第三章 采购需求

（一）项目概况

1.建设目标

根据国家的相关要求和海南自由贸易港建设需要，打造投资便利的营商环境，建设目标重点在放管服上，（放：在全面放开准入环境；管：加强商事主体和营商环境事中、事后监管；服：打造优质高效服务平台）。用三年左右的时间，围绕建设统一开放、竞争有序、诚信守法、监管有力的现代市场体系，依托统一的市场监管信息化技术架构，全面推进市场监管智慧化应用，加快构建统一的市场监管信息化体系，逐步形成“大平台支撑、大数据慧治、大系统融合、大服务惠民、大监管共治”的市场监管信息化创新发展格局，进一步完善市场监管领域智慧监管的制度规则，广泛运用云计算、大数据等现代技术，通过强化机制创新、流程再造、业务协同、资源统筹、数据共享、系统整合和安全管控，统筹推进总局与地方市场监管部门的智慧监管工作，初步形成及时感知、快速反应、系统监管、主动服务、融合共治的新时代市场监管治理体系与治理模式，**基本实现“一标贯全国、一照走四方、一码识信用、一号保维权、一库清底数、一网抓监管、一图知风险”的智慧监管目标**，落实大市场、大质量、打监管的要求，优化准入、准营、准出和事前、事中、事后各环节监管工具，依靠“制度+技术”、政策和服务、引导和监管，运用市场、行政、法律、经济、信用、科技赋能、社会参与等多种手段，着力破解监管资源和监管对象不匹配的矛盾，提高综合监管能力。

2.建设内容

e登记三期暨放管服项目建设将在海南省市场监管局现有业务系统的基础上，提升日常业务服务能力、强化重点领域监管支撑能力、

夯实底层基础支撑能力。其中提升日常业务服务能力相关建设功能模块有商事登记升级改造和信用监管，强化重点领域监管支撑能力相关建设功能模块为重点监管领域应用建设和升级改造，数据管理与分析应用，夯实底层基础支撑能力相关建设功能模块包括垂直应用模块建设（含省质监所实验室信息管理系统升级、省标信所标准信息管理系统升级、省食检中心天翼实验室检验电子系统优化升级、计量所实验室信息管理系统升级）。

（二）采购项目预（概）算

04 包预算：80000.00 元

（三）采购标的汇总表

包号	序号	标的名称	品目分类编码	计量单位	数量	是否进口	分包要求
04	04	网络安全等级保护测评	C16060000	项	1	否	不分包

（四）技术商务要求

04 包：网络安全等级保护测评

（1）技术要求

1.网络安全等保工作方案

该项目信息系统定为信息系统安全保护等级三级，需针对信息系统做信息系统网络安全等级保护测评工作。本项目等保测评涉及一体化政企服务平台、海南自贸区商事登记业务系统及公共服务平台资源池三个系统。

网络安全等级保护测评需要结合信息系统的构成特点，确定具体的测评对象，制定测评方案，通过访谈、检查和测试等方式判断其安全技术和安全管理各层面所对应测评指标的符合程度，判断被测系统的安全保护能力是否满足国家信息系统安全等级保护要求，找出与国家标准要求之间的差距。根据测评结果出具信息安全等级保护测评报告，作为后续安全整改的依据，帮助其达到信息系统安全等级保护要求。

信息系统网络安全等级保护测评过程需按照信息安全技术网络安全等级保护测评要求开展工作，等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析及报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。海南省市场监督管理局新建系统定为信息系统安全保护等级三级，需针对信息系统做信息系统网络安全等级保护测评工作。

1.1 网络安全等保定级备案

协助用户组织开展对信息化项目内的摸底调查，全面掌握信息化项目内网络基础设施等的数量、分布、业务类型、应用或服务范围、系统结构等基本情况，确定定级对象，依据《信息安全技术网络安全等级保护定级指南》（GA/T1389-2017），确定信息系统的安全保护等级，准备定级备案表和定级报告，协助用户向所在地区的公安机关办理备案手续。

1.2 网络安全等保建设整改

严格按照《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）和《信息安全技术网络安全等级保护安全设计技术要求》（GB/T25070-2019）的要求，从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运

维管理十个方面对整个信息化项目进行规划、设计、建设和整改。

1.3 网络安全等保等级评测

为用户选择满足国家要求的测评机构（在本省等保办推荐目录下且在本省备案的测评机构），完成对用户信息化项目的等级保护测评。

网络安全等级保护测评需要结合信息系统的构成特点，确定具体的测评对象，制定测评方案，通过访谈、检查和测试等方式判断其安全技术和安全管理各层面所对应测评指标的符合程度，判断被测系统的安全保护能力是否满足国家信息系统安全等级保护要求，找出与国家标准要求之间的差距。根据测评结果出具信息安全等级保护测评报告，作为后续安全整改的依据，帮助其达到信息系统安全等级保护要求。

信息系统网络安全等级保护测评过程需按照信息安全技术网络安全等级保护测评要求开展工作，等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析及报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。

1.4 网络安全等保监督检查

通过网络安全等级保护等级测评以后，严格遵守等级保护相关管理规范，及时开展等级保护测评或相关安全测试，避免系统带病上线，将安全隐患消除在萌芽阶段。同时，主动配合公安机关的安全监督、检查、指导，如实向公安机关汇报自主检查工作，并提供有关材料，接受公安机关的审查。

1.4.1 测评准备活动

测评准备工作包括编制项目启动、信息收集和分析、工具和表单准备。

详细要求见下表：

项目内容	工作内容	成果输出
1.项目启动	1.组建测评项目组	
	2.编制《项目计划书》	
	3.确定测评委托单位应提供的资料	
2.信息收集分析	定级报告及整改方案分析	《系统基本情况调研表》
	1.整理调查表单	

	2.发放调查表单给测评委托单位	
	3.协助测评委托单位填写调查表	
	4.收回调查结果	
	5.分析调查结查	
3.工具和表单准备	1.调试测评工具	确定测评工具、形成测评结果记录表
	2.模拟被测系统搭建测评环境	
	3.模拟测评	
	4.准备打印表单	

1.4.2 方案编制活动

方案编制活动包括测评对象确定、测评指标确定、测试工具接入点确定、测评内容确定、测评指导书开发及测评方案编制等六项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出成果
1.测评对象确认	识别被测系统等级 识别被测系统的整体结构 识别被测系统的边界 识别被测系统的网络区域 识别被测系统的重要节点和业务应用 确定测评对象	《测评方案》的测评对象部分
2.测评指标确定	识别被测系统业务信息和系统服务安全保护等级	《测评方案》的测评指标部分
	选择对应等级的 ASG 三类安全要求作为测评指标	
	就高原则调整多个定级对象共用的某些物理安全或管理安全测评指标	
3.工具测试点确定	确定工具测试的测评对象 选择测试路径 确定测试工具的接入点	《测评方案》的测试工具接入点部分
4.测试内容确定	识别每个测评对象的测评指标	《测评方案》的

	识别每个测评对象对应的每个测试指标的测试方法	单项测评实施和系统测评实施部分
5.测评指导书开发	从已有的测评指导书中选择与测评对象对应的手册	《测评方案》的测评实施手册部分
	针对没有现成测评指导书的测评对象，开发新的测评指导书	
6．测评方案编制	描述测评项目基本情况和工作依据	向用户提交《测评方案》
	描述被测系统的整体结构、边界和网络区域	
	描述被测系统的重要节点和业务应用	
	描述测评指标	
	描述测评对象	
	描述测评内容和方法	

1.4.3 现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调，为现场测评的顺利开展打下良好基础，然后依据测评方案实施现场测评工作，将测评方案和测评工具等具体落实到现场测评活动中。现场测评工作应取得分析与报告编制活动所需的、足够的证据和资料。

现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

1.4.4 报告分析及编制活动

在现场测评工作结束后，应对现场测评获得的测评结果（或称测评证据）进行汇总分析，形成等级测评结论，并编制测评报告。

测评人员在初步判定单元测评结果后，还需进行整体测评，经过整体测评后，有的单元测评结果可能会有所变化，需进一步修订单元测评结果，而后进行风险分析和评价，形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成及测评报告编制六项主要任务。

详细要求见下表：

工作内容	工作详细任务	工作依据（模版）
1.单项测评结果判定	分析测评项所对抗威胁的存在情况	等级测评报告的单项测评结果部分
	分析单个测评项是否有多方面的要求内容，依据“优势证据”法选择优势证据，并将优势证据与预期测评结果相比较	
	综合判定单个测评项的测评结果	
2.单元测评结果判定	汇总每个测评对象在每个测评单元的单项测评结果	等级测评报告的单项测评结果汇总分析部分
	判定每个测评对象的单元测评结果	
3.整体测评	分析不符合和部分符合的测评项与其他测评项（包括单元内、层面间、区域间）之间的关联关系及对结果的影响情况	等级测评报告的系统整体测评分析部分
	分析被测系统整体结构的安全性对结果的影响情况	
4.风险分析	整体测评后的单项测评结果再次汇总	等级测评报告的风险分析部分
	分析部分符合项或不符合项所产生的安全问题被威胁利用的可能性	
	分析威胁利用安全问题后造成的影响程度	
	为被测系统面临的风险进行赋值	
	评价风险分析结果	
5.等级测评结论形成	统计再次汇总后的单项测评结果为部分符合和不符合项的项数	等级测评报告的等级测评结论部分
	形成等级测评结论	
6.测评报告编制	概述测评项目情况	等级测评报告提交用户
	描述被测系统情况	
	描述测评范围和方法	
	描述整体测评情况	
	汇总测评结果	

	描述风险情况	
	给出等级测评结论和整改建议	

1.4.5 网络安全等保工作方案

本项目涉及众多业务应用系统，整体上按照等级保护三级要求提出工作方案。

1.4.5.1 系统定级备案

重要信息系统的定级工作，是开展等级保护的首要环节，是进行信息系统建设、整改、测评、备案、监督检查等后续工作的重要基础。

1.4.5.2 差距分析

差距分析工作内容就是根据网络和信息系统的安全保护等级，根据国家等级保护相应等级的技术和管理要求，分析评价网络和信息系统当前的安全防护水平和措施与相应等级要求之间的差距。

1.4.5.3 等保建设整改

等级保护建设整改是根据信息系统差距分析结果，对信息系统所依赖的服务器操作系统、数据库、网络及安全设备进行配置安全加固，安装和实施各项新增安全设备，保障信息系统的安全稳定性。

1.4.5.4 等保管理制度建设

等级保护管理制度建设是根据信息安全等级保护安全管理的要求，编写符合等级保护要求的信息安全管理规范和制度，通过安全管理的加强来规避管理风险。

1.4.6 定级备案

1.4.6.1 工作目的

协助完成安全等级保护的定级与备案。依据《信息系统安全等级保护定级指南》对未定级、备案信息系统进行梳理完成信息系统安全等级保护的定级与备案工作。

1.4.6.2 工作方式

在定级咨询过程中，咨询顾问将通过现场调研的方式来全面了解主要信息系统的基本情况，如数量、类别、名称、承载业务、服务范围、用户数量、部署方式，以进行汇总分析，初步进行系统归类、重要性划分，为下一步确定定级对象、确定级别、形成定级报告做准备。

现场信息资料收集，以及对系统管理员进行访谈及信息确认，是现场调研的

主要工作。通过现场的了解，可以较深入理解信息系统的重要程度，重要信息的分类情况，以及用户分布情况。一般系统的定级结果，不依赖于现有保护措施，所以通过现场的工作，可以基本准确理解信息系统及承载重要信息的侵害客体以及侵害程度，从而为进一步定级报告的编写打下良好基础。

1.4.6.3 工作内容

①协助定级

如果信息系统只承载一项业务，可以直接为该信息系统确定等级，不必划分业务子系统。如果信息系统承载多项业务，应根据各项业务的性质和特点，将信息系统分成若干业务子系统，分别为各业务子系统确定安全保护等级，信息系统的安全保护等级由各业务子系统的最高等级决定。信息系统是进行等级确定和等级保护管理的最终对象。

现场调研后，咨询顾问会准备《信息系统安全等级保护定级报告模板》，给出定级报告示例。信息管理部门和业务部门依据定级报告模板，起草各信息系统安全等级保护定级报告，咨询顾问根据已经掌握的信息系统情况，对各信息系统定级报告的合理性进行初步研究和审核把关，请相关单位派人共同讨论，按照系统类别梳理定级报告，对照国家对不同等级的要求，在报告内容、行文格式、定级准确性等方面给出修改意见。根据讨论的定级报告修改意见，统一汇总、整理后，形成定级报告的专家评审稿。

②专家评审

咨询顾问还将根据需要协助聘请等级保护专家、行业专家、主管机关领导等外部专家，召开信息系统定级评审会，对定级报告进行外部评审，形成评审意见。

咨询顾问将参考专家定级评审意见，最终协助确定信息系统等级，协助将各信息系统安全保护等级定级报告报经上级主管部门审批同意。

最后，咨询顾问将协助填写《信息系统安全等级保护备案表》，协助客户主要业务系统完成备案工作。

1.4.6.4 提交成果

《信息系统安全等级保护备案表》

《信息系统安全等级保护定级报告》

《专家评审意见》

1.4.7 差距分析

根据国家等级保护政策法规和标准规范，确定安全保护等级的信息系统应该具有相应级别的安全防护能力，其中主要是根据《网络安全技术网络安全等级保护基本要求》来分析承载于互联网和综合安防网上的业务应用系统目前的安全防护能力与基本要求中相应级别之间的差距。

1.4.7.1 工作目的

根据国家等级保护要求，对于确定了安全保护等级的信息系统规定了基本的安全保护要求，规定了应该具有的防护措施，以确保信息系统具有相当水平的安全防护能力。

差距分析就是根据《网络安全技术网络安全等级保护基本要求》，结合本项目的业务情况和行业要求，从安全技术和安全管理两个方面，全面分析信息系统现有防护措施和能力与相应等级基本要求之间存在的差距，用以为等级保护建设提供客观依据并指导信息系统等级保护体系设计。

1.4.7.2 工作方式

业务系统差距分析工作计划通过以下方式进行。

1）访谈

访谈是指评估人员与信息系统有关人员就差距分析所关注的问题进行有针对性的询问和交流的过程，该过程可以帮助评估者了解现状、澄清疑问或获得证据。

访谈深度（即访谈内容的详细程度）以及访谈的广度（即对被评估组织中员工角色类型以及每种类型中人数的覆盖程度）由评估人员依据不同的评估需要进行选择和判断。

2）检查

检查是指对评估对象（如规范、机制或行为）进行观察、调查、评审、分析或核查的过程。与访谈类似，该过程可以帮助评估者了解现状、澄清疑问或获得证据。

比较典型的检查行为包括：对安全配置的核查、对安全策略的分析和评审等。

3）测试

测试是指在特定环境中运行一个或多个评估对象（限于机制或行为）并将实际结果与预期结果进行比较的过程。测试的目标是判定对象是否符合预定的一组规格。测试过程可以帮助评估者获得证据。

4）调查表

根据系统业务情况和系统现状，制定详细的调查表，并由相关人员进行填写，以获得业务系统基础数据。具体包括应用信息系统调查表、物理资产调查表、软件资产调查表、各相关设备资产调查表。

1.4.7.3 工作内容

按照等级保护实施要求，不同安全等级的信息系统应该具备相应等级的安全防护能力，部署相应的安全设备，制定相应的安全管理机构、制度、岗位等。差距分析就是依据等级保护技术标准和管理规范，比较分析信息系统安全防护能力与等级要求之间的差距，为等级化体系设计提供依据。

1.4.7.4 提交成果

差距分析过程中将产生众多文档，其中包括过程文档和结果文档，过程文档用以支持咨询人员进行差距分析，并形成结果文档《等级保护差距分析报告》。

信息系统等级保护差距分析报告主要内容：差距分析是以现场调查和测试所收集的信息为依据，满足等级保护要求为目标，对现有系统安全做出的一种客观的、真实的评价。报告内容包括对各信息系统现有安全防护水平与相应等级之间差距的描述和整改建议等。差距分析是制定信息系统安全等级保护体系设计方案前的一个非常关键的环节，为信息系统安全等级保护体系设计方案的撰写提供参考。

1.4.8 等保建设整改

1.4.8.1 工作目的

根据前期等级保护整改、差距分析结果，结合项目的业务需求，对信息系统的服务器、网络设备、安全设备、数据库进行安全策略加强、调优等，加强网络、系统和设备抵御攻击和威胁的能力，整体提高网络安全防护水平。

1.4.8.2 工作方式

安全加固与优化将采用如下工作方式：

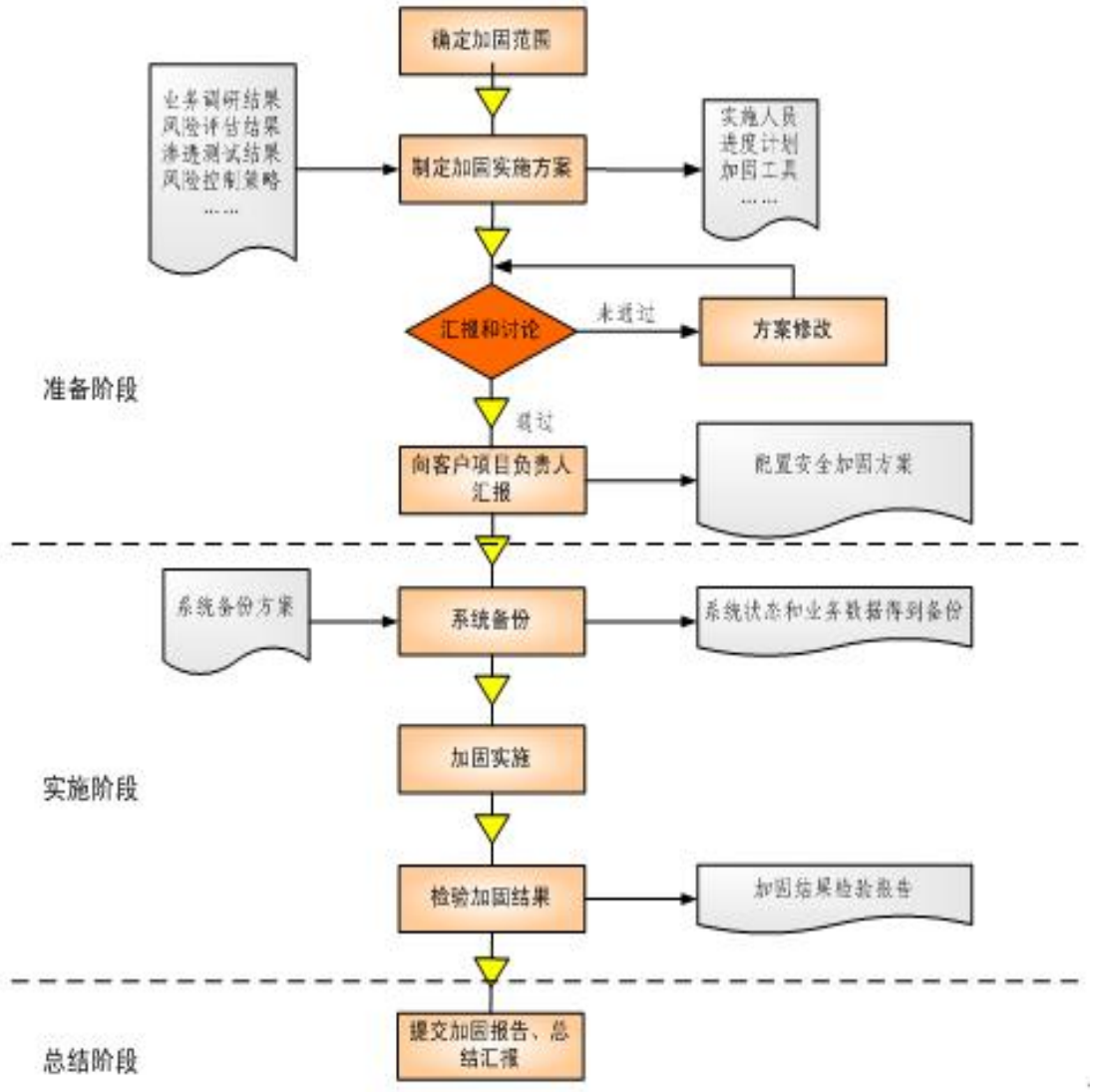
会议交流：项目组将根据脆弱性检测结果，提出安全加固与优化建议，并通过组织交流会的形式，与相关负责人就每台主机、网络与安全设备的具体加固内容进行协商，明确操作风险，探讨利害关系，确定加固方式，最终确定安全加固方案；

现场实施：项目组将赴现场，以安全加固方案为依据，协助和指导系统运维

人员进行加固与优化操作，逐项实施每台设备的安全加固项目。

1.4.8.3 工作流程

系统相关网络设备、安全设备、服务器操作系统以及数据库等配置安全加固与优化的工作流程如下图所示：



工作流程图

配置加固流程描述如下（项目实施中，可以根据实际情况需要，对流程进行调整、合并和展开等）：

确定加固范围：确定实施范围，如应用系统、资产等；

制定加固实施方案：确定实施人员、加固工具、进度计划等，为实施提供指导；

向项目负责人汇报：就配置加固实施方案向项目负责人汇报，并得到同意；

系统备份：对配置加固涉及的系统和数据进行备份；

加固实施：根据配置加固实施方案进行加固实施；

检验加固结果：验证配置加固的有效性；

提交加固报告、总结汇报：总结配置加固实施情况，并进行汇报。

1.4.8.4 提交成果

《系统安全扫描人工分析报告》、《安全配置检查和加固建议报告》、《系统主机设备加固报告》、《网络设备加固实施报告》。

通过对系统相关主机、网络与安全设备配置的加固与优化，将会减少安全漏洞和设备配置策略的不合理性，提高系统抗攻击的能力，从而可有效防范攻击、限制危害蔓延，充分发挥各项安全措施的作用，增强系统的安全性和稳定性。

1.4.9 等级保护管理制度建设

1.4.9.1 工作目的

以等级保护差距分析结果为依据，依照安全保障体系设计所提及的建设内容，按照等级保护标准要求，制定等级保护管理体系框架，明确管理方针、策略，以及相应的规定、操作规程、业务流程和记录表单；从贴合业务流程的原则出发，指导系统运维方按照等级保护三级系统的管理标准，编写管理制度文件，并进行反复沟通和修订，确保所制定的文件的适用性，且满足各系统相应保护等级的安全管理要求。通过制定和完善管理制度，明确责任权力，规范操作，加强对人员、设备和业务系统的管理，完备应急响应机制，将显著提升信息安全管理水平，有效控制信息系统所面临的安全风险，从而确保业务系统的安全、稳定运行。

1.4.9.2 工作方式

等级制度建设的工作方式主要如下：

调研访谈：采用定制的调研问卷进行访谈，了解本项目的详细情况，如组织机构（部门设置、人员职务、外部联系和接口）、业务流程（目标、流程、人员、物理位置、外部联系和接口）、信息资产（网络拓扑、主机和设备资料）、内部文件（运维程序、安全管理制度、建设方案）、原有管理相关文件及需遵守的法律法规文件等。

项目会议：召开会议，以调研访谈记录和差距分析结果为依据，研究制定安全管理制度框架和编写相应的管理制度。

交流：与相关人员就管理制度框架、管理制度内容进行反复的沟通、讨论和

修订，确保安全管理制度贴合业务实际，并满足等级保护标准和相关政策要求。

1.4.9.3 工作内容

制定和本项目相关的安全保护等级相适应的配套管理制度，制度相关内容如下：

安全管理机构：加强和完善安全机构的建设，设立指导和管理信息安全工作的信息安全领导小组，设立安全主管、安全管理各个方面的负责人，明确定义各个工作岗位的职责。建立各种安全管理活动的审批程序，明确对内对外的沟通协作方式，建立对各项安全管理活动的监督审核机制。

安全管理制度：在差距分析的基础上，建立信息安全工作总体方针、安全策略，以方针策略为依据建立配套的安全管理制度及流程规范，由专门的组织机构负责管理制度的制订、发布和贯彻落实。定期对制度进行评审和修订，确保安全管理制度的适用性。

人员安全管理：主要涉及两方面，对内部人员的安全管理和对外部人员的安全管理。具体包括人员录用、人员离岗、人员考核、安全意识教育和培训和外部人员访问管理等方面。

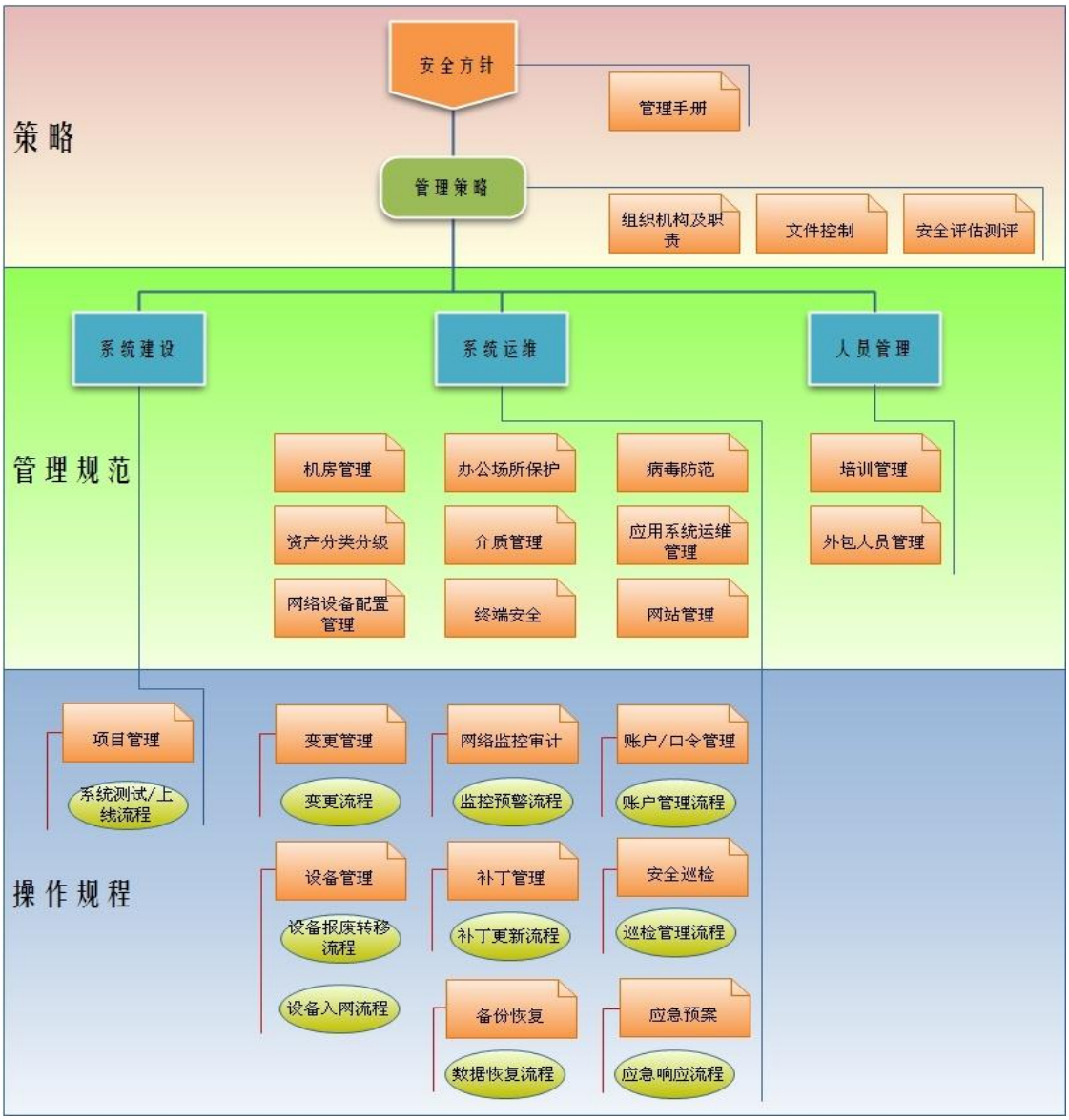
系统建设管理：为了建设符合安全等级保护要求的信息系统、系统建设管理主要关注的是信息系统生命周期中的前三个阶段（即设计、采购、实施）中各项安全管理活动，实现信息系统的安全管理贯穿系统的整个生命周期。系统建设管理分别从工程实施建设前、建设过程以及建设完毕交付等三方面考虑，具体包括系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评和安全服务商选择等方面。

系统运维管理：系统运行涉及到很多管理方面，要保证系统始终处于相应安全保护等级的安全状态中。要监控系统发生的重大变化，以便修改对应的安全措施。系统运维管理主要包括环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等方面。

1.4.9.4 工作成果

依照等级保护标准，综合考虑安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理各方面的具体要求，建立安全管理框架，如下图所

示：



安全管理框架图

以安全管理框架为基础，本次制度建设具体内容包括：

1）《信息安全管理手册》：规定了本项目安全管理的方针、目标和策略，明确应采取的相应控制措施，并对整套文档进行解释说明。

2）《组织机构及职责》明确安全管理机构及各成员职责，规定机房管理员、系统管理员、网络管理员、数据库管理员和安全管理员的岗位职责，并对单位对内对外的沟通等方面作出要求。

3）《机房管理》对机房环境要求、人员与设备进出、工作人员管理、日常监控管理、系统上线及变更管理等做出明确规定。

4）《办公场所保护》对办公场所安全管理和消防安全进行规定，以加强办公场所的防火、防盗、防信息泄露等工作。

5）《病毒防范》对防病毒的控制措施和操作程序制定管理规范，以预防病毒与各种恶意软件的入侵，提高对病毒的防御能力，保障本项目和日常工作的正常进行。

6）《资产分类分级》对资产进行分类和统一化标识，使本项目的资产受到有效的保护。

7）《介质管理》为加强对介质的使用控制和物理上的保护，防止其承载的敏感信息遭泄漏、篡改、丢失或破坏，对介质的处置做出明确规定。

8）《应用系统运维管理》对应用系统日常维护所涉及的巡检、配置管理、故障处置、系统优化、软件维护等工作进行相应规定，并明确考核措施。

9）《网络设备配置管理》对网络、安全设备配置的管理，以及配置变更所涉及的申请、审批和实施等事项作出明确规定。

10）《终端安全》规范终端的应用，对终端的使用和联网进行明确规定，以防止病毒、网络攻击及失泄密事件的发生。

11）《网站管理》对网站建设、信息发布、网站监控与维护作出明确规定，确保网站的安全性与可靠性。

12）《培训管理》要求定期开展培训，并对培训流程进行规范，对培训效果进行考核，确保人员的安全意识和技术水平得以有效提升。

13）《外包人员管理》对外包服务人员的派遣、监督和考核作出明确规定，确保外保服务质量。

14）《系统安全建设》以等级保护要求为依据，对信息系统建设的各阶段作出了相应规定，以提高本项目的安全保障能力和水平，保障并促进信息化建设。

15）《变更管理》明确需要执行申报审批手续的重要变更事项，如补丁更新、软件升级、设备更换等，并对变更的执行流程进行规定。

16）《设备管理》对设备的获取、接收、入账、维护、用途变更、报废处理等环节做出明确规定，防止因资产的丢失、损坏、失窃、使用不当而导致业务系统正常运行的中断。

17）　《网络监控审计》监控网络运行状况，对安全审计等设备的使用作出明确规定，以保云平台网络安全、高效运行。

18）　《补丁管理》对服务器操作系统、小型机操作系统、终端计算机操作系统、应用中间件和数据库软件的补丁更新要求和操作流程进行规范，确保系统防御病毒和网络攻击的能力。

19）　《备份恢复》确定业务数据的备份策略，并从数据恢复的申请、申请的审批、实施数据恢复、结果检查等方面做出明确规定，以保证业务系统数据的完整性和可用性。

20）　《帐户口令管理》明确帐户的角色及权限管理，并对口令的设置、保管与更新进行了明确规定，以防止非授权访问。

21）　《安全巡检》对网络与安全设备、服务器、应用系统和机房基础环境的巡检工作进行规范，以保证本项目业务应用系统的安全运行，有效消除安全隐患。

1.4.10 等级测评

等级测评过程中将对系统的技术体系和管理体系进行全方位的安全测评。其中，技术体系包含：物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复六个方面安全测评。管理体系包含：安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理五个方面的安全测评。

1.4.11 安全运维

主要工作为推动安全管理制度的落实工作，包括但不限于以下工作内容：

1）定期安全漏洞扫描工作；

2）定期进行设备安全基线核查工作；

3）组织安全整改工作；

4）组织安全培训；

5）其他安全管理工作。

（2）商务要求

1.采购标的所属行业

本次采购标的所属行业为软件和信息技术服务业。

2.交付（实施）的时间（期限）

服务期限：自本项目具备测试条件后采购人下发测试通知之日起60日内完成。

3.交付（实施）的地点（范围）

服务地点：海南省市场监督管理局。

4.支付方式

在合同签订后，支付合同金额的50%。项目通过竣工验收后，支付合同金额的50%。

5.售后服务

投标人必须提供详细的技术支持和服务方案，技术支持和服务方案包括（但不限于）：

1）如在测评中出现不符合项，中标人需要提供相应的整改建议及相关方案。对于测评中发现的主机和网络设备漏洞，投标方应提供项目验收合格后一年的跟踪服务，对本次评估范围内的问题提供远程技术咨询，对于漏洞的修补、问题的排除给出建议和指导，自项目验收通过之日起计算。

2）提供及时有效的售后服务，中标人在本地有服务机构或承诺如果中标则在海南省设置有不少2名技术人员的售后服务技术支持团队，并承诺提供的售后保障计划应包含7*24小时的技术支持服务，重大活动期间提供现场的技术支持服务，针对突发应急事件提供4小时内到现场处置的服务响应保障，问题解决后24小时内，提交问题处理报告，说明问题种类、问题原因、问题解决中使用的方法及造成的损失等情况。提供承诺函。

6.考核要求

审核测评方提交的相关文档和报告，完成合同要求的服务内容，直至满足以下条件才予以验收通过：

1)完成信息系统测评，并出具《测评报告》；

2)针对性的制定整改方案，并出具《整改建议方案》；

3)提交调研表、技术测评记录、会议纪要等服务过程材料；

4)符合省级以上公安部门提出的网络安全等级保护测评相关要求。