管理和质量体系要素 第2部分:服务指南
- [4]GB/T 19004.4-1994 质量管理和质量体系要素 第4部分:质量改进指南
- [5]YD/T 1621-2007 网络与信息安全服务资质评估准则
- [6]YD/T 1728-2008 电信网和互联网安全防护管理指南
- [7]YD/T 1799-2008 网络与信息安全应急服务资质评估方法
-

中 华 人 民 共 和 国
通 信 行 业 标 准
电信网和互联网第三方安全服务能力评定准则
YD/T 2669-2013

*

人民邮电出版社出版发行
北京市丰台区成寿寺路 11 号邮电出版大厦
邮政编码：100164
宝隆元（北京）印刷技术有限公司印刷
版权所有 不得翻印

*

开本：880×1230 1/16 2014 年 2 月第 1 版
印张：1.5 2014 年 2 月北京第 1 次印刷
字数：36 千字

15115 • 367

定价：20 元

本书如有印装质量问题，请与本社联系 电话：(010)81055492