内审检查表

编号：HZKJ/IS-JL-23

受审核部门	管理层	**负责人**	李强	
审核员	刘东	**审核日期**	2023.8.14	
ISO/IEC27001 条款及要求	**审核内容及方法**	**审核记录**		**判定**
	1.组织体系覆盖范围和过程是否有缺失？	无缺失、覆盖全面		符合
	2.组织对标准条款是否剪裁？如有，所剪裁条款中过程确凿没有？	在运用信息安全标准时，有不适用条款，已在《适用性声明》中做出不适用说明。		符合
4.1 理解组织及其环境	1、询问高管层，公司确定的对经营和战略方向有影响的内、外部因素主要有哪些？对这些内、外部因素的相关信息如何进行监视和评审的？ 有无制定相关的公司经营环境有关文件？行业地方的新的法规要求？ 组织的内部外部环境状况？有哪些需要应对和管理的风险和机遇？相关的会议纪要？	在策划和建立信息安全管理体系时考虑了以下内容：影响的外部因素有：目前造成影响的外部因素有：行业环境：供应商、竞争对手、替代品；外部环境：外部有：法律法规、经济、社会人口、技术等；内部有：价值、文件、资源因素和能力因素。 有形成《组织内部环境识别评审记录》列出了有影响的内外部因素，并制定了方案和措施。 在管理评审会议总结会上有进行了讨论，对措施的有效性进行评价和分析。 已基本识别理解所处环境，能运用到管理体系中。		符合
4.2 理解相关方的需求和期望	与组织信息安全管理体系有关的相关方有哪些？相关方有哪些要求？对相关方及其要求的监视和评审如何？法律法规要求的识别？	查《相关方需求和期望清单》公司的相关方包括：政府、顾客、供方、居民、员工等。 识别了相关信息安全相关的法律法规，并确定了符合法律法规要求。 建立相关方期望和需求识别记录，定期进行监视和评审，并及时更新。		符合
4.3 确定信息安全管理体系的范围	1、公司是否有明确的信息安全管理体系的边界和范围？并且该范围和边界应是已考虑公司内外部因素、相关方要求和公司产品服务； 2、公司的信息安全管理体系范围是否形成文件，并得到保持？ 3、组织有无界定管理体系的范围的文件？ 4、确定的地理边界和管理边界有哪些，表述是否准确？ 5、有无满足标准要求建立、实施、保持和持续改进管理系统的文件？	公司基于内、外部环境影响和相关方要求，结合公司产品和服务，在管理手册中确定了管理体系的边界和范围，覆盖以下场所四川省成都市办公区场所，确定边界和范围时考虑了内外部因素和相关方的要求及确定的合规性义务。 公司确定体系范围符合标准要求。 本公司根据在本部门运行的实际情况，组织相关部门编制了管理手册和程序文件，以支持管理体系在本公司的运行。		符合

4.信息安全管理体系	公司是否确定信息安全理体系的整个过程，包括：是否确定这些过程所需的输入和期望的输出？是否确定这些过程的顺序和相互作用？是否确定和应用所需的准则和方法（包括监视、测量和相关绩效指标），以确保这些过程有效的运行和控制？是否确定这些过程所需的资源并确保其可用性？是否分派这些过程的职责和权限？是否按照 6.1 的要求所确定的风险和机遇？是否对前述过程进行评价，是否按实实施变更，以确保实现这些过程的预期结果？是否有改进过程？	查有按照标准要求和企业实际，策划了信息安全体系所需的过程，有制定业务流程图，其中包括：软件开发系统集成过程等。 公司信息安全管理体系包括实现过程、支持过程、绩效评价、和改进过程，采用过程方法加以运作和控制。 支持过程：主要有人力资源、外部供方、工作环境、内外部沟通、文件控制等。	符合
5.1 领导和承诺 A.5.1	1、最高管理者是否能证实对管理体系的领导作用和承诺？包括: -确保体系的方针、目标；并与组织环境和战略方向相一致； -体系要求融入组织业务过程； -促进使用过程方法和基于风险的思维； -确保体系所需资源的可用性； 沟通管理体系的重要性和有效性； -确保体系实现预期效果； -促进、指导和支持人员为体系的有效性做出贡献； -推动改进； 2.公司管理方针、目标是否形成文件，由最高管理者批准颁发？	1、公司主要是通过标语、会议、文件学习、培训、等方式，向全体人员传达将环境信息安全方针管理体系要求融入业务过程、符合信息安全方针体系要求重要性、遵守法规、满足顾客要求和法律法规的重要性等。 2、管理层批准了信息安全方针与目标；提供的资源、环境能满足公司信息安全方针管理体系运行要求；本年度已按公司计划有效组织实施了管理评审。已提供管理承诺的相关证据。 3、包含的信息安全管理目标和管理方针的《管理手册》由总经理批准于 2022 年 2 月 25 日发布	符合
5.2 方针 A.5.1、A.5.4/A.5.7	1、最高管理者是否制定管理方针？是否形成文件？ a）适应组织的宗旨和环境并支持其战略方向； b）为制定信息安全管理目标提供框架； c）包括满足适用要求的承诺； d）包括持续改进管理管理体系承诺。 是否规定保护环境、履行合规义务、持续改进？ 是否满足要求和持续改进信息安全体系有效性承诺？ 是否有对组织员工、职能人员及利益相关方进行管理方针的沟通，确保管理方针被清晰地理解并贯穿于整个组织。	查：公司制订了文件化的信息安全管理方针：数据保密、信息完整、控制风险、持续改进、遵守法规方针适应组织的宗旨和环境并支持其战略方向；为制定信息安全方针目标提供框架；包括满足适用要求的承诺；包括持续改进信息安全方针管理体系的承诺。 通过标语、会议、文件学习、培训等方式加以沟通和理解。满足标准要求。	符合

5.3 组织的角色、责任和权限 A.5.2/A.5.3/A.5.4	公司内各职位职责是否明确？权限分派、沟通和理解是否适宜？各职责间关系是否明确？ 查看部门职责与权限，各部门职责是否有重叠或真空？权限是否明确？理解是否清晰？是否分派职责和权限，以包括确保体系符合标准要求？确保各过程获得预期效果？在组织推动以顾客为关注焦点？在策划和实施管理体系变更时保持完整性？有管理人员是否承诺对体系持续改进，并能在控制的领域内承担责任？	查公司信息安全管理手册：公司有划分组织架构图，包括：综合管理部、市场销售部、财务部、研发部，明确了各部门的职责、权限，通过文件加以规定和沟通。 公司任命管理者代表。经询问，管代能了解其职责和权限并履行，如按策划组织开展了内审和管理评审活动等。 查：岗位职责管理规范文件，有明确总经理、各部门主管和技术人员、销售员等岗位职责、权限，符合职能分配表，规定合理，完整。询问 3 名综合、客服人员了解其职责和权限。管理层有组织开展了公司内审、管理评审活动和外部联络工作。	符合
6.1.1 总则	公司是否有明确可能所需要应对的风险和机遇？为确定需要应对的风险和机遇： 1、公司在策划信息安全管理体系时，是否考虑内部和外部因素？ 2、公司在策划信息安全管理体系时，是否有理解相关方需求？ 策划环境管理体系时，是否考虑到 4.1 和 4.2 中所提及的问题？ 有无指出管理体系的范围？是否确定需要应对的风险和机遇？ 以及潜在的紧急情况？有无相应的需要应对风险和机遇的文件化信息？	查有制定“SWOT 分析报告及内外部分析”，“法律法规清单”及风险识别评价，考虑了企业所处的内外部环境，有影响的风险或机遇，制定有控制措施等。其中措施包括：法律法规变动时，及时组织相关人员进行合规性评价；与相关方保持信息沟通，对相关方的信息安管理体系方面的需求进行评估，并制定相应的应对措施等措施。 有通过检查和目标考核等方式进行措施有效性的评价，效果有效，减少了风险。	符合
6.2 信息安全目标及其实现规划	:1、公司信息安全管理目标是否与管理方针保持一致？ 2、信息安全管理目标是否可测量？ 3、信息安全管理目标是否适用于公司？ 4、信息安全管理目标是否与产品和服务合格以及增强顾客满意相关？ 5、是否对信息安全管理目标进行监视？ 6、是否将信息安全管理目标与各相关方进行沟通？ 7、信息安全管理目标是否适时更新？ 8、信息安全管理目标是否形成文件并保存？	查，制定了公司和各职能部门信息安全管理目标，信息安全管理目标包括满足产品要求所需的内容，可测量，与管理方针保持一致。有明确了目标、考核方法、完成时间等。 查目标统计达成情况： 制订的公司信息安全管理目标 ，具体见公司目标达成统计表。 经查以上目标均达成，查看其它月份目标统计均能达成。 公司与相关方进行传达本公司的信息安全管理目标；并定期对目标进行评审已符合公司管理的实际情况 公司制定目标时考虑相关要求，并每年对目标进行考核。	符合

	变更的策划管理？	公司在变更时考虑了变更的目的和潜在后果、体系的完整性、资源可获得、职责和权限的再分配，变更后公司及时对体系文件等进行了修订，及时对部门职责权限进行了调整。 较符合标准要求。	合格
7.1 资源	1、公司是否有对为满足管理体系要求的人力资源、材料、能力、信息、设施等进行评估？ 2、公司是否识别各种现有制约，即为减少不良影响或达成目标需要什么，以及需要什么措施？ 组织为建立、实施、保持和持续改进管理体系所需的资源有哪些？是否配备所需的人员、基础设施？如何确定、提供并维护所需的环境？是否有相应的文件确定组织所需的知识，并在必要的范围内可得到？	现场查看，组织已策划并按文件要求提供信息安全运行过程有关的资源，包括人力资源、设施、软硬件（软件）、信息、专项技术、工作环境和财务资源，公司为实施、保持信息安全管理体系并持续改进其有效性，增强顾客满意，对资源的需求予以识别并及时给予提供。	符合
9.1.1 监视、测量、分析和评价 A.5.1.2/A.5.36	1）组织对服务特性和接收准则是否进行了规定？ 2）对产品的监视和测量是否进行了策划？在服务实现过程的适当阶段进行哪些监视和测量，并形成文件？ 3）何时实施监规测量？何时对结果进行分析评价？是否保留成文的信息 2.目标的完成情况？运行过程中的准则的实际数据？确定为合规义务完成情况？环境绩效的内部信息的沟通方式？监视测量过程中是否使用计量器具，如何管理的？	查在手册中明确通过适当的方法对方针目标、过程运行、体系绩效等进行监视和测量，例如内审、管理评审、目标考核等。 通过内审、目标考核等评价体系绩效和有效性。已保留了相应记录。 查信息安全目标、方针均有评审和测量，风险评估管理等均有监视和控制，有效。	符合

9.3 管理评审 A.5.1	1 公司是否定期召开管理评审？并在管理评审中确定质量体系的运行是否适宜、充分和有效，并与组织的战略方向一致？ 2 管理评审输入资料是否满足要求？是否包括以为管理评审采取措施的情况？资源的充分性？来自相关方的有关信息交流？应对风险和机遇采取的措施是否有效？有无改进的机会？管理评审输出资料是否满足要求？并保留形成文件的信息？体系改进有关的信息？目标为实现时需要采取的措施？改进管理体系与其他业务过程融合的机遇？任何与组织战略方向相关的结论？..... 3 管理评审输出资料是否满足标准的要求？并保留形成文件的信息？有哪些改进的机遇？	经查有在《管理评审控制程序》明确了管理评审会议召开的频次为一年一次，以及管理评审输入输出的要求，每次管理评审不超过 12 个月等。 经查编制了《管理评审计划》明确了管理评审会议召开的时间，参加的人员，以及会议的议题。 会议由总经理主持，各部门主管参加计划于 2022 年 6 月召开管理评审 管理评审输出： 有以会议记录形式形成了管理评审报告，结论是：公司的信息安全管理体系是适宜的、充分的、且在持续有效地运行。方针符合，目标指标能实现，方针目标保持不变。资源需求方面目前没有。 管理评审决议：未实施。	符合
10.2 持续改进 A.5.35	公司是否对管理体系的有效性、适宜性和有效性对管理体系进行适当调整？	已基本建立了信息安全管理体系，管理层和相关职能部门通过定期环境巡查、培训、宣传、检讨等方式，对信息安全管理体系加以持续改进意愿。管理评审已提出了将内部审核常态化等持续改进需求。	符合
威胁情报:A.5.7	应收集、分析与信息安全威胁有关的信息，形成威胁情报。	指定相关管理要求，并定期对与信息安全威胁有关的信息进行分析整理，指定相关控制措施。	符合

内审检查表

编号：HZKJ/IS-JL-23

受审核部门	财务部	**负责人**	牟茂群	
审核员	刘东	**审核日期**	2023.8.14	
ISO/IEC27001 条款及要求	**审核内容及方法**	**审核记录**		**判定**
5.3 组织的角色、责任和权限 A.5.2/A.5.3/A.5.4	财务部的岗位职责权限情况	1.与部门负责人交流，对岗位要求明确。 2.关键岗位人员对职责权限较为清楚，适宜		符合
6.2 信息安全目标及其实现规划	1.财务部的目标是否得到分解并进行考核？ 员工是否清楚相应的目标？财务部是否按时对管理目标进行考核？ 2. 根据公司运行中环境状况是否建立相应的管理方案。	1.现场的目标根据体系运行实际情况得到了控制，由综合管理部对公司及各部门的管理目标进行考核。 2.询问员工管理目标能正确回答本部门管理目标；		符合
信息安全风险评估：8.2/6.1.2 信息安全风险处置：6.1.3/8.3 A.5.9	信息安全风险是如何进行识别和评价？是否有最近更新？部门的信安安全管理是否满足要求？信息安全风险处置管理？	公司建立《信息安全险评估管理程序》，通过程序文件明确了风险评估准则，资产赋值的过程是对资产在保密性、完整性、可用性和法律法规合同上的达成程度进行分析，并在此基础上得出综合结果的过程，部门按照公司编制的文件对配合综合管理部对涉及的信息安全风险进行识别评价， 部门现有信息安全风险较小，能满足要求。 公司信息安全体系运行以来未发生，信息安全管理体系运行良好，编制相关风险处置计划，我部门按照公司相关要求执行。		符合
PC机管理： A.5.17/A.5.32/A.7.7/A.8.1/A.8.7/A.8.9/A.8.13/A.8.18/A.8.19	是否按照文件要求设置登陆口令，有无设置屏保，电脑桌面清洁情况是否符合要求，有无安装杀毒软件并定期杀毒，财务数据的保管情况，电脑软件的安装是否符合文件规定？	公司制定了《计算机管理制度》、《计算机病毒防治管理制度》、《系统访问与使用安全管理制度》，严格按照程序的要求执行PC机的管理。 抽查的电脑设置情况，查登录操作系统时的口令设置：8位，由字母、数据组成、安装有Foxmail、VMware、QQ、设置屏幕保护功能，3分钟启动，用密码恢复、安装有360毒霸软件，设置有每周定期杀毒、业务数据及文件及时保存在电脑，本部门员工电脑使用管理满足要求。		符合
网银U盾的管理：A.8.24； 保险柜的管理： A.8.24/A.5.31；	是否制定和实施密钥的使用、保护的规定？	组织通过《财务软件管理制度》来管理相关要求。财务主管单独保管U盾，锁于文件柜内的中。		符合

内审检查表

编号：HZKJ/IS-JL-23

受审核部门	综合管理部	负责人	刘东	
审核员	李飞	审核日期	2023.08.14	
ISO/IEC27001条款及要求	审核内容及方法	审核记录		判定
5.3 组织的角色、责任和权限 A.5.2/A.5.3/A.5.4	综合管理部的岗位职责权限情况	1.与部门负责人交流，对岗位要求明确。 2.关键岗位人员对职责权限较为清楚，适宜		符合
6.2 信息安全目标及其实现规划	1.综合管理部的目标是否得到分解并进行考核？ 员工是否清楚相应的目标？综合管理部是否按时对信息安全管理目标进行考核？ 2. 根据公司运行中环境状况是否建立相应的管理方案。	1.现场的目标根据体系运行实际情况得到了控制，由本部门对公司及各部门的信息安全管理目标进行考核。 2.询问员工信息安全管理目标能正确回答本部门信息安全管理目标； 3.编制有方针、目标、指标和管理方案控制程序，其中有相关控制要求； 4、综合管理部根据体系运行的实际情况编定期对各个相关部门的完成情况进行检查		符合
移动介质管理： A.7.10	移动介质的授权使用？使用过程中的情况及介质的报废处置情况？	公司建立《移动介质使用管理制度》，得到妥善的管理和物理上的保护，使它们免遭破坏、偷盗和未经授权的访问，目前公司移动介质管理情况良好，未出现相关违规使用情况		符合
7.2 能力 A.6.1/A.6.2/A.6.6/A.5.33/A.5.34	1）是否对从事影响服务活动的部门、层次、岗位人员进行了识别，对各类人员所需的教育、培训、技能和经验提出了要求？ 2）针对需求是否提出了培训计划（包括特殊工种、工作人员）或采取其他措施并组织实施？ 3）通过何种方式宣传/培训确保员工意识到所从事活动的相关性和重要性，并为实现服务目标做出 贡献？ 4）是否适当地保存了教育、培训、技能、经验的记录？ 5）查培训需求是否合理？是否按计划实施？通过查相关记录验证计划完成情况，抽查相关培训和评价记录。	有编制人力资源控制程序明确了人员招聘、培训、考核、处置等要求。 编制了岗位职责对市场销售人员、技术人员、客服人员等能力要求进行了规定。经查有从教育、培训、技能、经验等方面进行了规定,规定合理。对产生重大环境/安全影响的人员进行了包括应急方面和有关法律法规方面的培训。 查提供的2023年培训计划，有对培训内容/时间等进行了策划。 ---查2023实施的管理体系文件培训记录，培训结果达到预期培训效果。		符合

7.3 意识 A.5.11/A.5.18/A.6.3/A.6.4	1、公司员工及各相关方是否知晓公司服务方针、服务目标 2、公司员工及各相关方是否明确服务的知识和理解。以及当产品和服务不满足规范时，该如何去做。 3、公司是否质量体系有相关沟通过程。	询问综合管理部、研发部、综合管理部各 2 名员工，询问服务方针和目标，能了解。能明白他们对管理体系有效性的贡献，包括改进服务绩效的益处；符合信息安全和信息技术服务管理体系要求的后果。	符合
7.4 沟通	Q：1）组织是否确定与信息安全管理体系相关的内部和外部沟通包括哪些方面？是否包括：沟通的职责、沟通对象、沟通内容、沟通时机、沟通方式？	经查阅管理手册，明确了内、外部信息交流和沟通的职责、沟通对象、沟通内容、沟通时机、沟通方式。 抽查：内外部协商与沟通计划表、信息交流记录 已通过书面沟通等方式与综合管理部等部门进行沟通。称目前沟通顺畅。 查外部沟通：已通过电话、邮件等与客户、供方和政府部门就环境、安全管理体系和安全方面进行有效沟通。	符合
7.5 文件信息 A.5.13/A.5.33/5.37	组织信息安全管理体系包括哪些文件？ 是否满足标准的要求和确保信息安全管理体系有效性的需要？ 在创建和更新文件时，是否确保了适当的：a）标识和说明；b）格式和媒介；c）评审和批准，以确保适宜性和充分性。 如何控制文件和记录？ 是否在需要时和需要的地方可获得相关文件？ 是否采取了措施防止泄密、不当使用和不完整？ 识别的外来文件有哪些？如何对外来文件进行控制？ 是否对记录实施了保护，防止非预期的更改？	有建立了《受控文件清单》等其中包括内部审核控制程序等,由综合管理部收集,识别将有关信息传达给相关部门和人员,外来文件归档保存妥当。 见文件有专用的文件夹存放于文件柜内，标识清晰，易于查询 查：有在手册和《文件化信息控制程序》文件，规定由综合管理部归口管理，明确了记录的编制、审批、填写、标识、贮存、保护、检索、保存和处置等要求。明确了记录的标识、归档、保存、处置等要求。 有建立了《记录清单》,其中明确了表单名称,保管部门,等。 现场查看：记录填写清楚，方便识别和检索，保存妥当。有专门的文件夹和文件柜进行记录的归档和存放,能防潮防雨	符合
9.2 内部审核	1 公司是否定期进行内部审核？内部审核的频次和结果是否满足企业体系运行要求？ 2 内部审核是否得到了有效的实施和保持？ 1）是否根据过程情况确定内审频次？ 2）是否选定适合的内审员进行内审？ 3）是否确定每次内审的准则和范围？ 4）内审结果是否上报相关管理者？ 5）内部审核中发生的问题是否采取纠正？ 6）内部审核相关文件是否有保留？	查制定有《内部审核控制程序》明确了信息安全管理体系内审要求及频次和方法。 查提供的内审方案计划，包含了审核方法/目的、范围、依据、时间、职责，参加的人员和分工等。 经查内审员有经过标准培训，在分工上具有独立性。 有编制了《内审检查表》，明确了检查的部门和条款，使用的方法，记录了审核的发现，经查检查的部门和条款完整，记录的发现具体，抽样合理，有代表性。	符合

信息安全风险评估：8.2/6.1.2 信息安全风险处置：6.1.3/8.3 A.8.1.1/A.8.1.2	信息安全风险是如何进行识别和评价？是否有最近更新？部门的信安安全管理是否满足要求？信息安全风险处置管理？SOA 的删减情况、版本和发布？	公司建立《信息安全险评估管理程序》《业务影响分析等，通过程序文件明确了风险评估准则，资产赋值的过程是对资产在保密性、完整性、可用性和法律法规合同上的达成程度进行分析，并在此基础上得出综合结果的过程，综合管理部对涉及的信息安全风险进行识别评价， 部门现有信息安全风险较小，能满足要求。 综合管理部负责识别公司体系运行中的信息安全风险，并及时进行管控。 公司信息安全体系运行以来未发生，信息安全管理体系运行良好，编制相关风险处置计划，我部门按照公司相关要求执行。 适用性声明： 密级一般，2023 年 1 月 10 日发布实施 A/0，共有 1 条不适用条款，见《适用性声明》。	符合
法律法规的识别：A.5.3	与组织有关的法律发规有哪些？有无形成文件的信息？其他要求的适用性如何？版本是否及时更新？判断是否准确？现场验证其适用性。 是否进行了法律法规收集，并识别出适用的法律法规。法律法规有否定时更新	查看部门的法律法规合规性评价表，有对法规符合性进行评价。 办综合管理部每年对法律法规符合性进行重新评价，在法律法规更新变更时及公司运行变更时进行更新。 查见综合管理部收集使用的环境安全相关法律法规，并形成法律法规及其它要求清单，版本有效。	符合
办公区域的物理安全： A.7.1/A.7.2/A.7.3/A.7.4/A.7.5/A.7.6 特殊区域的安全：A.7.3/A.7.6	对于公司的综合管理部等是否有设立访问屏障？（围墙）公司是否对区域进行划分，对含有敏感信息的安全区域入口进行控制，确保只有授权允许的人方可访问？是否有措施保护综合管理部的非授权进入？对外部的自然灾害的威胁是否有应对保护措施？对于在安全区域内工作有没有特定要求？如何对公共访问区域（接待区域）进行管理？部门的信息处理设备是否受到合理的保护？	本公司安全区域分为接待区域、普通安全区域和特别安全区域。特别安全区域包括机房、综合管理部、研发部；普通安全区域包括各隔断办公区；前台为接待区域。 外来人员进入公司区域要进行登记。 临时访问的第三方应在接待部门同意后，经前台登记可以进入。 进入特别安全区域须被授权，进出有记录。员工加班也需登记。 设备安装在距墙、门窗有一定距离的地方。并具有防范火灾、水灾、雷击等自然、人为灾害的安全控制措施。	符合
移动介质管理：A.7.10	移动介质的授权使用？使用过程中的情况及介质的报废处置情况？	公司建立《移动介质使用管理制度》，得到妥善的管理和物理上的保护，使它们免遭破坏、偷盗和未经授权的访问，目前公司移动介质管理情况良好，未出现相关违规使用情况	符合

信息安全风险评估：8.2/6.1.2 信息安全风险处置：6.1.3/8.3 A.5.9	信息安全风险是如何进行识别和评价？是否有最近更新？部门的信安安全管理是否满足要求？信息安全风险处置管理？SOA 的删减情况、版本和发布？	公司建立《信息安全险评估管理程序》等，通过程序文件明确了风险评估准则，资产赋值的过程是对资产在保密性、完整性、可用性和法律法规合同上的达成程度进行分析，并在此基础上得出综合结果的过程，综合管理部对本部门涉及的信息安全风险进行识别评价， 部门现有信息安全风险较小，能满足要求。 公司信息安全体系运行以来未发生，信息安全管理体系运行良好，编制相关风险处置计划，我部门按照公司相关要求执行。	符合
PC机管理：A.5.17/A.5.32/A.7.7/A.8.1/A.8.7/A.8.9/A.8.13/A.8.18/A.8.19	是否按照文件要求设置登陆口令，有无设置屏保，电脑桌面清洁情况是否符合要求，有无安装杀毒软件并定期杀毒，财务数据的保管情况，电脑软件的安装是否符合文件规定？	公司制定了《计算机管理制度》、《计算机病毒防治管理制度》、《系统访问与使用安全管理制度》，严格按照程序的要求执行PC机的管理。 抽查的电脑设置情况，查登录操作系统时的口令设置：8位，由字母、数据组成、安装有Foxmail、VMware、QQ、设置屏幕保护功能，3分钟启动，用密码恢复、安装有360毒霸软件，设置有每周定期杀毒、业务数据及文件及时保存在电脑，本部门员工电脑使用管理满足要求。 抽查市场部刘东的电脑发现，未对杀毒软件的病毒库进行更新，电脑存在信息安全风险。	不符合
IT 设备管理：A.5.10/A.7.9/A.7.10/A.7.11/A.7.13/A.7.14/A.7.8/A.8.1/A.8.32	是否有设备台账，并对设备进行标识 打印后请及时拿走；设备出现故障后的处理方式；办公电脑对软件安装的限制、保密要求、杀毒软件的安装和使用、数据备份要求；扫描仪的适用要求；组织场所外的 IT 设备使用要求等等，是否形成三级规程文件。 是否建立设备变更管理控制文件？公司本部和为外部客户提供的与软硬件系统相关的变更过程是否按变更文件规定执行？	公司建立 IT 设备台账，标识清晰符合要求；设备出现故障后的处理方式正确；办公电脑对软件安装的限制、保密要求、杀毒软件的安装和使用、数据备份要求形成三级规程文件； 建立设备变更管理控制文件。 严格执行变更文件。	符合
供应商管理：A.5.19/A.5.20/A.5.21/A.5.22	是否每个供应商都签订了对应的合同； 查看合同内容是符合要求； 是否对每个供方做了评价，并记录在《供应商评价表》； 合同是否发生过变更，并留有变更管理记录； SLA、OLA、UC 之间，多层 UC 之间的逻辑控制关系是否合理有效；供应商管理是否进行了服务改进管理。	公司能够按照供应商管理要求，对外部供方进行供应商评价、选择、绩效监视、组织年度确认，以采购合同、电话/微信/QQ 通知等明确采购产品规格、型号、数量、质量、价格、交付等 要求，验证采购产品质量。除进行供应商评价、选择、绩效监视、组织 年度确认，以合同、协议等明确各项要求外，在外包服务提供前需查看车辆证件、人员操作证等，另还通过发 放告知书、作业过程中随时监督检查等方式实施控制。抽查结果表明，采购过程及质量控制均符合要求。 合同目前未发生变更 各逻辑关系有效，无矛盾 目前变更进计划	符合