

XXX

XXX



中华人民共和国国家标准

GB XXXXXX - 200X

信息系统安全服务资质评估准则

Evaluation Criteria for Competence of Information System
Security Service Provider

(初稿)

2000年4月,北京

200X-XX-XX 发布

200X-XX-XX 实施

国家质量技术监督局 发布

前 言

本标准的目的是对提供信息安全服务的组织进行资质评估与认证，为国家有关主管部门的行政管理提供技术依据。

本标准的评估对象是提供信息安全服务的组织，包括信息安全工程的设计、施工及其相关的咨询和培训组织。

与本标准相关的其它评估标准、评估细则和评估方法包括：

信息安全工程质量管理要求

信息安全服务资质评估等级划分细则

信息安全服务资质等级评估方法

……

本标准起草单位：中国国家信息安全测评认证中心，中国国家信息安全测评认证中心系统工程实验室，信息产业部电子第 30 研究所，四川大学信息安全研究所，中国国防科技信息中心，解放军总装备部，北京普方德信息技术有限公司，北京天融信公司。

本标准主要起草人：关义章、叶征、崔玉华、任卫红、唐海波、龙毅宏、刘炳华、满林松、周恩志等

本标准于 200X 年 X 月 X 日起实施。

本标准委托中国国家信息安全测评认证中心负责解释。

目 录

1 适用范围	1
2 定义	1
2.1 信息安全服务	1
2.2 信息安全服务提供者	1
2.3 信息安全服务资质等级	1
2.4 信息安全工程过程能力级别	1
2.5 信息安全服务评估组织	1
3 服务类型与资质评定原则	1
3.1 信息安全服务的类型	1
3.2 信息安全服务资质等级的评判原则	1
4 提供信息安全服务的基本资格要求	2
5 提供信息安全服务的基本能力要求	2
5.1 组织与管理要求	2
5.2 技术能力要求	2
5.3 人员构成与素质要求	3
5.4 设备、设施与环境要求	3
5.5 规模与资产要求	3
5.6 业绩要求	3
5.7 质量保证要求	4
5.8 培训要求	4
6 信息安全工程过程及能力级别	4
6.1 概述	4
6.2 信息安全工程过程要求	5
6.2.1 评估安全对系统的影响	5
6.2.2 评估系统面临的安全威胁	5
6.2.3 评估系统的安全弱点	5
6.2.4 评估系统的安全风险	5
6.2.5 确定系统的安全需求	6
6.2.6 为系统提供必要的安全信息	6
6.2.7 监测系统的安全状况	6
6.2.8 管理系统的安全控制	7
6.2.9 安全性协调	7
6.2.10 检验并证实安全性	7
6.2.11 建立并提供安全性保证证据	7
6.3 信息安全工程过程能力级别	8
6.3.1 基本执行级	8

6.3.1.1	执行过程	8
6.3.2	计划跟踪级	8
6.3.2.1	制定过程执行计划	8
6.3.2.2	规范化执行	8
6.3.2.3	验证执行	8
6.3.2.4	跟踪执行	8
6.3.3	充分定义级	8
6.3.3.1	定义标准过程	8
6.3.3.2	执行已定义过程	8
6.3.3.3	协调项目和组织活动	9
6.3.4	定量控制级	9
6.3.4.1	建立可测量的质量目标	9
6.3.4.2	客观地管理执行	9
6.3.5	连续改进级	9
6.3.5.1	改进组织能力	9
6.3.5.2	改进过程有效性	9
7	信息安全服务资质等级划分	9
7.1	概述	9
7.2	信息安全服务资质等级划分	9
7.3	不同资质等级可从事的安全服务	11
8	引用标准与参考文献	12
8.1	计算机信息系统安全保护等级划分准则	12
8.2	系统工程能力成熟模型	12
8.3	系统安全工程能力成熟模型	12
8.4	系统安全工程能力成熟模型—评定方法	12
8.5	信息系统安全工程手册	12
8.6	软件工程能力成熟模型	12
8.7	信息安全工程质量管理要求	12
9	附录——系统安全工程主要术语	13
9.1	组织	13
9.2	项目	13
9.3	系统	13
9.4	安全工程	13
9.5	安全工程生命期	13
9.6	工作产品	14
9.7	顾客	14
9.8	过程	14
9.9	过程能力	14
9.10	制度化	14
9.11	过程管理	14

1 适用范围

本标准适用于评估机构对提供信息安全服务的组织进行信息安全服务资质的评估；信息安全服务的需方对服务提供方的选择依据；作为国家主管部门对评估对象进行管理和检查的技术规范。另外，也可为信息安全服务提供组织改进自身能力提供指导。

2 定义

2.1 信息安全服务

信息安全服务是指信息安全工程的设计、实施、测试、运行和维护，以及相关的咨询和培训活动。

2.2 信息安全服务提供者

信息安全服务提供者是指信息安全工程方案设计组织、承建信息安全工程的组织以及提供有关信息安全咨询和培训的组织。

2.3 信息安全服务资质等级

信息安全服务资质等级是指一个组织提供信息安全服务的综合能力。包括技术能力、组织结构与管理、资源配置、安全工程过程能力、业绩和质量保证等多个方面。

2.4 信息安全工程过程能力级别

信息安全工程过程能力级别是指提供信息安全服务的组织在完成工程、项目时，执行组织已定义过程的能力成熟程度。

2.5 信息安全服务评估组织

信息安全服务评估组织，是指对提供信息安全服务的组织的资质等级进行评估认证的第三方机构。在我国是指中国国家信息安全测评认证中心及其授权分支机构。

3 服务类型与资质评定原则

3.1 信息安全服务的类型

信息安全服务的类型主要指一个组织按照一定的合同或协议，为另一个组织所履行的安全服务的具体形式，包括：

- 1) 安全工程：为信息系统进行安全方案设计（开发）、施工（安全集成）、验证（测试）运行（监控）和维护；
- 2) 安全咨询和培训：从事信息系统安全咨询、培训、宣传和其它安全工程之外服务的业务。包括书面提出并制订信息系统安全方案，提供安全管理与操作规定的服务，提供安全性测试和监控，方案（安全方案、信息系统和安全产品等）试验，在公开场合或媒体宣讲传播安全知识的活动，信息系统安全的专家活动和政策制订工作，从事信息系统安全教育工作，其它可能影响信息系统安全性能的有偿或无偿服务或技术活动。

3.2 信息安全服务资质等级的评判原则

信息安全服务资质评估是对信息安全服务提供者的资格状况、技术实力和实施安全工程过程质量保证能力等方面的具体衡量和评价。资质等级的评定，是在其基本资格和能力水平、安全工程项目的组织管理水平、安全工程基本过程的实施和控制能力等方面的单项评估结果基础上，针对不同的服务种类，采用一定的权值综合考虑后确定，并由国家认证机构授予相应的资质级别。信息安全服务的资质等级的划分遵循以下原则：

1. 综合考虑原则：

信息安全服务资质等级的划分必须对组织的综合能力进行考察，它主要与组织的资格状况、技术实力、信息安全工程过程能力等级以及其他要求有关。

2. 与现行国家有关主管部门颁布的法律、法规、规章、制度相一致的原则：

安全策略要保持与现行的法律、法规、规章、制度相一致，不能相抵触。

3. 与我国已发布或即将发布的有关信息安全的标准相一致的原则：

我国已发布许多与安全服务有关的标准，本评估准则的资质等级划分必须与这些标准相一致。

4. 与组织的基本能力水平紧密结合的原则：

一个组织的基本能力是评估其资质等级的基本要求，有些基本能力要求可能决定一个组织是否具备参与资质评定的资格。

5. 与信息安全服务工程过程能力等级紧密结合的原则：

工程过程能力等级是反映组织实施工程的成熟程度，是评定资质的重要依据。

6. 可裁剪原则：

安全服务有多种类型，对不同类型的安全服务可进行适当的裁剪。

7. 可操作性原则

具有实际操作的可行性。

4 提供信息安全服务的基本资格要求

4.1 提供信息安全服务的组织必须是一个独立的实体，具有工商行政管理部门发给的合法的营业执照。

4.2 必须获得国家有关信息安全主管部门发给的从事信息安全服务的资格证书。

4.3 从事涉密(国家秘密)网络信息系统安全服务的组织必须获得国家主管部门的批准。

4.4 采用商密信息产品进行安全系统集成的组织必须获得国家主管部门的批准。

4.5 必须遵守国家现行法律、法规的规定。

5 提供信息安全服务的基本能力要求

5.1 组织与管理要求

从事信息安全服务的组织：

5.1.1 必须拥有健全的组织结构和管理体系，为持续的信息安全服务提供保证。

5.1.2 应制定符合国家保密机关要求的工作保密制度和相关的组织监管体系。

5.1.3 所有成员要签定保密合同，并遵守有关法律法规。

5.2 技术能力要求

从事信息安全服务的组织，应：

5.2.1 了解信息安全技术的最新动向，有能力掌握信息安全的最新技术。

- 5.2.2 具有不断的技术更新能力。
- 5.2.3 具有对信息系统所面临的安全威胁、存在的安全隐患进行信息收集、识别、分析和提供防范措施的能力。
- 5.2.4 须能根据对用户信息系统风险的分析，向用户建议有效的安全保护策略及建立完善的安全管理制度。
- 5.2.5 具有对发生的突发性安全事件进行分析和解决的能力。
- 5.2.6 从事安全系统集成和相关咨询的组织应具有足够的技术力量，对市场的信息安全产品进行功能分析、提出安全策略和安全解决方案、及安全产品的系统集成能力。
- 5.2.7 应具有足够的技术力量，根据服务业务的需求开发信息安全应用、产品或支持性工具的能力。
- 5.2.8 系统集成商应有对集成的系统进行检测和验证的能力。
- 5.2.9 有能力对信息安全系统进行有效的维护。
- 5.2.10 有跟踪、了解、掌握、应用国际、国家和行业标准的能力。

5.3 人员构成与素质要求

- 5.3.1 从事信息安全服务的组织应具有充足的人力资源和合理的人员结构。
- 5.3.2 所有与信息安全服务有关的管理和销售人员等应具有基本的信息安全知识。
- 5.3.3 应有一批相对稳定的技术队伍。
- 5.3.4 技术骨干人员应系统地掌握信息安全基础理论和核心技术，并有足够的专业工作经验。

5.4 设备、设施与环境要求

从事信息安全的组织，应：

- 5.4.1 具有固定的工作场所，良好的工作环境。
- 5.4.2 具有先进的开发、测试或模拟环境。
- 5.4.3 具有先进的开发、生产和测试设备。
- 5.4.4 具有实施相关服务的必需的开发、生产和测试工具。

5.5 规模与资产要求

从事信息安全的组织，应：

- 5.5.1 有足够的注册资金和充足的流动资金。
- 5.5.2 建立与所承担的业务范围和工程规模相适应的服务体系。
- 5.5.3 有足够的人员从事直接与信息安全服务相关的活动。

5.6 业绩要求

从事信息安全的组织，应具有与申请资质相符的从业经历，主要考查：

- 5.6.1 从业时间
- 5.6.2 工程或项目规模

5.6.3 工程或项目数量

5.6.4 工程或项目质量

5.6.5 合作项目参与程度

5.6.6 完成结果评价

5.7 质量保证要求

5.7.1 提供信息系统安全工程服务的组织要求通过“信息系统安全工程质量管理要求”；

5.7.2 提供信息系统安全咨询培训服务的组织要求通过经裁剪的“信息系统安全工程质量管理要求”；裁剪原则应与业务范围和控制环节相一致。

5.8 培训要求

提供培训服务的服务组织应：

5.8.1 有独立的法人资格；

5.8.2 有固定的培训场所，良好的培训环境；

5.8.3 有相应培训设备；

5.8.4 培训人员要有培训资格证书。

6 信息安全工程过程及能力级别

6.1 概述

信息安全工程是一组与信息安全相关的工程过程的集合，在应用到系统和应用的开发、集成、操作、管理、维护和改进等整个生命期中，应满足一组安全要求并能在系统中得到体现。信息安全工程至少包括以下 11 个基本过程，

- 评估安全对系统的影响；
- 评估系统面临的安全威胁；
- 评估系统的安全弱点；
- 评估系统的安全风险；
- 确定系统的安全需求；
- 为系统提供必要的安全信息；
- 监测系统的安全状况；
- 管理系统的安全控制；
- 安全协调；
- 检验并证实安全性；
- 建立并提供安全性保证证据。

信息安全工程过程的能力级别是用于评价组织完成已定义的安全工程过程的能力，直接反映组织的成熟程度。能力级别按成熟性排序，表示依次增加的组织能力。

本标准将信息安全服务组织的工程能力分为五个级别，即：

- 1 级：基本执行级；
- 2 级：计划跟踪级；
- 3 级：充分定义级；
- 4 级：量化控制级；
- 5 级：连续改进级。

本标准并不提出执行过程的特殊要求。组织可以按所选择的任何方式和顺序，自由地计划、定义、控制、跟踪和改进他们的过程。然而高级别能力依赖于低级别能力，因此组织在达到高级别之前必须满足低级别的要求。

6.2 信息安全工程过程要求

6.2.1 评估安全对系统的影响

本过程目的在于确认实施的安全工程对系统造成的影响，并对发生影响的可能性进行评估。包括以下一些活动：

1. 对在系统中起关键作用的运行、商务或任务能力进行确定、分析和按优先级排列。
2. 对支持系统的关键运行能力或安全目标的系统资产（资源和数据）进行确定和特征化。通过对给定环境中提供这种支持的每项资产的意义进行评估，来定义每项资产。
3. 选择用于评估影响的度量。
4. 标识所选影响的评估度量以及（若需要）度量转换因子之间的关系。
5. 利用多重度量或统一度量的合适方法对意外事件的影响进行识别和特征化。
6. 监视影响的变化。

6.2.2 评估系统面临的安全威胁

本过程的目的在于确定系统面临的安全威胁及其性质和特征。包括以下活动：

1. 识别由自然原因引起的威胁。
2. 识别由人为原因引起的威胁。
3. 识别特定环境中适当的测量方法和适用范围。
4. 评估由人为原因引起的威胁的动因和效力。
5. 评估出现威胁事件的可能性。
6. 监视各种威胁及其特征的变化趋势。

6.2.3 评估系统的安全弱点

本过程的目的在于识别和特征化系统本身的安全脆弱性。其中包括分析系统资产、定义特殊的脆弱性以及提供对整个系统脆弱性的评估。以掌握在确定环境中系统的安全脆弱性。包括以下活动：

1. 选择对确定环境中系统安全脆弱性进行标识和特征化的方法、技术和标准。
2. 识别系统安全脆弱性。
3. 收集与脆弱性相关的数据。
4. 评估由特定脆弱性及其组合所产生的系统脆弱性和脆弱性总和。
5. 监视脆弱性及其特征的变化趋势。

6.2.4 评估系统的安全风险

本过程的目的是确定在给定环境中，与某一系统有依赖关系的安全风险。尤其是识别和评估出现暴露的可能性，以掌握对给定环境中运行该系统带来的安全风险，并按照给定的方

法对风险问题进行优先级排序。包括以下活动：

1. 选择用于分析、评估和比较给定环境中系统安全风险所依据的方法、技术和准则。
2. 识别威胁/脆弱性/影响三者的组合（暴露），掌握这些威胁和脆弱性的利害关系，确定出现威胁和脆弱性将造成的影响。
3. 评估与每个暴露有关的风险，确定一个暴露出现的可能性。
4. 评估与该暴露风险有关的总体不确定性。
5. 按优先级对风险进行排列。
6. 监视各种风险及其特征的变化趋势。

6.2.5 确定系统的安全需求

本过程的目的在于确定系统的安全需求。涉及到为系统安全定义基本原则，以及有关的法律、策略和组织需求，并实现组织内部以及顾客对安全需求达成共识。包括以下活动：

1. 理解顾客对安全的需求，收集所有用于全面理解顾客安全需求所需的信息。
2. 为给定系统确定法律、策略、标准、外部影响和约束。
3. 确定系统的用途及其与安全的关联性。
4. 系统运行安全的高层规划。
5. 定义系统的安全性。
6. 定义与安全相关的需求。
7. 达成满足顾客要求的安全协议。

6.2.6 为系统提供必要的安全信息

本过程的目的在于为系统的规划者、设计者、实施者或用户提供他们所需的安全信息。包括安全体系结构、设计或实施选择以及安全指南。所有具有安全意义的系统问题都应受到检查，并按照安全目标的要求予以解决，所有项目组成员都理解安全问题，选择的解决方法应反映出所提供的安全输入。包括以下活动：

1. 确保设计者、开发者和用户对安全信息具有共同的理解。
2. 确定有科学依据的工程选择所需的安全约束和考虑。
3. 确定与安全相关的工程问题的解决办法。
4. 利用安全约束和考虑来分析和区分工程选项的优先级。
5. 向其它工程组提供与安全相关的指南。
6. 为系统的用户和管理员提供与安全相关的指南。

6.2.7 监测系统的安全状况

本过程的目的是保证能确定并报告所有的安全违规，并监视外部和内部环境可能影响系统安全的所有因素。包括以下活动：

1. 分析事件记录，以确定一个事件的原因。检测与安全相关的历史和事件记录（包括日志记录）。

2. 监视威胁、脆弱性、影响、风险和环境方面的变化。
3. 识别与安全相关的突发事件。
4. 监视安全防护措施的性能和有效性。
5. 检查系统安全状况以进行必要的改正。
6. 管理对有关安全突发事件的响应。
7. 保证与安全监视有关的设备得到适当的保护。

6.2.8 管理系统的安全控制

本过程的目的在于保证集成到系统设计中的预期的系统安全性确实由最终系统在运行状态下达到。管理和维护开发环境和运行系统的安全控制机制所需要的活动。保证在整个生命周期内不降低安全级别。包括以下活动：

1. 建立安全控制的职责和责任并通知到组织中的每一个人。
2. 管理系统安全控制的配置。
3. 管理所有用户和管理员的培训和教育大纲，提高安全意识。
4. 对管理安全服务及控制机制进行定期的维护。

6.2.9 安全性协调

本过程的目的在于保证所有部门都有一种参与安全工程的意识。这种协调涉及到保持安全组织、其他工程组织和外部组织之间的开放交流，使项目组的所有成员都具有并参与安全工程工作的意识，充分发挥他们的作用。包括以下活动：

1. 定义安全工程协调目标和相互关系。
2. 确定安全工程的协调机制。
3. 促进安全工程的协调。
4. 用确定的机制去协调有关安全的决定和建议。

6.2.10 检验并证实安全性

本过程的目的在于确保解决安全问题的办法已得到验证和证实。通过观察、示范、分析和测试，依照安全需求、体系结构和设计确认解决办法，依照顾客的运行安全需求证实解决办法。确保解决办法满足安全需求以及顾客运行安全要求。包括以下活动：

1. 确定待验证和证实的解决办法。
2. 定义验证和证实每种解决方案的方法和严密等级。
3. 通过证明能满足与上一抽象层相关的要求，最终满足用户的运行安全要求，实现对解决办法的证实。
4. 为其它工程组收集验证和证实的结果。

6.2.11 建立并提供安全性保证证据

本过程的目的是清楚地向顾客提供已满足其安全需求的证据。保证证据是一系列声明性保证目标。这些目标由多个不同来源和等级的抽象构成的保证证据组成。本过程包括对与需求有关的保证进行的识别和定义；证据的产生和分析；支持保证需求所需的附加证据；对所

生成的证据进行收集、打包并准备随时递交。包括以下活动：

1. 确定安全保证目标。
2. 所有保证目标定义一个安全保证策略。
3. 确定并控制安全保证证据。
4. 对安全保证证据进行分析。
5. 提供证明顾客安全需求得到满足的安全保证性论据。

6.3 信息安全工程过程能力级别

6.3.1 基本执行级

处于本能力级别的组织是基于个人的知识和努力去执行一些基本过程,而未经严格的计划和跟踪。能提供的证据是该过程的工作产品(输出)。由于缺乏适当控制,工作产品的一致性、性能和质量会存在极大的差异。

6.3.1.1 执行过程

此要求保证组织以某种方式执行一些基本过程,从而为顾客提供工作产品和/或服务。

6.3.2 计划跟踪级

处于本能力级别的组织计划并跟踪执行本组织已定义的过程,验证是否执行了特定的步骤,工作产品是否符合指定的标准和需求,测量用于跟踪过程的执行情况。组织能够基于实际执行活动进行管理。

6.3.2.1 制定过程执行计划

过程执行的计划涉及到过程文档的编制,执行过程的相应工具的提供、过程实施的计划、过程执行中的培训、过程资源的分配以及过程执行的责任分配。

6.3.2.2 规范化执行

此要求注重于控制覆盖过程的总数。需要列出过程执行计划的使用、基于标准和程序的过程执行、配置管理下依过程产生的工作产品。

6.3.2.3 验证执行

确认过程按预定的方式执行。涉及到验证执行过程与可应用的标准和程序是一致的以及对工作产品的审计。

6.3.2.4 跟踪执行

此要求注重于组织控制项目进展的能力。组织通过可测量的计划跟踪过程的执行情况,当过程实施与计划产生重大偏离时应采取纠正措施。

6.3.3 充分定义级

处于本能力级别的组织执行充分定义的过程。组织依据对已批准发布的、文档化的标准过程进行适当裁减,来充分定义组织的过程。

本级与级别2的主要区别在于利用组织范围内的标准过程来管理和规划。

6.3.3.1 定义标准过程

该要求注重于组织标准过程的制度化。一个组织的标准过程可能需要裁剪以适合特定环境的使用,因此,要求组织提出标准过程的文档,并为满足特定用途而对标准过程进行裁剪。

6.3.3.2 执行已定义过程

该要求注重于执行充分定义过程的可重复性。要求组织使用制度化过程,并对有缺陷的

过程结果和工作产品进行复查，执行过程并使用结果数据。

6.3.3.3 协调项目和组织活动

该要求注重项目和组织活动的协调。大的工程通常由多个组协作完成，缺乏协调将会导致延误和不可比对的结果。因此应确定组内、组间、组外活动的协调。

6.3.4 定量控制级

处于本能力级别的组织应收集和分析执行的详细测量，获得对过程能力和改进能力的量化理解以预测执行情况。这个级执行的管理是客观的，工作产品的质量是量化的。这一级与充分定义级的主要区别在于定义的过程是定量的表示和控制。

6.3.4.1 建立可测量的质量目标

该要求注重对组织所开发的产品（包括工作产品）建立可测量的质量目标。

6.3.4.2 客观地管理执行

该要求注重于确定过程能力的量化测量并使用量化测量来管理这一过程。提出了确定量化过程能力和以量化测量作为修正行动的基础。

6.3.5 连续改进级

处于本能力级别的组织基于组织的商务目标，并针对过程有效性和效率建立量化执行目标。通过执行已定义的过程和有创见的新概念、新技术的量化反馈来保证对这些目标进行连续的过程改进。

这一级与定量控制级的主要区别在于已定义的过程和标准过程基于对这些过程变化效果的量化理解，进行连续调整和改进。

6.3.5.1 改进组织能力

该要求注重在整个组织范围内使用标准过程，并在同的使用中进行比较。在使用这些过程时，寻找改进标准过程的机会，分析产生的缺陷以识别对标准过程的进行改进的可能性。

6.3.5.2 改进过程有效性

该要求注重于制定处于连续受控改进状态下的标准过程。组织能消除标准过程产生缺陷的原因，并提出连续改进的标准过程。

7 信息安全服务资质等级划分

7.1 概述

信息安全服务资质等级是对安全服务组织综合实力的客观评价，反映了安全服务组织的信息安全服务资格、水平和能力。

资质等级划分的主要依据包括：基本资格要求、基本能力要求、安全工程过程能力和其他补充要求等。

7.2 信息安全服务资质等级划分

基本资格要求是评定安全服务组织资质等级的起评条件，申请资质等级的安全服务组织必须完全满足基本资格要求。考查内容主要包括以下几个方面：

独立法人资格

安全服务许可资格

保密要求

基本能力要求是评定安全服务组织资质等级的基础，申请资质等级的安全服务组织在评定过程中体现的能力差异将成为资质等级划分的重要依据；根据具体服务类型和业务范围，

可针对性地裁剪基本能力要求，划分方法详见“信息安全服务资质评估等级划分细则”。对从事不同类型服务的组织有不同的基本要求。考查内容主要包括以下几个方面：

组织和管理

规模和资产

质量保证

技术能力

人员构成与素质

设备、设施与环境

业绩

培训

安全工程过程能力级别是评定安全服务组织资质的主要依据，标志着服务组织提供给客户的安全服务专业水平和质量保证程度。对提供不同类型服务的组织有不同的安全工程要求，即根据具体服务类型和业务范围，可针对性的裁剪安全工程过程要求。安全工程过程能力级别的高低，标志着从事安全服务的组织能力成熟程度，即已完成过程的管理和制度化程度的高低。主要对以下几个过程进行考查：

评估安全对系统的影响

如何对系统安全威胁进行评估

如何对系统安全弱点进行评估

如何对系统安全风险进行评估

如何确定系统的安全需求

如何提供系统的安全输入

如何监测系统的安全状况

如何进行安全控制的管理

如何进行安全协调

如何检验和证实系统的安全性

如何建立系统安全的保证证据

根据具体服务类型和业务范围，将适当增加有关工程、技术或管理要求安全服务资质等级分为5级，由1级到5级递增。如下表所示：

表 7-1 安全服务资质等级定义

资质等级	说明
1 级	达到全部基本资格要求和部分基本能力要求 ;执行基本的安全工程过程 ,安全工程过程能力达到 1 级。
2 级	达到全部基本资格要求和基本能力要求 ;执行基本的安全工程过程 ,安全工程过程能力达到 2 级 ,使安全工程过程质量得到基本保证。
3 级	达到全部基本资格要求和基本能力要求 ;执行基本的安全工程过程 ,安全工程过程能力达到 3 级 ,使安全工程过程质量得到良好保证。
4 级	达到全部基本资格要求和基本能力要求 ;执行基本的安全工程过程 ,安全工程过程能力达到 4 级 ,使安全工程过程质量得到良好控制。
5 级	达到全部基本资格要求和基本能力要求 ;执行基本的安全工程过程 ,安全工程过程能力达到 5 级 ,使安全工程过程质量实现优化运作。

表 7-2 提出了实现某级资质所必须达到的基本要求 ;服务组织根据自身情况可实现更多或更高的要求。

表 7-2 安全服务资质等级要求

资质等级	基本资格要求	基本能力要求	安全工程能力级别	其他补充要求
1 级	全部满足	基本满足 不同服务类型可裁剪	1 级 不同服务类型可裁剪	无
2 级	全部满足	满足 不同服务类型可裁剪	2 级 不同服务类型可裁剪	针对性补充要求
3 级	全部满足	满足 不同服务类型可裁剪	3 级 不同服务类型可裁剪	针对性补充要求
4 级	全部满足	满足 不同服务类型可裁剪	4 级 不同服务类型可裁剪	针对性补充要求
5 级	全部满足	满足 不同服务类型可裁剪	5 级 不同服务类型可裁剪	针对性补充要求

7.3 不同资质等级可从事的安全服务

根据国家法律、法规和有关主管部门对具体资质等级要求的规定执行。

8 引用标准与参考文献

- 8.1 计算机信息系统安全保护等级划分准则
(GB17859-1999, 国家质量技术监督局);
- 8.2 系统工程能力成熟模型
(SE-CMM, V1.1)
- 8.3 系统安全工程能力成熟模型
(SSE-CMM, V2.0)
- 8.4 系统安全工程能力成熟模型—评定方法
(SSAM, V2.0);
- 8.5 信息系统安全工程手册
- 8.6 软件工程能力成熟模型
(SW-CMM, V1.1)
- 8.7 信息安全工程质量管理要求

9 附录——系统安全工程主要术语

9.1 组织

组织定义为：公司内部单位、整个公司或其它实体(如政府机构或服务分支机构)。组织中通常存在许多项目，并作为一个整体加以管理。组织内的所有项目一般遵循上层管理的公共策略。一个组织机构可能由同一地方分布的或地理上分布的项目与基础支持设施所组成。术语“组织”的使用意味着一个支持共同战略、商务和过程相关功能的基础设施。为了服务提供的有效性，必须存在一个基础设施并对其加以维护。

9.2 项目

项目是各种实施活动和资源的总和，这些实施活动和资源用于开发或维护一个特定的产品或提供一种服务。产品可能包括硬件、软件及其它部件。一个项目往往有自己的资金，成本帐目和交付时间表。为了生产产品或提供服务，一个项目可以组成自己专门的组织，或是由组织建立一个项目组、特别工作组或其它实体。

9.3 系统

在本标准中，系统是指：

- 提供某种能力用以满足一种需要或目标的人员、产品、服务和过程的综合。
- 事物或部件的汇集形成了一个复杂或单一整体（即一个用来完成一个特定或一组功能组件的集合）。
- 功能相关的元素相互组合。

一个系统可以是一个硬件产品、硬软件组合产品、软件产品或是一种服务。在整个模型中术语“系统”的使用是指需要提交给顾客或用户产品的总和。当说某个产品是一个系统时意味着必须以规范化和系统化的方式对待产品的所有组成元素及接口，以便满足商务实体开发产品的成本、进度及性能（包括安全）的整体目标。

9.4 安全工程

安全工程是一个不断发展的领域，是一组与安全相关的工程过程的集合，它应满足一组安全要求，并应用到系统和应用的开发、集成、操作、管理、维护和改进以及产品的开发、交付和升级中。安全工程能够在系统、一个产品或一个服务的安全考虑中得到体现。

9.5 安全工程生命期

是指在一个项目或系统中，安全工程从启动到终止的完整过程。在整个安全工程生命期中执行的安全工程活动包括：

- 前期概念
- 概念开发和定义
- 证明与证实
- 工程实施、开发和制造
- 生产和部署
- 运行和支持
- 终止

9.6 工作产品

工作产品是指在执行任何过程中产生出的所有文档、报告、文件、数据等。SSE-CMM不是为每一个过程区列出各自工作产品，而是按特定的基本实施列出其“典型的工作产品”，其目的在于对所需的基本实施范围可做进一步定义。列举的工作产品只是说明性的，目的在于反映组织机构和产品的范围。这些典型的工作产品不是“强制”的产品。

9.7 顾客

顾客是为其提供产品开发或服务的个人或实体组织，顾客也包括使用产品和服务的个人和实体组织。顾客可以是经商议的或未经商议的。经商议是指依据合同来开发基于顾客规格的一个或一组特定的产品。未经商议是指市场驱动的，即市场真正的或潜在的需求。一个顾客代理如面向市场或产品代理也代表一种顾客。

9.8 过程

一个过程是指为了一个给定目的而执行的一系列活动。这些活动可以重复、递归和并发地执行。有的活动将输入工作产品转换为输出工作产品提供给其它活动。输入工作产品和资源的可用性以及管理控制制约着允许的活动执行顺序。一个充分定义的过程包括活动定义、每个活动的输入输出定义以及控制活动执行的机制。

9.9 过程能力

过程能力是遵循一个过程可达到的可量化范围。一个组织的过程能力可帮助预见项目目标的能力。低能力级别组织的项目在达到预定的成本、进度、功能和质量目标上会有很大的变化。

9.10 制度化

制度化是建立方法、实施和步骤的基础设施和组织文化。制度化提供了通过完善的安全工程性质获得最大益处的途径。

9.11 过程管理

过程管理是一系列用于预见、评价和控制过程执行的活动和基础设施。过程管理意味着过程已定义好。注重过程管理含义是项目或组织需在计划、执行、评价、监控和校正活动中既要考虑产品相关因素，也要考虑过程相关因素。