

# 贯标集团-江苏-CCRC信息安全服务认证

产品名称	贯标集团-江苏-CCRC信息安全服务认证
公司名称	贯标集团-华北公司
价格	.00/件
规格参数	
公司地址	华北公司地址：天津市河西区南京路35号亚太大厦13层；总部地址：江苏省南京市玄武区新庄村57号二楼
联系电话	022-23125802 15502200816

## 产品详情

什么是CCRC？

CCRC信息安全服务资质是对信息系统安全服务的提供者的技术、资源、法律、管理等方面的资质和能力，以及其稳定性、可靠性进行评估，并依据公开的标准和程序，对其安全服务保障能力进行认证的过程。

信息安全服务资质级别分为一级、二级、三级，其中一级最高，三级最低。资质级别是衡量服务提供者服务能力的尺度。

### 资质类别

#### 1.安全集成服务资质

信息系统安全集成服务是指从事计算机应用系统工程和网络系统工程的安全需求界定、安全设计、建设实施、安全bao证的活动。

安全集成服务提供方的服务能力主要从以下四个方面体现：基本资格、服务管理能力、服务技术能力和服务过程能力；服务人员的能力主要从掌握的知识、安全集成服务的经验等综合评定。

#### 2.安全运维服务资质

通过技术设施安全评估，技术设施安全加固，安全漏洞补丁通告、安全事件响应以及信息安全运维咨询，协助组织的信息系统管理人员进行信息系统的安全运维工作，以发现并修复信息系统中所存在的安全隐患，降低安全隐患被非法利用的可能性，并在安全隐患被利用后及时加以响应。

安全运维资质认证是对安全运维服务方的基本资格、管理能力、技术能力和安全运维过程能力等方面进行评价。

### 3.风险评估服务资质

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。

风险评估服务提供方的服务能力主要从以下四个方面体现：基本资格、服务管理能力、服务技术能力和服务过程能力；服务人员的能力主要从掌握的知识、风险评估服务的经验等综合评定。

### 4.应急处理服务资质

信息安全应急处理服务是通过制定应急计划使得影响网络与信息系统安全的安全事件能够得到及时响应，并在安全事件一旦发生后进行标识、记录、分类和处理，直到受影响的业务恢复正常运行的过程。应急处理服务是保障业务连续性的重要手段之一，它涵盖了在安全事件发生后为了维持和恢复关键业务所进行的系列活动。

信息安全应急处理服务资质认证是对应急处理服务提供方的基本资格、管理能力、技术能力和应急处理服务过程能力等方面进行评价。

### 5.软件安全开发服务资质

通过对软件开发过程的控制，将开发的软件存在的风险控制在可接受的水平。

软件安全开发资质认证是对软件开发方的基本资格、管理能力、技术能力和软件安全过程能力等方面进行评价。

### 6.信息系统灾准备份与恢复服务资质

信息系统灾准备份与恢复服务是将信息系统的数据库、数据处理系统、网络系统、基础设施、专业技术支持能力和运行管理能力进行备份，并在灾难发生时，将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态，将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计和提供的活动。

### 7.工业控制安全服务资质

工业控制系统安全服务围绕提升工业控制系统的高可用性和业务连续性，提升功能安全、物理安全和信息安全的保障能力为目标，涉及工业控制系统设计、建设、运维和技改各个阶段，主要包括系统集成、系统运维、应急处理、风险评估等工业控制系统安全服务，形成系统的、独立的、形成文件的过程。

工业控制系统安全服务资质认证是对工业控制系统安全服务方的基本资格、管理能力、技术能力和工业控制系统安全服务过程能力等方面进行评价。

### 8.网络安全审计服务资质认证

网络安全审计是指网络安全审计机构对被审计方所属的计算机信息系统的安全性、可靠性和经济性进行检查、监督，通过获取审计证据并对其进行客观评价所开展的系统的、独立的、形成文件的活动。

网络安全审计服务资质认证是对网络安全审计服务方的基本资格、管理能力、技术能力和网络安全审计过程能力等方面进行评价。

CCRC资质认证对企业有哪些好处？

1.信息安全服务认证可以为企业提高市场竞争力

2.规范企业的技术能力、管理能力

3.降低企业的运营风险；减少企业的经营成本

4.作为企业投标加分项

CCRC信息安全服务资质申请流程

CCRC信息安全服务资质申请流程主要分为4个阶段，包含准备阶段、审核阶段、认证决定阶段和制证阶段。各阶段主要工作为：

### 1、准备阶段

申请组织根据自身实际情况确定需要申请的服务资质类型，登录中国信息安全认证中心网站<https://www.isccc.gov.cn/>，下载《信息安全服务资质认证自评表-公共管理》、《信息安全服务资质认证申请书》，实施自评后（具体自评表的填写方法可参考中心网站上的《信息安全服务资质认证自评表填写指南》），将上述文档及自评证明提交中心。

2、审核阶段（此阶段工作应在三周内完成，如需要申请组织补充材料，应在五周内完成）

审核形式有较大差异，需重点关注：

（1）初次认证：一级、二级、三级资质审核形式均为文件审查+现场审核。

（2）监督审核：一、二、三级资质均为文件审查+现场审核+服务点审核。服务点审核抽样要求：

一级：在申请组织提交正在进行的项目中，现场审核时随机抽查1个项目；

二级：在申请组织提交正在进行的项目中，现场审核时随机抽查1个项目；

三级：在申请组织提交正在进行中的项目中，现场审核时随机抽查1个项目；

审核流程：

项目管理人员指派审核组长，协调审查员组建审核组；审核组长编制《审核计划》，通过项目管理人员发送给审核组全体成员；审核组对申请组织提交的材料进行审核工作，判断该组织目前对外提供的信息安全服务管理及技术能力是否符合《信息安全服务规范》的要求。如满足要求，审核组长在通知项目管理人员向申请组织出具《受理通知单》（如申请组织有需求，也可签订《服务资质认证合同》）、收取认证费用后，编写《非现场审核报告》，并汇总《信息安全服务资质认证公共管理审核记录表》等审核材料提交中心进行认证决定；如不满足要求，审核组长通知申请组织补充材料重新提交，并对补充材料进行审核（如申请组织所补充的材料仍无法满足要求，审核组长应将此情况告知项目管理人员，项目管理人员通知申请组织目前尚不能满足申请资质的条件）。

3、认证决定阶段（此阶段工作应在两周内完成）

中心认证决定人员对审核组长提交的审核材料进行认证决定；如认证决定通过，则通知项目管理人员进行制证；如认证决定不通过，则通知申请组织不通过原因。