变更记录：

序号	变更原因	变更内容	编制（变更）人/时间	批准人/时间	备注
1	新建	全部，版本A/0	葛方隽/2021.3	吕萍/2021.3	

安全建设管理（S3A3G3）作业指导书					
控制点	**安全要求**	**要求解读**	**测评方法**	**预期结果或主要证据**	**符合情况**
定级和备案	a)应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由	《等级保护对象安全等级保护定级报告》是全国各类等级保护对象定级报告的通用模板，具体文档内容参见www.djbh.net.	1)核查定级文档是否明确测评系统的安全保护等级 2)核查是否给出了定级的方法和理由	具有明确描述定级方法理由和最终定级结果的定级报告书	符合情况：系统具有定级报告，报告中明确了系统的安全保护等级，且描述了安全保护等级确定的方法和理由。 部分符合情况：无。 不符合情况：无定级报告。
	b）应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定	定级结果的准确性需要安全技术专家论证评审。若初步定级结果为第二级、第三级，可组织本行业和网络安全行业专家进行评审，若为四级，则需网络安全等级保护专家评审委员会专家进行评审	1)核查是否对测评系统组织相关部门或相关专家对定级结果进行了认证和审定 2)核查是否有定级结果的评审和论证记录文件	具有相关专家对定统结果论证意见	符合情况：组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定，具有专家评审意见。 部分符合情况：无。 不符合情况：未组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定。
	c)应保证定级结果经过相关部门的批准	定级结果需由上级部门或本单位相关部门的批准	1)核查是否获得了相关主管部门的批准 2)核查是否有定级结果的审批文件	具有主管部门审批意见或本单位相关部门的审批意见	符合情况：有上级主管部门，通过上级主管部门审批；无上级主管部门的，有公司内部业务部门、信息安全部门等的批准。 部分符合情况：无。 不符合情况：定级结果未经过相关部门的批准。
	d）应将备案材料报主管部门和相应公安机关备案	有主管部门的，备案材料需向主管部门和公安机关备案，没有主管部门的，备案材料需向相应公安机关备案	1）核查是否向主管部门备案 2）核查是否有备案证明证书	具有主管部门和公安机关的备案证明	符合情况：备案材料已报主管部门和相应公安机关备案，具有公安局出具的备案证明。 部分符合情况：无。 不符合情况：未将备案材料报主管部门和相应公安机关备案。
	a)系统确定安全保护等级后,安全规划设计需根据其安全保护等级确定基本安全保护措施	系统确定安全保护等级后,安全规划设计需根据其安全保护等级确定基本安全保护措施	1)核查是否根据系统等级选择相应的安全保护措施 2)核查是否根据风险分析的结果补充安全措施 3)核查设计类文档是否根据系统等级或风险分析结果采取相应的安全保护措施 这里的安全规划设计类文档要求根据等级保护对象的安全保护，判断等级保护对象现有的安全保护水平与国家等级保护管理规范和技术标准之间的差距，提出等级保护对象的基本安全保护需求	安全设计文档有明确描述系统安全保护等级，并在相关章节中描述安全措施设计是依据系统等级和其特殊安全需求进行选择	符合情况：具有《系统安全设计方案》，方案中明确根据安全保护等级确定安全保护措施。 部分符合情况：无 不符合情况：未设计安全方案。

安全方案设计	b)应根据保护对象的安全保护等级及与其他级别保护对象的关系进行整体安全体划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件	被测系统是整个单位等级保护对象的一部分，其安全方案应作为单位整体安全规划的一部分，且其安全性在设计上与其位系统可能存在共享，譬如在网络结构设计、安全措施部署上都具有共享关系，因此单位的整体安全规划也很有必要，安全规划是等级保护对象安全等级保护实施的环节之一，也是确保安全等级保护有效实施的重要环节，其目标是根据等级保护对象的划分情况，等级保护对象的定级情况、等级保护对象承载业务情况，通过分析明确等级保护对象安全需求设计合理、满足等级保护要求的安全方案	1)核查是否有保护对象的相关设计文档 2）核查保护对象的总体规划和设计文档，且文档内容是否连贯配套，内容是否含密码技术相关内容 一般情况下，配套文件中包括总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案等内容。在定期开展等级测评和安全评结后，如果发现等级保护对象安全现状已经不满足等级保护的基本安全要求或者发现等级保护对象有新的安全需求，则应该调整和修订安全保证体系的相关配套文件 安全规划管理示例: a)安全规划设计是指对系统总体安全建设规划，近期和远期安全建设工作计划、安全方案等进行设计、编制 b)安全方案设计是指根据系统的定级情况、承载业务情况，通过分析明确等级保护对象的安全需求，设计既满足自身需求又满足等级保护要求的、合理的安全方案，包括总体安全方案和详细设计方案 c)总体安全方案包括总体安全策略、安全技术框架、安全管理框架，详细设计方案包括技术措施实现内容和管理措施实现内容 d)XX处负责依据相关文件，委托设计单位编制系统安全规划设计系列文件，并不断完善 e)编制完成的系统安全规划设计系列文件经各处审核、网络安全领导小组及相关专家论证评审，XX审批	具有单位总体的安全规划文档和被删系统安全设计文档，且包含相关密码设计内容(如果采用了密码产品和算法)	符合情况：《系统安全设计方案》中包含与其他级别保护对象的关系进行整体安全体划和安全方案设计，其中包含密码技术相关内容，并形成配套文件。 部分符合情况：《系统安全设计方案》未中包含密码技术相关内容，或无与其他系统如何进行交互的内容。 不符合情况：《系统安全设计方案》及其他配套文件与其他系统如何进行交互的内容，也未包含密码相关内容。
	c)应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施	设计合理的安全方案是保障等级保护对象安全建设和运行的基础，安全设计方案应当对系统安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等内容作出具体的规划和设计，并经过论证、审定和批准	1)核查是否组织相关人员对系统规划和建设文档进行论证和评审 2)核查评审的文档和批准意见	具有总体安全规划和安全设计方案的专家论证、批准意见	符合情况：该系统的安全规划、安全设计方案及其配套文件均已进行评审。具有评审意见，批准后正式实施。 部分符合情况：无。 不符合情况：未组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定。
	a)应确保网络安全产品采购和使用符合国家的有关规定	我国对网络安全产品的管理在不同发展阶段可能存在不同的管理政策,因此在该条款的理解上，应根据当下国家的管理要求去落实，目前而言，在此方面国家的主要管理要求是连从产品获得《计算机等级保护对象安全专用产品销售许可证》才能在市场上流通的政策。产品购买方在采购过程中应从已获得销售许可证的产品系列中选取	1)访谈建设负责人产品采购的流程或流通的标准2)抽样核查网络安全产品的销售许可标志	网络安全产品均具有销售许可证	符合情况：该系统相关网络安全产品有安全产品采购流程及符合国家有关规定。 部分符合情况：无 不符合情况：未有采购流程，未遵守合国家有关规定。

产品采购和使用	b)应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求	如若被测系统中采用了商用密码产品，则该产品的采购和使用需符合国家的用密码管理部门的要求，(如《信息安全等级保护商用密码管理办法》等)	1)访谈建设负责人是否采用了商用密码产品或服务 2)核查使用的密码产品的许可证明或批文 密码产品是指采用密码技术对信息进行加密保护或安全认证的产品，如加密电子证书等	密码产品符合国家相关部门的要求	符合情况：该系统使用的密码产品或服务，符合国家密码主管部门的要求。 部分符合情况：无 不符合情况：使用的密码产品不符合国家密码主管部门要求。
	c)应预先对产品进行选型测试，确定产品的候选范围,并定期审定和更新候选产品名单	在采购产品时，不仅要考虑产品的使用环境、安全功能、成本(包括采购和维护成本)等因素，还要考虑产品本身的质量和安全性，因此需要预先对产品进行选型测试	1)访谈建设负责人产品来购流程 2)核查产品采购管理制度或要求 3)核查采购管理内容是否覆盖产品的选择方式以及定期审定和更新产品列表 通常情况下，产品采购的管理需要制定相关制度要求，产品采购管理示例: 产品采购管理是指对等级保护对象软硬件产品采购过程的管理，包括安全产品、网络产品、服务器以及应用和系统软件等 由XX处提出产品采购需求，由XX处按照政府采购流程进行产品采购，对于大宗产品的采购必须经过XX审批 采购的防火墙， IDS.防病毒软件等安全产品必须具有公安部下发的《计算机安全产品销售许可证》，采购的密码产品必须符合国家密码管理部门的相关规定	具有产品选型测试报告、候选产品清单和定期更新名单	符合情况：产品采购由专门部门对产品进行选型测试，留存有产品选型测试文档、候选产品采购清单等。 部分符合情况：无。 不符合情况：产品采购前未进行选型测试。
	a)应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制	为避免开发过程中对系统造成影响，要保证开发环境与实际运行环境纷开，测试数据和测试结果受到控制	1)访谈建设负责人,开发的控制流程和控制措施有哪些 2)核查软件开发相关管理的规定和要求 3)管理内容是否覆盖开发环境和运行环境分开的规定以及测试数据是否受控 开发人员和测武人员分离，即开发人员不能做测试人员，测试数据和测试结果受到控制，是指它们应该与软件设计相关档文一起有专人管理，并且对他们的使月和访问进行严格限制	1)开发环境与运行环境分离 2)有明确的管理要求控制测试数据和测试结果的使用	符合情况：部署有独立的开发和测试环境，与生成环境物理隔离，测试部门具有独立的测试库等，设置访问权限，对测试数据和结果进行控制。 部分符合情况：开发环境与实际运行环境物理分开，对测试数据和结果无法实现安全可控，或开发环境与实际运行环境未物理分开，但测试部门具有独立的测试库等，设置访问权限，对测试数据和结果进行控制。 不符合情况：开发环境与实际运行环境未物理分开，对测试数据和结果无法实现安全可控。
	b)应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则	为保证软件开发过程的安全性和规范性，应制定软件开发方面的管理制度，规定开发过程的控制方法和人员行为准则	1)访谈安全建设负责人，是否有软件开发方面的管理制度 2)核查管理制度内容是否覆盖软件开发的整个生命周期 3)开发过程中是否覆盖开发过程的控制方法和行为准则	具有软件开发管理制度，明确了开发过程中相关管理要求	符合情况：制定《软件开发管理制度》，内容包括开发过程的控制方法和人员行为准则等 部分符合情况：无。 不符合情况：未制定《软件开发管理制度》。

自行软件开发	c)应制定代码编写安全规范，要求开发人员参照规范编写代码	一般一个应用软件需要多名开发人员共同开发，然而不同开发人员有不同的代码编写风格，这给代码的维护、整合等工作带来了很大的困难。因此，要求针对不同的开发语言制定相应的代码编写规范，并要求所有开发人员都按照相应d的规范编写代代码，这将给代码的阅读、理解、维护、修改、跟踪调试、整合等带来极大的方便	1）访谈系统建设负责人是否有代码编写安全规范 2）代码编写规范是否明确代码的编写规则	具有代码编写安全规范	符合情况：制定《代码编写安全规范》，对排版要求、注释规范、方法（函数）等进行定义。 部分符合情况：无。 不符合情况：无制定《代码编写安全规范》。
	d)应具备软件设计的相关文档和使用指南，并对文档使用进行控制	系统开发过程中，开发人员需编制软件设计的相关文档和使用指南，而且，系统开发文档的保管、使用应严格管理，加以限制。	1)访谈系统建设负责人是否有人负责对软件设计的相关文档进行管控 2)被测评系统是否有开发文档和使用说明文档	具有软件开发过程中的相关文档(如软件概要设计文档、软件详细设计文档等)和使用指南	符合情况：具有系统软件设计的流程图、效果图、设计文档、系统使用指南等文档，具有文档使用范围，对文档使用进行控制。 部分符合情况：无。 不符合情况：未有系统设计的相关文档和使用指南。
	e)应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在恶意代码进行检测	应在软件开发过程中加强软件的安全性测试，以便及早发现软件的安全漏洞、在软件安装前进行代码安全审计，通过工具测试和人工确认的方式识别恶意代码，这是保证软件安全运行的最后一道屏障。 可通过第三方检测机构内或机构内部自行测试	1）访谈安全建设负责人，是否在软件开发的生命周期中进行安全性测试 2)核查是否具有安全性测试报告和代码审计报告	具有阶段性软件安全测试报告和软件安装前代码审计报告	符合情况：系统在开发过程中，进行了恶意代码检测等安全测试，并出具相关报告。 部分符合情况：系统在开发过程中，进行了恶意代码检测等安全测试，未出具相关报告。 不符合情况：系统在开发过程中，未对恶意代码检测等安全测试。
	f)应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制	对程序资源库的访问，维护等应进行严格管理	1)访谈建设负责人是否对程序资源库进行管控 2)核查是否有管控记录文件 要求对程序源代码及源程序库的修改、更新和发布都得到授权和批准。这里的发布-方面包括向程序员发布程序源代码，另一方面包括修改或更新程序代码后应用软件重新上线	具有程序资源库修改、更新、发布的授权、批准记录	符合情况：已对程序资源库的修改、更新、发布的流程进行管理，并对资源库进行严格的版本控制。 部分符合情况：对程序资源库的修改、更新、发布的流程进行管理，未对资源库进行严格的版本控制。 不符合情况：未对程序资源库的修改、更新、发布进行授权和批准。
	g)应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查	软件开发需保证开发人员为专职人员，并对其开发过程能够有效的控制	1)访谈建设负责人开发人员是否为专职人员 2)核查软件开发管控制度是否对开发过程和人员的行为准则进行了规定和要求	开发人员为专职人员，有相关管理要求或手段对开发人员进行控制、监视或审查	符合情况：所有人员均为专职人员，签署劳动合同，并对开发人员的开发活动受到控制、监视和审查。 部分符合情况：开发人员为专职人员，但开发人员的开发活动未受到控制、监视和审查。 不符合情况：未保证开发人员为专职人员，开发人员的开发活动未受到控制、监视和审查
	a)应在软件交付前检测其中可能存在的恶意代码	同自行软件开发一样,对于外包软件,在交付前同样需要进行恶意代码检测，以保证软件的安全性,可要求外包方进行检测或机构内部自行检测	1)访谈建设负责人是否做恶意代码检测 2)核查是否有恶意代码检测报告	具有恶意代码检测报告	符合情况：软件交付前进行恶意代码检测，并出具相关报告。 部分符合情况：软件交付前检测进行恶意代码检测，未出具相关报告。 不符合情况：软件交付前未进行恶意代码检测。

外包软件开发	b)应保证开发单位提供软件设计文档和使用指南	软件开发完成之后，应要求外包开发单位提供软件设计相关文档和使用指南	1)访谈建设负责人是否有软件设计的相关文档和使用指南 2)核查是否提供了软件生命周期中的所有文档	具有软件开发的相关文档， 如需求分析说明书、 软件设计说明书、使用指南等	符合情况：开发单位提供的交付清单包括软件审计文档和使用指南。 部分符合情况：无。 不符合情况：开发单位未提供软件设计文档和使用指南。
	c)应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道	后门和隐蔽信道的审查在可专业的测试进行，若开发单位无法提供该类报告，则需提供书面材料保证软件源代码中不存在后门和隐蔽信道	1)访谈建设负责人，外包开发单位是否提供源代码 2)核查是否提供源代码的安全检查报告 3)核查软件源代码及源代码的审查记录 审查软件中可能存在的后门时，一般通常在系统的设计者利用应用系统的开发时机，故意设置机关，用以监视计算机系统，但有时也因偶然考虑不周而存在(如漏洞)。可以通过人工或采用专业工具(如 Fortify SCA、Checkmarx 等)事方式进行源代码审查，发现软件中可能存在的后门	1.提供软件源代码 2.具有软件测试报告，内容涵盖后门和隐蔽信道的测试	符合情况：开发单位已提供源代码，对系统源代码进行审计工作，对可能存在的后门和隐蔽信道进行检测。 部分符合情况：无。 不符合情况：开发单位未提供软件源代码。进行审查。
工程实施	a)应指定或授权专门的部门或人员负责工程实施过程的管理	等级保护对象工程实施应当指定或授权专门的部门或人员负责工程实施过程的管理，以保证实施过程的正式有效性	1）访谈建设负责人，工程实施是否指定专门部门或人员进行工程实施过程的管控 2）核查部门或岗位职责文档	指定了专门部门或人员对工程实施过程进行进度和质量控制	符合情况：指定部门负责工程实施过程的管理。 部分符合情况：无。 不符合情况：未指定部门负责工程实施过程的管理。
	b)应制定安全工程实施方案控制实施过程	工程实施过程的控制需要事先制定实施方案，对工程时间限制、进度控制和质量控制等内容进行规定	1)访谈建设负责人是否有工程实施方案 2)核查工程实施方面的管理制度以及控制方法 总体的工程实施方案应说明任务量、计划进度、实施阶段、各阶段结束的标志和开始的条件、完成时提交的内容等。一旦实施方案确定，就必须按照方案的阶段安排逐步开展工作,并进行量化和考核，否则将造成工程实施组织的混乱，无法保证工程的顺利完成。 详细的工程实施方案要求的正式执行行是相对于系统工程能力成熟度模型(SSE-CMM)中所定义的一级，非正式执行。该级仅要求对所有基本实践都被执行，而对执行的结果并无明确要求。因此，正式执行意味着对执行结果和执行工程必须严格控制，根据制定的工程实施方案落实各个执行中间结果，保证实施结果与预定目标相符	具有工程实施方案，内容包括工程时间限制、进度控制等方面的方面	符合情况：制定《系统实施方案》，方案中对项目各阶段进行要求。 部分符合情况：无。 不符合情况：未制定《系统实施方案》控制实施过程。

	c)应通过第三方工程监理控制项目的实施过程	一般来讲，对于外包实施项目，需要第三方工程监理的参与，来控制项目的实施过程，对工程进展，时间计划、控制措施、工程质量等进行把关	1)访谈建设负责人测评系统是否为外包项目 2)核查是否聘请了第三方监理 3)核查监理报告以及主要控制措施	第三方工程监理，工程监理报告明确了工程进展、时间计划、控制措施、工程质量等	符合情况：聘请监理单位进行项目监理工作。 部分符合情况：无。 不符合情况：未聘请第三方工程监理控制项目的实施过程
测试验收	a)应制订测试验收方案，并依据测试验收方案实施测试验收,形成测试验收报告	此处的测试验收，可以包括外包单位项目实施完成后的测试验收，也可包括机构之间的内部开发部门移交给运维部门过程的验收等	1）访谈建设负责人是否对测试验收进行管控 ）2核查是否有调试验收方案和测试验收报告	1）具有工程测试验收方案，方案中明确说明了参与测试的部门、人员、测试验收内容、现场操作过程等内容 2)测试验收报告具有相关部门和人员对测试验收报告进行审定的意见	符合情况：制定《系统测试验收方案》，方案明确测试部门、人员，验收内容、操作内容等，并出具测试验收报告。 部分符合情况：制定《系统测试验收方案》，方案明确测试部门、人员，验收内容、操作内容等，未出具测试验收报告。 不符合情况：未制定《系统测试验收方案》。
	b)应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容	为保证系统建设工程按照既定方案和要求实施，并达到预期要求，在工程实施完成之后，系统交付使用之前，应当指定或授权专业机构依据安全方案进行安全性测试	1访谈建设负素人在系统证线前是否展开安全性测试 2)安全性测试是否括密码应用方面的内容 一般情况下，上线前的安全测试由第三方测试单位进行，第三方测试单位是指非系统拥有者和系统建设方，第三方测试有别于开发人员或用户进行的测试，其目的是为了保证测试工作的客观性。第三方一般属于权威的专业测试机构，针对物理环境、硬件设施、软件设施等方面可能存在的缺陷或问题进行测试	具有上线前的安全测试报告，报告包含密码应用安全性测试相关内容	符合情况：系统上线前进行了安全性测试，具有测试报告，包含密码应用安全测试性相关内容。 部分符合情况：系统上线前进行了安全性测试，具有测试报告，报告未包含密码应用安全测试性相关内容。 不符合情况：系统未做上线前安全性测试
系统交付	a)应制定交付清单， 并根据交付清单对所交接的设备、软件和文档等进行清点	系统在工程实施并验收完以后，需要根据协议有关要求，按照交付清单对设备备、软件、文档进行交付	1访谈建设负责人是否对系统交付建立管控流程以及交付清单 2)核查交付清单内容	具有交付清单，交付清单对交付的各类设备、软件、文档等有明确的说明	符合情况：制定交付清单，包括交接的设备、软件和说明文档等。 部分符合情况：无。 不符合情况：未制定交付清单。
	b)对负责运行维护的技术人员进行相应的技能培训	系统交付时，交付单位或部门需要对运维和操作人员进行必要的培训	1)访谈建设负责人是否对运行维护人员进行技能培训 2)核查培训记录相关记录文档	具有运维技术培训相关文档，内容包括培训内容、培训时间和参与人员等方面的信息	符合情况：系统上线前对负责系统运维的技术人员进行技能培训。 部分符合情况：无 不符合情况：未对负责系统运维的技术人员进行技能培训。
	c)应提供建设过程文档和运行维护文档	交付单位或部门需提供建设过程中的文档和指导用户进行运行维护的文档，以便指导运维人员和操作人员后期的运行维护	1)访谈建设负责人建设过程的管控措施 2） 核查建设过程文档和运行维护文档	在系统交付的文档中包括指导用户进行维护的文档等，且符合管理规定相关要求	符合情况：系统交付文档中包含建设过程文档和运行维护文档。 部分符合情况：无。 不符合情况：未供建设过程文档和运行维护文档。
	a)应定期进行等级测评，发现不符合相应等级保护标准要求的应及时整改还	对等级保护对象进行等级测评是检验系统达到相应等级保护要求的途径，也是发现系统安全隐患的重要途经，通过选择有资质的测评机构对系统进行定期的测评，有助于系统发现问题并进行及时的整改，就目前来说，第三级等级保护对象应当每年至少进行一次测评	1)访谈等级测评负责人是否每年定期开展等级测评 2)核查等级测评报告和整改记录	1)定期开展测评工作，且非首次，以往进行过几次测评，并根据测评结果进行相应的安全整改 2)具有以往等级测评报告和安全整改方案	符合情况：本次系统测评为首次测评。系统每年开展等级测评，针对测评的不符合项问题进行整改。 部分符合情况：无。 不符合情况：未定期进行等级测评。

等级测评	b)应在发生重大变更或级别发生变化时进行等级测评	系统在发生重大的网络结构调整或大范围的设备更换，应用系统功能变化等变更时，应重新进行等级测评，并评估系统级别是否发生变化，若变化，则需按照最新的安全保护等级要求进行测评	1)访谈测评系统是否发生过重大变更或开级 2)核查重大升级变更或改造的文件	1）有过重大变更或级别发生过变化，若有，及时开展了等级测评 2)具有相应情况下的等级测评报告	符合情况：系统在发生重大变更或级别发生变化时，重新进行等级测评。系统尚未发生重大变更或级别发生变化，在管理制度中规定，发生变化时进行等级测评、 部分符合情况：无。 不符合情况：在发生重大变更或级别发生变化时未进行等级测评。
	c)应确保测评机构的选择符合国家有关规定	目前国家对等级保护测许机构的管理遵从测评机构名录管理要求,即在国家网络安全等级保护工作协调小组办公室推荐测评机构名单内的测评机构均可透，具体参见www.dibh.net	1)访谈测评负责人是否选择了具有测评资质的测评机构 2)到www.djbh.net上核查该机构是否符合要求	等级测评的测评单位具有国家相关等级测评资质的单位	符合情况：由测评公司进行测评，该测评公司符合国家规定。 部分符合情况：无。 不符合情况：测评机构的选择未符合国家有关规定。
服务供应商的选择	a)应确保服务供应商的选择符合国家的规定	对各类供应商的选择均应符合国家对其的管理要求 (如相关资质管理要求、销售许可要求等)	1访谈建设负责人如何选择服务商 2)核查服务商资质文件	选择的安全服务商符合国家有关规定	符合情况：由XX公司提供安全服务，该公司具有资质。符合国家有关规定。 部分符合情况：无。 不符合情况：服务供应商的选择未符合国家的规定。
	b)应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务	服务提供商所提供服务的质量，将直接影响到系统的安全，为了减少或者杜绝这些服务带来新的安全问题，在选择服务商的时候，除了选择具有相应服务资质的机构，还要以协议或合同方式明确其职责以及后期的服务承诺等	1)访谈建设负责人对服务供应商的管控措施 2)核查服务供应商的服务内容和协议	具有与安全服务商签订的服务合同或安全责任合同书，并明确了后期的技术支持和服务承诺等内容	符合情况：该系统与服务提供商签订服务协议，协议中明确双方的责任和义务。 部分符合情况：无 不符合情况：未与服务供应商签订相关协议。
	c)应定期监督、评审和审核服务供应商提供的服务,并对其变更服务内容加以控制	对供应商的监视和评审主要基于与其所签订协议中的网络安全相关条款和条件,验证其所提供服务与协议的符合程度，通过定期评审其工作服务报告，确保有足够的服务能力按照可行的工作计划履行其服务职责	1访谈建设负责人是否对服务供应商进行定期监督、评审和审核 2)核查对服务供应商的管理规定或要求 3)核查服务供应商服务报告或服务审核报告	1）具有安全服务商定期提交的安全服务报告 2)定期审核评价安全服务供应商所提供的服务，具有服务审核报告 3)具有安全服务商评价审核管理制度，明确了针对服务商的评价指核内容等	符合情况：指定部门对安全服务公司进行监督，对安全服务商服务变更申请，进行审核；明确一旦安全服务商变更服务内容，须评价是否符合要求。 部分符合情况：无。 不符合情况：未定期监督、评审和审核服务供应商提供的服务,并对其变更服务内容加以控制。