# 通信网络安全服务能力评定准则

## 1. 通信网络安全服务概述

### 1.1 概念

本准则所述的通信网络包括电信网和互联网，所涉及的安全服务是指为了适应通信网络安全管理的需要，运用科学的方法和手段，通过有效的措施来保障通信网络的正常运行，为企业提供全面或部分安全评估、设计与集成的服务，包含从安全体系到具体的技术解决措施。

### 1.2 类型

本准则涉及到的通信网络安全服务可以分为两种类型：风险评估、安全设计与集成。

1）风险评估

运用科学的方法和手段，系统地分析通信网络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，防范和化解通信网络及相关系统安全风险，将风险控制在可接受的水平，为最大限度地保障通信网络及相关系统的安全提供科学依据。

2）安全设计与集成

对所服务的通信网络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、安全加固或其它的安全技术和咨询服务。

2. 通信网络安全服务能力等级的评判原则

通信网络安全服务能力是对通信网络安全服务单位的客观评价，直接反应了通信网络安全服务单位的服务资格、水平和能力。

通信网络安全服务能力要求分别针对每一类服务单位分为基本要求和分类要求，基本要求是指所有通信网络安全服务单位都必须要达到的安全能力要求；分类要求是指对不同类型的通信网络安全服务单位提出了不同的能力要求，其中风险评估、安全设计与集成类服务分别提出了三级能力要求，由高到低依次是三级、二级、一级能力。在本准则中，高等级能力的要求涵盖了低等级能力要求的所有方面。

通信网络安全服务能力评定要求是对通信网络安全服务单位的资格状况、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。

3. 通信网络安全服务能力等级基本要求

3.1　法律要求

1) 在中华人民共和国境内注册成立（港澳台地区除外）；

2) 由中国公民投资、中国法人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）；

3) 从事涉密的通信网络安全服务单位必须满足国家保密机关的相关要求；

4) 从事通信网络安全服务工作一年以上且无违法记录；

5) 法人及主要业务、技术人员无犯罪记录。

3.2　组织与管理要求

1) 拥有健全的组织与管理体系，拥有清晰的组织结构图，具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等内部管理制度，并能有效组织实施与考核；

2) 落实保密规章制度，对通信网络安全服务保密，制度中至少规定了：保守安全服务过程中知悉的国家秘密、商业秘密、技术秘密和公民隐私信息，具备严格的控制方法来防范服务过程中产生的泄密风险，不得出售或者非法向其他组织和个人提供在安全检测过程所获信息，具备相应的控制办法；

3) 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责任。

3.3　设备、设施与环境要求

1) 具有固定的办公场所；

2) 具有专门从事通信网络安全服务的相关工具或软件；

3) 具有进行安全服务所必须的实验环境。

3.4 项目管理要求

1) 具有成文的项目管理制度，并提供项目管理制度有效运行的证据，例如管理制度流程中具有核心流程、支持流程、管理流程等制度体系；

2) 具有对员工进行安全技术、项目管理的培训机制和计划，并有效组织实施与考核的相关记录。

3.5 质量保证要求

1) 建立并落实质量管理体系，并提供质量保证有效实现的证据；

2) 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。

4. 风险评估能力评定要求

4.1 一级能力评定要求

4.1.1 资格要求

1) 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3章通用性要求的所有条款；

2) 进行涉密集成的组织必须获得国家保密部门的能力证书。

4.1.2 规模与资产

1) 单位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。

4.1.3 人员构成和素质要求

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。

4.1.4 业绩要求

1) 单位应具备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。

4.1.5 组织与管理要求

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责任。

4.1.6 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。

4.1.7 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。

4.1.8 技术能力要求

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。

4.1.9 服务队伍要求

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）。

4.1.10 设备、设施与环境要求

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。

4.1.11 服务过程能力要求

从事风险评估的组织应具有以下基本能力:

— 评估系统安全威胁的能力;

— 评估系统脆弱性的能力;

— 评估安全对系统的影响的能力;

— 评估系统安全风险的能力;

— 确定系统的安全需求的能力;

— 确定系统的安全输入的能力;

— 进行管理安全控制的能力;

— 进行监测系统安全状况的能力;

— 进行安全协调的能力;

— 进行检测和证实系统安全性的能力;

— 进行建立系统安全的保证证据的能力;

— 根据风险评估结果进行系统整改的能力。

4.2 二级能力评定要求

应达到本标准4.1风险评估服务商一级能力要求的所有条款，并在以下方面增强或增加要求:

4.2.1 规模与资产

1) 单位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。

4.2.2 人员构成和素质要求

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。

4.2.3 业绩要求

1) 单位应具备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。

4.2.4 组织与管理要求

1) 应具有专门从事电信网和互联网安全风险评估服务的部门或团队；

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。

4.2.5 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。

4.2.6 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）。

4.2.7 技术能力要求

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评估服务；

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。

4.2.8 服务队伍要求

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）。

4.2.9 设备、设施与环境要求

1) 应具有针对网络安全问题研究的实验环境;

2) 应具有成熟的的工具、软件体系。

4.3 三级能力评定要求

应达到本标准4.2风险评估服务商二级能力要求的所有条款，并在以下方面增强或增加要求:

4.3.1 规模与资产

1) 单位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。

4.3.2 人员构成和素质要求

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。

4.3.3 业绩要求

1) 单位应具备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) 单位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。

4.3.4 组织与管理要求

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单位二级部门；

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。

4.3.5 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ISO27001制定完善的信息安全管理体系规范（ISMS）。

4.3.6 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。

4.3.7 技术能力要求

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。

4.3.8 服务队伍要求

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（有相关的能力证书如：CIW、CISP、CISSP、CISA等）；

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。

4.3.9 设备、设施与环境要求

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。

## 5 安全设计与集成服务能力评定要求

### 5.1 一级能力评定要求

应达到本标准第3章通信网络安全服务能力评定通用性要求的所有条款。

5.1.1 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。

5.1.2 规模与资产

1) 单位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。

5.1.3 人员构成和素质要求

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。

5.1.4 业绩要求

1) 单位应具备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。

5.1.5 组织与管理要求

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责任。

5.1.6 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。

5.1.7 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。

5.1.8 技术能力要求

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侧率和安全解决方案，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。

5.1.9 服务队伍要求

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（有相关的能力证书如：CIW、CISP、CISSP、CISA、CCNA、CCIE等）。

5.1.10 设备、设施与环境要求

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。

5.2 二级能力评定要求

应达到本标准5.1安全设计与集成服务商一级能力要求的所有条款，并在以下方面增强或者增加要求：

5.2.1 规模与资产

1) 单位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。

5.2.2 人员构成和素质要求

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。

5.2.3 业绩要求

1) 单位应具备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3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2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。

5.2.4 组织与管理要求

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。

5.2.5 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。

5.2.6 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）。

5.2.7 技术能力要求

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。

5.2.8 服务队伍要求

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（有相关的能力证书如：CIW、CISP、CISSP、CISA、CCNA、CCIE等）。

5.2.9 设备、设施与环境要求

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。

5.3 三级能力评定要求

应达到本标准5.2安全设计与集成服务商三级能力要求的所有条款，并在以下方面增强或者增加要求：

5.3.1 规模与资产

1) 单位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。

5.3.2 人员构成和素质要求

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。

5.3.3 业绩要求

1) 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3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5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。

5.3.4 组织与管理要求

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单位二级部门；

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。

5.3.5 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）。

5.3.6 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。

5.3.7 技术能力要求

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。

5.3.8 服务队伍要求

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（有相关的能力证书如：CIW、CISP、CISSP、CISA、CCNA、CCIE等）；

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。

5.3.9 设备、设施与环境要求

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；

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。

## 证书使用说明

中国通信企业协会颁发的通信网络安全服务能力资格证书，是证明证书持有单位符合通信网络安全服务相应能力准则要求。证书持有单位在使用中国通信企业协会颁发的证书时，应遵守以下规定：

1. 评定证书

1.1 证书持有单位必须遵守《中国通信企业协会通信网络安全服务能力评定管理办法》（以下简称《办法》 中的规定。）

1.2 证书包括以下基本内容：

a) 证书评定标志

b) 证书名称

c) 证书类型（风险评估、安全集成与设计）

d) 证书等级

e) 证书编号

f) 评定依据

g) 申请单位注册地址

h) 评定工作进行地址

i) 评审工作进行地址

j) 发证日期及有效期

k) 发证机构及批准人签字

l)　年检盖章

2.　证书使用要求

2.1 获证单位可在证书有效期内从事有关的通信网络安全服务工作，并接受中国通信企业协会通信网络安全专业委员会（以下简称通信安委会）和单位注册地通信行业协会的监督。

2.2 获证单位可在对内、对外的各种宣传场合中使用评定证书和标志，应遵守以下规定：

2.21 获证单位在宣传评定结果时不得损害评定机构的声誉,对评定的宣传应符合评定机构的要求。

2.22 获证单位在使用评定证书和评定标志进行商业活动时，需经发证机构准许。

3.　处置

获证单位被暂停、取消证书使用资格时，应立即停止使用证书，并销毁有关有资格信息的宣传材料和证实材料，通信安委会收回其证书。通信安委会所做的处置决定以书面形式通知对方单位，并在官方网站上进行公告。

中国通信企业协会通信网络安全专业委员会

二〇一三年八月二十九日