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	

安全管理机构（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
岗位设置	a)应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权	为保证安全管理工作的有效实施，应设立指导和管理网络安全工作的委员会或领导小组，负责单位网络安全管理的全局工作，是网络安全组织的最高管理层	1)访谈信息/网络安全主管是否成立了指导和管理网络安全工作的委员会或领导小组 2)核查部门职责文档是否明确了网络安全工作委员会或领导小组构成情况和相关职责 3)核查相关委任授权文件是否明确其最高领导由单位主管领导委任或授权 一般情况下，一个机构成立了指导和管理网络安全工作的委员会或领导小组，均需有正式的发文 通常，在单位的内部结构上建立一整套从单位最高管理层(网络安全领导小组并且由单位最高领导委任或授权)到执行管理层(网络安全管理工作职能部门及安全主管)以及系统日常运营层(系统管理员、网络管理员、安全管理员等) 的三层及金字塔式的管理结构来约束和保证各项安全管理措施的执行。网络安全领导小组主要的职责包括对安全管理制度体系合理性和适用性的审定、对机构内关键网络安全工作进行授权和审批等,但其最主要的是负责单位网络安全管理的全局工作:网络安全管理职能部门的主要职责是对机构内重要网络安全管理工作的授权和审批、内部相关业务部门和安全管理部门之间的沟通协调以及与机构外部单位的合作、定期对系统的安全措施落实情况进行检查，以便发现问题进行改进等	1)机构成立了网络安全工作委员会或领导小组,且有明确的文件明确其组成机构及工作职责 2)具有由单位主管领导委任或授权的相关文件	符合情况：《XXX公司信息安全方针》中已明确成立了网络安全工作领导小组，明确了人员构成情况和相关职责，同时已明确其最高领导由XXX部门领导担任，组长为XXX，组员为XXX。 部分符合情况：《XXX公司信息安全方针》中已明确成立了网络安全工作领导小组，明确了人员构成情况，同时已明确其最高领导由XXX部门领导担任，组长为XXX，组员为XXX，但相关职责不明确。 不符合情况：XXX公司未成立指导和管理网络安全工作的委员会或领导小组。
	b)应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责	网络安全管理工作的职能部门是机构的执行管理层，一般负责对网络安全管理工作的授权和审批， 内部相关业务部门和安全管理部门之间的沟通协调以及与机构外部单位的合作，定期对系统的安全措施落实情况进行检查，系统安全运行维护管理工作	1)访谈信息/网络安全主管，是否设立了网络安全管理职能部门和各方面负责人(如机房负责人、系统运维负责人，系统建设负责人等) 2)核查部门职责文档是否明确网络安全管理工作的职能部门和各负责人职责 “安全主管“一般是一个单位安全管理工作的主要责任人，全面负责等级保护对象安全规划、建设、运行维护等安全管理工作，一般由单位的高层或某一部门的主管担任。“安全管理各方面的负责人”一般包括物理安全负责人(其是保护等级保护对象物理进行环境和办公环境安全的责任人），系统建设方面负责人(其是保证等级保护对象安全规划、建设、工程实施过程的责任人)和系统运行维护方面的责任人(其是保证等级保护对象日常运行安全的责任人)等	1)机构设立了网络安全管理职能部门，并指定了各部门负责人 2)具有明确的职责文件明确部门和负责人的工作职质	符合情况：已指定由XXX部门担任网络安全管理工作的职能部门，且具备人员职责划分文档，文档中明确了部门及各个工作岗位的职责。 部分符合情况：已指定由XXX部门担任网络安全管理工作的职能部门，但未设立安全管理各个方面的负责人岗位，未定义各负责人的职责。 不符合情况：

	c)应设立系统管理员、 审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责	系统管理员、网络管理员、安全管理员等为机构的日常运营层，主要负责具体落实各项网络安全等级保护工作具体要求，负责日常的具体安全维护工作	1)访谈信息/网络安全主管是否设立了系统管理员、网络管理员和安全管生员等岗位 2)核查岗位职责文档是否明确了各岗位职责	1）机构设立了系统管理员、网络管理员、安全管理员岗位， 2）具有明确的各岗位职责说明文档	符合情况：XXX公司已进行安全管理岗位的划分，包括网络管理员、系统管理员、安全管理员等管理岗位，且具备人员职责划分文档，文档中明确了部门及各个工作岗位的职责。 部分符合情况：管理员岗位设立不完善，如当前实际情况缺失审计管理员等。 不符合情况：XXX公司未进行安全管理岗位的划分，未设置审计管理员、安全管理员等相关管理岗位。
人员配备	a)应配备一定数量的系统管理员、审计管理员和安全管理员等	由于部分岗位人员拥有关键的操作权限，为避免人员失误或渎职现象的发生，应配备一定数量的安全管理人员，如系统管理员、审计管理员和安全管理员等	1)访谈信息/网络安全主管各个安全管理岗位人员配备情况 2) 核查管理人员名单，查看其是否明确机房管理员、系统管理员、网络管理员、安全管理员等重要岗位人员的信息. 3)与技术核查结合，各个岗位是否根据管理人员名单予以授权，如主机核查时系统管理员是否和管理人员名单一致	1)人员配备文档中明确了各岗位人员的配备人员及数量 2)管理人员名单中明确机房管理员、系统管理员、网络管理员、安全管理员等重要岗位人员的信息 3)各个岗位根据管理人员名单任职	符合情况：XXX公司实际已配备相应的网络管理员、系统管理员、安全管理员，当前配备有网络管理员1名，安全管理员1名等。 部分符合情况：XXX公司实际已配备相应的网络管理员、系统管理员、安全管理员，当前配备有网络管理员1名，安全管理员1名等，但授权管理人员名单与实际管理人员不一致。 不符合情况：XXX公司仅配备一位系统管理员，无审计管理员及安全管理员，人员配备不完善。
	b)应配备专职的安全管理员，不可兼职	安全管理员不能兼任其他与等级保护对象相关的管理岗位，如系统管理员、网络管理员等	1）访谈安全主管，询问安全管理员的配备情况，是否是专职 2)核查管理人员名单，确认安全管理员是否是专职人员	1）人员配备文档表明安全管理员没有兼任系统管理员、 网络管理员等 2）这货没有兼职干别的活。	符合情况：XXX公司已配备专职安全管理员，不存在兼任情况，当前安全管理员由XX领导担任。 部分符合情况：暂无 不符合情况：XXX公司安全管理员非专职，存在兼任情况。
	a)应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等	通过对部门和岗位职责的描述，应能明确指出部门或岗位可以进行审批的事项内容	1)访谈安全主管，询问对哪些等级保护对象活动进行审批，审批部门是什么部门，审批人是什么岗位 2)核查部门职责文档是否明确各部门的审批事项和审批岗位 3)核查岗位职责文档是否明确各岗位的审批事项 4)核查审批记录，是否与相关职责文件描述一致。	1)部门和各岗位的职责文件中包含了相关事项的审批描述 2)审批记录和相关职责文件描述一致	符合情况：已制定《XXX部门职责文档》，相关制度中已明确了各个部门岗位的具体职责划分以及授权审批事项、审批部门和批准人等，具备审批记录。 部分符合情况：已制定《XXX部门职责文档》，相关制度中已明确了各个部门岗位的具体职责划分以及授权审批事项、审批部门和批准人等，但无法提供相应的审批记录等表单。 不符合情况：XXX公司未根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等内容。

授权和审批	b)应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按审批程序执行审批过程，对重要活动建立逐级审批制度	相关的管理制度文档中一般对系统变更(如变更管理制度).物理访问(如机房管理制度)、系统接入(如网络管理制度)等重要活动明确审批流程，包括逐级审批流程。另外，要求保存审批过程记录文档，并要求保证执行中的审批程序、审批部门及批准人与审批制度文档中规定的一致性	1)访谈安全主管，询问其对重要活动的审批范围(如系统变更、重要操作、物理访问和系统接入、重要管理制度的规定和发布，人员的配备和培训、产品的采购、外部人员的访问等)，审批程序如何， 其中哪些事项需要逐级审批 2)核查系统变更、重要操作、物理访问和系统接入等事项的相关管理制度是否明确相关操作的逐级审批程序 3)核查经逐级审批的记录，查看是否具有各级批准人的签字和审批部门的盖章，是否与相关制度一致 系统变更，一般分为重大变更和普通变更，前者如系统运行业务改变或系统核心设备更换等，后者如点如系统或设备配置更改等；重要操作，如设备加电或断电等；物理访问主要指对机房或重要办公区域的访问；:系统接入一般指外部系统或网络接入等级保护对象 逐级审批活动的重要程度可以是从执行管理层(安全主管、负责人)到运营层(各管理员)的二级审批，也可以是从最高层(网络安全领导小组)到执行管理层再到运营层的三级审批。	1相关管理制度中明确了系统变更、物理访问和系统接入等重要操作的审批流程 2)具有相关事项的审批记录 3逐级审批的记录，具有各级批准人的签字和审批部门的盖章，与相关制度一致	符合情况：已制定《XXX公司信息系统变更管理办法》、《XXX公司第三方安全管理规定》、《XXX公司信息系统项目管理规定》等制度，相关制度中对系统变更、重要操作、物理访问和系统接入等事项执行过程进行了审批流程规定，并特别强调了“系统上线”等重要活动的逐级审批要求，具体工作中通过OA线上审批。 部分符合情况：已制定《XXX公司信息系统变更管理办法》、《XXX公司第三方安全管理规定》、《XXX公司信息系统项目管理规定》等制度，相关制度中对系统变更、重要操作、物理访问和系统接入等事项执行过程进行了审批流程规定，并特别强调了“系统上线”等重要活动的逐级审批要求，但无法提供审批过程记录表单。 不符合情况：XXX公司未对系统变更、重要操作、物理访问和系统接入等事项进行审批。
	c)应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批等信息	审批事项可能会根据审批部门变更、审批人变更以及相关审批流程发生变更，因此需要及时根据实际情况变化进行审查并更新相关内容。另外需定期对相关审批事项进行审查，以更新需要更新的相关信息	1访谈信息/网络安全主管对各类审批事项进行更新 2)核查是否具有对相关审批事项的定期审查记果和授权更新记录 需要形成审批事项列表，在该列表中明确审批事项、涉及的审批部门、批准人等，并要求定期对该列表进行更新维护，如部门职责或岗位职责改变则某-审批活动涉及的审批部门和批准人则会改变，活动的重要程度改变则该活动的审批流程也会改变等	具有定期审查审批事项的记录和授权更新记录	符合情况：XXX公司每年对各类审批项目、审批部门和审批人进行更新，记录表单类文档中具有更新需授权和审批的项目、审批部门和审批人等信息，记录日期与审查周期一致。 部分符合情况： 不符合情况：XXX公司未定期审查审批事项。
	a)应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作，定期召开协调会议，共同协作处理网络安全问题	一个单位的等级保护对象运行可能涉及到多个业务部门， 因此，为保障整个等级保护对象安全工作的顺利完成，需要各业务部门的共同参与和密切配合。此处沟通方式的要求，要求采取例会或不定期召开会议的形式进行网络安全问题处理	1)访谈信息/网络安全主管，是否建立了各类管理人员之间、组织内部机构之间以及网络安全职能部门内部的合作与沟通机制 2)核查相关会议记录，是否涵盖安全相关内容。其中，针对组织内部机构之间以及网络安全职能部门内部的安全工作会议文件或会议记录，查看是否具有会议内容、会议时间、参加人员和会议结果等描述，是否具有安全管理委员会或领导小组安全管理工作执行清况的文件或工作记录(如会议记录/纪要，网络安全工作决策文档等)	1)内部机构之间网络安全职能部门内部建立了相相关沟通交流机制 2)具有定期召开会议的记录	符合情况：XXX公司已建立各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通机制，每年组织一次工作会议进行沟通合作，共同协调处理信息安全相关问题，具备相关会议记录。 部分符合情况：不定期召开协商会议或协商会议周期过长，无相关会议记录。 不符合情况：XXX公司未定期与各类管理人员、组织内部机构和网络安全管理部门之间进行合作沟通，不具备沟通合作记录。

沟通和合作	b)应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通	与外界各类单位、部门的沟通与合作机制可能有多种方式,如与网络管理部门定期汇报、检查工作,与供应商定期会议商讨系统中的安全问题，与业界专家进行安全评审咨询等方式	1)访谈信息/网络安全主管,是否建立了与网络安全管理部门、各类供应商、业界专家及安全组织的合作与沟通机制 2)核查相关沟通合作记录，是否具有与网络安全管理部门、各类供应商、业界专家沟通交流的记录	1）与网络安全管理部门、各类供应商、业界专家及安全组织的合作与沟通机制 2）具有日常沟通交流的记录和文件	符合情况：XXX公司已建立与网络安全职能部门、各类供应商、业界专家及安全组织等的沟通、合作机制，通过会议、电话、邮件等方式进行交流沟通。 部分符合情况：无法提供日常沟通交流的记录和文件，导致留档缺失。 不符合情况：XXX公司未定期与网络安全职能部门、各类供应商、业界专家及安全组织等进行合作沟通，不具备沟通合作记录。
	c)应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息	与外联单位的联系应建立联系列表并根据实际情况维护更新列表信息、明确合作内容以及联系人等相关的信息	核查外联单位联系列表，是否记录外联单位名称、合作内容、联系人和联系方式等信息	具有外联单位联系列表，且包括外联单位名称、合作内容、联系人和联系方式等信息	符合情况：XXX公司已建立外联单位联系列表，包含外联单位名称、合作内容、联系人和联系方式等信息。 部分符合情况：XXX公司已建立外联单位联系列表，但列表数据不全面。 不符合情况：XXX公司未建立外联单位联系列表。
审核和检查	a)应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据份等情况	常规的安全检查不同于日常的安全巡检，常规的安全检查一般是每周或每月开展，汇总一段时间内的系统状态	1)访谈信息/网络安全主管是否定期进行了常规安全核查 2)核查常规安全核查记录是否包括了系统日常运行|系统漏洞和数据备份等情况	1)定期(如每周或每月)进行安全检查,检查内容涵盖系统日常运行状态、数据备份、漏洞检查等内容 2)具有相关的检查记录	符合情况：XXX公司每月/季度进行一次常规安全检查，具有常规安全检查记录表单，记录明确了检查日期，检查内容包括系统日常运行、系统漏洞和数据备份等情况，且出具有巡检报告。 部分符合情况：XXX公司每月/季度进行一次常规安全检查，具有常规安全检查记录表单，但检查内容不够详细，未包含系统漏洞和数据备份情况等内容。 不符合情况：XXX公司未定期进行常规安全检查。
	b)应定期进行全面安全检套，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等	全面的安全检查可自行组织或通过第三方机构进行，无论哪种方式，检查内容均应涵盖技术和管理各方面安全措施的落实情况，如果是单位内部进行的全面安全检查相当于对等级保护对象安全的自评估。定期可以是半年一次也可以是一年一次	1)访谈信息/网络安全主管，是否定期进行了全面安全核查，核查内容都有哪些 2)核查全面安全核查记录类文档，是否包括了现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等	1)定期开展全面安全检查，检查内容覆盖技术有效性和管理措施落地执行情况等 2）具有全面安全检查记录	符合情况：XXX公司每年进行一次全面的安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等，且具备检查记录。 部分符合情况：暂无 不符合情况：XXX公司未定期进行全面安全检查。
	c)应制定安全检查表格实施安全，汇总安全检查数据,并对安全检查结果进行通报	无论是日常检查还是定期全面的安全检查都需要制定安全检查格,记录全面检查结果，并形成安全检查报告，同时也要求将安全检查结果通知给相关人员，尤其是运营层的各岗位管理员	1)访谈安全管理员，询问是否制定安全核查表格实施安全检查,是否对检查结果进行通报 2)核查安全检查表格，安全检查记录，安全检查报告等文档，是否具有安全检查表格、安全检查记录、安全检查报告，安全检查结果通报记录 3)核查安全检查报告，查看报告日期与检查周期是否一致，报告中是否具有检查内容、检查时间、检查人员，检查数据汇总表、检查结果等的描述	1）具有安全检查表格，安全检查记录，安全检查报告等文档 2）安全检查报告日期与检查周期一致，报告中具有检查内容、检查时间、检查人员，检查数据汇总表、检查结果等的描述	符合情况：XXX公司具备安全检查表格、安全检查记录、安全检查报告、安全检查结果通报记录等；安全检查表记录包含常规检查、全面检查的相关数据，每年形成安全检查报告，通过邮件、会议等方式对安全检查结果进行通报。 部分符合情况：XXX公司具备安全检查表格、安全检查记录、安全检查结果通报记录等；安全检查表记录包含常规检查、全面检查的相关数据，通过邮件、会议等方式对安全检查结果进行通报，但未编写最终安全检查报告。 不符合情况：XXX公司未制定安全检查表格实施安全检查。