信息安全等级保护备案上海同城申办

产品名称	信息安全等级保护备案上海同城申办
公司名称	上海道商企业服务中心
价格	.00/个
规格参数	
公司地址	浦东新区金沪路99弄3号
联系电话	15021594806 15021594806

产品详情

三者的基本概念和工作背景 等级保护 基本概念：信息安全等级保护是指对国家秘密信息、法人和其他组织和公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的安全产品实行按等级管理，对信息系统中发生的信息安全事件等等级响应、处置。这里所指的信息系统，是指由计算机及其相关和配套的设备、设施构成的，按照一定的应用目标和规则对信息进行存储、传输、处理的系统或者网络；信息是指在信息系统中存储、传输、处理的数字化信息。 工作背景：1994年×××颁布的《×××计算机信息系统安全保护条例》2规定：计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。1999年公安部组织起草了《计算机信息系统安全保护等级划分准则》（GB17859-1999），规定了计算机信息系统安全保护能力的五个等级，即：级：用户自主保护级；第二级：系统审计保护级；第三级：安全标记保护级；第四级:结构化保护级；第五级：访问验证保护级。GB17859中的分级是一种技术的分级，即对系统客观上具备的安全保护技术能力等级的划分。2002年7月18日，公安部在GB17859的基础上，又发布实施五个GA新标准，分别是：GA/T387-2002《计算机信息系统安全等级保护网络技术要求》、GA388-2002《计算机信息系统安全等级保护操作系统技术要求》、GA/T389-2002《计算机信息系统安全等级保护数据库管理系统技术要求》、GA/T390-2002《计算机信息系统安全等级保护通用技术要求》、GA391-2002《计算机信息系统安全等级保护管理要求》。这些标准是我国计算机信息系统安全保护等级系列标准的一部分。《关于信息安全等级保护工作的实施意见的通知》3（简称66号文）将信息和信息系统的安全保护等级划分为五级，即：级：自主保护级；第二级：指导保护级；第三级：监督保护级；第四级：强制保护级；第五级：专控保护级。特别强调的是：66号文中的分级主要是从信息和信息系统的业务重要性及遭受破坏后的影响出发的，是系统从应用需求出发必须纳入的安全业务等级，而不是GB17859中定义的系统已具备的安全技术等级。 风险评估 基本概念：信息安全风险评估是参照风险评估标准和管理规范，对信息系统的资产价值、潜在威胁、薄弱环节、已采取的防护措施等进行分析，判断安全事件发生的概率以及可能造成的损失，提出风险管理措施的过程。 工作背景：风险评估不是一个新概念，金融、电子商务等许多领域都有风险及风险评估需求的存在。当风险评估应用于IT领域时，就是对信息安全的风险评估。国内这几年对信息安全风险评估的研究进展较快，具体的评估方法也在不断改进。风险评估也从早期简单的漏洞扫描、人工审计、***性测试这种类型的纯技术操作，逐渐过渡到目前普遍采用BS7799、OCTAVE、NISTSP800-26、NISTSP800-30、AS/NZS4360、SSE-CMM等方法，充分体现以资产为出发点、以威胁为触发、以技术/管理/运行等方面存在的脆弱性为诱因的信息安全风险评估综合方法及操作模型。×××信息化工作办公室2004年组织完成了《信息安全风险评估指南》及《信息安全风险管理指南》标准草案的制定，并在其中规定了信息安全风险评估的工作流程、评估内容、评估方法和风险判断准则

，对规范我国信息安全风险评估的做法具有很好的指导意义。目前，国信办正组织在全国北京、上海、黑龙江、云南等省市及税务、银行、电力等行业领域作风险评估试点工作，探讨对上述两个风险评估/风险管理标准草案的理解修订及相关管理问题的研究，预计2005年9月份前完成试点工作，并在试点工作的基础上形成有关开展信息安全风险评估工作的指导意见。 系统安全测评 基本概念：由具备检验技术能力和政府授权资格的机构，依据国家标准、行业标准、地方标准或相关技术规范，按照严格程序对信息系统的安全保障能力进行的科学公正的综合测试评估活动，以帮助系统运行单位分析系统当前的安全运行状况、查找存在的安全问题，并提供安全改进建议，从而大程度地降低系统的安全风险。 工作背景：在我国，中国信息安全产品测评认证中心（简称CNITSEC）是较早并较有影响的开展有关系统安全测评认证的机构。这里强调一下测评和认证的区别：测评如前述定义，认证则是对测评活动是否符合标准化要求和质量管理要求所作的确认，认证以标准和测评的结果作为依据。在美国，系统认证的结果通常作为主管部门对新建系统投入运行前的安全审批或已建系统安全动态监管（即系统认可）的依据。根据美国FISMA6及NISTSP800-37的规定，系统认证是「对信息系统的技术类、管理类和运行类安全控制所进行的综合评估」，认可则是「由管理层作出的决策，用来授权一个信息系统投入运行」。我国的系统认证虽然起步较早，但由于认证周期、建设差异等多方面的原因，目前的系统认证数量还非常少。特别是国家认监委成立后，强调了信息安全要「一个统一认证出口」的要求。国家认监委等8部委联合下发的《关于建立国家信息安全产品认证认可体系的通知》4（简称57号文）中已明确规定了对信息安全产品进行「统一标准、技术规范与合格评定程序；统一认证目录；统一认证标志；统一收费标准」的「四统一」的认证要求。在国家认监委对信息系统的安全认证相关具体意见尚未出台前，多数情况下，系统安全测评的结果可直接作为主管部门对系统安全认可的依据。典型例子如上海市信息安全测评认证中心，在相关职能部门授权下，已完成了对上海市100余家重要信息系统、涉密信息系统、区县以上综合医院的信息系统的安全测评工作，并为市信息委、市×××、市卫生局等信息化主管部门或行业主管部门提供了重要的技术决策依据。