ICS 33.040
M 21

YD

中华人民共和国通信行业标准

YD/T 2252-2011

网络与信息安全风险评估
服务能力评估方法

Evaluation criteria of service capability for network and information security risk assessment

2011-06-01 发布　　2011-06-01 实施

中华人民共和国工业和信息化部　发布

目　次

前　言

本标准与YD/T 1621-2007《网络与信息安全服务资质评估准则》保持一致。

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：国家计算机网络应急技术处理协调中心、清华大学、北京启明星辰信息技术有限公司、北京神州绿盟科技有限公司。

本标准主要起草人：舒　敏、陈晓桦、叶　红、翟亚红、曹亚斌、孙东红、禄　凯、何清林、黄元飞、王红虹、王红阳、陈　彪、姚伟栋。

网络与信息安全风险评估服务能力评估方法

1 范围

本标准规定了网络与信息安全风险评估服务提供者应具备的服务能力要求，以及对信息安全风险评估服务提供者进行评价的要求。

本标准适用于对网络与信息安全风险评估服务提供者的服务能力评价，可作为信息系统所有者选择信息安全风险评估服务提供者的依据，及有关主管部门对信息安全风险评估服务提供者进行管理的技术性规范，也可为信息安全风险评估服务提供者改进自身服务能力提供参考。

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　　信息技术词汇 第8部分：安全

GB/T 20984　　信息安全技术 信息安全风险评估规范

3 术语和定义

GB/T 5271.8《信息技术词汇第8部分：安全》、GB/T 20984《信息安全技术 信息安全风险评估规范》中的术语和定义及以下术语和定义适用于本文件。

3.1

风险处置　Risk Treatment

对风险进行处理的一系列活动，如接受风险、规避风险、转移风险、降低风险等。

3.2

信息安全风险评估　Information Security Risk Assessment

依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

从风险管理角度，运用科学的方法和手段，系统地分析网络与信息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，提出有针对性的抵御威胁的防护对策和整改措施。

3.3

信息安全风险评估服务提供者　Information Security Risk Assessment Service Provider

具备一定的风险评估能力，按照合同或协议，为信息系统所有者提供信息安全风险评估服务的组织。

4 概述

4.1 信息安全风险评估服务概述

信息安全风险评估是信息安全保障的基础性工作和重要环节，贯穿于网络和信息系统建设运行的全过程。风险评估服务提供者通过对信息系统提供风险评估服务，系统地分析网络与信息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，提出有针对性的抵御威胁的防护对策和安全整改措施，防范和消除信息安全风险，或将风险控制在可接受的水平，为网络和信息安全保障提供科学依据。

信息安全风险评估服务能力等级是衡量风险评估服务提供者服务能力的尺度。能力等级分为一级、二级、三级共三个等级，其中一级最高，三级最低。

在本标准中，信息安全风险评估服务能力等级要求包含基本能力要求、过程能力要求和不同等级的特殊要求三个部分，详见第5章、第6章、第7章。

4.2 实施风险评估服务的原则

4.2.1 标准性原则

信息系统安全风险评估应参照国际、国家、行业标准等进行实施。

4.2.2 核心业务原则

信息安全风险评估应以被评估组织的关键业务为核心，涉及关键业务的相关网络与系统为评估的重点，重点包括基础网络、业务网络、操作系统、应用基础平台、业务应用平台等。

4.2.3 可控性原则

a）服务可控性

在评估工作沟通会议中，事先向用户介绍评估服务流程，明确需要得到用户协作的内容，以确保安全评估工作顺利进行。

b）人员可控性

所有参与评估的人员均应签署保密协议以进行项目安全约束，对过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，确保项目成员的安全控制与管理。

c）过程可控性

应依据项目管理规范进行项目管理，组建项目实施团队，实行项目经理负责制，做到项目过程的可控。

d）工具可控性

安全服务人员所使用的评估工具应事先通告用户，在项目实施过程中应获得用户对产品、工具、策略的许可。

4.2.4 最小影响原则

对于在线业务系统的风险评估，首先应保障业务系统稳定运行。对于需要进行攻击性测试的工作内容，应与用户充分沟通并进行应急备份，选择避开业务的高峰时间进行。

5 风险评估提供者基本能力要求

5.1 基本条件

风险评估服务提供者应：

a）具有中华人民共和国境内的独立法人资格，具有相关部门颁发的合法经营资格；

b）从事涉密信息系统的风险评估服务提供者应满足国家保密机关的相关要求；

c）具有固定的工作场所；

d）近两年内经济状况良好，财务数据真实可信，并应经国家相关部门认定的会计师事务所核实；

e）遵守国家现行法律、法规的规定。

5.2 基本管理能力要求

风险评估服务提供者应：

a）采取技术和管理措施确保客户信息的安全、可控，这些信息包括但不限于客户资料、风险评估活动中产生的文档、最终评估报告等。

b）制定保密管理要求，明确保密岗位与职责，定期对服务人员进行保密教育与培训，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责任，并负责落实。

c）建立人员管理程序，使每一位服务人员持续满足岗位职责的需求；制定风险评估技能培训计划，定期对服务人员进行培训、指导、考核。

d）按照持续改进的要求制定风险评估项目的管理制度；制定风险评估项目计划及监督检查要求，具体包括对组织内外的交流机制、规划关键技术活动、选择服务小组、设立项目的里程碑及评审要求、日常的监督检查。

e）使用符合标准要求的检查列表、文档模板、测试工具，保证评估质量的一致性。

5.3 基本技术能力要求

风险评估服务提供者应：

a）具有建立适当的风险分析模型、选择适当的风险计算方法的能力；具有识别并分析组织和信息系统的信息资产价值的能力；能够全面、准确了解组织和信息系统所面临的各种威胁；能够对组织和信息系统的脆弱性进行有效识别和分析。

b）具备对风险处置、安全整改提出有效措施的能力。

c）具备独立的测试环境及必要的软、硬件设备，用于满足技术培训和模拟测试的需要；具备满足承担风险评估项目所需的工具，如漏洞扫描工具、渗透测试工具、协议分析仪等；对测试工具的功能、性能进行确认，保证测试工具的可用性、稳定性、安全性。

d）可采用远程、本地两种方式进行安全评估，安全评估方法可包括工具扫描、渗透测试、配置检查、人工评估、白盒测试、顾问访谈等。

e）具备风险评估有关的工作流程及操作规范。

f）具备风险评估方案；能够按照标准要求提供信息安全风险评估报告，报告应包括安全评估的结果及安全建议。

g）有专门的技术人员关注国内外权威机构发布的安全公告及漏洞公告；了解信息安全技术、安全标准的动向，有能力掌握信息安全的最新技术和标准；有专门的人员持续对最新的安全攻防技术进行研究。

6 信息安全风险评估服务过程要求

6.1 信息安全风险评估服务过程

信息安全风险评估服务过程可分为评估准备、风险识别、风险分析、风险处置4个关键阶段。评估准备是评估实施有效性的保证，是风险评估工作的开始；风险识别主要是对评估活动中的各类关键资产、

威胁、脆弱性、安全措施进行识别与赋值；风险分析主要是对识别阶段中获得的各类信息进行关联分析，得出风险值；风险处置主要针对风险评估得出的风险，提出必要的处置建议，也包括实施安全加固后进行残余风险的处置等内容。

信息安全风险评估服务过程包括 4 个阶段，16 个主要控制措施，见表 1。控制措施定义了为满足阶段内容的要点以及支持控制要点的最佳实践。

表 1 信息安全风险评估服务过程控制措施

阶段	控制措施
评估准备	服务需求界定 服务合同签订 服务方案制定 人员和工具准备
风险识别	资产识别 威胁识别 脆弱性识别 已有安全措施确认
风险分析	风险分析模型 风险计算方法 风险分析与评价 风险评估报告
风险处置	处置原则 安全整改建议 组织评审会 残余风险处置

信息安全风险评估服务提供者应按照每一阶段的要求为被评估对象提供评估服务。每一阶段的要求有必备要求和可选要求，具体要求见6.2至6.5。

6.2 评估准备阶段

6.2.1 主要内容

评估准备阶段是整个风险评估过程有效性的保证，风险评估的结果可能会受到评估对象的业务战略、业务流程、安全需求、系统规模和结构等各方面的影响。因此，在风险评估实施前，应充分做好服务需求界定、服务合同签订、服务方案制定、人员和工具准备等工作。

6.2.2 控制措施：服务需求界定

1）应确定评估目标。充分了解评估对象，了解各项业务功能及各项业务功能之间的相关性，确定支持各种业务功能的相应信息系统资源及其他资源，确定系统执行的关键功能，并确定执行这些功能所需的特定系统资源。

2）应确定评估范围。在确定风险评估目标之后，应进一步明确风险评估的评估范围，可以是组织全部的信息及与信息处理相关的各类资产、管理机构，也可以是某个独立的信息系统、关键业务流程、与组织知识产权相关的系统或部门等。

在确定评估范围时，应结合已确定的评估目标和组织的实际信息系统建设情况，合理定义评估对象和评估范围边界，可以参考以下依据作为评估范围边界的划分原则：

a）业务系统的业务逻辑边界；

b）网络及设备载体边界；

c）物理环境边界；

d）组织管理权限边界；

e）其他。

6.2.3 控制措施：服务合同签订

1）应签订服务合同或协议。

2）应明确双方的职责和责任。

3）应明确评估的具体行为。应明确哪些具体的评估行为是可接受或者禁止的，哪些行为需要系统管理者的事先批准，尤其是对于关键系统的拒绝服务尝试、对敏感信息的破解尝试。

6.2.4 控制措施：服务方案制定

1）应进行充分的系统调研。服务方案应在充分掌握评需求的基础上进行制定，事先需进行充分的系统调研，为风险评估依据和方法的选择、评估内容的实施奠定基础。

2）宜根据风险评估目标以及调研结果，确定评估依据和评估方法。评估依据包括（但不仅限于）：

a）适用的法律、法规；

b）现有国际标准、国家标准、行业标准；

c）行业主管机关的业务系统的要求和制度；

d）系统互联单位的安全要求；

e）系统本身的实时性或性能要求等。

3）应形成较为完整的风险评估实施方案，为后面的风险评估实施活动提供一个总体计划，用于指导实施方开展后续工作，并作为评估项目验收的主要依据之一。风险评估方案的内容应包括（但不限于）：

a）风险评估工作框架：包括评估目标、评估范围、评估依据等内容；

b）评估团队组织：包括组织结构、评估团队成员、角色、责任等内容；

c）评估工作计划：风险评估各阶段的工作计划，包括工作内容、工作形式、工作成果等内容；

d）评估工作中的风险规避：包括保密协议约定、评估工作环境要求、评估方法和工具的选择等内容；

e）时间进度安排：评估实施的时间进度安排；

f）项目验收方法：包括验收方式、验收依据、验收结论定义等。

6.2.5 控制措施：人员和工具准备

1）应组建评估团队。为了保障风险评估工作顺利开展，风险评估实施团队应由管理层、相关业务骨干、IT技术人员等组成风险评估小组。必要时，可组建由评估方、被评估方领导和相关部门负责人参加的风险评估领导小组，聘请相关专业的技术专家和技术骨干组成专家小组。

2）应根据服务对象的需求准备必要的工具包，包括合格的评估系统、工具软件等。工具包应保存在不可更改的移动介质上，并定期更新和具备完善的版本控制。

3）宜做好评估前的表格、文档等各项准备工作，进行风险评估技术培训和保密教育，制定风险评估过程管理相关规定。可根据被评估方要求，双方签署保密合同，适情签署个人保密协议。

4）为确保风险评估工作的顺利有效进行，应采用合理的项目管理机制，明确主要相关人员的角色与职责。

信息安全风险评估服务评估准备阶段的要求见表2。

表2 信息安全风险评估服务评估准备阶段的要求

要求		必备	可选
评估准备阶段			
服务需求界定	1）确定评估目标，充分了解评估对象	√	
	2）确定评估范围，合理定义评估对象和评估范围边界	√	
服务合同签订	1）应签订服务合同或协议	√	
	2）应明确双方的职责和责任	√	
	3）应明确评估的具体行为	√	
服务方案制定	1）进行充分的系统调研	√	
	2）确定评估依据和评估方法		√
	3）形成方案，提供总体计划	√	
人员和工具准备	1）组建评估团队	√	
	2）根据需求准备必要的工具包，定期更新	√	
	3）做好评估前的表格、文档等准备工作		√
	4）采用合理的项目管理机制，明确主要人员的权责	√	

6.3 风险识别阶段

6.3.1 主要内容

在组织和信息系统中，资产、威胁、脆弱性都是产生风险的重要因素。识别出这些重要因素并进行分析评估，是进行整体风险评估的前提。

6.3.2 控制措施：资产识别

风险评估服务提供者应：

1）对组织的资产进行分类。在风险评估实施中，可以按照GB/T 20984-2007中的资产分类方法，如资产价值、面临的威胁、存在的脆弱性、可采取的安全措施等方面对组织的资产进行分类。

2）识别组织和信息系统中的重要资产。一方面应识别出组织具有哪些资产，另一方面要识别出每项资产自身的关键属性。

3）表示资产的重要程度。在资产调查的基础上，分析资产的保密性、完整性和可用性等安全属性的等级要求，为这些安全属性等级赋值，以表示资产的重要程度。

4）通过资产识别和资产赋值，形成资产列表和资产赋值报告。

6.3.2 控制措施：威胁识别

风险评估服务提供者应：

1）具有依据GB/T 20984-2007中的威胁分类方法对威胁进行分类的能力。

2）能够初步识别出组织和信息系统中潜在的对组织和信息系统造成影响的威胁，包括威胁源、威胁方式、威胁影响，并进而识别那些发生可能性较大、可能造成重大影响的重大威胁。

3）采用多种方法进行威胁调查。可以根据组织和信息系统自身的特点进行调查，可以根据组织和信息系统历史发生的安全事件进行调查；也可以根据组织或系统外面临威胁的情况进行调查。

4）能在风险调查的基础上进行威胁分析，通过威胁源攻击能力、威胁源攻击动机、威胁发生频率、威胁影响程度确定计算威胁值的方法。

5）在威胁调查和威胁分析的基础上，形成威胁分析报告。

6.3.4 控制措施：脆弱性识别

风险评估服务提供者应：

1）进行安全技术脆弱性核查。一方面应检查组织和资产自身在技术方面存在的脆弱性；另一方面应核查所采取的安全措施的有效程度，包括物理环境安全脆弱性核查、网络安全脆弱性核查、主机系统安全脆弱性核查、应用系统安全脆弱性核查、数据安全脆弱性核查等。

2）根据被评估单位安全保障管理要求，对管理及运行维护部门进行安全管理核查。安全管理核查主要通过查阅文档、抽样调查和询问等方法，针对被测单位在信息安全方面制定的规章制度的合理性、完整性、适用性等进行核查。包括安全管理组织脆弱性核查、安全管理策略核查、安全管理制度脆弱性核查、人员安全管理核查、系统运维管理核查等。

3）对脆弱性严重程度进行等级化处理，不同的等级分别代表资产脆弱性严重程度的高低，并形成脆弱性分析报告。

6.3.5 控制措施：已有安全措施识别

风险评估服务提供者应对已采取的安全措施的有效性进行确认。有效的安全措施应继续保持，应防止安全措施的重复实施。对确认为不适当的安全措施应核实是否应取消或进行修正，或进行更新。

信息安全风险评估服务风险识别阶段的要求见表3。

表3 信息安全风险评估服务风险识别阶段的要求

要求		必备	可选
风险识别阶段			
资产识别	1）应对组织的资产进行分类	√	
	2）应识别组织和信息系统中的重要资产	√	
	3）应表示资产的重要程度	√	
	4）在通过资产识别和资产分析的基础上，形成资产列表和资产赋值报告	√	
威胁识别	1）风险评估服务组织应具有依据 GB/T 20984-2007 中的威胁分类方法对威胁进行分类的能力	√	
	2）应初步识别出组织和信息系统中潜在的对组织和信息系统组成影响的威胁，包括威胁源、威胁方式、威胁影响，并进而识别那些发生可能性较大、可能造成重大影响的重大威胁	√	
	3）应采用多种方法进行威胁调查		√
	4）应能在风险调查的基础上进行威胁分析，通过威胁源攻击能力、威胁源攻击动机、威胁发生频率、威胁影响程度确定计算威胁值的方法	√	
	5）应在威胁调查和威胁分析的基础上，形成威胁分析报告	√	
脆弱性识别	1）应进行安全技术脆弱性核查，一方面检查组织和资产自身在技术方面存在的脆弱性，另一方面核查所采取的安全措施的有效程度	√	
	2）应根据被评估单位安全保障管理要求，对管理及运行维护部门进行安全管理核查	√	
	3）应对脆弱性严重程度进行等级化处理，不同的等级分别代表资产脆弱性严重程度的高低，并形成脆弱性分析报告	√	
已有措施确认	1）风险评估服务提供者应对已采取的安全措施的有效性进行确认	√	

6.4 风险分析阶段

6.4.1 主要内容

风险分析阶段是风险评估实施的关键阶段。在本阶段工作中，需要构建风险分析模型，对识别阶段产生的资产信息、威胁信息、脆弱性信息等进行综合的风险分析。

6.4.2 控制措施：风险分析模型

1）构建风险分析模型应将资产、威胁、脆弱性三个基本要素及每个要素各自的属性进行关联并推导出风险值。

2）资产价值应依据资产在保密性、完整性和可用性上的赋值等级，经过综合评定得出。综合评定时，可根据组织的业务特点确定。

3）威胁的赋值应通过对威胁的属性，即威胁源的能力、动机、出现的频率及产生的影响进行综合分析获得。

4）技术脆弱性的赋值可直接引用基于CVSS（通用安全脆弱性评估系统）标准的脆弱性分析工具的检查值。管理脆弱性的赋值可以技术脆弱性的赋值原则作为参考，对上述各因素综合分析获得。

6.4.3 控制措施：风险计算方法

1）风险定性计算方法是将风险的各要素资产、威胁、脆弱性等的属性进行量化赋值，然后选用具体的计算方法（相乘法或矩阵法）进行风险计算。

2）风险定量计算方法是通过将资产价值和风险等量化为财务价值的方式来进行计算的一种方法。

3）在风险计算时，应根据实际情况选择定性计算方法或定量计算方法。

6.4.4 控制措施：风险分析与评价

1）应对风险的计算值进行等级化处理，目的是对风险的识别直观化，便于对风险进行评价。可根据实际情况划分级别。

2）风险等级化后，应对不同等级的安全风险进行统计、评价，形成最终的总体安全评价。

6.4.5 控制措施：风险评估报告

1）风险评估报告中应对本次评估建立的风险分析模型进行说明，并应阐明本次评估采用的风险计算方法及风险评价方法。

2）风险评估报告中应对计算分析出的风险给予比较详细的说明，应重点分析说明该风险对业务及系统的影响范围、影响程度。风险的评价结果表明了被评估组织的信息系统目前的整体风险状况。

信息安全风险评估服务风险分析阶段的要求见表4。

表4 信息安全风险评估服务风险分析阶段的要求

要求		必备	可选
风险分析阶段			
风险分析模型	1）构建风险分析模型时应将资产、威胁、脆弱性三个基本要素及每个要素各自的属性进行关联并推导出风险值	√	
	2）资产价值应依据资产在保密性、完整性和可用性方面的赋值等级，经过综合评定得出。在综合评定时，可根据组织的业务特点确定	√	
	3）威胁的赋值应通过对威胁的属性，即威胁源的能力、动机、出现的频率及产生的影响来综合分析获得	√	
	4）技术脆弱性的赋值可直接引用基于CVSS（通用安全弱点评估系统）标准的脆弱性分析工具的检查值；管理脆弱性的赋值可以技术脆弱性的赋值原则作为参考，对上述各因素综合分析获得	√	
风险计算方法	1）风险定性计算方法是将风险的各要素资产、威胁、脆弱性等的属性进行量化赋值，然后选用具体的计算方法（相乘法或矩阵法）进行风险计算	√	
	2）风险定量计算方法是通过将资产价值和风险等量化为财务价值的方式来进行计算的一种方法		√
	3）在风险计算时，可根据实际情况选择定性计算方法或定量计算方法		√

表4（续）

要 求		必 备	可 选
风险分析阶段			
风险分析与评价	1）应对风险的计算值进行等级化处理，目的是对风险的识别直观化，便于对风险进行评价。可根据实际情况划分级别	√	
	2）风险等级化后，应对不同等级的安全风险进行统计、评价，形成最终的总体安全评价	√	
风险评估报告	1）风险评估报告中应对建立的用于本次评估风险分析的模型进行说明，并需要阐明本次评估采用的风险计算方法及风险评价方法	√	
	2）风险评估报告中应对计算分析出的风险给予比较详细的说明	√	

6.5 风险处置阶段

6.5.1 主要内容

风险处置是风险评估实施的最后阶段，主要针对风险分析阶段发现的安全风险进行建议性的安全处置，从而使风险控制在可接受的范围内。

6.5.2 控制措施：风险处置原则

1）风险评估服务提供者应协助被评估组织确定风险处置原则，以及风险处置原则适用的范围和例外情况。

6.5.3 控制措施：安全整改建议

风险评估服务提供者应综合考虑脆弱性问题的严重程度、加固措施实施的难易程度、降低风险的时间紧迫程度等因素，为被评估组织提出安全整改建议。

6.5.4 控制措施：组织评审会

风险评估服务提供者应：

1）协助被评估组织召开评审会，并依据合同内容准备各类文档供参会人员进行评审；

2）依据最终的评审意见进行相应的整改，并将最终的整改材料与评估文档一并提交被评估对象，作为评估项目结束的移交文档。

6.5.5 控制措施：残余风险处置

在被评估组织按照风险评估的安全整改建议全部或部分实施安全加固后，风险评估服务提供者可对仍然存在的安全风险进行识别、控制和管理。

信息安全风险评估服务风险处置阶段的要求见表5。

表5 信息安全风险评估服务风险处置阶段的要求

要 求		必 备	可 选
风险处置阶段			
风险处置原则	风险评估服务提供者应协助被评估组织确定风险处置原则，以及风险处置原则适用的范围和例外情况	√	
安全整改建议	风险评估服务提供者应综合考虑脆弱性问题的严重程度、加固措施实施的难易程度、降低风险的时间紧迫程度等因素，为被评估组织提出安全整改建议		√
组织评审会	风险评估服务提供者应协助被评估组织召开评审会，并依据合同内容准备各类文档供参会人员进行评审	√	
	风险评估服务提供者应依据最终的评审意见进行相应的整改，并将最终的整改材料与评估文档一并提交被评估对象，作为评估项目结束的移交文档	√	
残余风险处置	在被评估组织按照风险评估的安全整改建议全部或部分实施安全加固后，风险评估服务提供者可对仍然存在的安全风险进行识别、控制和管理		√

7 信息安全风险评估服务能力分级评价要求

风险评估服务提供者应满足基本要求（见5.1）、管理要求（见5.2）、技术能力要求（见5.3），除此之外，根据风险评估服务提供者的机构注册资金、从业经验、人员素质要求、项目经验、管理能力和技术能力等要素，可将风险评估服务提供者的能力划分为三个等级，各级别的具体要求见7.1、7.2、7.3。

7.1 信息安全风险评估服务三级能力要求

7.1.1 基本资格

7.1.1.1 基本条件（见 5.1）。

7.1.1.2 注册资本/开办资金：产权关系明晰，注册资本/开办资金不少于 100 万元人民币。

7.1.1.3 人员素质要求：机构人员总数 20 人以上；信息安全风险评估服务人员 10 名以上；本科以上学历人员占机构总人数的比例在 60%以上；具有相关资质的信息安全风险评估服务人员至少 2 人。

7.1.1.4 从业时间：从事信息安全风险评估服务 1 年以上。

7.1.1.5 从业经验：能独立完成省级范围的信息系统风险评估项目或中小型企业的信息系统风险评估项目；近 3 年内至少完成 4 个以上完整的信息安全风险评估项目，无客户投诉，项目合同总金额不少于 50 万元人民币。

7.1.2 管理能力（见5.2）

7.1.3 技术能力（见5.3）

7.1.4 服务过程要求（见第6章）

7.2 信息安全风险评估服务二级能力要求

7.1.5 基本资格

7.1.5.1 基本条件（见 5.1）。

7.1.5.2 注册资本/开办资金：产权关系明晰，注册资本/开办资金不少于 500 万元人民币。

7.1.5.3 人员素质要求：机构人员总数 80 人以上；信息安全风险评估服务人员 15 名以上；本科以上学历人员占机构总人数的比例在 70%以上；具有相关资质的信息安全风险评估服务人员至少 6 人。

7.1.5.4 从业时间：从事信息安全风险评估服务 3 年以上。

7.1.5.5 从业经验：能独立完成省级范围的信息系统风险评估项目或大型企业的信息系统风险评估项目；近3年内至少完成6个以上完整的信息安全风险评估项目，无客户投诉，项目合同总金额不少于100万元人民币。

7.1.6 管理能力

7.1.6.1 基本管理能力（见 5.2）。

7.1.6.2 制定项目风险管理制度，评估项目风险，制定项目风险控制措施并跟踪其有效性。

7.1.6.3 制定服务质量持续改进制度，并跟踪落实情况。

7.1.7 技术能力

7.1.7.1 基本技术能力（见 5.3）。

7.1.7.2 有专门人员进行风险评估标准研究。

7.1.7.3 有专门人员跟踪、发现和挖掘安全漏洞。

7.1.7.4 有专门人员进行风险评估工具开发，并将工具应用到实践中。

7.1.8 服务过程要求（见第6章）

7.3 信息安全风险评估服务一级能力要求

7.1.9 基本资格

7.1.9.1 基本条件（见5.1）。

7.1.9.2 注册资本/开办资金：产权关系明晰，注册资本/开办资金不少于1000万元人民币。

7.1.9.3 人员素质要求：机构人员总数150人以上；信息安全风险评估服务人员30名以上；本科以上学历人员占机构总人数的比例在60%以上；具有相关资质的信息安全风险评估服务人员至少10人。

7.1.9.4 从业时间：从事信息安全风险评估服务5年以上。

7.1.9.5 从业经验：能独立完成全国范围的信息系统风险评估项目；近3年内至少完成10个以上完整的信息安全风险评估项目，无客户投诉，项目合同总金额不少于500万元人民币。

7.1.10 管理能力

7.1.10.1 基本管理能力（见5.2）。

7.1.10.2 制定项目风险管理制度，评估项目风险、制定项目风险控制措施并跟踪其有效性。

7.1.10.3 制定服务质量持续改进的制度，跟踪其落实情况。

7.1.10.4 参考GB/T 22080标准建立信息安全管理体系。

7.1.11 技术能力

7.1.11.1 基本技术能力（见5.3）。

7.1.11.2 应具备独立的测试环境及必要的软、硬件设备，用于满足信息系统仿真。

7.1.11.3 有专门团队跟踪、发现和挖掘和安全漏洞；并提交给国际或国内权威机构。

7.1.12 服务过程要求（见第6章）

8 评价要求

对风险评估服务提供者的服务能力主要是从基本资格、管理能力、技术能力、过程要求等4个方面综合评价。

基本资格主要包括基本条件、注册资本、人员素质要求、从业时间、从业经验等方面。管理能力包括保密管理、人员管理、项目管理、质量管理等方面；技术能力包括风险识别与分析、风险评估报告编写、安全技术的研究与跟踪能力等多个方面；过程要求包括4个方面。

评价所依据的证明材料至少包含：

a）营业执照、独立法人资格证明；

b）从事信息安全风险评估服务的相关资质证明材料；

c）安全保密制度及措施；

d）人员构成与素质证明材料；

e）组织结构、规模与资产、设施环境相关材料；

f）项目案例及业绩证明材料；

g）风险评估流程与操作规范、质量管理等材料。

参 考 文 献

[1] GB/T 22081-2007 《信息技术 安全技术 信息安全实施规则》

[2] ISO/FDIS 31000 《风险管理—规则与指南》

[3] ISO/IEC 27005:2008 《信息技术 安全技术 信息安全风险管理》

[4] NISTIR_7328 《安全评估提供者要求和客户职责》

[5] GB/Z 20286 《信息安全技术 信息安全事件分类分级指南》

[6] GB/T 22081 《信息技术 安全技术 信息安全管理实用规则》

[7] YD/T 1799-2008 《网络与信息安全应急处理服务资质评估方法》

[8] GB/T 19000.3 《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》

[9] GB/T 19001 《质量管理体系标准 要求》

[10] GB/T 19004.2 《质量管理和质量体系要素 第2部分：服务指南》

[11] GB/T 19004.4 《质量管理和质量体系要素 第4部分：质量改进指南》