项目编号：20945-2025-QEO

管 理 体 系 审 核 报 告

（第二阶段）

组织名称：北京国测信安科技有限公司

审核体系：质量管理体系、环境管理体系、职业健康安全管理体系

审核组长（签字）： 王冰

审核组员（签字）： 王冰、岳艳玲

报告日期： **2025 年 7 月 29 日**

北京国标联合认证有限公司编制

地　址： 北京市朝阳区北三环东路 8 号 1 幢-3 至 26 层 101 内 8 层 810
电　话： 010-8225 2376
官　网： www.china-isc.org.cn
邮　箱： service@china-isc.org.cn

联系我们，扫一扫！

审核报告说明

1．本报告是对本次审核的总结，以下文件作为本报告的附件：

■管理体系审核计划（通知）书■首末次会议签到表■文件审核报告

■第一阶段审核报告■不符合项报告□其他

2．免责声明：审核是基于对受审核方管理体系可获得信息的抽样过程，考虑到抽样风险和局限性，本报告所表述的审核发现和审核结论并不能 100% 地完全代表管理体系的真实情况，特别是可能还存在有不符合项；在做出通过认证或更新认证的决定之前，审核建议还将接受独立审查，最终认证结果经北京国标联合认证有限公司技术委员会审议做出认证决定。

3．若对本报告或审核人员的工作有异议，可在本报告签署之日起 30 日内可北京国标联合认证有限公司提出（专线电话：010-58246011 信箱：service@china-isc.org.cn）。

4．本报告为北京国标联合认证有限公司所有，可在现场审核结束后提供受审核方，但正式版本需经北京国标联合认证有限公司确认，并随同证书一起发放。本审核报告不能做为最终认证结论，认证结论体现为认证证书或年度监督保持通知书。

5. 基于保密原因，未经上述各方允许，本报告不得公开。国家认证认可机构和政府有关管理部门依法调阅除外。

审核组公正性、保密性承诺

（本承诺应在首、末次会议上宣读）

为了保护受审核方和社会公众的权益，维护北京国标联合认证有限公司(ISC)的公正性、权威性、保证认证审核的有效性，审核组成员特作如下承诺：

1．在审核工作中遵守国家有关认证的法律、法规和方针政策，遵守 ISC 对认证公正性的管理规定和要求，认真执行北京国标联合认证有限公司工作程序，准确、公正地反映被审核组织管理体系与认证准则的符合性和体系运行的有效性。

2．尊重受审核组织的管理和权益，对所接触到的受审核方未公开信息保守秘密，不向第三方泄漏。为受审核组织保守审核过程中涉及到的经营、技术、管理机密。

3．严格遵守审核员行为准则，保持良好的职业道德和职业行为，不接受受审核组织赠送的礼品和礼金，不参加宴请，不参加营业性娱乐活动。

4．在审核之日前两年内未对受审核方进行过有关认证的咨询，也未参与该组织的设计、开发、生产、技术、检验、销售及服务等工作。与受审核方没有任何经济利益和利害冲突。审核员已就其所在组织与受审核方现在、过去或可预知的联系如实向认证机构进行了说明。

5．遵守《中华人民共和国认证认可条例》及相关规定，保证仅在北京国标联合认证有限公司一个认证机构执业，不在认证咨询机构或以其它形式从事认证咨询活动。

6．如因承诺人违反上述要求所造成的对受审核方和北京国标联合认证有限公司的任何损失，由承诺人承担相应法律责任。

承诺人审核组长：王冰

组员：岳艳玲

受审核方名称：北京国测信安科技有限公司一、审核综述

1.1 审核组成员

序号	姓名	组内职务	注册级别	审核员注册证书号	专业代码
A	王冰	组长	审核员	2024-N1EMS-1456075	33.02.01,33.02.04,34.06.00
A	王冰	组长	审核员	2024-N1QMS-1456075	33.02.01,33.02.04,34.06.00
A	王冰	组长	审核员	2024-N1OHSMS-1456075	33.02.01,33.02.04,34.06.00
B	岳艳玲	组员	审核员	2024-N1EMS-1319559	33.02.01,33.02.04,34.06.00
B	岳艳玲	组员	审核员	2024-N1QMS-1319559	33.02.01,33.02.04
B	岳艳玲	组员	审核员	2024-N1OHSMS-1319559	33.02.01,33.02.04,34.06.00

其他人员

序号	姓名	审核中的作用	来自
1	唐晓莉、李经通	向导	受审核方
2	/	观察员	

1.2 审核目的

本次审核的目的是依据审核准则要求，在第一阶段审核的基础上，通过检查受审核方管理体系范围覆盖的场所、管理体系文件、过程控制情况、相关法律法规和其他要求的遵守情况、内部审核与管理评审的实施情况，判断受审核方（**质量管理体系、环境管理体系、职业健康安全管理体系**）与审核准则的符合性和有效性，从而确定能否推荐注册认证。

1.3 接受审核的主要人员

管理层、各部门负责人等，详见首末次会议签到表。

1.4 依据文件

a) 管理体系标准：

GB/T19001-2016/ISO9001:2015 、 GB/T 24001-2016/ISO14001:2015 、 GB/T45001-2020 / ISO45001：2018

b) 受审核方文件化的管理体系；本次为☑结合审核☐联合审核☑一体化审核；

c) 相关审核方案，FSMS专项技术规范：/；

d) 相关的法律法规：

e) 适用的产品（服务）质量、环境、职业健康安全及所适用的食品职业健康安全及卫生标准：

f) 其他有关要求（顾客、相关方要求）。

1.5 审核实施过程概述

1.5.1 审核时间：2025年07月28日上午至2025年07月29日下午实施审核。

审核覆盖时期：自 2025年 1 月 10 日至本次审核结束日。

审核方式：■现场审核 □远程审核 □现场结合远程审核

1.5.2 审核范围（如与审核计划不一致时，请说明原因）：

Q:网络安全咨询服务，信息系统风险评估服务，网络安全运维服务，软件测试

E:网络安全咨询服务，信息系统风险评估服务，网络安全运维服务，软件测试所涉及场所的相关环境管理活动

O:网络安全咨询服务，信息系统风险评估服务，网络安全运维服务，软件测试所涉及场所的相关职业健康安全管理活动

1.5.3 审核涉及场所地址及活动过程（固定及临时多场所请分别注明各自活动过程）

注册地址： 北京市朝阳区容创路 17 号楼-3 至 8 层 101 号 7 层 710
办公地址：北京市朝阳区容创路 17 号楼-3 至 8 层 101 号 7 层 710
经营地址：北京市朝阳区容创路 17 号楼-3 至 8 层 101 号 7 层 710
临时场所（需注明其项目名称、工程性质、施工地址信息、开工和竣工时间）： 无

1.5.4 一阶段审核情况：

于 2025 年 07 月 25 日 9：00 至 2025 年 07 月 25 日 17：30 进行了第一阶段审核，审核结果详见一阶段审核报告。

一阶段识别的重要审核点：

Q 服务过程控制；EO 运行策划和控制；EO 绩效测量和监视。

1.5.5 本次审核计划完成情况：

1）审核计划的调整：☑未调整；□有调整，调整情况：

2）审核活动完成情况：☑完成了全部审核计划内容，未遇到可能影响审核结论可靠性的不确定因素

□未能完成全部计划内容，原因是（*请详细描述无法接近或被拒绝接近有关人员、地点、信息的情况，或者断电、火灾、洪灾等不利环境*）：

1.5.6 审核中发现的不符合及下次审核关注点说明

1）不符合项情况：

审核中提出严重不符合项（0）项，轻微不符合项（1）项，涉及部门/条款:综合部/QEO7.2 条款

采用的跟踪方式是：□现场跟踪☑书面跟踪；

双方商定的不符合项整改时限：2025 年 8 月 29 日前提交审核组长。

具体不符合信息详见不符合报告。

拟实施的下次现场审核日期应在 2026 年 7 月 29 日前。

2）下次审核时应重点关注：

本次不符合的验证；服务过程控制；重要环境因素和不可接受风险的识别评价和运行控制情况；任何变更情况。

3）本次审核发现的正面信息：

该公司管理体系能够持续有效运行，未发生相关方投诉。相关运行要求保持较好，环境因素和危险源进行了确认。人员质量、环境和安全意识等较好。相关资质手续保持有效。资源比较充分，能保证方针和目标方案的实现。

1.5.7 管理体系成熟度评价及风险提示

1）成熟度评价：

企业各部门职责明确，质量、环境和职业健康安全管理体系，能够全面有效地予以贯彻实施，各部门人员能基本理解和实施本部门涉及的相关过程。各部门能识别的相关环境因素和危险源，质量、环境和职业健康安全管理过程能有效予以控制。

2）风险提示：加强培训，提高各层级人员对环境因素和危险源的辨识及意识，提高内审员审核能力。

1.5.8 本次审核未解决的分歧意见及其他未尽事宜：无

二、受审核方基本情况

1）组织成立时间：2009-06-10；年月日体系实施时间：2025.01.10

2）法律地位证明文件有：

营业执照（统一社会信用代码 91110105690005940X）,经营范围覆盖认证范围，有效期内。

3）审核范围内覆盖员工总人数：17 人。

倒班/轮班情况（若有，需注明具体班次信息）：无

4） 范围内产品/服务及流程：

Q:网络安全咨询服务，信息系统风险评估服务，网络安全运维服务，软件测试

E:网络安全咨询服务，信息系统风险评估服务，网络安全运维服务，软件测试所涉及场所的相关环境管理活动

O:网络安全咨询服务，信息系统风险评估服务，网络安全运维服务，软件测试所涉及场所的相关职业健康安全管理活动

客户需求分析→签订合同→方案设计→采购物资实施技术、服务→测试、验证→甲方验收→运维

三、组织的管理体系运行情况及有效性评价

3.1 管理体系的策划 □符合 ☑基本符合 □不符合

企业成立于 2009-06-10，注册资本 1,000 万(元)，法定代表人张强。
注册地址：北京市朝阳区容创路 17 号楼-3 至 8 层 101 号 7 层 710；经营地址：北京市朝阳区容创路 17 号楼-3 至 8 层 101 号 7 层 710。单一场所。主要从事网络安全咨询服务，信息系统风险评估服务，网络安全运维服务，软件测试。经营范围覆盖认证范围。
该公司按照 GB/T19001-2016、GB/T24001-2016 和 GB/T45001-2020 标准要求建立并实施了编制了质量环境安全管理手册，于 2025 年 1 月 10 日发布、实施。公司现有：综合部、档案事业部、销售部职能部门，组织结构清晰，各岗位职责明确；现有人员 17 人，无倒班情况。
企业建立了质量环境职业健康安全方针：
提升服务质量，改善环境。保证职业健康，实现持续改进。
方针包含在管理手册中，经总经理批准，与手册一起发布实施。公司方针适应组织的宗旨和环境并支持其战略方向，为建立质量环境职业健康安全目标提供了框架。方针体现了对满足顾客要求、法规要求、污染预防、合规义务、消除危险源和降低职业健康安全风险的承诺、持续改进管理体系的承诺等内容，符合要求。
经确认该组织外包过程：云服务器租赁。
为达到管理方针最终实现，总经理及各职能部门负责人通过培训、宣传等方式使全体员工都充分理解并坚持贯彻执行。并将管理方针通过相关方告知提供给适宜的相关方。管理方针的制定适宜有效。
最高管理者制定了公司质量环境职业健康安全目标：
-质量管理目标为：
顾客满意率≥90％
产品一次交付合格率 100%
项目交付合格率 100%
环境管理目标为：
潜在火灾发生为 0；
固体废弃物合规处理率 100%；
职业健康安全管理目标为：
潜在火灾发生为 0；
意外伤害为 0
管理目标在《管理手册》中进行了规定并已形成了文件，体系运行以来以来至今质量环境职业健康安全目标已经完成。
查见《环境、职业健康目标管理方案》针对每项指标分别制定了管理措施，重要环境因素、重大危险源、目标、管理方案、完成日期、预计投资、责任部门等，详见各部门审核记录。
经查编制了《质量、环境、职业健康安全目标展开考核表》，检查结果表明，自 2025 年 1 月份以来各部门质量环境职业健康安全目标和管理方案均已经完成。
企业规定了因顾客和市场等原因而导致管理体系变更时，应对这种变更进行策划。依照 GB/T19001-2016 标准，结合实际情况，围绕管理方针、管理目标设置了组织机构，配置了必需的资源，确定了实现目标的过程、资源以及持续改进的相应措施，对员工进行了适宜的培训等。经营地址变更未影响质量管理体系的完整性，没有变更的策划。
为了确保获得合格的服务，确定了运行所需的知识。从内部来源获取的有，业务人员以往多年的工作经验（员工过去所有的），特别是岗位作业人员的操作技能；管理经验；作业指导书等。外部来源获取有：顾客提供的服务信息；国家、行业标准等。组织知识予以存档保管，在需要时可以随时获取。为应对不断变化的需求和法律趋势，企业策划进行了质量管理体系标准及相关知识的再培训、招聘有技能的业务人员等方式对确定的知识及时更新。
编制《环境因素的识别与评价控制程序》，《危险源辨识、风险评价和控制程序》符合实际和标准要求。
查看和查阅环境因素识别评价表，包括：复印机废粉的排放、旧电池的废弃、废 U 盘的废弃、生活污水的排放、生活垃圾的排放、火灾的发生、纸口杯的废弃等，上下班涉及车辆尾气的排放、车辆噪声的排放等。

识别基本齐全等，基本符合要求。
重要环境因素为：潜在火灾、固废排放，识别基本准确，符合要求。
查看和查阅危险源辨识和风险评价记录，包括：电长时间坐着工作、电脑辐射、电器开关失效、违章使用电器、潜在的火灾、电线老化裸露、乱接乱搭、室内吸烟引起火灾、制动、转向失灵、超员超载、其他机械故障、交通事故等。基本符合要求。
不可接受风险清单：潜在火灾、意外伤害，重大危险源识别准确，基本符合要求。
策划有《法律法规与其他要求控制程序》《合规性评价控制程序》，基本符合要求。组织建立了适用法律法规和其他要求获取的渠道，获取途径均为网上查询下载。收集了企业适用的法律法规和其他要求文件，并识别了适用性，同时落实到相关部门贯彻实施。提供环境安全法律法规清单，获取比较充分，识别合理、无遗漏，基本符合要求。
识别的标准法规：相关的法律法规：
中华人民共和国民法典、中华人民共和国消费者权益保护法、中华人民共和国反不正当竞争法、中华人民共和国价格法、中华人民共和国环境保护法、中华人民共和国安全生产法、突发环境事件应急管理办法、中华人民共和国噪声污染防治法、中华人民共和国节约能源法、中华人民共和国环境影响评价法、中华人民共和国固体废物污染环境防治法、北京市安全生产条例、北京市消防条例、北京市环境噪声污染防治条例、北京市大气污染防治条例等。均为有效版本，符合要求。

3.2 产品实现的过程和活动的管理控制情况及重要审核点的监测和绩效□符合 ☑基本符合 □不符合

QMS:企业最高管理者为增强顾客满意，确保顾客和适用的法律法规的要求得到满足，对建立、实施、保持和改进质量管理体系做出了承诺。建立和实施并初步形成了纠正、预防和持续改进机制。严格执行了体系文件规定要求，认真贯彻执行 GB/T19001-2016 标准，产品质量稳定并符合产品标准和顾客要求。实现了企业方针和目标，达到了预期结果。
企业建立了较完善的人力资源、基础设施、工作环境、技术信息、资金等资源确定和提供等渠道，能够确保满足建立、实施、保持、改进质量管理体系，提供符合要求的产品的实际需求。
企业在策划建立质量管理体系时较充分地识别了所需的过程，包括服务实现所需的过程，包括明确顾客及其规定用途和已知的预期用途所必需的要求、适用的法律法规要求、组织附加的要求，对各种要求进行评审，确认可以满足要求，并传递到相关岗位。
企业明确了所提供产品的质量目标和要求、文件和资源的需求，所需的过程和产品监视与测量活动及接收准则，所需的记录表格等。
按照服务实现的流程，通过查阅记录、现场观察、与岗位人员面谈，表明在服务实现的策划，顾客要求的识别和评审、采购、服务提供的控制、标识和可追溯性、顾客财产、产品防护、以及监视和测量的控制等能够按照规定准则正常运行，并保证提供产品符合规定的要求。
该组织策划了实现流程图，经识别，
需确认过程/关键过程:方案设计过程
对需确认过程进行服务质量考核控制及监督，基本符合要求。
产品/服务设计和开发：
编制《设计和开发控制程序》，按标准要求，规定了设计和开发过程及相互作用，对设计开发过程进行了界定，明确了设计开发的流程为：策划--输入--控制--输出--更改。各过程要求基本符合标准要求。
业务流程：
客户需求分析→签订合同→方案设计→采购物资实施技术、服务→测试、验证→甲方验收→运维
（一）网络安全咨询服务
根据用户安全建设和防护需求，检查客户当前安全状况，提出安全建设方案或者整改方案。
抽查北京桧城教育科技有限公司密码工程技术人员实训平台网络安全项目（已交付）
——策划：
现场提供：《北京桧城教育科技有限公司密码工程技术人员实训平台网络安全整改建议书》
整改目标设定　本次整改工作旨在全面提升密码工程技术人员实训平台的网络安全防护能力，通过针对性的整改措施，有效解决当前平台存在的网络架构不合理、系统配置有漏洞、安全措施不完善等问题。具体

目标如下：网络架构冗余性显著增强，关键链路故障风险降低 80% 以上；系统漏洞修复率达到 100%，服务器与网络设备安全配置合规率提升至 95% 以上；安全设备效能充分发挥，攻击检测与拦截成功率提高至 90% 以上；数据备份与恢复机制完善，数据丢失风险降低 90%，数据恢复时间缩短至 4 小时以内；安全管理制度健全，员工安全意识明显提升，违规操作行为减少 95% 以上，确保平台在复杂网络环境下稳定、安全运行，为教学活动提供坚实的安全保障。

性质持续时间及资源：2025.02.25-2025.5.25

项目负责人：李经通等。

资源：整改实施保障

（一）组织保障

成立由北京桧城教育科技有限公司分管领导任组长，信息技术部负责人、北京国测信安科技有限公司项目负责人任副组长，各相关部门骨干为成员的整改工作领导小组，负责整改工作的统筹协调、资源调配与进度监督，每周召开整改工作例会，及时解决整改过程中出现的问题。

（二）技术保障

北京国测信安科技有限公司组建专业技术团队，提供 7×24 小时技术支持服务，在整改过程中遇到技术难题时，及时组织专家进行会诊，确保整改措施的技术可行性与有效性。同时，提供必要的技术工具支持，如漏洞扫描工具、配置管理工具等，保障整改工作顺利开展。

（三）资源保障

北京桧城教育科技有限公司合理安排整改预算，确保链路优化、设备升级、系统部署等工作的资金投入，根据整改需求采购必要的硬件设备、软件工具与服务。协调内部机房空间、网络带宽等资源，为整改工作提供良好的实施环境。

沟通机制（例会、邮件、企业微信等工具）

文件的策划:策划了相关的设计开发资料，包括《设计和开发控制程序》等内容

人员接口控制:技术部负责相关的人员接口的控制；

过程和接收准则：建立了相关的管理制度和文件，包括《设计和开发控制程序》,对过程的控制及接收的验证都做了规定；

阶段划分及主要内容：

为保证项目的顺利实施，按要求工期交付使用，项目经理按计划周期，严格控制各阶段结束时间点，规划项目实施计划内容。

——输入：

现场沟通，设计开发的输入内容主要包括：客户需求、法律法规、以往类似项目经验等；

输入包括:

客户需求：服务器系统安全优化 ，预期效果：服务器高危漏洞修复率达到 100%，中低危漏洞修复率达到 95% 以上，用户权限违规配置问题全部整改，服务器被恶意入侵风险大幅降低。

网络设备固件升级 ，网络设备固件安全漏洞修复率达到 100%，设备运行稳定性提升，因固件漏洞导致的攻击风险消除。

应用系统漏洞修复 ，应用系统漏洞扫描结果为零高危漏洞，中低危漏洞数量控制在 3 个以内，成功抵御常见的 SQL 注入与 XSS 攻击。 安全措施整改建议 ，数据备份覆盖率达到 100%，备份数据完整性与保密性得到保障，全量数据恢复时间控制在 4 小时以内，恢复成功率达到 100%。

查以前类似设计和开发活动：负责人介绍，公司长期从事该类设计开发活动，以往设计中积累充足的经验在本项目中运用；

查由产品和服务性质所导致的潜在的失效后果：为无法为顾客提供满足要求的服务，目前以过程、结果控制的方式规避，如真实发生，按协议约定进行处理

输入充分适宜，清晰完整，无自相矛盾等。

——输出：

提供北京桧城教育科技有限公司密码工程技术人员实训平台网络安全咨询方案：

经评估，平台网络架构存在链路冗余不足、区域访问控制不精细、设备配置有隐患等问题；系统配置方面，

服务器、网络设备及应用系统均存在漏洞；安全措施上，安全设备效能未充分发挥、数据备份策略有缺陷、安全管理制度不完善。风险评估显示，网络架构、系统配置、安全措施各环节均存在不同概率和程度的风险，可能导致业务中断、数据泄露、经济损失及声誉受损等后果。

——评审验证确认：

主要表现为对报告的评审；

提供评审记录:

项目名称：北京桧城教育科技有限公司密码工程技术人员实训平台网络安全咨询

报告名称：北京桧城教育科技有限公司密码工程技术人员实训平台网络安全整改建议书（V2.0）

编制人：李喜冬

编制时间：2025.5.25

审核人：李经通

审核问题：（三）安全管理制度健全与培训强化责任分工未明确

处理情况：已修改

（二）信息系统风险评估服务

参考国家标准，对用户系统安全管理和配置情况进行检查分析，出具风险评估报告。

贵州亨达集团信息安全技术有限公司数据安全风险评估--已完成

——策划：

现场提供：《贵州亨达集团信息安全技术有限公司数据安全风险评估报告》

总体目标

通过系统化的风险评估流程，全面识别数据安全风险评估报告编制平台（以下简称 “平台”）在数据生命周期各环节存在的安全风险，科学分析风险等级与影响范围，提出针对性的风险处置建议，为平台建立健全安全防护体系提供决策依据，保障平台数据资产的机密性、完整性和可用性。

具体目标

完成平台资产全面梳理与价值分级，明确核心数据资产保护优先级；

识别平台面临的内外部威胁、技术与管理脆弱性，形成完整风险清单；

量化分析风险发生可能性与影响程度，确定高、中、低风险边界；

评估现有安全措施有效性，找出防护体系薄弱环节；

制定可落地的风险处置计划，降低风险至可接受水平。

项目负责人：李经通等。

（一）评估范围

1. 系统边界范围

硬件环境：平台部署的服务器（含应用服务器、数据库服务器）、存储设备（磁盘阵列、备份设备）、网络设备（交换机、防火墙、负载均衡器）、终端设备（管理员工作站、运维终端）；

软件系统：操作系统（Windows Server 2019、Linux CentOS 7）、数据库系统（MySQL 8.0）、应用系统（报告编制系统 V2.0、用户管理系统、数据加密模块）、安全软件（杀毒软件、入侵检测系统）；

网络环境：平台所在局域网（192.168.10.0/24）、内外网交互链路、远程访问通道（VPN）；

数据资产：平台存储的各类数据，包括用户信息（账号、权限数据）、评估报告模板数据、已生成的风险评估报告数据、客户敏感数据（若有）、系统配置数据等； 业务流程：报告编制（数据录入、分析、生成）、用户管理（账号创建、权限分配）、数据传输（内部流转、外部导出）、数据备份与恢复等流程。

2. 时间范围

评估工作覆盖平台当前运行状态，历史数据追溯至最近 6 个月的安全事件与操作记录。

沟通机制（例会、邮件、企业微信等工具）

文件的策划:策划了相关的设计开发资料，包括《设计和开发控制程序》等内容

人员接口控制:技术部负责相关的人员接口的控制；

过程和接收准则：建立了相关的管理制度和文件，包括《设计和开发控制程序》,对过程的控制及接收的验证都做了规定；
阶段划分及主要内容：
为保证项目的顺利实施，按要求工期交付使用，项目经理按计划周期，严格控制各阶段结束时间点，规划项目实施计划内容。
评估流程与实施步骤
（一）评估准备阶段（第 1 周）
成立评估项目组，明确 roles 分工（项目经理 1 人、技术评估师 2 人、安全分析师 1 人）；
与甲方对接，获取平台架构文档、资产清单、安全制度等基础资料；
制定详细评估计划，明确各阶段时间节点与交付物；
搭建评估测试环境，配置相关工具，准备调查问卷与访谈提纲；
组织评估团队培训，熟悉平台业务流程与评估方法。
（二）资产识别与价值分析阶段（第 2 周）
发放《资产调查表》，收集甲方提供的资产台账；
运用 Nessus 工具扫描网络资产，补充完善资产清单；
按资产类型分类梳理，建立资产台账（含资产名称、型号、位置、责任人等信息）；
组织甲方技术人员与业务人员开展资产价值评分，确定资产等级；
编制《资产价值分析报告》，经甲方确认后归档。
（三）威胁与脆弱性识别阶段（第 3-4 周）
威胁识别： 收集行业威胁情报，分析平台历史安全事件记录； 识别外部威胁（黑客攻击、恶意代码、供应链攻击等）与内部威胁（误操作、恶意行为等）； 组织专家研讨会，评估威胁发生可能性，形成《威胁分析报告》。
脆弱性识别：
技术脆弱性：使用 AWVS 扫描 Web 应用漏洞，对服务器进行系统漏洞扫描，开展针对性渗透测试；
管理脆弱性：审查安全管理制度、流程文件，访谈管理员与操作人员，评估制度执行情况；
整理脆弱性清单，标注严重程度，编制《脆弱性分析报告》。
（四）已有安全措施评估阶段（第 4 周末）
梳理平台现有安全措施，包括技术措施（防火墙策略、数据加密、访问控制等）与管理措施（人员培训、应急演练等）；
测试验证技术措施有效性（如防火墙规则有效性、加密算法强度）；
评估管理措施执行效果（如培训记录完整性、制度覆盖率）；
编制《已有安全措施分析报告》，指出存在的不足。
（五）风险分析与评价阶段（第 5 周）
建立资产 - 威胁 - 脆弱性关联关系矩阵，明确风险场景；
采用风险值计算公式量化分析各风险场景的风险值；
对照风险等级划分标准，确定每个风险的等级；
统计高、中、低风险数量与分布情况，分析风险聚集领域；
编制《风险计算表》，形成《风险评估报告（初稿）》。
（六）风险处置建议阶段（第 6 周）
根据风险等级与影响范围，制定差异化风险处置策略；
针对高风险提出紧急处置措施，中风险制定短期整改计划，低风险提出持续改进建议；
明确各项措施的责任部门、完成时限与资源需求；
编制《风险处置计划》，与甲方沟通确认可行性。
（七）报告编制与交付阶段（第 7 周）
汇总各阶段成果，完善《风险评估报告》，补充风险图谱、整改优先级矩阵等图表；
组织内部评审，邀请技术专家对报告进行审核；

根据评审意见修改报告，形成终稿；
向甲方提交全套评估文档，召开成果汇报会，解答甲方疑问；
协助甲方制定风险整改 roadmap，提供技术咨询支持。

——输入：

现场沟通，设计开发的输入内容主要包括：客户需求、法律法规、以往类似项目经验等；
输入包括：
法律法规：《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《关键信息基础设施安全保护条例》、GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》、GB/T 20984-2007《信息安全技术 信息安全风险评估规范》、GB/T 31509-2015《信息安全技术 数据安全能力成熟度模型》、GB/T 35273-2020《信息安全技术 个人信息安全规范》
资产价值评估法：从机密性、完整性、可用性三个维度评分（1-5 分），资产价值 =（机密性得分 + 完整性得分 + 可用性得分）/3，划分为极高（4.1-5 分）、高（3.1-4 分）、中（2.1-3 分）、低（1-2 分）四级；
威胁可能性评估法：结合历史发生频率、行业统计数据评分（1-5 分），划分为极高（4.1-5 分）、高（3.1-4 分）、中（2.1-3 分）、低（1-2 分）四级；
脆弱性严重程度评估法：从技术修复难度、暴露程度评分（1-5 分），划分为严重（4.1-5 分）、较高（3.1-4 分）、一般（2.1-3 分）、轻微（1-2 分）四级；
风险值计算法：风险值 = 资产价值 × 威胁可能性 × 脆弱性严重程度，风险等级划分为：极高风险（＞40 分）、高风险（25-40 分）、中风险（10-24 分）、低风险（≤10 分）。
查以前类似设计和开发活动：负责人介绍，公司长期从事该类设计开发活动，以往设计中积累充足的经验在本项目中运用；
查由产品和服务性质所导致的潜在的失效后果：为无法为顾客提供满足要求的服务，目前以过程、结果控制的方式规避，如真实发生，按协议约定进行处理
输入充分适宜，清晰完整，无自相矛盾等。

——输出

提供：贵州亨达集团信息安全技术有限公司数据安全风险评估报告编制平台风险评估方案
北京国测信安科技有限公司于 2024 年 9 月 1 日 - 10 月 30 日对贵州亨达集团数据安全风险评估报告编制平台开展风险评估，形成 V1.0 版本报告。评估覆盖平台硬件、软件、网络、数据及业务流程等，采用 “定性 + 定量” 方法，历经五个阶段，投入 160 工时。梳理出 28 项资产，含 4 项极高价值资产，识别 12 类威胁，其中 Web 应用 SQL 注入等威胁可能性高，还发现 15 项技术脆弱性和 8 项管理脆弱性。现有安全措施存在防火墙规则不足等问题，共识别 32 个风险场景，5 项为高风险，主要集中在 Web 应用、数据安全领域。针对高、中、低风险分别提出紧急、高、中优先级的处置建议，以保障平台安全。
评估结论与建议
（一）总体结论
平台整体风险等级为 “中等”，未发现极高风险，但存在 5 项高风险隐患需紧急处置；
核心数据资产保护存在短板，Web 应用与数据存储安全是主要风险聚集领域；
现有安全措施有效性不足，技术防护与管理流程均需优化。
（二）核心发现
技术层面：文件上传漏洞、数据加密缺失、权限控制不严构成主要技术风险；
管理层面：制度更新滞后、备份验证缺失、人员培训不足放大风险敞口；
资产保护：极高价值数据资产的防护措施与价值等级不匹配。
（三）实施建议
短期行动（1-2 个月）：优先修复高风险漏洞，完成核心数据加密与权限梳理；
中期计划（3-6 个月）：完善安全制度体系，部署 WAF 与日志审计系统，建立漏洞管理闭环；
长期规划（6-12 个月）：开展数据分类分级，构建数据安全治理框架，每季度执行一次风险复评。
（四）上线建议

建议在完成 5 项高风险处置措施并通过验证后，方可启动平台新版本上线；上线后首月需加强安全监控，每日执行漏洞扫描与日志分析，确保风险可控。

——评审验证确认：

主要表现为对报告的评审；

提供评审记录:

报告名称：贵州亨达集团信息安全技术有限公司 数据安全风险评估报告编制平台风险评估报告（V1.0）

编制人：冯河

编制时间：2024.10.30

审核人：李经通

审核意见：无

（三）网络安全运维服务

按照用户安全运维需求提供现场和远程安全配置核查，安全事件监控，事件分析及协助处置等。

抽查北京桧城教育科技有限公司密码工程技术人员实训平台网络安全运维项目（已交付）

——策划：

现场提供：《北京桧城教育科技有限公司密码工程技术人员实训平台网络安全运维实施方案》

方案目标　本次安全运维服务旨在通过专业的技术手段和规范的管理流程，保障密码工程技术人员实训平台的安全稳定运行，及时发现并处理各类安全事件，持续提升平台的安全防护能力，为甲方的教学活动提供可靠的安全保障。具体目标如下：实现平台安全事件平均响应时间控制在 30 分钟以内，关键系统可用性达到 99.9% 以上，高危安全漏洞修复率达到 100%，中低危安全漏洞修复率达到 95% 以上。

资源保障

（一）人员保障

乙方组建由项目经理、安全工程师、网络工程师、系统工程师、应用工程师等组成的运维团队。团队成员均具备 CISP、CCIE、RHCE 等相关专业资质，具有丰富的网络安全运维经验。项目经理负责整体运维工作的协调和管理，其他人员各司其职，确保运维工作的顺利开展。

（二）技术保障

采用先进的网络安全技术和工具，如 SIEM 系统、漏洞扫描工具、服务器监控工具、数据备份与恢复工具等，提高运维服务的技术水平和效率。不断跟踪网络安全技术的发展趋势，引入新的技术和方法，持续提升运维服务能力。

（三）工具保障

配备必要的运维工具和设备，如笔记本电脑、网络测试仪、漏洞扫描设备等，确保运维人员能够顺利开展工作。建立工具管理机制，对工具进行定期维护和更新，保证工具的正常运行。

性质持续时间及资源：2025.2.25-2025.5.25

项目负责人：冯河 等。

资源：整改实施保障

（一）组织保障

成立由北京桧城教育科技有限公司分管领导任组长，信息技术部负责人、北京国测信安科技有限公司项目负责人任副组长，各相关部门骨干为成员的整改工作领导小组，负责整改工作的统筹协调、资源调配与进度监督，每周召开整改工作例会，及时解决整改过程中出现的问题。

（二）技术保障

北京国测信安科技有限公司组建专业技术团队，提供 7×24 小时技术支持服务，在整改过程中遇到技术难题时，及时组织专家进行会诊，确保整改措施的技术可行性与有效性。同时，提供必要的技术工具支持，如漏洞扫描工具、配置管理工具等，保障整改工作顺利开展。

（三）资源保障

北京桧城教育科技有限公司合理安排整改预算，确保链路优化、设备升级、系统部署等工作的资金投入，根据整改需求采购必要的硬件设备、软件工具与服务。协调内部机房空间、网络带宽等资源，为整改工作

提供良好的实施环境。
沟通机制（例会、邮件、企业微信等工具）
文件的策划:策划了相关的设计开发资料，包括《设计和开发控制程序》等内容
人员接口控制:技术部负责相关的人员接口的控制；
过程和接收准则：建立了相关的管理制度和文件，包括《设计和开发控制程序》,对过程的控制及接收的验证都做了规定；
阶段划分及主要内容：
为保证项目的顺利实施，按要求工期交付使用，项目经理按计划周期，严格控制各阶段结束时间点，规划项目实施计划内容。
——输入：
现场沟通，设计开发的输入内容主要包括：客户需求、法律法规、以往类似项目经验等；
输入包括:
安全事件响应时间：平均响应时间≤30 分钟，重大安全事件响应时间≤15 分钟。
安全事件解决率：安全事件解决率达到 100%，重大安全事件解决时间≤24 小时。
漏洞修复率：高危漏洞修复率达到 100%，中低危漏洞修复率达到 95% 以上。
系统可用性：关键系统可用性达到 99.9% 以上，年度非计划停机时间≤8.76 小时。
数据备份成功率：数据备份任务成功率达到 100%，备份数据恢复成功率达到 100%。
客户满意度：每季度进行一次客户满意度调查，客户满意度评分≥90 分。
查需求：
组建专业的运维团队，配备必要的技术人员、工具和设备，确保运维服务的质量和效率
按照本方案的要求，开展日常安全监控、安全事件处理、漏洞管理等运维工作。
定期向甲方提交运维服务报告，汇报平台安全状况、运维工作进展和存在的问题。
为甲方提供安全培训和技术支持服务，提高甲方人员的安全意识和操作技能。
严格遵守保密协议，对在运维服务过程中获取的甲方敏感信息予以保密。
查以前类似设计和开发活动：负责人介绍，公司长期从事该类设计开发活动，以往设计中积累充足的经验在本项目中运用；
查由产品和服务性质所导致的潜在的失效后果：为无法为顾客提供满足要求的服务，目前以过程、结果控制的方式规避，如真实发生，按协议约定进行处理
输入充分适宜，清晰完整，无自相矛盾等。
——输出：
提供：北京桧城教育科技有限公司密码工程技术人员实训平台网络安全运维巡检报告
巡检时间
2025 年 5 月 1 日 - 5 月 5 日（共计 5 个工作日）
巡检范围
本次巡检严格依据《密码工程技术人员实训平台安全运维实施方案》确定的服务范围，具体涵盖：
网络设备：含华为 AR6300 路由器 2 台、华为 S5720 交换机 8 台、Cisco ASA 5585 防火墙 2 台、启明星辰天阗入侵防御系统（IPS）1 台；
服务器：Windows Server 2019 服务器 5 台（含核心教学服务器 2 台、数据库服务器 1 台、应用服务器 2 台），Linux CentOS 7 服务器 3 台（含实验数据服务器 2 台、文件服务器 1 台）；
应用系统：教学管理系统 V3.2、实验环境应用系统 V2.1、用户身份认证系统 V1.5；
数据资产：教学课件库（约 200GB）、实验案例数据（约 500GB）、学生信息数据库（含 8000 条学生敏感信息）、系统配置数据（约 10GB）。
巡检依据
核心依据：《密码工程技术人员实训平台安全运维实施方案》（编号：GCXC - 2025 - 001）；
国家标准：GB/T 22239 - 2019《信息安全技术 网络安全等级保护基本要求》、GB/T 20984 - 2007《信息安全技术 信息安全风险评估规范》；

行业规范：《教育行业网络安全运维指南》《密码应用安全管理规范》； 内部标准：甲方《实训平台安全管理手册》《网络设备配置基线 V2.0》。
整改建议
（一）网络设备整改
固件升级计划：
针对 SW - 06 交换机，7 月 10 日前下载最新固件版本 V200R020C00SPC500，在测试环境验证 24 小时无异常后，于 7 月 12 日凌晨 2 - 4 点进行生产环境升级，升级前备份配置文件；
同步检查其他设备固件版本，制定季度固件升级计划，优先升级存在已知漏洞的设备。
日志配置优化：
登录华为路由器命令行，执行 “info - center logfile size 10240”（设置日志文件大小为 10GB），“info - center logfile save - days 60”（设置留存时间 60 天），7 月 8 日前完成配置并验证。
（二）服务器整改
补丁安装安排：
7 月 10 日前完成 CVE - 2025 - 5678 补丁在测试环境的最终验证，7 月 15 日凌晨 3 点在生产环境安装，安装后重启服务器并验证数据库服务正常启动；
建立 “补丁测试专用虚拟机”，提前 7 天进行新补丁兼容性测试，缩短补丁延迟安装时间。
日志配置调整：
对 Linux 服务器执行 “vi /etc/audit/auditd.conf”，修改 “max_log_file = 10240”（设置单日志文件大小 10GB），“num_logs = 10”（保留 10 个日志文件），7 月 9 日前完成配置并重启 auditd 服务。
——评审验证确认：
主要表现为对报告的评审；
提供评审记录:
编制人：冯河
编制时间：2025.5.25
审核人：李经通
审核问题：四、巡检依据 GB/T 20984 - 2007《信息安全技术 信息安全风险评估规范》该标准版本号应更新为 GB/T 20984 - 2022
处理情况：已修改

（四）软件测试
通过人工或自动化手段验证软件是否满足项目需求，如发现问题，协调建设方进行修正后复测，并出具测试报告。
抽查北京桧城教育科技有限公司密码工程技术人员实训平台测试项目（已交付）
——策划：
现场提供：《北京桧城教育科技有限公司密码工程技术人员实训平台测试计划》
核心目标 ：通过多维度、全流程的测试活动，全面验证实训平台的功能完整性、性能稳定性、安全可靠性及环境兼容性，确保平台上线后能够满足密码工程技术教学与实训的核心需求，将线上故障发生率控制在 0.5% 以内，用户操作满意度达到 95% 以上。
测试范围涵盖教学管理系统 V3.2、实验环境应用系统 V2.1、用户身份认证系统 V1.5 的多个模块及子模块。其中，教学管理系统的课程管理涉及课程信息与资源维护，成绩管理包含录入、统计和查询，用户管理涉及教师与学生账号等信息维护；实验环境应用系统的实验环境配置含模板和实例管理，文件上传下载涉及素材上传与文件管理，实验结果管理包括报告提交与评分；用户身份认证系统的登录验证支持账号密码及第三方登录，权限控制涉及角色管理与校验，会话管理涵盖会话维护与控制。不测试范围包括第三方开源组件内部代码、硬件设备物理故障修复、未纳入需求规格的定制功能及超纲性能场景，原因分别为开源组件由厂商维护、硬件故障修复属运维范畴、定制功能未在需求文档明确、超纲场景超出平台设计承载

范围。
开始时间：2025 年 2 月 25 日
项目负责人：李经通等。

里程碑	完成时间	交付成果	验收标准
测试准备完成	第 1 周周五（4 月 11 日）	《测试计划文档 V2.0》《测试用例文档 V1.0》、测试环境搭建完成	文档通过甲方评审，测试环境满足配置要求
功能测试完成	第 3 周周五（4 月 25 日）	《功能测试执行报告》《缺陷清单 V1.0》	功能用例通过率≥95%，高危缺陷数量

资源详细安排
5.1 测试团队组成及职责

角色	姓 名	所属部门	具体职责
测试负责人	冯 河	北京国测信安测试部	整体测试规划、进度把控、资源协调、缺陷评审主持、测试报告审批、与甲方沟通对接
功能测试工程师	周 伟鹏	北京国测信安测试部	功能测试用例设计与评审、UI 测试执行、缺陷记录与跟踪、测试文档编写
功能测试工程师	李 喜冬	北京国测信安测试部	接口测试脚本编写与执行、业务流程测试、回归测试执行、测试数据准备
性能测试工程师	王娅	北京国测信安性能测试组	性能测试场景设计、JMeter 脚本开发、性能监控指标分析、性能瓶颈定位、性能报告编写
安全测试工程师	张 涛	北京国测信安安全测试组	安全漏洞扫描、渗透测试执行、安全风险评估、敏感数据保护验证、安全测试报告编写

5.2 测试工具资源清单

工具类别	工具名称	数 量	版本	用途说明	负责人
用例管理工具	TestLink	1 套	1.9.24	测试用例编写、版本管理、执行跟踪、覆盖率统计	冯河
缺陷管理工具	JIRA	1 套	9.15.0	缺陷创建、状态跟踪、优先级管理、缺陷统计分析	周伟鹏
接口测试工具	Postman	5 套	10.16.0	API 测试脚本编写、自动化执行、接口文档生成	李喜冬
性能测试工具	JMeter	3 套	5.6	负载测试脚本开发、并发场景执行、性能数据采集	王娅
安全测试工具	AWVS	1 套	15.0	Web 应用漏洞扫描、安全配置检查	张涛
安全测试工具	Burp Suite	1 套	2023.9	渗透测试、请求拦截与修改、漏洞验证	冯河

5.3 硬件资源清单

设备名称	型号	数量	配置	用途	存放位置
测试服务器	戴尔 PowerEdge R740	4台	配置见 4.2.1 服务器环境	应用服务器、数据库服务器	甲方测试机房
测试客户端 PC	联想 ThinkCentre M900	6台	Intel i5-6500，16GB 内存，512GB SSD	功能测试、UI 测试执行	测试团队办公区
安全测试专用机	惠普 Z4 G4 工作站	1台	Intel Xeon W-2133，32GB 内存，1TB SSD	安全漏洞扫描、渗透测试	安全测试实验室
网络测试仪	福禄克 NetScout	1台	OptiView XG	网络流量监控、带宽测试、丢包分析	刘洋
存储设备	西部数据 My Cloud EX2 Ultra	1台	8TB 存储容量	测试数据备份、测试用例库存储	测试服务器机房

沟通机制（例会、邮件、企业微信等工具）
文件的策划:策划了相关的设计开发资料，包括《设计和开发控制程序》等内容
人员接口控制:技术部负责相关的人员接口的控制；
过程和接收准则：建立了相关的管理制度和文件，包括《设计和开发控制程序》,对过程的控制及接收的验证都做了规定；
阶段划分及主要内容：
为保证项目的顺利实施，按要求工期交付使用，项目经理按计划周期，严格控制各阶段结束时间点，规划项目实施计划内容。
——输入：
现场沟通，设计开发的输入内容主要包括：功能性能需求、客户需求、法律法规、以往类似项目经验等；
输入包括:
测试类型及详细实施方法
4.1.1 功能测试

测试层面	实施方法	具体操作
单元测试	白盒测试	开发团队采用 JUnit（Java）、PyTest（Python）框架进行单元测试，测试覆盖率≥80%，测试报告提交测试团队备案
接口测试	黑盒测试 + 自动化	使用 Postman 编写接口测试脚本，覆盖所有 RESTful API，验证请求参数校验、响应格式、错误码返回、权限控制，每日自动执行并生成报告
UI 测试	黑盒测试 + 自动化	基于 Selenium 构建 UI 自动化测试框架，覆盖核心业务流程（如课程创建 - 学生选课 - 实验提交 - 成绩录入），关键路径自动化率≥70%
业务流程测试	场景测试	设计端到端业务场景，如 “教师创建课程→上传实验素材→学生选课→创建实验环境→提交实验报告→教师评分” 全流程验证

4.1.2 性能测试

测试场景	测试工具	参数设置	指标监控
负载测试	JMeter	模拟 100 并发用户持续操作 2 小时，操作包括课程查询、实验环境创建、文件上传等混合场景	
		监控指标：响应时间、吞吐量（TPS）、服务器 CPU / 内存 / 磁盘 IO 使用率	
压力测试	JMeter	从 100 并发逐步增加至 300 并发，每次增加 50 用户，持续 10 分钟	
		监控指标：系统崩溃阈值、性能拐点、错误率变化趋势	
耐久测试	JMeter	50 并发用户连续操作 72 小时，模拟平台长时间运行场景	
		监控指标：内存泄漏情况、数据库连接池状态、系统稳定性	
数据量测试	自定义脚本	生成 10 万条学生数据、1 万门课程数据、50 万条实验记录，验证查询与统计性能	
		监控指标：大数据量下页面加载时间、报表生成时间、数据库查询效率	

4.1.3 安全测试

测试类型	测试工具	测试内容
漏洞扫描	AWVS、Nessus	OWASP Top 10 漏洞检测（注入攻击、 Broken Authentication 等）、服务器配置漏洞、弱密码检测
渗透测试	Burp Suite 、Metasploit	模拟黑客攻击流程，尝试 SQL 注入、XSS 攻击、CSRF 攻击、权限越界等攻击手段
数据安全测试	自定义工具	敏感数据（身份证号、成绩）传输加密验证（HTTPS）、存储加密验证（AES-256）、脱敏展示验证
安全配置检查	OpenSCAP	操作系统安全配置基线检查、网络设备防火墙规则检查、应用服务器安全参数检查

4.1.4 兼容性测试

测试维度	测试环境	测试方法
浏览器兼容性	Chrome 118.0、Edge 117.0、Firefox 118.0、Safari 17.0	在各浏览器中执行核心功能用例，验证页面布局、功能按钮可用性、JavaScript 执行正确性

操作系统兼容性	Windows 10（64 位）、Windows 11（64 位）、Linux CentOS 7、macOS Ventura	在各系统安装客户端组件（如远程桌面工具），验证系统交互功能正常
分辨率兼容性	1366×768、1920×1080、2560×1440	验证不同分辨率下页面无横向滚动条、关键内容不被遮挡

4.1.5 回归测试

测试触发条件	测试范围	测试方法
高危缺陷修复后	修复缺陷相关模块及关联模块	执行缺陷对应的测试用例及 5 条关联用例
版本迭代更新后	全系统核心功能模块	执行回归测试用例集（选取 80% 高频使用功能用例）
环境变更后	受影响模块（如数据库升级影响的数据操作模块）	针对性执行相关功能用例

查功能性能需求：

测试类型	量化指标
功能测试	功能点覆盖率 100%，关键功能用例通过率 100%，非关键功能用例通过率≥98%
性能测试	100 并发用户下核心操作响应时间≤1 秒，200 并发用户下响应时间≤3 秒，无系统崩溃现象
安全测试	高危漏洞数量为 0，中危漏洞修复率 100%，低危漏洞修复率≥90%，敏感数据加密传输与存储合规率 100%
兼容性测试	主流浏览器（Chrome/Edge/Firefox）适配率 100%，操作系统（Windows/Linux）兼容性问题≤2 个
回归测试	缺陷修复验证通过率≥95%，无新增严重缺陷

查以前类似设计和开发活动：负责人介绍，公司长期从事该类设计开发活动，以往设计中积累充足的经验在本项目中运用；

查由产品和服务性质所导致的潜在的失效后果：为无法为顾客提供满足要求的服务，目前以过程、结果控制的方式规避，如真实发生，按协议约定进行处理

输入充分适宜，清晰完整，无自相矛盾等。
——输出：
提供北京桧城教育科技有限公司密码工程技术人员实训平台测试报告
测试结论与建议
（一）测试结论
总体评价：密码工程技术人员实训平台整体测试结果符合预期，核心功能完整可用，性能指标达标，未发现高危安全漏洞，基本满足教学与实训需求。
达标情况：功能测试通过率 97.67%、性能测试全部达标、安全测试高危漏洞为 0、兼容性测试通过率 97.5%，均达到测试计划设定的量化目标。
上线建议：建议在修复当前未解决的中危缺陷及关键低危缺陷后，于 9 月 10 日前完成上线；上线前需进行最终一轮回归测试，确保核心功能无异常。
（二）改进建议
功能优化建议
增强课程代码、学生学号等关键字段的实时校验机制，添加明确的错误提示；
优化大文件上传功能，增加断点续传失败重试机制及进度提示；
完善第三方登录后的权限同步逻辑，确保角色权限即时生效。
性能优化建议
对高频访问的课程列表、学生信息等数据添加缓存机制，降低数据库压力；
优化文件上传组件，采用分片上传技术提升高并发下的上传成功率；
针对大数据量报表生成功能进行 SQL 优化，减少查询耗时。
安全加固建议
完善所有页面的安全响应头设置（如 X-Content-Type-Options、Content-Security-Policy）；
加强文件上传全流程安全控制，同时校验文件后缀与内容类型；
定期进行安全漏洞扫描与渗透测试，建议每季度执行一次全面安全评估。
兼容性改进建议
针对 Firefox 浏览器进行专项适配优化，修复按钮样式与布局问题；
增加前端代码的浏览器兼容性测试覆盖率，引入自动化兼容性测试工具；
制定统一的 UI 组件库，确保各浏览器展示效果一致。
测试过程建议
扩大自动化测试覆盖范围，将核心业务流程的自动化率提升至 80% 以上；
建立缺陷复盘机制，定期分析高频缺陷类型，从源头减少同类问题；
加强测试与开发的协作，在需求评审阶段提前介入，识别潜在风险。
——评审验证确认：
主要表现为对报告的评审；
项目名称：北京桧城教育科技有限公司 密码工程技术人员实训平台软件测试
报告名称：北京桧城教育科技有限公司 密码工程技术人员实训平台 测试报告（V1.0）
编制人：李喜冬
编制时间：2025.5.25
审核人：李经通
测评报告审核问题应答：审核意见：无
审核人员意见：同意
--设计开发过程中适宜的监视测量设备的使用
监视测量设备：软件有 Wireshark 网络抓包分析工具、Nessus 漏洞扫描工具、Nmap 资产扫描工具
设计开发过程中适宜的基础设施和环境：
设计开发人员使用的电脑由公司提供，配置等级均采用同型号中高配。保证过程顺利进行，资源保证。同时，设计开发使用办公场，采光好，有空调/暖气，办公环境舒适，适于设计人员静心创意，精心设计。

--设计和开发的更改，以上项目没有发生较大更改，设计差错在控制过程中已予以更正。如有重大变更会依据《设计和开发控制程序》进行控制；
设计开发过程控制基本有效

产品和服务要求有关的要求的评审：
公司制定并实施《与顾客有关要求的评审程序》，销售采用上门拜访、会议、计算机网络等方式与顾客进行沟通。了解客户要求的产品的相关信息；问询、合同或订单的处理，包括对其修改；顾客反馈，包括顾客抱怨；处置或控制顾客财产；当有重大异常时，制定有关的应急措施及客户特定的要求；
对市场进行调研，定向顾客提供的产品和服务的要求，从以下几个方面来确定与服务有关的要求：
（1）顾客对产品规定的要求,包括产品项目内容、技术、进度和费用要求以及设计、策划后期服务要求；
（2）与产品有关的法律、法规要求；
（3）公司确定的其他附加要求,如保密、特殊资历等
顾客有合作意向时或发放招标文件时，介绍公司产品，了解顾客要求，并结合企业标准进行确定，且明示在合同或订单上，确定顾客对产品的具体要求。
查见销售合同：
密码工程技术人员实训平台安全咨询、安全运维软件测试技术服务合同（已交付）
客户：北京桧城教育科技有限公司
时间：2025 年 2 月 25 日。
服务内容:网络安全咨询服务/网络安全运维服务、软件测试服务
对应审核范围:网络安全咨询服务，网络安全运维服务，软件测试

安全咨询、安全运维及软件测试技术服务合同(已交付）
客户：中创泰和信息技术研究院有限公司
时间：2025 年 3 月 11 日。
服务内容:网络安全咨询服务/网络安全运维服务、软件测试服务
对应审核范围:网络安全咨询服务，网络安全运维服务，软件测试

3、网络安全服务合同(进行中）
客户：北京星立方云科技有限公司
时间：2025 年 1 月 13 日。
服务内容:网络安全咨询服务/网络安全运维服务、软件测试服务
对应审核范围:网络安全咨询服务，网络安全运维服务，软件测试

4、数据安全风险评估报告生成系统软件测试及代码审计技术服务合同(已交付)
客户:贵州亨达集团信息安全技术有限公司
时间：2024 年 7 月 15 日。
服务内容:信息系统风险评估服务、软件测试服务
对应审核范围:信息系统风险评估服务/软件测试

5、数据安全风险评估报告编制平台风险评估及安全审计技术服务合同(已交付)
客户:贵州亨达集团信息安全技术有限公司
时间：2024 年 9 月 11 日。
服务内容:信息系统风险评估服务
对应审核范围:信息系统风险评估服务

6、信息安全技术服务合同(进行中)

客户:北京博创中联科技有限公司
时间：2025 年 3 月 25 日。
服务内容:信息系统风险评估服务
对应审核范围:信息系统风险评估服务
以上合同包含服务要求，服务内容，履行期限、项目验收等内容，满足要求；
为了明确与服务有关的要求，确保公司有能力满足顾客要求；在公司向顾客做出提供产品的承诺之前对产品有关要求进行了评审
经查：近来以来，没有发生合同更改的情况，如果需要更改，需对更改内容重新评审。并将变化的要求及时通知有关人员。
另外，该公司确定并收集了产品质量法、民典法等相关法律法规，将其中的相关要求作为与产品有关要求的补充。该公司目前在销售服务提供过程中没有附加要求。
外部提供的过程、产品和服务的控制-
公司制定并实施《采购控制程序》，用于对质量/环境/安全有影响的采购产品的控制及供方选定、评价。
综合部是采购的归口管理部门。负责组织供方评审、选择和对供方提供服务的控制，对供方提供服务的经济性、及时性质量负责，对物资采购计划的编制及组织实施负责。对供方提供的服务的验证工作负责，对供方质保能力的评价负责。负责对供方生产能力的评价负责。
外包过程：云服务器租赁
提供《合格供方名录》，合格供方包括：河北申石信息技术有限公司、北京国测中培教育科技有限公司、杭州中电安科现代科技有限公司等。
提供《合格供应商导入批准》，供应商评审项目包括：产品质量、交付时间、生产能力、技术能力、售后服务等。评定合格后纳入合格供方名录。
抽查“河北申石信息技术有限公司、北京国测中培教育科技有限公司、杭州中电安科现代科技有限公司”供方评定情况，技术部李经通、销售部张涛、综合部唐晓莉参加了评定，评定结论： 同意列为公司合格供应商。批准：张磊。日期：2025 年 1 月 10 日。
抽查合同签订情况：
——与河北申石信息技术有限公司签订的采购合同
供货内容：东软 NetEye 入侵检测系统*1、东软 NetEye 防病毒网关系统*1、东软 NetEye 日志收集与分析系统*1（含三年的软件版本及特征库升级服务）
合同内容主要包括：合同标的、合同总价及服务、付款、交货、验收标准与方式、双方的权利与义务、知识产权和所有权、违约条款、合同变更、争议解决方式等。合同内容完整、质量要求明确、双方权力义务清晰，有双方盖章，签署规范。
签订日期：2025 年 3 月 26 日
——与北京国测中培教育科技有限公司签订的采购合同
服务内容：国高新、体系认证、信息安全管理体系培训；
合同内容主要包括：咨询服务的内容，范围，形式、甲方责任、乙方责任、违约责任、合同有效期限、解决争议方式等。合同内容完整、质量要求明确、双方权力义务清晰，有双方盖章，签署规范。
——与杭州中电安科现代科技有限公司签订的采购合同
服务内容：专业咨询服务（构建工业控制领域安全合规模型服务）
合同内容主要包括：服务内容及明细、服务价款及支付方式、双方的权利和义务、验收、知识产权、保密、违约责任、适用法律及争议解决等。合同内容完整、质量要求明确、双方权力义务清晰，有双方盖章签字，签署规范。
签订日期：2025 年 4 月 20 日
——与阿里云计算有限公司有限公司签订的电子订单截图
服务内容：云服务器 ECS-包年包月
包年包月-按年(1 年)
服务开始时间：2024-11-07 00:00:00

服务结束时间：2025-11-07 00:00:00
综合部负责人介绍，日常采购的主要内容为办公耗材，主要供应商为天猫、京东自营，为线上采购；采购的日常办公耗材以数量外观等进行初步验收，使用中如有问题会与天猫、京东进行沟通退换货，目前无任何问题。
外部提供的咨询服务、软件及支持性服务，公司采取项目验收的方式进行验收，抽查 2025 年 4 月 5 日“东软 Netye 入侵检测系统、东软 NetEye 防病毒网关系统、东软 NetEye 日志收集与分析系统”设备验收单，验收结论：通过。
外部提供的过程、产品和服务的控制基本符合要求。
生产/服务提供过程、产品和服务放行及交付后活动
公司目前服务的内容主要有：网络安全咨询服务，信息系统风险评估服务，网络安全运维服务，软件测试。
网络安全咨询服务：根据用户安全建设和防护需求，检查客户当前安全状况，提出安全建设方案或者整改方案。
信息系统风险评估服务：参考国家标准，对用户系统安全管理和配置情况进行检查分析，出具风险评估报告。
网络安全运维服务：按照用户安全运维需求提供现场和远程安全配置核查，安全事件监控，事件分析及协助处置等。
软件测试：通过人工或自动化手段验证软件是否满足项目需求，如发现问题，协调建设方进行修正后复测，并出具测试报告。
执行的作业文件有：服务提供控制程序等
执行的流程：
流程：客户需求分析→签订合同→方案设计→采购物资实施技术、服务→测试、验证→甲方验收→运维
依据的标准有：客户要求、合同要求、所咨询服务行业应该执行的相关国家国际标准（规范）、行业标准、地方标准及相关的法律法规要求，如：电信网和互联网大数据平台安全防护要求 YD/T 3800-2020、计算机软件文档编制规范 GB/T 8567-2006、计算机软件测试规范 GB/T 15532-2008、信息技术软件生存周期过程配置管理 GB/T 20158-2006、网络安全等级保护基本要求 GB/T 22239-2019、《计算机软件测试规范 GB/T 15532-2008》等。
产品检验有：验收评审等方式
过程控制情况，
关键过程/需确认过程：方案设计过程。
1、关键过程/需确认过程:提供 2025.1.10 方案设计过程确认记录
--过程概述:研发人员经过培训，人员能达到仿真计算所要求水平。工具材料:电话、传真、电脑、打印机、网络等;服务方法:相关管理制度;
--人员资格鉴定:
■本次确认全过程中的岗位工作人员经过相关培训和考核，具备上岗资格;
■所有岗位工作人员已在本岗位试工作过且获得认可。
--过程方法鉴定;
■部门已将管理制度发放到相关岗位;
■全过程中岗位工作人员确实已按照调试管理制度的方法进行执行。
■对公司的调试具有指导作用，适宜。
--设备鉴定
■制定了年度的设备维修保养计划，并按照计划进行实施;
■办公设备、网络均正常运行，能满足工作需求。
--过程控制：
服务中规定要控制的要求：
已按调试管理制度执行
--结论：■过程能力充分，达到实现所策划的结果的能力;

过程确认人员签字/日期：李经通　　2025.1.10
总经理签字/日期：张磊　　2025.1.10
服务主要为服务报告的编写，详见 Q8.3
现场查看，正在进行中的项目北京博创中联科技有限公司(信息系统风险评估服务)、北京星立方云科技有限公司（网络安全咨询服务，网络安全运维服务，软件测试）技术部正在进行对应工作的资料准备。
提供北京桧城教育科技有限公司密码工程技术人员实训平台项目运维服务记录：
基本信息
巡检日期：2025 年 05 月 1 日
巡检时间：09 时 00 分 至 11 时 30 分
巡检人员：冯河
巡检方式：远程 VPN 连接
巡检地点：通过 VPN 远程访问数据中心机房设备
网络设备巡检情况：正常
服务器巡检情况：正常
应用系统巡检情况:教学管理系统/实验环境应用系统/用户身份认证系统,正常
数据资产巡检情况：教学课件库/实验案例数据/学生信息数据库/系统配置数据正常；
巡检总结：总体情况：本次通过远程 VPN 连接巡检的网络设备、服务器、应用系统及数据资产均运行正常，各项指标处于合理范围内，机房环境参数符合设备运行要求。
在适当阶段进行监视和测量，以验证过程或输出的控制及产品和服务的接收准则已得到满足；
提供 2025.03.10 项目服务考核记；对关键技术人员从工作态度、职能履行、工作绩效等维度进行考核打分，均合格；
提供 2025.03.10 服务过程质量控制和检查记录表，对服务人员从服务人员仪表、标识的佩戴情况、服务设施维护使用及完好情况等 16 项维度进行打分考核，服务人员均合格；
使用适宜的设备和过程环境；
公司主要办公设施：电脑、打印机等，基本满足要求。
过程环境：详见 7.1.4 审核记录
指派胜任的人员，企业人员有多年网络安全咨询服务，信息系统风险评估服务，网络安全运维服务，软件测试经验，经确认符合要求。
实施防止人为错误的措施：
通过流程、作业文件的培训，现场指导的方式 防止人为错误。方案（报告）、通知等编制过程的控制由各自项目组人员检验合格后，在经负责人审批批复，方可放行。
定稿的文件必须经项目经理确认后方可交付。
交付，报告采用快递或者技术人员送至客户指定地点；
交付后活动:针对报告内容，在合同约定期限内，提供技术咨询及解答，提供远程安全意识培训，提供远程网络安全事件响应咨询等；
提供客户验收报告：
项目名称:数据安全风险评估报告生成系统 软件测试及代码审计；
客户：贵州亨达集团信息安全技术有限公司
验收内容：数据安全风险评估报告生成系统 软件测试及代码审计
见客户及企业盖章，客户方王*签字；企业方魏*签字；
2、项目名称:数据安全风险评估报告生成平台 风险评估及安全审计；
客户：贵州亨达集团信息安全技术有限公司
验收内容：数据安全风险评估报告生成平台 风险评估及安全审计
见客户及企业盖章，客户方王*签字；企业方魏*签字；
满足要求

EMS/OHSMS 环境与安全的运行控制情况：

编制《环境与职业健康安全运行控制程序》、《环境及安全监视和测量控制程序》、《相关方施加影响管理程序》、《废弃物管理程序》、《环境保护责任制》、《固体废弃物管理规定》、火灾应急预案、触电应急预案等，策划合理，内容符合标准要求。通过管理制度对环境职业健康安全进行控制，基本适用。

综合部是运行控制的主控部门。

公司确定的重要环境因素为潜在火灾、固废排放；不可接受风险为潜在火灾、意外伤害。

围绕重要环境因素和不可接受风险，综合部对环境安全运行情况控制情况如下：

查看运行情况：

1、资源能源消耗：查看办公区域宽敞明亮，通风较好。员工所用饮水机定期清洗。主要消耗的办公用品是纸张，废纸回收再利用。水电的消耗，办公室均使用节能灯,做到人走灯灭；洗手间无滴水浪费现象。目前建立了相应和管理制度，要求各部门人员提高节约意识。

2、火灾管理，主要包括：线路老化；违规吸烟；物品不合理堆放；消防设施失效；人走未断电等。管理方案：对公司人员进行教育培训，增强员工的消防安全、环保意识。配备足够的消防器具。定期检查电器设备的使用及老化情况。建立应急预案并定期演练。2025 年 3 月 5 日组织进行了消防应急演练。

3、意外伤害，主要包括：外出办公违章驾驶、疲劳驾驶等；管理方案：组织培训交通规则，要求外出严格按照交通规则执行；加强对外出人员的管理，要求其必须乘坐正规的交通工具；建立健全安全责任制，加强各部门人员的自我安全管理；禁止在雨雪台风等恶劣天气的时候外出；施工现场准守安全规章制度，合理佩戴安全防护措施，定期对人员进行安全教育。2025 年 3 月 19 日进行触电应急预案演练。

4、固废管理：废弃包装物、废弃的废墨盒、硒鼓、防疫物资的遗弃等，管理方案：确定控制部门和人员职责；组织控制岗位人员培训；设置收集点或固废物回收容器,进行分类收集(可回收、不可回收、有毒有害)；识别可回收、不可回收、有毒有害废弃物；综合部组织每月对控制部门进行定期监控；生活垃圾由物业处置。

5、废水：主要为办公、生活污水的排放：直接排入市政污水管网，无工艺废水。

6、与员工签订劳务劳动合同。抽查刘春国、唐晓莉、张涛劳务合同。内容包括：劳务合同双方当事人基本情况、劳动合同期限、工作内容和工作地点、工作时间和休息休假、劳动报酬、劳动保护、劳动条件和职业危害防护、劳动合同的解除、终止和经济补偿、劳动争议处理及其它等内容。有员工签名和单位公章。

7.查见《北京市社会保险个人权益记录(单位职工缴费信息))》，为全体员工缴纳养老、医疗、失业、工伤、生育保险。

8、环境安全运行检查：

提供《环境检查记录》，抽查 2025 年 1 月、2025 年 3 月、2025 年 6 月《环境检查记录》，检查项目：固体废弃物处理、水电等能源使用、办公用品使用、生活垃圾处理、部门环保意识培训、环保、安全标识、文件培训、消防器材齐全、有效、消防器材检查、保养、消防作业演练、生活污水的排放、噪声的排放、废气的排放等；检查结果节约用纸、碳粉盒、墨盒、废旧电池、灯管分类回收保管、无人为敲击和长时间大声喧哗、办公区无扬尘产生、办公固废垃圾已进行分类、没有污水随意排放问题、有无长明灯、或开关损坏、空调温度是否按规定使用、有无未关水龙头或水管漏水的、办公设备运转是否正常,有无异常噪音。检查结论：合格。检查人：综合部；内容完整，符合要求。

提供《安全检查记录》，抽查 2025 年 1 月、2025 年 3 月、2025 年 6 月《安全检查记录》，检查项目：应保持整洁，禁止乱拉电线、电话线等，地面、走道和楼梯应无松动的物体、废纸篓、瓶子等。房间所有部分应能保持无障碍通行。不得私自维修任何电器设备，应由专业人员进行。电线和插座应得到良好的维护，插座无松动、绝缘无磨损。电源线应整齐规范布线，临时接线插座应无绊人或遇水短路可能。电器设备在不用时应关闭电源。禁止挪用消防器材。临时用电必须规范，各种电源线布线应整齐、规范、无老化、裂纹等现象。吸烟应到指定区域，在允许吸烟的场所应提供烟灰缸；禁烟区应张贴“禁止吸烟”的警告标志。办公区域不得放可燃包装品、材料、废品等。检查结论：合格。检查人：综合部；内容完整，符合要求。

查见《固体废弃物分类处理表》，类别：不可回收固废；具体内容：各种生活垃圾；临时存放：各地垃圾桶；处理方法：委托环卫处理；其余分类有害固废、可回收固废均有处理规定；

9、查见《劳动保护用品发放记录》。主要是发放口罩、手套等，每月发放一次，有领用记录。工作时间平

均每天不超过 8 小时。
11、与部门负责人沟通企业水电费随物业费缴纳。每月定期缴纳水电费，物业费按年缴纳；
12、查员工体检：部门负责人介绍，因工作场所内不涉及职业病危害因素，所以，未组织员工进行职业病体检。
组织员工进行普通体检。
抽查李喜冬体检报告，体检日期 2025 年 6 月 9 日，体检医院：北京瑞慈瑞海综合门诊部。
抽查李经通体检报告，体检日期 2024 年 9 月 7 日，体检医院：北京美年美佳门诊部。
抽查冯河体检报告，体检日期 2024 年 9 月 20 日，体检医院：北京瑞慈瑞海综合门诊部。
13、用于环境及职业健康安全资金投入情况：2025 年 1-6 月投入包括员工社保、员工体检、劳保用品、培训、水电费等合计 194000 元。能保证环境、职业健康安全资金的使用。
查看，手提式干粉灭火器、烟感报警器、喷淋系统、消防栓（物业提供）等应急救援器材，灭火器、消防栓（物业提供）维护保养良好。现场平面设置应急、安全警示标牌齐全，由物业统一管理。编制火灾应急预案，对员工进行了防火安全的培训。现场无安全隐患。有效。
与负责人交流得知：公司管理层始终把安全工作放在所有工作的首位，长期以来采取多种措施，致力于消除危险源，降低职业健康风险。据了解，从未发生过环境和职业健康安全方面的事故事件。
规定了变更管理控制要求，规定了当发生新的产品/服务和过程，或对现有产品/服务和过程的变更（包括：工作场所的位置和周边环境；工作组织；工作条件；设施；工作人员数量），法律法规要求和其他要求的变更，有关危险源和职业健康安全风险的知识或信息的变更，知识和技术的发展。应评审非预期性变更的后果，以及需要应对的风险和机遇，必要时采取适当的控制措施，符合标准和企业实际。负责人介绍说，目前没有发生影响职业健康安全绩效的临时性和永久性变更。因此，没有进行更改管理。
经现场确认，工作场所内无职业病危害因素。对环境职业健康安全的运行控制基本有效。
基本符合要求。

3.3 内部审核、管理评审的有效性评价☐符合 ☑基本符合 ☐不符合

经调阅相关记录确认，企业在 2025.04.18 策划和实施了完整的内审。内审员经过了标准培训，对内审方案进行了有效策划，规定了审核准则、范围、频次和方法，并得到了有效实施。内审记录清晰完整，并表明内审员具备必要的能力和能够保持独立性，提出了 1 项不符合，形成内部审核不合格报告，判标准确，对不符合项责任部门进行了分析原因、采取纠正、纠正措施并验证了有效性。已于 2025.04.21 进行有效整改并验证关闭；内审报告表述清楚，对质量环境职业健康安全管理体系的符合性和运行有效性进行了评价，并得出结论意见，基本符合标准要求。
审核现场与企业内审员沟通，该两名内审员对内审知识比较欠缺，还需要加强持续培训学习。对于能力方面开具的不符合。
企业最高管理者在 2025.05.21 进行了管理评审，管理评审由总经理主持，管理评审目的明确，输入充分，管理评审记录表明评审真实有效，管理评审输出提出 1 项改进建议，于 2025.05.26 完成。管理评审真实有效。
现场与总经理交流管理评审控制情况，其对管评流程，包括管评策划、管评输入内容、输出内容、改进项及其纠正措施情况等不是特别熟悉，是在咨询老师帮助下完成的额管理评审，现场交流。建议后期加强此方面的学习，持续关注管评工具的运用，管评的深入程度方面需持续关注。

3.4持续改进 ☐符合 ☑基本符合 ☐不符合

1）不合格品/不符合控制
策划保持《不合格输出控制程序》，规定了发现不合格应采取纠正措施的具体要求，并按要求进行了控制，基本符合企业实际和标准要求。
2）纠正/纠正措施有效性评价：
内审发现的不符合，形成内部审核不合格报告，有原因分析，措施，实施及有效性验证等。管理

评审中的改进，制定有措施单。日常中发现的不符合，公司通过实施纠正措施，要求相关部门举一反三也检查自己的工作，消除同类型错误的原因。基本有效。总体上看，公司纠正及改进机制已形成，能够形成自我完善自我提高的良性循环机制。自体系运行以来组织未发生顾客投诉和质量、环境和安全事故。基本符合要求。

3）投诉的接受和处理情况：

建立了对外交流的渠道，可接收外部投诉及建议，年度无质量环境安全事故发生，也没有发生相关方投诉，现场也没有发现顾客投诉资料。基本符合要求。

3.5 体系支持 ☐符合 ☑基本符合 ☐不符合

1）资源保障（基础设施、监视和测量资源，关注特种特备）：

现场与企业人员沟通，公司位于北京市朝阳区容创路 17 号楼-3 至 8 层 101 号 7 层 710，总人数共计 17 人，其中管理人员 4 人，其他职员 13 人。

建筑面积 328 平方米。无库房。此场所为租赁性质，出具了租赁合同；出租方：北京时代凌宇科技孵化器有限公司；租赁期：两年，自 2024 年 7 月 16 日至 2026 年 7 月 15 日止。

公司办公设备设施：配置有电脑、服务器、网络、打印机、办公桌椅、空调等。其维护保养由供应商进行，现场观察设备运行正常，设备能力稳定。

网络安全咨询服务，信息系统风险评估服务，网络安全运维服务，软件测试使用的系统、工具等；

台式机、笔记本、服务器、路由器、5G 上网设备、iKuai AP、电视、门禁、会议设备、二层交换机、打印机、手机、windows11、centos7、mysql、Nmap 资产扫描工具、aircrack－ng 无线网络扫描工具、SQLmap 数据库注入测试工具、Burp Suite 定制攻击工具、Wireshark 网络抓包分析工具、Nessus 漏洞扫描工具、Xshell 远程访问工具

特种设备：无。

监视测量设备：无硬件，软件有 Wireshark 网络抓包分析工具、Nessus 漏洞扫描工具、Nmap 资产扫描工具

办公通信设备：网络、电脑、电话等。

支持性设施：企业名下没有车辆，业务往来联系采用打车方式进行，文件类的资料主要采取快递的形式。公司无食堂。

环境职业健康安全设备设施：消防栓（走廊物业维护）、灭火器、垃圾桶等。

办公室内设备布置合理，通道畅通，照明设施齐全，均配备了空调、消防设施等设施，作业场所光线较充足。目前工作环境符合经营需要。

运行环境及资源满足组织的要求。

2）人员及能力、意识：

企业规定了工作人员岗位任职要求，另有人员能力评价表，在教育、培训、技能与经验方面要求做出规定。根据任职要求，对各岗位人员进行了能力评定，评定结果均符合岗位任职要求。企业为确保相应人员具备应有的能力和意识所采取的措施基本充分有效。企业相关人员基本具备相应能力和意识。基本符合要求。

3）信息沟通：

企业在手册中规定了沟通内容，包含沟通的对象、沟通的主责部门、沟通的内容、方式等内容，符合标准要求。使各部门了解信息沟通渠道及要求,便于组织内各部门的协调，以确保管理体系的有效性进行。沟通内容包括：内部信息和外部信息，信息沟通渠道畅通。基本满足要求。

4）文件化信息的管理：

文件化信息的管理：公司编制了管理体系文件，按体系文件结构包括：管理手册、程序文件汇编、管理文件汇编等。其中方针、目标也形成了文件并纳入到管理手册中。文件覆盖了组织的管理体

系范围，体现了对管理体系主要要素及其相关作用的表述，并将法律法规和标准的要求融入到体系文件中。文件的审批、发放、更改订控制有效。经现场确认，该公司的体系文件基本符合据GB/T19001-2016、GB/T24001-2016、GB/T45001-2020 标准要求，体现了行业和企业特点，有一定的可操作性和指导意义。

四、被认证方的基本信息暨认证范围的表述

E:网络安全咨询服务，信息系统风险评估服务，网络安全运维服务，软件测试所涉及场所的相关环境管理活动

Q:网络安全咨询服务，信息系统风险评估服务，网络安全运维服务，软件测试

O:网络安全咨询服务，信息系统风险评估服务，网络安全运维服务，软件测试所涉及场所的相关职业健康安全管理活动

五、审核组推荐意见:

审核结论：根据审核发现，审核组一致认为，北京国测信安科技有限公司

☑质量☑环境☑职业健康安全☐能源管理体系☐食品安全管理体系☐危害分析与关键控制点体系：

审核准则的要求	☐符合	☑基本符合	☐不符合
适用要求	☐满足	☑基本满足	☐不满足
实现预期结果的能力	☐满足	☑基本满足	☐不满足
内部审核和管理评审过程	☐有效	☑基本有效	☐无效
审核目的	☑达到	☐基本达到	☐未达到
体系运行	☐有效	☑基本有效	☐无效

通过审查评价，评价组确定受审核方的管理体系符合相关标准的要求，具备实现预期结果的能力，管理体系运行正常有效，本次审核达到预期评价目的，认证范围适宜，本次现场审核结论为：

☐推荐认证注册

☑在商定的时间内完成对不符合项的整改，并经审核组验证有效后，推荐认证注册。

☐不予推荐

北京国标联合认证有限公司

审核组：王冰、岳艳玲

被认证方需要关注的事项

（本事项应在末次会议上宣读）

审核组推荐认证后，北京国标联合认证有限公司将根据审核结果做出是否批准认证的决定。贵单位获得认证资格后，我们的合作关系将提高到新阶段，北京国标联合认证有限公司会在网站公布贵单位的认证信息，贵单位也可以对外宣传获得认证的事实，以此提升双方的声誉。在此恳请贵公司在运作和认证宣传的过程中关注下列（但不限于）各项：

1、被认证组织使用认证证书和认证标志的情况将作为政府监管和认证机构监督的重要内容。恳请贵单位按照《认证证书和认证标志、认可标识使用规则》的要求，建立职责和程序，正确使用认证证书和认证标志，认证文件可登录我公司网站查询和下载,公司网址：www.china-isc.org.cn

2、为了双方的利益，希望贵单位及时向我公司通报所发生的重大事件：包括主要负责人的变更、联系方法的变更、管理体系变更、给消费者带来较严重影响的事故以及贵单位认为需要与我公司取得联系的其他事项。当出现上述情况时我公司将根据具体事宜做出合理安排，确保认证活动按照国家法律和认可要求顺利进行。

3、根据本次审核结果和贵单位的运作情况，请贵公司按照要求接受监督审核，监督评审的目的是评价上次审核后管理体系运行的持续有效性和持续改进业绩，以保持认证证书持续有效。如不能按时接受监督审核，证书将会被暂停，请贵单位提前通知北京国标联合认证有限公司，以免误用证书。

4、为了认证活动顺利进行，请贵单位遵守认证合同相关责任和义务，按时支付认证费用。

5、认证机构为调查投诉、对变更做出回应或对被暂停的客户进行追踪时进行的审核，有可能提前较短时间通知受审核方，希望贵单位能够了解并给予配合。

6、所颁发的带有 CNAS（中国合格评定国家认可委员会）认可标志的认证证书，应当接受 CNAS 的见证评审和确认审核，如果拒绝将会导致认证资格的暂停。

7、根据《中华人民共和国认证认可条例》第五十一条规定，被认证方应接受政府主管部门的抽查；根据《中华人民共和国认证认可条例》第三十八条规定在认证证书上使用认可标志的被认证方应配合认可机构的见证。当政府主管部门和认可机构行使以上职能时，恳请贵单位大力配合。

违反上述规定有可能造成暂停认证以至撤销认证的后果。我们相信在双方共同努力下，可以有效地避免此类事件的发生。

在认证、审核过程中，对北京国标联合认证有限公司的服务有任何不满意都可以通过北京国标联合认证有限公司管理者代表进行投诉，电话：010-58246011；也可以向国家认证认可监督管理委员会、中国合格评定国家认可委员会投诉，以促进北京国标联合认证有限公司的改进。

我们真诚的预祝贵单位获得认证后得到更大的发展机会。