管理体系审核记录表

|  |  |  |  |
| --- | --- | --- | --- |
| 过程与活动、  抽样计划 | 涉及  条款 | 受审核部门：管理层 主管领导：张志 陪同人员：李红 | 判定 |
| 审核员：吉洁 审核时间：2022年12月22日 |
| 审核条款：4.1/4.2/4.3/4.4/5.1/5.2/5.3/6.1/6.2/6.3/7.1/9.1.1/9.3/10.1/10.3 |
| 资质查验、范围再确认、证书使用情况、相关方投诉情况、上级检查情况、上次不符合的验证 |  | 企业基本情况  1、总经理：张志，管代：刘丛  2、按照认证范围公司提供的法律证明文件有：  1）《营业执照》 统一社会信用代码：91130104794191469Q； 有效期：2006年10月23日至2026年10月22日  2）《网络安全等级测评与检测评估机构服务认证证书》；编号：SC202127130010054 ； 有效期至2024年11月17日；  3、公司情况介绍：河北恒讯达信息科技有限公司成立于2006年，注册资本为1600万元人民币，占地400平米，是公安部授权的专业信息安全等级保护测评机构，是从事网络安全风险评估、信息安全等级保护测评、安全咨询的专业机构，用户主要覆盖政府机关、电信、金融等多类行业。  4、认证范围：信息安全技术服务（包含网络安全等级保护测评、信息安全风险评估）  5、公司设有管理层、办公室、测评部、市场部等部门，设立了管理者代表。  6、企业目前经营状况：网上查询，显示正常，无被投诉情况，无质量事故，  7、政府主管部门监管情况：无  8、相关方投诉：无  9、上次不符合验证：上次不符合为办公室7.1.6条款，经验证已改，未发现类似问题，措施有效。  10、证书使用情况：证书主要用于投标及客户要求，未发现违规使用情况。 | Y |
| 组织及其环境 | 4.1 | ●管理层识别并确定了与战略、目标相关、影响实现管理体系预期结果的内、外部因素，并且实时关注、评审不断变化的内外部信息。  ●查企业编制了《公司内、外部环境因素识别、评价表》JL/4.1-01，进行了公司内外部环境因素分析，识别人：刘丛；评价人：张志 ； 日期：2022.03.15  --外部因素7项，主要有经营环境、政府行政监管、技术环境、行业壁垒、竞争对手、供应商、重大公共传染疾病；  --抽政府行政监管分析：市场监督局对日常服务质量的监管和随机抽查；国安部对所涉及软件评测的现场安全措施、应急措施以及相关人员具备的特殊工种证件进行监管和查处  监视和控制措施：遵守政府相关部门所推行的各项政策和监督要求，更好的能从另一个方面提升自我监督意识和自我质量、环境、安全控制要求；更好的配合部门进行抽查，也能提高政府信誉度，营造良好的社会效益；提升社会价值；  --抽竞争对手分析：质量的竞争，服务及时性和态度；  监视和控制措施：1、加强软件评测产品质量的过程控制；  2、提高软件评测产品人员技术质量的能力和责任心  3、展现公司的技术优势  --内部因素7项，主要有战略环境、责任环境、协调环境、人才环境、内控环境、激励环境、重大公共传染疾病  --抽人才环境分析：  目前状况: 1、学历专业结构较为合理，个人素质总体良好  2、年轻化，平均年龄为30岁左右  3、员工素质培训尚未系列化  4、中高层干部稳定性较高，服务期限较长  5、高素质市场营销人才不足  监视和控制措施: 1、引进必需人才，提高工程施工人员整体素质  2、针对人员状况和岗位需求制定培养计划和实施  3、增加人才发展资源投入，加强对员工新知识、新标准的培训  4、了解、满足人员需求期望，做好员工调查分析  另：政策风险、资源风险、业务风险、财务风险、质量服务安全风险、管理风险，并制定了相应措施，符合要求。  ●内外部环境识别充分，风险、机遇识别充分，措施有效。 | Y |
| 相关方的需求和期望 | 4.2 | ●查企业编制了《相关方需求和期望清单》，识别并确定了影响公司提供产品和服务能力的利益相关方：顾客、员工、供应商、投资者、政府机构等，识别人：刘丛，时间：2022年03月10日  ●管代介绍公司通过投标、合同约定、不同形式沟通（如：电话、当面拜访等）形式了解相关方的需求，然后提供出满足他们要求提供优质产品和完善的服务，目前公司能满足相关方的需求和期望。  ●相关方进行监视和评审的方式方法：公司通过走访、会议、客户要求等方式对相关方的信息进行监视和评审。抽相关方需求分析：  --员工需求和期望：工作满意。包括得到承认、工作满意和个人发展等  --客户需求和期望：等级保护测评质量，包括符合性、可靠性、价格、安全性等。测评报告的质量。售后服务的及时响应。  --供应商需求和期望：继续经营的机会，包括制定共同的战略，共享知识和利润，共同承担损失，合作共赢等  另抽其他相关方需求，均保存完好，符合要求。  目前企业未发生处罚、相关方投诉事件 | Y |
| 质量管理体系范围 | 4.3 | ●查企业编制了《质量手册》文件编号：HXD／SC-2018；版本A/1,发布时间2018年5月10日，实施时间2018年5月15日。管理体系文件包括《质量手册》HXD／SC-2018、《程序文件》HXD-CX-2018、作业文件和记录表格等内容，质量手册中包含管理方针和管理目标。质量手册中明确了体系的范围，管理手册可获得并得到保持，有发放记录，有签收人签名。  ●公司明确了质量管理体系的边界：  注册地址：河北省石家庄市桥西区裕华西路128号乐活大厦B座20层2009室  经营地址：河北省石家庄市桥西区裕华西路128号乐活大厦B座20层2009室  体系范围：信息安全技术服务（包含网络安全等级保护测评、信息安全风险评估）  无变化。  ●在确定质量管理体系的范围时考虑了公司的内外部因素和相关方的需求和期望，考虑了公司的产品和服务，与公司的宗旨和战略方向一致。符合标准要求。 | Y |
| 质量管理体系及其过程 | 4.4 | 组织对过程及相互关系进行了理顺，确定了组织机构，明确了职责，确定管理体系的边界和适用性，考虑了内外部问题、组织单元、风险控制、职能；明确了活动、产品和服务、包括实施控制与施加影响的顺序和相互作用、权限、所需的准则和方法，改进措施等，据此建立了文件化的管理体系，以确保体系在运行中的完整性。配备了各种资源满足体系运行的需要。确立了监视测量的方法。  经识别，在信息安全技术服务（包含网络安全等级保护测评、信息安全风险评估）中不存在外包过程。 | Y |
| 领导作用和承诺  总则 | 5.1.1 | --查《质量手册》HXD／SC-2018中明确了企业最高管理者对管理体系的领导作用和承诺主要通过以下方面体现：  a) 对质量管理体系的有效性承担责任；  b) 组织制定公司的质量方针和质量目标，并与公司环境和战略方向相一致；  c) 组织制定公司的质量目标，并在相关职能部门进行分解，确保质量管理体系要求融入与公司的业务过程；  d) 在建立、实施、运行质量管理体系的全过程使用过程方法和基于风险的思维；  e) 为质量管理体系的建立、实施、保持和改进提供必要的资源（包括人、财、物、技术），确保获得质量管理体系所需的资源；  f) 不断加强自身的质量意识，采取培训、宣传或会议等方式，向公司内全体员工传达满足顾客和相关法律、法规要求的重要性；  g) 对质量管理体系日常运行检查，确保实现质量管理体系的预期结果；  h) 制定奖励制度，促使、指导和支持员工努力提高质量管理体系的有效性；  i) 主持管理评审，确保质量管理体系的适宜性、充分性和有效性，推动改进；  j) 组织办公室制定公司的各岗位任职资格条件，明确各部门、各岗位的职责和权限；  k)授权了管理者代表，代表总经理主持有关的体系管理工作，详细的职责见管理者代表任命令。  与总经理沟通，清楚自己等于体系的领导作用和承诺。 | Y |
| 以顾客为关注焦点 | 5.1.2 | 与总经理沟通，公司主要通过投标、当面拜访、市场调研、满意度调查等方式了解顾客的需求，确定服务要求。  通过定期对顾客满意度进行测量了解顾客对服务的意见。  在确定顾客的需求和期望时，公司同时考虑与产品有关的义务和法律法规要求，并采取措施，使其得到落实。 | Y |
| 方针 | 5.2 | ●查见《质量手册》HXD／SC-2018中制定了企业的质量方针：  “客观公正 方法科学 结果准确 服务最优”  质量方针经总经理批准实施。  质量方针体现了标准的要求，包括：公司的宗旨和环境并支持其战略方向，为目标制定了框架，满足适用要求的承诺，持续改进质量管理体系的承诺，质量方针通过会议传达、文件下发、公司内部群内、网络宣传等形式进行贯彻，可为相关方获取。  ●质量方针基本适宜。 | Y |
| 组织的角色、职责的权限 | 5.3 | ●企业在策划和建立管理体系时，成立了组织机构：管理层、办公室、市场部、测评部，设立了管理者代表，并对各部门的作用、职责、权限进行了划分。《质量手册》HXD／SC-2018确定了组织机构图、职能分配表，各部门作用、职责、权限界定基本清楚，并与实际情况基本相符。最高管理者负责岗位的设定、职责和权限的指派工作。并通过文件下发、会议、培训等方式将职责、权限传达到组织相关部门及层次。  ●组织的角色、职责和权限基本得到有效沟通和贯彻实施。 | Y |
| 策划  应对风险和机遇的措施 | 6.1 | ●查企业编制了《风险分析及应对措施记录表》对风险和机遇的措施进行了识别和控制  分析人：刘丛 时间：2022.03.10 评审结果：各项措施良好执行 评审人：张志 2022.05.10  ●企业目前识别风险点共计24项，主要有：人员技术能力、环境、安全意识、人员流失、招聘情况、相关方检查施工情况、市场价格竞争（市场推广、投标等）、人员流失对于客户信息的泄露、客户回款率情况、工资待遇的调整、资金状况风险、疫情期间人员流动、办公环境等。  抽--人员技术能力、环境、安全意识。  风险管理措施：制定人员培训计划、上岗考核制度等。定期组织技术比拼、技术标兵等内容评选活动。定期进行环境、安全等方面的教育和培训。  --人员流失对于客户信息的泄露  风险管理措施：登记和统计客户信息，对于离职人员的工作交接和客户回访进行规定和要求。保证客户的不丢失。  --抽工资待遇的调整  风险管理措施：制定岗位考核机制，提高员工待遇，签订劳动合同，上保险，安排各种带薪休假和带薪培训等福利。  抽其他风险和机遇的分析评价及应对措施，风险、机遇识别充分，措施有效。 | Y |
| 质量目标及其实现的策划 | 6.2 | ●查《质量手册》HXD／SC-2018中制定了公司总的质量目标为：  测评数据差错率小于0.5%；  客户投诉处理率100%；  客户满意度大于95%；  委托合同履约率100%；  测评人员持证上岗率100%。  ●查企业编制了《2022年质量目标分解表》，进行了目标分解：   |  |  | | --- | --- | | 办公室 | 文件受控率100% | | 培训计划执行率100% | | 测评人员持证上岗率100% | | 测评部 | 测评数据差错率＜0.5% | | 终测测评报告出具时间符合规定要求率100% | | 市场部 | 顾客满意度≥95%； | | 处理顾客反馈信息率100%。 | | 委托合同履约率100% |   质量目标分解规定了计算方法，和考核周期为每季度考核一次。  经总经理张志批准，批准时间：2022.3.5  ●查编制了《2022年分解质量目标考核记录表》，  抽2022年第3季度目标考核情况：考核人：刘丛2022.09.30  文件受控率100%  培训计划执行率100%  测评人员持证上岗率100%  测评数据差错率 0.1%  终测测评报告出具时间符合规定要求率100%  顾客满意度96%  处理顾客反馈信息率100%。  委托合同履约率100%  经查，符合要求。 | Y |
| 变更的策划 | 6.3 | ●企业通过过程业绩分析，监视、测量、分析、评价、管理评审，内部审核结果等收集可能发生的变更信息，当组织内外环境、客户及利益相关方的需求、企业经营等方面发生重大变化，具体包括产品质量监视和测量过程中持续未达到预期结果、组织机构变化、重大人员调整、持续的经营亏损等情况下，需要对体系进行变更。企业有充分识别识别潜在的变更需求，并确保在必要时做出相应的变更。  ●受审核方明确了变更评估及实施的流程，即当发生变更时，确定变更的目的、考虑变更的潜在后果，质量管理体系的完整性，识别变更的风险和机遇，确定资源的可获得性并制定应对措施，责任和权限的分配或再分配。并要求对变更前、变更中、变更后的全过程实施监控，并组织对变更的有效性进行评价，确保质量管理体系的完整性。  体系运行以来，暂无变更情况发生。 | Y |
| 资源总则 | 7.1 | ●公司为了实施管理体系运行并持续改进其有效性，增强顾客满意度，提供了各方面的资源保证。  人力资源：公司目前员工45人，其中管理、测评、技术服务人员有20余人，可满足产品和服务控制需要。  基础设施：  办公设施：现场巡视，办公场地为租赁乐活时尚广场B座2009室，配备有办公室，会议室，测评室等；  测评设施：电脑、设计软件、打印机等；  3、工作环境：办公区域面积1600平米，布局合理，场所卫生干净整洁，工作环境良好；  4、资金支持：注册资金1600万元。  5、外部资源：如供方、客户等相关方。  ●目前企业所提供的内外部资源基本能满足管理体系运行的需要。 | Y |
| 监视、  分析与评价 | 9.1.1 | 公司通过质量目标考核、内审、管理评审等对体系的有效性进行评价。  1）提供了顾客满意调查表，并进行了分析。  2）通过内审中发现的不符合，确定改进措施并实施。  3）通过管理评审，提出改进措施，以便发现改进方向。 | Y |
| 管理评审 | 9.3 | ●查编制了《管理评审程序》，文件规定每年至少进行一次管理评审。  ●查企业于2022年9月30日组织进行了一次管理评审。  --查《管理评审计划》策划了管理评审目的、参加人员、各部门准备资料、评审会议要求等。  编制：刘丛 日期：2022.09.20 审批：张志 日期：2022.09.20  管理评审输入由管代和各部门收集并提供相关材料，内容基本涵盖：资源充分性、方针目标适宜性、质量目标的完成情况、体系策划和运行情况、可能的变更、外部供方的绩效、内审情况、顾客满意情况及纠正措施完成情况，应对风险和机遇所采取措施的有效性以及改进的建议等等。  ●--查《管理评审报告》，对评审情况进行了总结，查见个部门工作汇报。管理评审结论：本公司质量管理体系总的来说是适宜的、充分的、有效的，质量方针和质量目标是适宜的和有效的。  审批：张志 日期：2022.09.30  ●《管理评审报告》提出了改进方向：  1、稳定现有客户，积极进行客户回访；  2、逐步扩充业务份额，提升投标精准度；  抽管理评审改进措施完成情况：实施中，符合要求。 | Y |
| 改进总则 | 10.1 | ●企业通过建立管理方针、质量目标，改进服务质量、纠正、避免和减少非预期情况带来的不利影响，改进质量管理体系的绩效和有效性以及定期的内审、管理评审，合理化建议等，并通过管理目标建立与考核，明确了改进、努力的方向，建立一个自我完善、持续改进的机制和良好氛围。  ●企业充分识别和评价存在的改进机会，以持续满足顾客和相关方要求改进的方法措施包括：  1）引导创新、修改和改进现有过程或实施新过程的突破项目；  2）在现有过程中开展渐进、持续的改进活动；  3）纠正所存在不符合的原因等。 | Y |
| 改进 | 10.3 | ●企业管理体系按策划的管理手册、程序文件等文件化信息要求实施、运行，并通过内审、管理评审、分析和评价、纠正和纠正措施、管理方针和管理目标等有关信息来源来实现对管理体系的持续改进，同时通过日常运行中发现的问题及时调整解决，以达到持续改进管理体系的目的，以提升产品测评和服务过程质量和管理体系绩效。  ●日常监视和测量过程中发现的不合格、不符合要求相关责任部门及时制定相应的改进、纠正和纠正措施，以实现管理体系的持续改进。 | Y |

管理体系审核记录表

|  |  |  |  |
| --- | --- | --- | --- |
| 过程与活动、  抽样计划 | 涉及  条款 | 受审核部门：办公室 主管领导：刘丛 陪同人员：李红 | 判定 |
| 审核员： 吉洁 审核时间：2022年12月22日 |
| 审核条款：5.3/6.2/8.4/9.2/10.2 |
| 职责和权限 | 5.3 | ●查《质量手册》HXD／SC-2018规定了各部门主要负责人的岗位职责和权限，及各部门通用职责；  办公室主任主要职责如下：贯彻执行公司质量方针和质量目标以及体系文件，制定本部门质量目标，并组织实施予以实现负责制定和实施公司人力资源管理制度；协助用人部门，合理配置质量保证的人力资源；负责人力资源的管理工作和员工意识、技能培训及资格认定工作；负责对新招聘员工的入职前教育；针对公司范围内转岗技能要求，组织开展培训工作，保证转岗后的人员经培训合格后才能上岗；负责按公司要求和质量管理的需要，制定员工的培训计划；掌握本公司人员培训的需求，使每个对质量管理有影响岗位的员工技能满足各岗位的要求。负责组织人员对本公司的采购进行管理；负责安排人员严格做好测评对象接收、登记；负责安排测评报告打印发放以及原始记录、测评报告相关资料的整理归档；  负责申诉、投诉和抱怨的受理工作；及时向有关方面反馈质量信息和统计汇总情况等；  ●经询问，刘主任了解自己的职责及权限 |  |
| 质量  目标 | 6.2 | ●抽《2022年质量目标分解表》，分解到办公室的质量目标及完成情况如下：  1、文件受控率100%  2、培训计划执行率100%  3、测评人员持证上岗率100%  ●查《2022年分解质量目标考核记录表》，质量目标每季度进行一次考核  2022年1-3季度质量目标完成情况：均完成；考核人：刘丛 |  |
| 外部提供过程、产品和服务过程管理 | 8.4 | ●查企业编制了《采购控制程序》HXD-CX-04，确定了对外部供方实施的具体控制要求，  ●提供了《合格供应商名册》HXD-ZJ-05-02，合格的供应商3家，均进行了评审，首次列入日期2021.03.10，批准人张志。  包括：  中关村信息安全测评联盟 提供服务内容：提供等级测评工具技术支持服务  河北卓望电子科技有限公司 提供服务内容：检测网络中的各类脆弱性风险，提供专业、有效的安全分析和修补建议  京东自营店 提供服务内容：办公用品  抽供应商综合能力评价表：  ---供应商：中关村信息安全测评联盟  评价内容：经营资格和信誉、产品质量、产品价格、售后服务  评定结论：继续列为合格供方  批准：张志 2022年5月20日 |  |
| 内审 | 9.2 | ●查公司编制《内部审核程序》，文件规定每年至少进行一次内部审核。  ●提供了《内部质量审核计划》  策划了审核目的、审核依据、审核范围、审核时间、审核要求、审核组成员等内容。  内审时间：2022年9月15-16日。组长： 刘丛 组员： 骆峰  内审计划由总张志批准，批准时间：2022年9月5日  ●公司按计划实施了内审。  提供了内审员任命书，写明了内审员任职要求及审核要求。内审员经过了内审员培训，了解审核要求，能胜任内审工作。  提供有首末会议签到表。提供了内审检查表，审核员未审核自己部门。  ●内审不符合1项，为测评部8.5.5条款，对不符合进行了原因分析，并已整改。验证人：刘丛 日期：2022.09.17  ●编制了内审审报告，显示本公司的质量体系运行是适应、有效的。并发放至各部门。  组长： 刘丛 2022年09月16日 审批： 张志 2022年09月16日 |  |
| 不合格输出的控制 | 10.2 | ●查企业编制了《不符合工作控制程序》，本程序对不符合测评/评估工作的范围和分类、识别、处置做出了规定。不符合测评/评估工作按其影响程度和造成的后果，可分为一般不符合和严重不符合。质量负责人对所发现的严重不符合组织相关人员进行分析、评价，提出处置意见，对不符合工作的可接受性作出决定，明确纠正措施要求。  目前没有发生不符合的情况。 |  |

说明：不符合标注N

管理体系审核记录表

|  |  |  |  |
| --- | --- | --- | --- |
| 过程与活动、  抽样计划 | 涉及  条款 | 受审核部门： 测评部 主管领导：骆峰 陪同人员：李红 | 判定 |
| 审核员：吉洁 审核时间：2022.12.22 |
| 审核条款：  5.3/6.2/7.1.3/7.1.4/7.1.5/8.1/8.3/8.5/8.6/8.7 |
| 组织的岗位、职责权限 | 5.3 | ●测评部主管领导：骆经理  ●查《质量手册》HXD/SC-2018中规定了测评部主任的主要职责：  a全面负责测评部的人员管理，对测评工作进行安排；  b负责组织人员收集、跟踪、购买测评所需标准、最新版本的技术资料；保证测评在用测评标准、规范的现行有效；  c负责制定测评仪器的大修、降级和报废计划，并组织实施；  d负责测评硬件设备、软件测评平台的支持工作；  e负责组织实施能力验证和实验室间比对；  f负责组织相关人员实施期间核查，并保留相关记录；  g负责对公司测评人员进行技术知识培训；  h负责安排人员做好各项记录，对测评部人员进行监督；  i负责组织测评硬件设备定期比对校核；  j负责保证测评硬件设备、软件测评平台处于有效的运行工作状态；  k考核本部门人员的出勤情况、工作情况和工作质量；  l对本部门人员晋升、晋级、技术职称评定提出建议；  ●与负责人沟通，清楚其职责。 |  |
| 质量目标 | 6.2 | ●抽《2022年质量目标分解表》，分解到测评部的质量目标及完成情况如下：  1、测评数据差错率＜0.5%  2、终测测评报告出具时间符合规定要求率100%  ●按要求每季度进行考核，查《2022年分解质量目标考核记录表》，对2022年1-3季度目标进行了考核。  经查显示目标均已完成，考核人：刘丛 |  |
| 设施设备管理 | 7.1.3 | ●办公设施：租赁乐活时尚广场B座2009室，配备办公室，洽谈室，会议室，测评室等；  ●测评设施：电脑、打印机，漏洞测试仪等  ●基本满足测评、销售要求。  ●软件、电脑维护：负责人介绍各测评人员根据具体情况各自定期对软件进行升级维护。 |  |
| 过程运行环境管理 | 7.1.4 | ●租赁乐活时尚广场B座2009，配备办公室，会议室，洽谈室，测评室等，办公区域面积：400平米；测评过程无特殊环境要求。  ●现场巡视，办公现场环境整洁，秩序良好。  2、办公区内有消防器材，工作环境可满足需要。工作环境可满足需要。 |  |
| 监视和测量资源 | 7.1.5 | ●测评部负责对所用监视和测量设备按该程序进行校准、维护和管理。公司保留校准、校验等相关成文信息，作为监视和测量资源适合其用途的证据。  ●测量溯源 ：《测量台账》显示公司目前监视和测量设备为2种；  ①漏洞扫描仪1台（北京神州绿盟信息安全科技股份有限公司）  ②测评作业工具5套（软件中关村信息安全测评联盟机构）。  ⑶由测评软件销售或技术代理商不定期通过网络进行指定升级服务。  ●测评部现场测评需用的监视和测量设备漏洞扫描仪（系统集成）及测评作业工具软件，已编制绿盟RSAS远程安全评估系统作业指导书及网络安全等级保护测评作业工具作业指导书。 |  |
| 运行的策划和控制 | 8.1 | ●此次审核的范围：Q：信息安全技术服务（包含网络安全等级保护测评、信息安全风险评估），全适用\*\*\*  ●与测评部主任沟通，公司成立多年，已有成熟的工艺文件及行业标准、国家标准等，以及反映产 品特性和功能的指标，顾客要求等。有文件规定测评部的岗位职责权限。  ●查为信息安全技术服务质量，配备了适用的过程以及支持过程指令性文件：  GB/T22239—2019《中华人民共和国国家标准信息安全技术网络安全等级保护基本要求》；  GB/T20984—2015《信息安全技术信息系统安全风险评估规范》；  GB/T28448-2019《中华人民共和国国家标准信息安全技术网络安全等级保护测评要求》；  《中华人民共和国计算机信息系统安全保护条例（国务院147号令）》；《信息安全等级保护管理办法（公通字【2007】43号）》；  GB/T22240—2008《信息安全技术信息系统安全等级保护定级指南》；  GB/T25058—2010《信息安全技术信息系统安全等级保护实施指南》等。  ●资源：公司的主要办公服务设施，信息服务设备齐全，检测资源具备，公司总人数：45人，其中管理技术人员20余人，能满足服务的要求。  ●策划了工作流程：  网络安全等级保护测评：信息调研---方案设计、编制---现场测评---对方整改------复评---分析---编制报告。  信息安全风险评估：信息调研---方案设计、编制（渗透方式）---渗透测试---分析评估---编制报告。  ●部门规定了必要的评测和风险评估报告记录，抽查 2021年3月至11月设计、评测和评估记录，记录符合规定要求。  现场查看各类服务过程实现策划符合要求。 |  |
| 设计与开发 | 8.3 | 网络安全等级保护测评、信息安全风险评估设计：  1、负责人介绍，主要设计的是网络安全等级保护测评实施方案及信息安全风险评估方案，包含了测评/评估目的、依据、对象描述、测评内容（单元）、设备及线材清单、安装位置图等内容。  查看了已完成的网络安全等级保护测评项目-“河北省作家协会”项目资料：  2、查看了设计和开发策划，查看了设计和开发策划文档信息表（含保密申明），明确了网络安全等级保护测评编制人员、审阅、批准等。策划阶段明确了测评目的、依据、信息调研、内容、风险规避措施等。  3、查看了设计和开发输入信息调研测评对象描述。对本地出行的物理环境、主机、网络、业务应用系统、安全管理制度和人员等。安全测评通过静态评估、现场测试、综合评估等相关环节和阶段，从物理安全、网络安全、主机安全、应用安全、数据安全与备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等十个方面进行输入。   1. 设计开发评审、验证和确认：对输入充分性进行了内部评审。查见河北省作家协会项目《测评方案评审记录表》，评审日期：2022年9月6日，系统名称及级别（SxAx）：河北作家网（S2A2），评审内容全面，提出了评审意见：略，评审结论：修正以上问题后可定稿。 2. 目前无设计开发变更发生。 |  |
| 生产和服务提供的控制 | 8.5.1 | ⑴策划了信息安全技术服务（包含网络安全等级保护测评、信息安全风险评估）流程：  ①测评：调研---方案编制---现场测评---对方整改------复评---分析---编制报告。  ②评估：调研---方案（渗透方式）---渗透测试---分析评估---编制报告。  策划形成了等级保护测评作业指导书、和相关测评运行程序等。策划充分。  ⑵关键过程和需确认过程的策划和实施：  ㈠需确认的过程是信息调研过程。  查看了已完成的网络安全登记保护测评项目“河北省作家协会网络等级测评”项目资料：  需要前期做好信息调研，“河北作家网安全等级测评”方案出具前进行评审确认。  ①查看了设计和开发策划文档信息表（含保密声明），明确了网络安全等级保护测评编制人员、审阅、批准等。策划阶段明确了测评目的、依据、信息调研、内容、风险规避措施等。  ②查看了设计和开发输入信息调研测评对象描述。对公司应用软件、主机存储设备、网络互联设备、安全设备、安全人员相关人员信息、安全管理文档进行输入。对信息调研充分性进行了内部评审。2022年9月1日评审，方案可行出具了信息调研报告，填表人：孔京京。  ③设计开发评审、验证和确认：于2022年9月6日公司魏永红、骆峰、董凯评审。评审、验证、确认项目设计方案的可行性，设计方案合理。  ㈡关键过程为现场测评过程：  ——控制要求：  1、现场含网络安全等级保护测评、信息安全风险评估应符合以下要求：本次测评采取访谈方式涉及对象  a、为物理安全、网络安全、系统安全、应用安全、数据安全、安全管理等方面内容。其中物理安全、安全管理重点采取访谈方 式。在访谈的广度上，访谈覆盖不同类型的系统运维管理人员，包括系统负责人、机房管理员、系统管理员、网络管理员、开发人员、应用业务人员、文档管理员等。对测评对象采取抽样的形式确定测评数量；在访谈的深度上，访谈包含通用和高级的问题以及一些有难度和探索性的问题。测评人员访谈技术负责人、系统 管理员、业务开发人员等系统技术架构的实现及配置；访谈系统负责人系统的整体运行状况、安全管理的执行成效。  b、本次测评采取检查方式主要涉及对象为物理安全、网络安全、主机系统安全、 应用安全、数据安全及安全管理等方面的内容。除物理安全、安全管理主要采取本地出行网络安全等级保护测评方案文档核查方式外，其它方面主要采取系统配置核查方式。在核查的广度上，数量上采取抽样的形式，基本覆盖系统包含的网络设备、安全设备、主机设备、应用软件、管理制度文档等不同类型对象；在核查的深度上，详细分析、观察和研究除了功能级上的文档、机制和活动外，还包括总体/概要和一些详细设计以及实 现上的相关信息。  ●测试，包括案例验证测试、漏洞扫描测试、渗透性测试。  本次测评采取测试方式主要涉及对象为网络安全、主机系统安全、应用安全、数据安全等方面的内容。其中，案例验证测试主要通过测试工具或案例验证网络安全、应用安全、数据安全的安全功能是否有效。漏洞扫描测试主要分析网络设备、操作系统、数据库等安全漏洞。在核查的广度上，基本覆盖不同类型的机制，在数量、范围上采取抽样方式；在测试的深度上，功能测试涉及机制的功能规范、高级设计和操作规程等文档及深度验证系统的安全机制是否实现，包括冗余机制、备份恢复机制的实现。  ●风险分析方法  项目依据安全事件可能性和安全事件后果对信息系统面临的风险进行分析，  分析过程包括：  1) 判断信息系统安全保护能力缺失（等级测评结果中的部分符合项和不符合项）被威胁利用导致安全事件发生的可能性；  2) 判断由于安全功能的缺失使得信息系统业务信息安全和系统服务面临的风险；  3) 结合信息系统的安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的风险。  ——控制的证据：  ①《河北作家网网络安全等级测评》项目的《测评方案》进行了评审，具有可操作性。  ②抽查其出具的现场测评实施记录，包括：  1.《安全通信网络（二级）现场测评记录表》，主要针对网络架构、通信传输、可信验证等方面；测评日期：2022.9.7，测评师：杨开飞，复核人：孔京京；《安全区域边界（二级）现场测评记录表》主要针对边界保护、访问控制、恶意代码和垃圾邮件防范、安全审计等方面；测评日期：2022.9.8，测评师：杨开飞，复核人：孔京京  2.《云计算——安全物理环境（二级）现场测评记录表》，主要针对基础设施位置、网络架构、访问控制、入侵防范、安全审计、数据完整性和保密性、数据备份恢复等方面；测评日期：2022.9.8-21测评师：杨开飞，复核人：孔京京  3.另《安全计算环境（二级）安全设备现场测评记录表》、《安全计算环境（二级）操作系统现场测评记录表》、《安全计算环境（二级）管理软件现场测评记录表》、《安全计算环境（二级）业务应用现场测评记录表》、《安全计算环境（二级）数据安全现场测评记录表》、《安全管理中心（二级）现场测评记录表》、《安全管理制度（二级）现场测评记录表》等。  记录内容均填写完整，详实，有各项人员的签字和日期；  ⑶需确认过程确认项目涉及方案出具过程和关键过程现场测评过程的资源保障：  ①使用的文件：项目的测评方案、客户提供的主机存储设备、网络互联设备、安全设备、安全人员相关人员信息、安全管理文档。  ②使用设备和工具：到达测评现场的车辆、接线板、数码相机等。  ③使用的监视和测量资源：主要是漏洞扫描仪。  (4)查看完工项目：《河北作家网网络安全等级测评》网络安全等级保护测评、信息安全风险评估过程控制资料：  ①项目概况为物理安全、网络安全、系统安全、应用安全、数据安全、安全管理等方面内容。其中物理安全、安全管理重点采取访谈方式。在访谈的广度上，访谈覆盖不同类型的系统运维管理人员，包括系统负责人、机房管理员、系统管理员、网络管理员、开发人员、应用业务人员、文档管理员等。对测评对象采取抽样的形式确定测评数量；在访谈的深度上，访谈包含通用和高级的问题以及一些有难度和探索性的问题。测评人员访谈技术负责人、系统管理员、业务开发人员等系统技术架构的实现及配置；  ②测评情况：测评项目于2022年9月1日实施，计划2022年9月30日编制完成测评和风险评估报告。  ③查见测评部，2022年9月6日由专人编制、审批的测评实施方案63页内容。  ④查看了测评对象信息调研描述，2022年9月1日对业务应用软件、主机存储设备、安全人员资质、安全文档进行了调研，由测评部人员和甲方共同评审复核。  ⑤查看了项目实施日志及记录  ——抽查2022年9月11日《物理安全核查记录表》，主要针对《物理位置的选择》、《物理访问控制》等方面，填写了人员和实测情况等，信息全面。  ——抽查2022年9月18日《默认核查记录表》主要包括网络设备、安全设备两个大项内容、文档材料的安全管理办法、例外情况等测评实施正常。  注明：因甲方要求项目测评数据保密，审核组现场记录文档隐含了部分测评数据和过程。  ⑷公司的测评流程发生变更时，由测评部提出并进行评审后方可变更；在测评内容或项目进行变更时根据客户提出的变更需求进行变更，变更前由测评部组织评审，可行后方可变更。目前未发生。  ⑸对于测评及评估项目，交付后无其它需要服务的情况；主要是针对客户在后期的活动中有技术咨询的事情进行解答，客户有需求时由测评部实施技术咨询服务，解答客户的疑惑。 |  |
| 标识和可追溯性  产品防护 | 8.5.2  8.5.4 | ⒈现场查看标识和可追溯性分四个方面控制：项目合同、编制的报告、测评人员、测评设备进行控制。  ⑴测评项目采用合同号/项目号作为唯一性标识；  ⑵测评报告上通过报告编号作为唯一性和可追溯性标识；  ⑶测评人员在测评现场通过持证、名片等方式进行标识。  ⑷测评设备采用检定状态标识和设备编号的方式进行唯一性的标识。  2.现场评测和评估的防护控制：  ⑴对于使用的测评设备由专人管理，不用时放置于库房妥善保管，定期检查其检定/校准状态。  ⑵测评报告的防护采用备份的方式专人管理，保密管理，长期保存。  ⑶测评现场的防护：测评人员现场测评时有防护要求时遵循甲方的要求，佩戴相应防护用品，操作各项设备时按规程操作。 |  |
| 顾客财产 | 8.5.3 | 现场查看顾客财产主要有：顾客信息。客户信息由市场部妥善保管并做好保密工作，截至目前未发生泄露。 |  |
| 变更的控制 | 8.5.6 | 公司的测评流程发生变更时，由测评部提出并进行评审后方可变更；在测评内容或项目进行变更时根据客户提出的变更需求进行变更，变更前由测评部组织评审，可行后方可变更。目前未发生。 |  |
| 产品和服务的放行 | 8.6 | ⑴信息安全技术服务（包含网络安全等级保护测评、信息安全风险评估）服务的接收准则以及符合接收准则：GB/T22239—2019《中华人民共和国国家标准信息安全技术网络安全等级保护基本要求》；  GB/T20984—2015《信息安全技术信息系统安全风险评估规范》；  GB/T28448-2019《中华人民共和国国家标准信息安全技术网络安全等级保护测评要求》；  GB/T20984—2007《信息安全技术信息系统安全风险评估规范》  GB/T22240—2008《信息安全技术信息系统安全等级保护定级指南》；  GB/T25058—2010《信息安全技术信息系统安全等级保护实施指南》等，以及相关公安、银行金融系统的行业规范等。  ⑵网络安全等级保护测评：  抽取了2022年9月30日由委托单位：河北省作家协会，《网站安全等级保护河北作家网等级测评报告》  委托单位和测评单位均背书信息。  1671698132776 1671698172431 1671698240391 1671698280529  ⑶信息安全风险评估：抽取了2022年04月13日由委托单位：河北省科学技术厅，《河北省科技特派员综合管理服务平台风险评估报告》 |  |
| 不合格输出的控制 | 8.7 | --查企业编制了《不符合工作控制程序》，本程序对不符合测评/评估工作的范围和分类、识别、处置做出了规定。不符合测评/评估工作按其影响程度和造成的后果，可分为一般不符合和严重不符合。质量负责人对所发现的严重不符合组织相关人员进行分析、评价，提出处置意见，对不符合工作的可接受性作出决定，明确纠正措施要求。  公司明确办公室和测评部负责对编制的测评和风险评估报告不合格和服务情况进行管理，以防止不符合要求的产品和服务的非预期使用和交付。  对已发出的报告如需要作补充或实质性修改，以追加文件或资料调换的形式实施；  现场审核查目前未出现编制的测评和风险评估报告不合格现象。 | Y |

管理体系审核记录表

|  |  |  |  |
| --- | --- | --- | --- |
| 过程与活动、  抽样计划 | 涉及  条款 | 受审核部门：市场部 主管领导：王丽强 陪同人员：李红 | 判定 |
| 审核员：吉洁 审核时间：2022.12.22 |
| 审核条款：5.3/6.2/8.2/9.1.2 |
| 组织的岗位、职责权限 | 5.3 | ●市场部负责人：  ●查《质量手册》规定了市场部职责：  a负责测评业务受理、报告的发放、客户满意度调查、客户申诉与投诉的受理工作；  b受理时，要对测评对象介质（光盘、硬盘等）进行病毒检查和可读性检查，无误后，双方签字接收。如发现病毒或内容无法读取，可拒收；  c负责测评报告的发放；  d负责客户满意度调查，每年做好统计分析工作；  e受理申诉与投诉，并向相关部门反映；处理后及时将结果答复客户；  f遵守职业道德，不得拷贝、使用测评对象。  g完成部室领导交办的其他工作。  ●与市场部负责人沟通，清楚其职责。 | Y |
| 质量目标 | 6.2 | ●查《2022年质量目标分解表》，分解到市场部的质量目标及完成情况如下：  市场部部门质量目标3项：  1、顾客满意度≥95%  2、处理顾客反馈信息率100%  3、委托合同履约率100%  ●按要求每季度进行考核，查《2022年分解质量目标考核记录表》，显示2022年1-3季度目标均已完成，考核人：刘丛  ●从目前的统计结果来看，基本达到目标要求。 | Y |
| 顾客沟通 | 8.2.1 | ●公司通过当面拜访、电话、调研等方式与顾客交流，主要进行以下沟通：  1、在产品交付中向顾客提供保证产品品质的有关信息。  2、接受顾客问询、询价、合同的处理。  3、根据合同要求进行有关的事宜，对顾客的投诉或意见进行及时处理和答复。  到目前为止，未发生顾客不满意及投诉现象。 | Y |
| 与产品有关要求的确定 | 8.2.2 | ●查公司产品销售合同，提供了销售合同台账，  ——抽合同签订日期为2022年4月22日    技术服务的内容:依据相关法规、标准及行业管理规范，通过访谈、检查、测试等多种方式对甲方指定的【河北省科技型中小企业综合管理平台】进行风险评估，并出具评估报告.  服务期限：签订合同起30个工作日内完成。  另合同有权利义务，违约责任等内容，见双方盖章.  ——抽合同签订日期为2022年2月28日    服务内容：依据信息安全相关法规、标准及行业管理规范，通过访谈、检查、测试、风险分析等多种方式对甲方指定的【河北作家网】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、安全管理建设、安全管理运维等方面进行单元测评，并从安全控制间安全、层面间安全、  区域间安全、系统结构安全等方面进行整体测评，给出测评结论，提出安全建设整改建议，并出具测评报告  技术服务期限及进度: 自等级测评首次会议(甲方、乙方、市级公安三方参加)召开且甲方提供乙方相关完整资料并配备专人配合测评工作起 60 个工作日内完成。  另有双方分工，技术要求，测试服务质量保证及售后服务等内容，见双方盖章。    另抽其他合同2份，均进行了相关明示，有双方盖章。经查，符合要求。 | Y |
| 产品有关要求的评审及变更 | 8.2.3  8.2.4 | ●查合同的评审记录，提供了《合同评审表》  评审在合同签订之前进行。总经理签名或中标视为评审通过，均符合要求。  ●评审内容包括技术服务内容，技术能力，服务期限 等方面。评审结果：全部通过。  ●公司目前暂无合同更改情况。 |  |
| 顾客满意度 | 9.1.2 | ●公司主要通过电话，走访等形式，接受顾客反馈，了解顾客满意度信息，发放调查表对顾客满意度进行定量测量。  ●提供了《顾客满意程度调查表》，调查主要内容：工作态度、技术能力、测评质量、国家有关信息安全标准规范的掌握情况、是否有违反安全保密等方面的满意程度等，各项得分求平均值得最终结果。  查企业对2022年的完工项目进行了顾客满意度调查，第三季度的顾客满意率96%。  --抽河北作家协会，负责人：董凯，综合得分100，调查时间：2022年9月30日    经查，符合要求。 | Y |