数据安全专业委员会数据安全服务能力评定管理办法（试行）

# 1. 总 则

1.1 为提高数据安全服务质量，确保服务过程的安全可控性，促进数据安全服务行业的健康发展，协助政府主管部门加强对数据安全服务的指导，依据《中国计算机行业协会数据安全专业委员会协会章程》，制定本办法。

1.2 本办法适用于对中华人民共和国境内的数据安全服务提供商提供安全服务的能力进行评定，可作为把握数据安全服务整体情况的参考，选择数据安全服务的依据，也可以作为数据安全服务提供商改进自身能力的指导。

1.3 数据安全服务能力评定（以下简称能力评定）是指对数据安全服务提供商从事数据安全服务综合能力的评定，包括技术能力、服务能力、质量保证能力、人员构成与素质、经营业绩、资产状况等要素。

1.4 能力评定是行业自律行为，数据安全服务提供商经过能力评定可取得中国软件评测中心和数据安全专业委员会联合颁发的《数据安全专业委员会数据安全服务能力评定资格证书（试行）》（以下简称《评定证书》）。

# **2.** 能力评定组织管理

2.1 数据安全专业委员会负责能力评定的发证工作，数据安全专业委员会（以下简称数据安全专业委员会）负责能力评定的协调和管理工作，包括受理评定申请、组织技术人员评定、组织专家评审、公布能力评定结果和管理证后监督。

2.2 数据安全专业委员会数据安全专业委员会负责相应等级的能力评定组织、协调和监督工作，包括组织和协调能力评定工作、报送能力评定结果和证后监督。

# 3. 能力评定类型与等级

3.1 数据安全服务能力分为二个类型：数据安全评估、数据安全建设。

数据安全评估是指运用科学的方法和手段，系统地分析数据及相关系统所面临的威胁及其存在的脆弱性，评估数据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，防范和化解数据及相关系统安全风险，将风险控制在可接受的水平，为最大限度地保障数据及相关系统的安全提供科学依据。

数据安全建设指对所服务的数据主体的全生命周期过程的安全进行框架设计，形成数据安全建设规划，并对计划实施的数据安全策略细化，在数据安全解决方案的基础上，实施数据安全产品集成部署、数据安全软件定制开发、数据安全加固与整改或其它的数据安全技术和咨询服务。

3.2 数据安全服务能力目前分为两个级别：一级、二级。

3.3 对各级别能力的具体要求可参见附件2《准则》的有关规定。

# 4. 能力评定申请与评审

4.1 数据安全服务提供商申请能力评定应具备以下基本条件：

4.1.1 在中华人民共和国境内注册成立（港澳台地区除外）；

4.1.2 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）；

4.1.3 拥有健全的组织与管理体系，有专门从事数据安全服务的部门或团队；

4.1.4 具有固定的办公场所；具有专门从事数据安全服务的相关工具或软件；具有进行安全服务所必须的实验环境；

4.1.5 具有系统的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；

4.1.6 建立并落实质量管理体系；

具体条件可参见《准则》的有关规定。

4.2 数据安全服务提供商申请能力评定，可对照《准则》确定申请能力评定的能力级别。

4.3 数据安全服务提供商申请能力评定，应当提交以下材料：

4.3.1 《数据安全专业委员会数据安全服务能力评定申请书》；

4.3.2 《企业法人营业执照》或《事业单位法人登记证书》副本

（或上级主管部门批准成立的文件副本，需有年检标识）复印件；

4.3.3 法人及主要负责人任职文件、职称、身份证复印件；

4.3.4 固定办公场所证明材料。

前款材料中信息发生变化的，数据安全服务提供商应当自信息变化之日起一个月内向公司注册地行协申请变更。

数据安全服务提供商提交材料中的信息应当真实、完整。

4.4 数据安全服务提供商申请能力评定等级为一级或二级的，应当将申报材料提交到数据安全专业委员会数据安全专业委员会，能力评定按下列程序进行：

数据安全服务提供商的提交材料申请，由专业委员会进行材料初审，审查合格后正式受理，数据安全专业委员会组织专家对提供商提交的数据安全服务提供商能力评定报告进行评审，提出评审意见，并出具评定报告，专业委员会接到正式评定报告后，组织专家对提供商进行现场评定工作，提出评审意见。

4.5 评审通过后，申请能力评定的数据安全服务提供商签订《承诺书》，由数据安全专业委员会颁发《评定证书》。《评定证书》分为正本和副本，正本和副本具有同等效力。

# 5. 能力评定监督管理

5.1 能力评定监督管理是指对获证的数据安全服务提供商能力保持的监督检查和能力变更的管理。

5.2 《评定证书》有效期为三年。

获证的数据安全服务提供商应每年进行一次自查，并将自查结果报送专业委员会；数据安全专业委员会对获证单位每年进行一次年检。获证单位在《评定证书》到期前自觉接受换证检查。

5.3 换证检查工作按以下程序进行：

5.3.1 申请换证的数据安全服务提供商在《评定证书》到期前三个月向数据安全专业委员会提交《数据安全专业委员会数据安全服务能力评定换证申请表》、《评定证书》原件、《企业法人营业执照》或《事业单位法人登记证书》复印件。

5.3.2 按照本办法第十三条、第十四条的规定对数据安全服务提供商进行换证审查，审查通过的，发放新的《评定证书》。

5.4 年检工作按以下程序进行：

5.4.1 获证的数据安全服务提供商向数据安全专业委员会提交

《评定证书》（副本）和《数据安全专业委员会数据安全服务能力评定资格年度调查表》（以下简称《调查表》），《调查表》内容必须真实可靠，如有质量事故或用户投诉，必须及时向专业委员会报告。

5.4.2 年检包括二个方面：数据安全服务提供商的能力和被服务单位对安全服务提供商的服务情况的反馈；数据安全专业委员会对年检合格者的《评定证书》（副本）上加盖年检合格章。

5.5 检查结论分为“通过”、“降级”、“取消”三种。对于检查结论为“降级”的数据安全服务提供商，将根据相适应等级换发新的《评定证书》；对于检查结论为“取消”的数据安全服务提供商， 将收回其《评定证书》。

5.6 没有按时申请换证检查或拒绝接受监督检查的数据安全服务提供商，视为自动放弃资格，其《评定证书》予以注销。

5.7 凡申请能力评定升级的数据安全服务提供商，应向公司注册地行协提出申请，按照本办法第四章办理。

5.8 获证的数据安全服务提供商发生分立、合并后原有《评定证书》应交由数据安全专业委员会重新审查。

5.9 获证的数据安全服务提供商变更名称、地址、法人、技术负责人等，应在变更内容发生之日起一个月内向专业委员会报告变更情况，并根据实际情况决定是否重新审核其能力。

# 6. 罚 则

6.1 获证的数据安全服务提供商没有按照相适应的能力等级进行数据安全服务，造成严重安全事件或被电信管理机构投诉、检查发现重大问题的，给予停止使用《评定证书》三至六个月、降级、直至收回《评定证书》的处罚。

6.2 数据安全服务提供商在申请能力评定或能力评定监督检查中，采取弄虚作假、行贿等不正当手段虚报能力评定条件或有关资料的，数据安全专业委员会和公司注册地行协除应严格按照能力评定等级标准对其重新核定能力外，对情节严重的，给予停止使用《评定证书》六至十二个月、降级、直至收回《评定证书》的处罚。

6.3 获证的数据安全服务提供商应保守客户商业秘密，正确理解与宣传数据安全服务能力评定制度，正确使用《评定证书》。对于涂改、伪造、出借、转让或出卖《评定证书》的将给予警告、停止使用或收回《评定证书》的处罚；情节严重构成犯罪的，由相关部门追究其法律责任。

6.4 所有从事能力评定工作的人员在评定过程中必须坚持公正、科学的原则。在工作中严重失职、索贿、受贿或者侵害企业合法权益的，由所在单位给予行政处分；情节严重构成犯罪的，由相关部门追究其法律责任。

# 7. 公 布

7.1 数据安全专业委员会对数据安全服务能力评定结果和监督检查结果实行公布制度，并通过数据安全专业委员会官方网站向社会公布能力评定结果和监督检查结果。

7.2 获证的数据安全服务提供商遗失《评定证书》，须通知注册地行协，通过数据安全专业委员会官方网站向社会声明作废后，方可申请补领。

7.3 数据安全专业委员会设立专门的公布网页和查询电话，社会各界可通过指定的网站和电话，查询能力评定的各项情况。

# 8. 附 则

8.1 本办法由数据安全专业委员会负责解释。

附件：

1. 数据安全专业委员会数据安全服务能力评定工作流程图（试行）。
2. 数据安全专业委员会数据安全服务能力评定准则（试行）。

附件1:

数据安全服务能力评定工作流程图（试行）



附件 2：

数据安全专业委员会数据安全服务

能力评定准则（试行）

# 数据安全服务概述

## 概念

本准则所述的数据是指任何以电子或者其他方式对信息的记录，所涉及的安全服务是指为了适应国家《数据安全法》及数据安全相关管理的需要，运用科学的方法和手段，通过有效的措施来保障数据的正常运行及处理，包括数据的收集、存储、使用、加工、传输、提供、公开等，为企业提供全面或部分数据安全评估、数据安全建设的服务，包含从数据安全体系咨询、评估到具体的技术解决措施。

## 类型

本准则涉及到的数据安全服务可以分为两个类型：数据安全评估、数据安全建设。

### 数据安全评估：运用科学的方法和手段，系统地分析数据及相关系统所面临的威胁及其存在的脆弱性，评估数据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，防范和化解数据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数据及相关系统的安全提供科学依据。

### 数据安全建设：对所服务的数据主体的全生命周期过程的安全进行框架设计，形成数据安全建设规划，并对计划实施的数据安全策略细化，在数据安全解决方案的基础上，实施数据安全产品集成部署、数据安全软件定制开发、数据安全加固与整改或其它的数据安全技术和咨询服务。

# 数据安全服务能力等级的评判原则

数据安全服务能力是对数据安全服务提供商的客观评价，直接反应了数据安全服务提供商的服务资格、水平和能力。数据安全服务能力要求针对每一类服务提供商分别提出基本要求和分类要求。基本要求是指所有数据安全服务提供商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数据安全服务提供商提出的不同的能力要求，其中数据安全评估、数据安全建设服务分别提出了两级能力要求，由高到低依次是二级、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。

数据安全服务能力评定要求是对数据安全服务提供商的资格状况、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。

# 数据安全服务能力等级基本要求

## 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. 从事涉密的数据安全服务提供商必须满足国家保密机关的相关要求；
		4. 从事数据安全服务工作一年以上，无违法记录；
		5. 法人及主要业务、技术人员无犯罪记录。

## 组织与管理要求

* + 1. 拥有健全的组织与管理体系，有专门从事数据安全服务的部门或团队；
		2. 落实保密规章制度，对数据安全服务保密，安全服务过程中不得制造漏洞或者利用安全服务所获得的安全漏洞从事破坏、窃取机密等行为；
		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。

## 设备、设施与环境要求

* + 1. 具有固定的办公场所；
		2. 具有专门从事数据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。

## 项目管理要求

* + 1. 具有成文的项目管理制度，并符合相关项目管理准则；
		2. 具有系统的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. 能提供项目管理制度可有效运行的证据。

## 质量保证要求

* + 1. 建立并落实质量管理体系；
		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。

# 数据安全评估能力要求

## 一级能力要求

### 基本要求

* + 1. 应达到数据安全服务能力等级基本要求的所有条款；
		2. 从事数据安全评估的数据安全服务提供商应对数据主体及其业务的安全状况、安全要求有相应的了解。

### 服务商规模与资产

* + - 1. 企业正式编制人员应不少于15人，直接从事数据安全评估服务的人员不低于8人；
			2. 注册资本：产权关系明晰，注册资金（或开办资金）不少于500万元人民币。

### 业绩要求

* + - 1. 企业应具备一年以上的数据安全行业从业时间；
			2. 至少有2个数据安全评估服务及同类型项目，单个合同金额不低于20万元人民币，项目合同总金额不低于100万元人民币；
			3. 至少成功完成2个以上的完整的数据安全评估服务项目，且终验通过；
			4. 近二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数据安全评估服务项目。

#### 客户服务要求

从事数据安全评估服务的数据安全服务提供商应提供 7×24小时电话热线支持。

#### 技术能力要求

* + - * 1. 了解安全防护系列准则，对数据主体有深入了解；
				2. 有专门的人员持续对最新的数据安全技术进行研究；
				3. 能够独立完成数据安全相关渗透测试；
				4. 能够评估数据安全风险、脆弱性、管控能力及安全对数据的影响力；
				5. 具有确定数据的安全需求的能力；
				6. 具有对数据安全系统有效维护的能力；
				7. 具备切实可行的应急服务方案。

### 服务队伍要求

* + - 1. 从事数据安全评估的队伍内至少应有1名经过数据安全防护技术和标准的系统培训，曾参与起草数据安全防护系列标准的人员可等同参加过此类培训；
			2. 应有一批相对稳定的技术队伍，每个数据安全服务项目至少应有1名项目经理，直接从事数据安全评估的服务人员需大学本科及以上学历
			3. 至少有2人具有一年以上的数据安全服务项目经验，并具有相关数据安全评估服务的成功案例；
			4. 具有相应的评估工具，如渗透测试工具等。

## 二级能力要求

* + 1. 基本要求

应达到本准则 4.1 节数据安全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者增加要求。

* + 1. 服务商要求

#### 规模与资产

* + - * 1. 企业正式编制人员应不少于40人，直接从事数据安全评估服务的人员不低于20人；
				2. 注册资本：产权关系明晰，注册资金（或开办资金）不少于500 万元人民币。

#### 业绩要求

* + - * 1. 企业应具备二年以上的数据安全行业从业时间；
				2. 至少有3个数据安全评估服务及同类型项目，单个合同金额不低于30万元人民币，项目合同总金额不低于180万元人民币；；
				3. 至少成功完成4个以上的完整的数据安全评估服务项目，且终验通过；
				4. 近二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数据安全评估服务项目。
		1. 服务队伍要求
1. 从事数据安全评估的队伍内至少应有2名经过数据安全防护技术和标准的系统培训，曾参与起草安全防护系列标准的人员可等同参加过此类培训；
2. 至少有4人具有二年以上的数据安全服务项目经验，并具有相关数据安全评估服务的成功案例。

# 数据安全建设能力要求

## 一级能力要求

### 基本要求

* + - 1. 应达到数据安全服务能力等级基本要求的所有条款；
			2. 从事数据安全建设的数据安全服务提供商应对数据主体及其业务的安全状况、安全要求、数据安全建设流程有相应的了解，具备承接数据安全域各方面数据安全建设项目的前提能力。

### 服务商要求

* + - 1. 资格要求

从事涉密的数据安全服务提供商必须满足国家保密机关的相关要求；

* + - 1. 规模与资产
				1. 企业正式编制人员应不少于20人；
				2. 注册资本：产权关系明晰，注册资金（或开办资金）不少于500万元人民币。

### 人员构成和素质要求

* + - * 1. 直接从事数据安全建设服务的人员不低于10人，每个数据安全建设项目至少应有1名项目经理，大学本科以上学历人员占企业总人数比例不少于80%；
				2. 企业至少有5人具有三年以上的数据安全建设服务项目经验，并具有数据安全建设服务的成功案例。

### 业绩要求

* + - * 1. 企业应具备一年以上的数据安全行业从业时间；
				2. 至少有2个数据安全建设及同类型项目，单个合同金额不低于50万元人民币，项目合同总金额不低于150万元人民币；
				3. 至少成功完成2个完整的数据安全建设项目，且终验通过；
				4. 近一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数据安全建设服务项目。

### 客户服务要求

从事数据安全建设服务的数据安全服务提供商应提供7×24 小时电话热线支持。

### 技术能力要求

* + - * 1. 了解安全防护系列准则，对数据主体有深入了解；
				2. 能对市场的数据安全产品进行功能分析、提出安全策略和安全解决方案，具有安全产品的系统集成部署能力；
				3. 具有对集成部署的系统进行安全性检测和验证的能力；
				4. 能对集成部署的系统进行有效的安全性维护。

### 服务队伍要求

* + - 1. 从事数据安全建设的队伍中的相关人员应是中国公民；
			2. 从事数据安全建设的队伍内至少应有2名经过数据安全防护技术和准则的系统培训，曾参与起草安全防护系列标准的人员可等同参加过此类培训；
			3. 从事数据安全建设的队伍内至少应有2名国家和相关机构认可的安全工程师；
			4. 具有相应的国家权威单位认可的测试设备和环境，如渗透测试工具等。

## 二级能力要求

* + 1. 基本要求

应达到本准则5.1节数据安全建设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。

### 服务商要求

* + - 1. 规模与资产
				1. 企业正式编制人员应不少于100人；
				2. 注册资本:产权关系明晰，注册资金（或开办资金）不少于1000 万元人民币。

#### 人员构成和素质要求

* + - * 1. 直接从事数据安全建设服务的人员不低于15人，每个数据安全建设服务项目至少应有1名项目经理，大学本科以上学历人员占企业总人数比例不少于80%；
				2. 企业至少有8人具有三年以上的数据安全建设服务项目经验，并具有数据安全建设服务的成功案例。

### 业绩要求

* + - * 1. 企业应具备三年以上的数据安全行业从业时间；
				2. 至少有3个数据安全建设及同类型项目，单个合同金额不低于80万元人民币，项目合同总金额不低于250万元人民币；
				3. 至少成功完成3个完整的数据安全建设项目，且终验通过；
				4. 近一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数据安全建设服务项目。

### 服务队伍要求

1. 从事数据安全建设的队伍中的相关人员应是中国公民；
2. 从事数据安全建设的队伍内至少应有3名经过数据安全防护技术和准则的系统培训，曾参与起草安全防护系列标准的人员可等同参加过此类培训；
3. 从事数据安全建设的队伍内至少应有3名经过国家和相关机构认可的安全工程师（有相关的能力证书）；
4. 具有相应的国家权威单位认可的测试设备和环境，如渗透测试工具等。

# 评审团队说明

## 评审团队组成

该准则遵循科学、合理的原则，满足评审团成员组成非单一性要求，评审团队从数据安全专业委员会组建的技术专家库中抽取，专家库由来自计算机行业协会政府、事业单位、运营企业的安全技术专家组成。

## 人数要求

评审团人员人数须为奇数，由数据安全专业委员会专家指导组成员组成，每批评审随机抽取不少于5名专家进行评审。