**重庆中烟工业有限责任公司信息安全运维系统建设合同**

合同编号：

签订日期：

签订地点：

甲方：重庆中烟工业有限责任公司

乙方： 东华软件股份公司

甲乙双方在相互信任、相互支持的基础上，本着诚实信用、平等互利的原则，经友好协商，就甲方安全信息系统建设事宜签署本合同,以资共同遵守：

第一条 服务内容与范围

1.1服务要求:（见服务方案）

1.2 服务内容：（见服务方案）

1.3服务地点：重庆中烟工业有限责任公司公司指定地点

第二条 履行期限

2.1服务期限要求： 项目整体建设周期为15个月。其中9个月内完成设计、开发、实施、部署、初验，初验后进入 6 个月的试运行期，试运行期结束后，进行项目终验。

第三条 费用及支付方式

3.1 合同总金额（含税）：为中标金额 ￥

3.2 支付方式：

乙方开具税务监章的有效增值税专用发票后，甲方将按以下方式支付费用：

3.2.1在软件完成定制开发、安装、调试并初验合格后30个工作日内支付合同金额50%。

3.2.2终验合格并交付需求规格说明书及评审记录、概要和详细设计说明书及评审记录、测试报告、试运行报告、用户使用手册、系统维护手册、源代码、验收报告等相关技术文档后30个工作日内支付合同金额45%。

3.2.3合同金额的5%作为质量保证金，在一年质保期满后，如无服务和产品质量问题则支付合同总金额的5%。

3.2.4若增值税专用发票税率受国家税收政策调整变化，则不含税价不受税率变化影响并以此为基础计算税额进行结算；否则，凭乙方开具的符合规定的发票，并扣除因此对甲方造成的损失后进行结算。

3.3 本合同项下的全部款项,甲方应按银行转账方式支付。乙方开户行账号如下：

单位名称：东华软件股份公司

纳税识别号：911100007226188818

开户银行：北京银行中关村科技园区支行

银行账号：01090879400120105069382

3.4乙方按中标金额10%交纳履约保证金，项目终验结束之日起30日内，由甲方不计息退还乙方履约保证金，如履约保证金被扣减，则扣减部分不予退还。

第四条 甲方的权利义务

4.1 甲方有责任委派专人与乙方的服务人员一起协调系统建设服务关联成员单位及相关部门。

4.2 甲方提供信息安全系统建设服务工作试运行所需要的工作环境。

4.3 甲方应向乙方提供本项目所涉及的硬件配置、数量需求，并配合乙方获取信息安全系统建设服务所需的相关数据及双方认可的相关配合，以方便乙方开展服务工作。

4.4 甲方应负责安排接受本项目各种培训的人员，保证其按时参加培训。

4.5 甲方应承担保守乙方的技术秘密和商业秘密的要求。

4.6 甲方有权对乙方工作进行监督、审查，并提出意见或建议。如甲方认为乙方指派的服务人员不能胜任工作的，乙方应按照甲方要求及时更换人员。

4.7 甲方按照本合同约定向乙方支付合同款项。

第五条 乙方的权利义务

5.1乙方提供的服务分阶段实施。在分阶段实施过程中，乙方应及时向甲方提供各子阶段的工作成果并经甲方认可。上一阶段的工作成果经甲方书面确认后，乙方方可进入下一阶段的服务工作。

5.2在本合同签订后两日内，乙方应根据其提交的工作计划向甲方提交更为详细和具体的实施进度安排表，经甲方同意后，严格按表执行。

5.3乙方原则上应在实施进度安排表规定的期限内完成本项目全部服务工作，若确因技术等客观原因无法按规定进度完成的，乙方应提前 15 日向甲方提出延期申请，经甲方同意后，可以顺延。逾期未完成的，除非甲方同意继续实施本项目，否则按本合同约定处理。

5.4 乙方有权根据本合同的规定和服务需要，向甲方了解与本项目有关情况，调阅有关资料。对此甲方应该予以积极配合，向乙方提供有关信息和资料。甲方向乙方提供的信息和资料，乙方保证用于且仅用于本项目，不得向任何第三方扩散或用作其他用途。

5.5乙方有权利在按照合同向甲方提供服务后，要求甲方按照本合同第三条约定支付相应款项。

5.6 乙方须保证遵守甲方的相关保密规定，未经许可不得复制、带走和传播本项目的技术方案和资料，以及涉及的其他信息。

5.7 乙方在系统评审时须向甲方提供本项目的完整文档、记录资料。甲方保证相关文档资料仅用于本项目，不得向任何第三方扩散或用作其他用途。

5.8本系统上线前必须符合《烟草行业网络完全基线安全规范》检查条件，终验前也必须符合《烟草行业网络完全基线安全规范》才能进行验收。本系统定级为二级等保，终验时需提供第三方检测机构出具的二级等保证书，相关检测费用由乙方承担”。

第六条 项目移交

6.1交付时间：乙方应在进行每项交付前10个工作日内，以书面方式通知甲方。甲方应当在接到通知后的3个工作日内安排接受交付。乙方在交付前应根据甲方检测标准对该交付件进行测试，以确认其符合本合同的规定。如由于甲方的原因而导致交付不能按照规定的时间进行，乙方将按延期时间顺延交付。如因延期交付而导致乙方损失，甲方应赔偿乙方的实际损失。如甲方能接受而不接受交付，则视为乙方已经交付，甲方应当按照约定付款，甲、乙双方对此另有约定的除外。

6.2交付内容：乙方应按照合同所约定的内容进行交付，所交付的文档与文件应当是电子版式和可供人阅读的。如由于甲方运行、检测不当或其它原因而导致所交付项目存在故障或问题，经甲方要求，乙方应在10个工作日内帮助处理此项故障或问题。

第七条 领受

甲方在领受了上述交付件后，应立即对该交付件进行测试和评估，以确认其是否符合开发软件的功能和规格。甲方应在10个工作日内，向乙方提交书面说明以表示接受该交付件。如有缺陷，应递交缺陷说明及指明应改进的部分，乙方应立即纠正该缺陷，并再次进行测试和评估。甲方应于10个工作日内再次检验并向乙方出具书面领受文件或递交缺陷报告。甲、乙双方将重复此项程序直至甲方领受。

第八条 项目验收

8.1初验：乙方应于签署本合同9个月内，完成系统功能的设计、开发、安装和调试后，向甲方提请验收，经甲方对系统各项功能、性能均达到本合同规定和不低于针对招标文件的技术要求，视为初验合格。初验合格后，甲、乙双方签署《初验合格报告》。如验收不合格，则乙方应按照甲方要求进行重新开发调试直至验收合格。

8.2试运行：试运行于《初验合格报告》签署之日开始，时间周期为6个月，试运行结束后，系统运行正常，甲、乙双方签署《试运行合格报告》。进入试运行阶段，因乙方原因使系统运行不能达到合同要求或甲方使用需求的，甲方以书面方式要求乙方予以整改，直至达到合同要求，同时试运行期限顺延，顺延时间为解决问题所花费的时间，由此引发的所有责任与不利后果均由乙方承担。如因乙方原因使系统运行不能达到合同要求且超过30个工作日仍未解决，则甲方有权解除本合同，并要求乙方赔偿因此造成的损失（包括但不限于直接损失、间接损失、律师费、诉讼费等）。

8.3 终验：项目终验在试运行期满并系统运行无故障后，乙方提交本项目全部终验所需的各项工程技术文档后10个工作日内进行。项目终验方式由甲、乙双方协商，甲方最终予以确定。终验合格后，甲、乙双方签署《终验合格报告》。如终验不合格，则按本合同的约定办理，质量保证期相应顺延，且乙方应承担由此给甲方造成的损失（包括但不限于直接损失、间接损失、律师费、诉讼费等）。项目终验文档包括但不限于以下内容：

（1）项目需求规格说明书

（2）概要设计

（3）详细设计

（4）测试报告

（5）初验报告

（6）试运行报告

（7）项目技术文档（用户使用手册、维护手册等技术文档）

（8）源代码（指定制开发软件）

（9）终验报告

第九条、服务承诺要求

9.1技术咨询

乙方应在实际操作过程中提供指导，并解决系统在使用过程中出现问题，同时须向甲方提供解决问题的方法、建议和其它信息．其中主要包括：软件系统答疑，系统功能介绍，系统使用技巧，系统框架结构说明，用户关心的系统其它问题的答疑，系统升级说明等。

9,2系统开发

9.2.1系统开发自合同签订之日起，乙方应履行其在开发计划中所规定的义务，按时完成并交付给甲方。

9.2.2乙方应依据标书和用户的要求进行系统详细设计，项目过程中任何改进与调整须与用户方协商一致；

9.2.3乙方应按照评审后的《详细设计说明书》和《开发计划》进行开发，依据开发计划分阶段达成，每个阶段的任务完成后，应及时进行检测和交付，交付成果物应与系统设计中的成果物完全一致，并由甲方和乙方代表确认并签字。

9,3系统集成

9.3.1乙方应根据招标要求，实现与相关的原有应用系统的集成，并进行集成测试，测试结果应作记录，同时该记录应在移交测试合格后的10个工作日内由甲方和乙方代表确认并签字。

9.3.2乙方应安排至少1名运维人员应从系统建设开始即需参加开发、集成工作。负责所开发集成系统的日常运维，确保系统达到正常工作状态。对所开发集成系统生成的报表、告警、安全事件等的情况进行归纳和日常分析，并对处置情况进行跟踪、协调，以确保系统工作的有效性。

9,4安装及系统测试

9.4.1 乙方应在安装工作开始前1周向甲方提供2份有关合同系统安装的技术文件。

9.4.2 如果甲方现场环境没有按时达到本合同规定的条件或甲乙双方共同认可的标准，安装和调试也将作相应的推迟，甲方应在约定的预计日期前1周通知乙方，乙方应根据甲方的要求调整时间进度表。

9.4.3 应用系统的安装和系统测试应由甲乙方人员严格按照乙方安装及测试的技术程序执行。

9.4.4 甲方应提供足够的和合格的技术人员配合应用系统的安装及系统测试。

9.4.5 测试应由甲方的技术人员在乙方人员的指导和协助下按照有关测试规定进行。测试结果应作记录，同时该记录应在移交测试合格后的10个工作日内由甲方和乙方代表确认并签字。

9.4.6 如果甲方确认所有合同系统指标都达到验收的要求，测试验收报告应在测试合格后的3个工作日内由甲方和乙方代表签署。测试验收报告一式二份，双方各执一份。

9,5系统上线及试运行

9.5.1 在实施部署完成后，将进行系统上线和试运行工作。

9.5.2 为了监控系统的详细运行情况，系统须进行6个月的试运行。试运行期间应用软件的功能和性能应符合重庆中烟工业有限责任公司信息安全运维系统项目设计要求。

9.5.3 如果在试运行期内的任何时刻发现任何合同系统与本合同约定的不符之处，甲方有权按照如下方式解决：

 如果应用系统在功能和性能上不能满足甲方现场要求，同时不超出项目集成实施服务合同的功能范围，乙方应当尽快进行软件修订和更新。

9.5.4 在试运行阶段，乙方应在甲方配合下进行系统的联调测试。如果甲方确认所有合同系统指标均达到终验的要求，则联调测试合格。联调测试合格后，甲方应及时组织终验，乙方应积极配合，甲方和乙方的授权代表应在终验通过后签署终验报告。

9.2培训服务

乙方对甲方培训操作和使用该系统，并使甲方操作人员明白使用该系统所能带来的帮助；系统培训师在项目计划阶段为我方建立符合需求的、完善的培训计划，帮助用户安全熟悉软件系统。培训内容主要包括：系统总体框架以及模块划分介绍，各单元模块的使用操作方法培训，系统的安装、调试方法培训，系统配置、使用的注意事项，与系统相关的其它软硬件知识的培训和指导。

9.3 系统维护

9.3.1系统维护工作主要包括以下主要内容：

提供安装服务，安装时设定软件系统缺省状态，向甲方传授必备的操作技术，将软件错误的发生率降到最低，提供对数据管理操作的建议帮助用户更好的处理数据。其中包括：为甲方设定数据文件，管理磁盘存储设备，备份并存档所有技术支持活动，对软件本身存在的问题（新的需求除外）免费提供补丁，故障诊断等。

9.3.2本项目质保期为1年，质保期内乙方必须负责免费维护及必须免费提供系统功能优化完善、营销活动支持所需的技术支持和服务。

9.3.3乙方应向甲方提供运行维护服务的有关技术支持，提供24小时维护技术服务响应，乙方保证甲方可以得到7×24小时的实时技术支持响应。投标人应提供热线电话、Email、传真等其它咨询服务渠道随时回答甲方的各种问题。

9.3.4乙方在出现系统故障后的2小时内给予问题解答,在8小时内派技术人员到达现场解决问题。

9.3.5乙方须向甲方承诺质保期满后，将继续提供维护工作，质保期满后的服务的方式、范围和收取的费用标准以后续协议为准。

第十条 知识产权

10.1 本合同履行过程中，甲方提供给乙方的所有资料（包括但不限于文案、图片、视听资料等）的所有权和知识产权归甲方所有，未经甲方同意，乙方不得将该等资料用于本合同之外的目的，也不得提供、许可第三方使用。

10.2 本合同履行过程中产生的咨询内容等智力成果的所有权和知识产权归甲方所有，未经甲方同意，乙方不得将该等智力成果用于本合同之外的目的，也不得提供、许可第三方使用。

10.3 乙方保证，根据本合同向甲方提供的技术和服务不会侵犯任何第三人知识产权或其他权利，否则，因此给甲方造成损失的，乙方应当赔偿甲方的全部损失（包括但不限于赔偿金、罚金、律师费、诉讼费等）。

第十一条 保密

11.1 保密范围

11.1.1 本合同项下的所有条款。

11.1.2 乙方工程师在维护过程中接触到的甲方系统软件的相关信息及甲方其他经营管理信息，甲乙双方为履行本合同向对方提供的一切资料及合同的一切条款。

11.2 保密责任

11.2.1 双方负责确保其雇员和受雇第三方严格遵守保密义务。

11.2.2 乙方承诺绝对保密任何有关甲方的资料。

11.2.3 甲乙双方应保守在履行本合同过程中知悉的对方的商业秘密以及其他保密信息，未经对方事先书面同意，任何一方不得以任何形式向第三方泄露或采用任何方式使用或许可他人使用该商业秘密以及其他保密信息。

第十二条 违约责任

12.1 乙方擅自使用或向任何第三方泄露其在合同履行中获悉的甲方的秘密或不为公众知悉的信息的，甲方有权解除合同，并有权要求乙方向甲方赔偿由此给甲方造成的一切损失。

12.2乙方在履行合同过程中发生侵害第三方权利的，相关争议由乙方负责解决，相关法律责任亦由乙方承担；如甲方由此遭受损失的，乙方应给予全额赔偿。

12.3乙方应对其指派在甲方工作场所服务人员所有行为负责，乙方或乙方工作人员的行为给甲方造成任何损害的，由乙方承担赔偿责任。

12.4 如乙方未按本合同约定定期完成工作，甲方可要求乙方立即履行。每出现一次违约情况，乙方应向甲方支付本合同总金额【5%】的违约金，如出现三次以上，甲方有权解除合同，并要求乙方赔偿全部损失。

12.5 甲、乙双方中任一方不履行和违反本合同约定的任何条款均属违约行为，违约金额按合同金额5%计算，违约一方除按本合同约定承担违约责任外，并应赔偿守约一方由此受到的全部损失。

第十三条 争议解决

履行本合同发生争议时，双方应协商解决；协商不成可向甲方所在地人民法院起诉。

第十四条 合同的变更

14.1 双方协商一致的，可以变更、解除本合同。

14.2 本合同的变更或解除，必须采用书面形式。

第十五条 合同生效及其他

15.1 如果本合同的任何条款在任何时候变成不合法、无效或不可强制执行而不从根本上影响本合同的效力时，本合同的其它条款不受影响。

15.2 本合同各条标题仅为提示之用，应以条文内容确定各方的权利义务。

15.3 本合同替代此前双方的所有关于本合同事项的口头或书面的纪要、备忘录、合同和协议。附件是合同不可分割的组成部分，与合同具有同等法律效力。

15.4 甲乙双方因执行本合同或与本合同有关的一切的通知都必须按照本合同中的地址（见签字盖章页）或通讯方式进行。采用信函形式的应采用具有良好声誉的特快专递进行送达。如使用传真或类似的通讯方式，通知日期即为通讯发出日期，如使用特快专递，通知日期即为邮件寄出日期并以邮戳为准。

15.5 本合同由甲乙双方法定代表人或其授权代理人签字并盖章后生效。本合同一式陆份，甲方肆份，乙方贰份，具同等法律效力。

15.6 未尽事宜由甲、乙双方协商解决。

**甲方：**

**签约人：**

**乙方：东华软件股份公司**

**签约人：**

**二、廉政合同**

项目名称：重庆中烟工业有限责任公司信息安全运维系统项目

甲方：重庆中烟工业有限责任公司

乙方：东华软件股份公司

为加强对重庆中烟工业有限责任公司经济活动中的廉政建设和规范管理，防止发生谋取不正当利益的违法违纪行为，保护国家、集体和当事人合法权益，根据国家法律法规及烟草行业有关规定，订立本廉政合同。

一、甲、乙双方责任：

（一）严格遵守国家、地方和烟草行业有关法律、法规和相关政策以及廉洁从业各项要求。

（二）严格执行项目经济合同。

（三）经济活动中必须坚持公开、公平、公正、诚实守信的原则，不得采取任何违法违纪行为损害国家、集体利益和当事人合法权益。

（四）发现对方在经济合同签订和履行过程中有违规、违纪、违法行为的，应向其纪检监察、上级主管部门及司法机关等举报。

二、甲方责任：

甲方人员在经济合同签订和履行过程中应按照有关法律法规和程序开展工作，并严格遵守以下规定：

（一）不准向乙方或乙方的相关方索要或接受回扣、现金、有价证券、贵重物品、挂职工资、津贴、好处费、感谢费等。

（二）不准在乙方和乙方的相关方报销任何应由甲方或甲方人员个人支付的费用。

（三）不准要求、暗示和接受乙方或乙方的相关方为个人装修住房、安排婚丧嫁娶活动及为其配偶、子女、亲属及其他利害关系人安排工作以及出国（境）、旅游等提供方便。

（四）不准参加乙方或乙方的相关方组织的宴请、娱乐和赌博等活动。

（五）不准与乙方或乙方的相关方串通，谋取不正当利益。

（六）不准让配偶、子女、亲属及其他利害关系人参与乙方或乙方的相关方的业务活动，谋取不正当利益。

 (七)不准违反廉洁从业其他相关规定。

三、乙方责任：

乙方(含乙方的相关方)应与甲方保持正常的业务往来，按照有关法律法规和程序开展业务工作，并严格遵守以下规定：

（一）不准以任何理由向甲方的工作人员及其亲属赠送或提供回扣、现金、有价证券、贵重物品、挂职工资、津贴、好处费、感谢费等。

（二）不准以任何名义为甲方或甲方工作人员及其利害关系人报销应由甲方或个人支付的费用。

（三）不准为甲方的工作人员及其亲属装修住房、安排婚丧嫁娶活动或为甲方的配偶、子女、亲属和其他利害关系人安排工作以及为其出国（境）、旅游等提供方便。

（四）不准以任何理由为甲方的工作人员及其亲属和其利害关系人组织宴请、娱乐和赌博等活动。

（五）不准与甲方的工作人员串通，谋取不正当利益。

（六）不准与甲方的工作人员及其配偶、子女、亲属和其他利害关系人开展业务活动，谋取不正当利益。

四、责任追究：

（一）甲方的工作人员有违反本合同规定的，由纪检监察部门按照干部（职工）管理权限，依据国家和行业有关规定给予组织处理或党纪、政纪处分；涉嫌犯罪的，移交司法机关依法追究法律责任；给乙方单位造成经济损失的，应予以赔偿。

（二）乙方或乙方的工作人员有违反本合同规定的，甲方有权视情节轻重终止或解除经济合同并追究其违约责任，给甲方造成经济损失的，应予以赔偿，同时，将永久性的取消乙方参与甲方工程、物资和服务采购项目的资格。涉嫌犯罪的，甲方将向项目所在地司法机关报案，追究乙方及乙方相关人员的法律责任。

 五、附则：

（一）本合同作为经济合同的补充条款，具有同等法律效力，经双方签署后立即生效。

（二）凡未签订廉政合同的项目，公司（企业）领导不予审批，审计部门不予审核，财务部门不予拨款。

本合同与经济合同一同归档备查。

甲方（盖章）： 乙方（盖章）：东华软件股份公司

法定（授权）代表人： 法定（授权）代表人：

地址： 地 址：北京市海淀区紫金数码园3号楼15层1501

电 话：　　　 电 话：010-62662288

年　 月　 日　　　　 　　 年 　月　 日

**附件：服务要求和内容**

**一、项目基本情况**

信息安全运维系统项目建设总体需求是：构建行业资产管理、安全管理、运维管理、服务管理等安全运维管理四个中心，实现信息化基础平台和运行在基础平台上的应用系统资产可知、状态可视、运维可管、安全可控。遵循行业CT-155信息化发展框架和公司信息化发展规划对安全运维保障体系的要求，采用统一架构、集中管控的方式，实现对信息系统网络安全和运维工作的全面管控。按照标准化、流程化的方式理顺工作流程，提高工作效率，优化运维资源，有力支撑信息化持续协调健康发展。

信息安全运维系统项目实现如下需求：

（1）服务咨询与设计。基于ISO20000、ISO27001、ITIL运维理念、等级保护、三全工作等标准对公司的运维业务运营组织架构、流程、资产编码等现状进行调研与设计工作；

（2）资产全面管理。支持以项目管理和资产生命周期管理为主线，所涉及供应商、信息化人员、体系文件、知识库等统一管理。同时，打通与安全管理、运维管理关键环节和数据一致性。资产管理要同设备发放、回收、巡检和维修等活动高度关联，实现一处操作多处数据完成变更的功能。对资产数据的新增修改需要增加一个或多个审核环节。支持对不同客户采取不同的资产管理模式和不同的具体实现方法；

（3）安全集中管理。实现应用系统运行环境所涉及的各类IT资源集中监控和统一展示。同时，对现有网络安全产品日志收集和流量回溯，通过网段IP管理、安全策略管理、弱密码检测、渗透攻击预警、业务异常登录预警、威胁情报感知、运维审计、应急管理等功能，实现安全联防联控、安全态势感知；

（4）服务流程管理。基于咨询设计结果，实现符合实际的运营服务流程，包括：事件管理、问题管理、变更管理、发布管理、计划管理、运维权限集中管理、服务报告、服务绩效等；

（5）运维移动应用。信息安全运维系统移动应用作为公司移动平台的一部分，主要实现故障告警及时通知和服务流程快速办理，快速响应效果；

（6）集成能力管理。系统提供多元化的API，如snmp、syslog、webservice等标准接口方式，方便系统间集成和数据交互。主要包括网络安全产品、门户系统、资产管理系统、投资采购系统、短信邮件系统、动力环境监控系统、工控安全管理系统、国家局运维系统等；

（7）服务报告管理。为运维商例会提供服务报告，系统可以根据定义了月、季、年报模板，设置时间让报告自动生成。服务报告内容包括：总体运维情况概述、基本运维工作情况、重点运维工作事项、工作遗留问题、下一步工作计划与改进措施、系统服务情况汇总表，以及服务绩效情况等；

（8）综合大屏展示。实现可定制的集中统一的管理界面，通过与底层技术平台及其它系统的集成，将资产信息、安全态势和管理流程等管控能力在大屏中以直观、具备科技感的方式进行统一展示；

（9）可视化机房监控。支持浏览器访问可视化机房系统的交互操作和浏览。展示效果以直观形式表现机房环境、机柜、空调、独立设备和架式设备，在系统中实现机房环境、机房子区域、机柜、设备、设备端口连接情况和运行告警信息直观展示等。

**二、项目内容**

总体建设内容：运维管理咨询与流程设计、构建行业资产管理、安全管理、运维管理、服务管理等安全运维管理四个中心。

1 运维管理咨询与流程设计

（1）运维管理体系咨询需基于ISO20000、ISO27001、ITIL运维理念、等级保护、三全工作等标准，并参考主要用户的相关IT运维管理制度，对公司的运维业务运营组织架构、运维流程、资产编码、指标体系、安全基线等现状并进行调研、分析，找出存在的问题和不足，并提出改进建议。

（2）需结合实际情况，收集运维管理制度、人员（包括客户及供应商人员）及岗位职责等现状，建立统一集中的运维管理组织机构，科学的人员岗位职责。

（3）需结合实际情况，采用ITIL方法论，进行安全运维管理流程设计，主要包括服务请求、事件管理、问题管理、变更管理、发布管理、运维权限等。

（4）需遵循行业编码标准，制定符合公司的一套编码规范，主要包括：项目合同、组织结构、服务人员、资产设备、配置模型、工单流程等。

（5）现有重庆中烟相关用户集成需求梳理，对用户已有或预期需要监控的相关信息化设备、系统等进行梳理，按用户的要求对接口方式、监控内容等进行明确，作为本项目的集成需求。

（6）需结合现有指标体系，制定符合公司的一套指标体系，主要包括资产配置指标体系、监控指标体系、运维人员评价体系、供应商评价指标体系等。

（7）需结合现有安全基线管理办法，制定符合公司的一套安全基线体系，并通过与网络安全产品结合，实现对IT资产的安全基线审计、异常提醒、安全处置等闭环管理。

2 资产管理中心

2.1 项目管理

项目管理实现对信息化项目的全过程管理，主要包括可研分析、预算管理、立项管理、投资计划管理、招投标管理、项目过程管理等模块。其中项目立项、计划、招投标信息需与投资采购项目集成对接，确保项目信息一致。项目过程管理模块提供了对软件开发、软硬件采购、运维、服务等不同类型的项目特点，分别进行过程文档的收集、流程审批和付款管理等功能。系统支持为项目建设相关单位以及产品供应商提供可限制权限的账号，以便他们上传各种文档，便于在整个项目生命周期内进行项目文档、资料提交和痕迹化归档管理。

（1）可研分析：实现项目可研报告分析和审批过程管理；

（2）预算管理：实现根据资产及资源库（CMDB）和服务级别协议，按照预定的规则自动生成预算。实现各预算的收集、合并汇总等功能；

（3）立项管理：实现投资类项目的立项管理，对立项过程产生的各种文件、批复等资料进行归集；

（4）项目计划管理：实现对投资、采购的年度计划进行管理，支持年中调整和汇总、查询等功能；

（5）招投标管理：实现对项目招投标过程产生的各种材料、评标结果等资料进行归集。具体的招投标流程在机关采购系统中实现，未来将通过系统集成实现两个系统间的信息共享；

（6）付款管理：通过上传项目合同、设置付款批次、付款条件、归集付款材料，实现付款过程的痕迹化管理；

（7）软硬件采购项目管理：实现软硬件设备采购项目的过程文件归集和进度跟踪；

（8）软件开发项目管理：实现了软件开发类项目从需求调研、设计开发到部署实施全过程的文档归集。可实现系统软件实施过程的进度跟踪；

（9）服务类、运维类项目管理：根据服务类和运维类项目的特点，实现对各项目阶段的文档归集和审批以及进度跟踪。

（10）项目合同管理：实现与实际合同相一致的合同管理，包括合同签订日期、合同服务内容等信息管理，也支持创建虚拟合同。同时，支持以项目合同为主线，实现与供应商、服务目录、服务水平协议、服务报告、服务评价等进行关联管理。

（11）统计报表：实现项目不同维度、权限的统计报表，包括但不限于立项项目统计、预算批复与执行情况统计、执行项目情况统计、项目合同执行质量统计等。

2.2 资产管理

资产管理实现对信息化软硬件资产的全生命周期管理。可以通过项目合同资产初始化或人工维护方式，满足资产入库、变更、报废等流程管理，对资产生命周期进行有效监控；

（1）资产入库：支持与终端安全管理软件、国资系统等集成，实现资产信息一致。提供资产审核功能，能够审计每次扫描资产配置（包括软件、硬件）的变化；允许手动录入资产或者导入资产；

（2）资产变更：实现资产变更跟踪记录，包含资产上架、移动、闲置等信息；同时满足硬件设备属性记录,包含序列号、品牌、型号、安装位置、维保情况、供应商等信息。也可以添加额外的字段来记录特殊信息。

（3）资产维修：通过运维管理事件、问题功能，可触发资产维修，同时记录维修时间、故障原因、处理结果信息，满足资产维修过程全面详细记录。

（4）资产报废：实现资产报废流程过程跟踪，包含资产报废详情、报废去向、报废残值、报废时间等信息记录。

（5）资产统计查询：实现资产详情记录查询，包括资产序列号、资产类别、品牌、型号、版本、国产化情况、供应商、IP地址、维保情况等。

（6）资产盘点：按照规范有计划地开展资产盘点。通过二维码、移动应用等功能完成资产盘点。

（7）耗材申请：对于耗材申请流程，支持审核发放时可以进行修改，支持不同耗材申请数量限制设置，支持耗材关联到具体设备，并统计设备使用耗材情况，如果不满足要求则不能申请，不符合条件的需要走单独流程。

2.2.1 备品备件与库存管理

（1）库房管理：应具有灵活的库房管理功能，实现库房自定义，管理对象自定义，支持不同物理位置的库房的逻辑合并和拆分管理。

（2）备品备件与库存管理：记录库房资产情况，包含备品配件、介质、机房应急材料等。同时跟踪库房出入库流程信息，记录库房资产使用、库存情况。对不同批次的同型号备件支持不同时间采购价格的统计管理。支持先入先出模式的出库提示。

（3）库存统计查询：实现灵活多角度的库存使用、剩余情况统计查询功能，可通过模糊查询快速找到库存备品备件所在位置、品牌、型号、数量等信息。支持多维度的统计展示。

2.2.2 配置管理

（1）配置管理数据库：应包含有配置管理数据库（CMDB），存储所有配置管理的数据和信息，为事件管理、问题管理、变更管理提供查询、诊断、记录的基础；系统应能够记录各种生产环境中需要被管理的对象：数据库、中间件、硬件、文档等，实现全面的信息记录。而且记录对象的分类可以定制；系统的配置管理数据库不仅记录了配置元素的详细信息，还能够记录各元素之间的关系：父配置项、子配置项、关联配置项等逻辑关系；系统应能够维护自身的配置管理数据库（CMDB），对其进行各种管理操作。

（2）配置关系管理：支持修改、调整配置项之间的关联联系，并对关系进行定义；

（3）配置类别及属性管理：可以对配置进行自定义的分类；根据不同的分类信息可以自定义该分类中的属性信息和配置信息。

（4）配置审计：支持配置审计创建、执行、结果发布；配置审计结果之后可以通过配置项变更，修改和调整错误的配置信息。

（5）配置权限管理：可以对人员、组织、角色权限对配置项实例进行管理控制，例如查询、新增、删除以及编辑等。

（6）识别配置项：新增加配置项后自动赋予唯一识别号（搜索代码）。能够以多级层次化的结构描述配置项的关联逻辑，能够以多层次的树状结构视图以及图形化形式展现给操作者；系统可以按照用户的需要新增客户化字段；系统采用适当的措施存储资产的合同、文档、手册、拓扑图等附件信息，并避免对数据库性能的影响；不同配置项之间的字段不尽相同。

2.2.3 知识管理

（1）创建知识：可以手动创建知识，可以通过引用某个事件或者文件创建知识，知识库支持导入、导出功能。

（2）知识分级分类：可对知识的分类、级别进行修改，默认的分类有制度、FAQ、流程等分类信息；其中FAQ和技术知识可供事件处理、问题处理、变更发布流程在事件处理、需求分析、项目立项、变更实施过程当中调用。

（3）审批发布知识：所有提交的知识都需要进行审核才能发布，未经发布的知识不可以查看，发布过程也可以选择不同的对象和用户进行发布。

（4）更新知识：可以对知识进行更新修改，需要记录知识的更新日志，包括时间、人员、更新内容、版本。

（5）知识评价与知识报表：支持知识的评价功能，可对知识的内容，进行自定义评分；有默认的知识报表（最常用知识、评分高的知识、最新知识、知识清单等），也可以自定义其他知识报表。

（6）知识共享：提供开放的、集成的知识库，能够实现多个知识库中知识的互访互通。如有新增其他的知识库（如企业知识库），应与本知识库系统集成，实现统一的知识库管理。

（7）知识地图搜索查询：可以对知识进行模糊搜索查询，也可以通过筛选条件过滤等方式快速查找到用户需要的知识，用户还可以对常用的知识进行收藏。

（8）知识接口：支持各个流程模块在过程当中对知识的智能匹配和推送提醒功能（详见各流程功能需求）；可以将不同的子系统知识进行收集整合，并进行分类统一展示。

2.2.4 供应商管理

（1）供应商和合同数据库：提供供应商和合同的数据库（SCD）存放供应商和合同的信息，并可以对该信息进行有效的更新、维护，支持供应商清单查看，可进行搜索、查询、筛选。

（2）供应商和合同分类配置：可以对供应商和合同的类型进行自定义，记录该供应商的合同编号；对已经记录的供应商和合同进行统计分析。

（3）供应商的监视和审查：可以通过服务级别的监控对不同供应商的合同SLA进行监视；可抽取某个供应商的合同对其合同的履行进行审查。

（4）运维商绩效考核：根据运维服务合同和合同的服务水平协议，从主客观两方面对运维商进行评价和绩效考核，主观应结合客户对系统运行情况、运维服务满意度调查等。

2.2.5 信息化人员管理

（1）系统支持对内部信息化从业人员、外部协作人员及其他重要信息相关人员的基本信息管理，支持对人员信息的录入和统计查询。

（2）系统支持根据人员所属组织结构、拥有角色、工作职责等进行分权分域管理。包括实现对项目信息、资产信息、流程审批、工单信息、运维权限等按照不同人员所属组织、拥有角色、工作职责进行分权分域管理。

（3）运维服务人员和供应商分类配置：可以对运维人员和供应商的关系进行自定义；对已经记录的运维人员和供应商进行统计分析，统计供应商人员情况、驻场情况、人员考勤情况、人员绩效情况等。

（4）运维服务人员的服务评价和考核：可以通过对照服务目录，从主客观两方面对运维人员进行评价与绩效考核。

2.2.6 体系文件管理

系统支持按照三全工作要求，对信息化文件进行集中管理。文件管理可以分为文书档案、项目档案和标准制度的分类管理，同时，对文档分类支持自定义管理。系统支持采用树形结构方式对体系文档进行导航，树形结构节点的级数可以无限制延伸，用户可自定义每一级的节点。

3 安全管理中心

安全管理主要是实现行业下发工作、主被动发现安全隐患处置、安全预防性工作三方面安全管理工作。通过与网络安全产品的能力集成，实现安全业务全覆盖、安全操作全留痕、提升安全智能化能力。具体实现内容如下：

3.1 系统运行监控

系统运行监控功能实现对IT基础层的网络、主机（服务器）、数据库、中间件、应用系统等的全面监管，帮助管理人员及时了解IT架构（各类IT资源）的运行情况，支持策略管理，能自动或手工设定启动相关事件处理流程。

IT基础环境监控对被管理对象主要进行性能采集和事件管理，即采集必要的性能参数及异常状况，根据系统运行状况或自动或手工设定的产生相应的事件，并完成异常事件的关联分析。支持前端多纬度、多要素综合管理的需求。

可通过与预设配置规则和指标阈值对比进行分析，对于异常结果进行告警，告警信息可自动通知相关运维人员进行后续处理，并支持启动相关运维流程，并可按照设备、应用、网络拓扑等多个视角进行图形化展示。系统监测采集功能要求支持通过网络日志标准采集协议，如Syslog、SNMP等进行全网日志采集，以确保全面收集日志信息。对于各类被监控对象的应用系统运行状态，系统还要支持通过主动探测感知。

系统支持通过配置过滤和聚合功能消除无关数据，并可合并重复的各类告警和运行日志。支持广泛的采集对象Windows、Unix、Linux等操作系统，华为、Cisco、H3C等主流网络设备，国内主流IDS、防火墙、VPN等安全设备的日志采集及基于其私有mib库的性能监控。

支持安全事件、行为事件、状态监控日志的事件描述，支持事件目标对象归类、事件行为归类、事件特征归类、事件结果归类、攻击分类、检测设备归类。支持多种解析方法，接入设备数量不影响日志解析性能。支持对CPU、内存、设备存储空间、系统进程、端口、网络流量等设备状态信息的监控及故障的预警，具有时间曲线图，能够按时间动态展示相关状态的变化。各类海量日志信息的统计与报表、海量日志的存储与快速检索以及平台的管理。支持各种监测日志的归一化处理，实现高性能的海量事件存储和检索优化功能，提供高速的事件检索能力、事后的合规性统计分析处理，可对数据进行二次挖掘分析。

3.2 监控对象管理

系统能够将主机、存储、网络设备、安全设备、容灾设备等硬件和操作系统、数据库、中间件、业务应用、虚拟化环境等软件作为监控对象，可实时监控其运行状态，一旦发现异常，能够及时生成告警；系统支持按照安全域、业务系统等进行监控对象的管理和统计分析。

3.3 监控指标管理

3.3.1 主机系统监控

主机监控范围应包括公司各类应用系统，支持对Windows、Linux、HPUX、IBM AIX、虚拟机（华为、Vmware）等各种操作系统主机的资源自动监控。可提供灵活的、可定制的监控机制，协调一致、灵活的设置监控指标、抽取监控数据、发布故障报警以及集中展示，帮助管理员及时发现故障和故障隐患。并至少实现以下基本要求：

（1）可根据不同情况设置预警或报警阀值，当指标超出阀值时能够及时生成报警，以便采取措施干预，并支持“动态设置阀值—报警”功能。

（2）能提供指标、阈值统一管理和展示的系统，提供方便的图形化设置工具，并能根据需要进行相关指标的再加工。

（3）能够对最近30天内的主机系统的运行状态进行追溯。

系统能够对主机系统的如下指标进行监控（包括但不限于）：

（1）能够监控主机运行状态，通过监控采集工具获取主机系统基础运行信息，包括：CPU整体使用率、内存使用率、内存动态信息、硬盘使用率动态信息、磁盘IO信息、用户访问信息和审计信息等。

（2）能够实现对关键进程(包括系统进程、数据库进程和业务应用进程等)的进程状态、进程资源占用情况、同名进程数、进程活动状态的监控；对内存使用最多的进程识别、消耗CPU最高进程的监控。

（3）能够监控操作系统日志、事件、故障、计划等。

（4）能够监控端口开放和运行情况。

（5）能够建立全面性能监控指标体系，可以通过一定时间观察给出监控趋势图，通过分析，为不同的指标设定合理的指标阀值。

3.3.2 网络设备监控

网络监控范围应包括全网网络设备，应涵盖目前主流的网络设备（Cisco、华为、Juniper、H3C等）及国内主流网络安全设备,具备网络拓扑管理、网络故障管理等功能。至少实现以下基本要求：

（1）能基于多种协议快速进行拓扑结构自动发现，迅速搜索整个网络内的所有节点，自动呈现出网络内的所有结点及之间的连接关系，能发现设备端口及对端端口；可自动发现二层和三层网络设备，包括路由器、交换机、防火墙等设备以形成网络拓扑结构。

（2）网络拓扑图支持按区域、父子关系逐级钻取，在拓扑图上能显示设备的类型、线路及设备的通断情况，故障设备和线路以及线路实时流量能够清楚地在拓扑图上显示，各类设备运行状态可在拓扑图中实时反映，并能以不同颜色显示。能对各类监控指标设定阈值，实现对链路状态异常、延时报警和短信通知功能。

（3）能实现网络故障管理，实现统一集中（事件分级）报警，并能对报警、故障进行统计，可实现分时、分类、对应设备的事件和故障信息统计。故障应能对物理宕机、链路中断、端口宕等常见事件进行判断和归类。

（4）能实现中烟公司、卷烟厂专线链路的监控。

（5）能够对最近30天内网络设备的运行状态进行追溯。

系统能够对网络设备的如下指标进行监控（包括但不限于）：

（1）网络设备性能监控包括CPU和内存利用率、缓存占用率、板卡工作状态、电源和风扇状态、设备工作温度、端口的基本信息、路由表、邻接协议数据、线路通断情况等。

（2）系统监控网络运行状态，包括：WAN状态、LAN状态、接口流入、出量、误码率、丢包率、错包率、带宽利用率等。

（3）能实时监测重要链路中断情况、路由器端口等异常情况，并根据流量异常判断触发性能告警。

（4）通过与网络设备集成，能够监控启动时配置文件、运行时配置文件等配置文件，进行对比分析。

3.3.3 安全设备监控

网络安全设备监控范围应包括全网的各类网络安全设备，设备类型包括漏洞扫描设备、防火墙、IDS、IPS、带宽管理设备、网络版防病毒系统、数据库审计、网络行为审计、网页防篡改设备等，应能支持主流品牌厂家的产品和目前公司已经使用的网络安全产品，并支持后续购置的安全设备纳入监控范围。

网络安全设备监控主要为满足等级保护工作要求，从上述产品中抓取相关网络安全管理要素的基础数据，形成“数据采取—综合分析、统计—统一展示（评价）”体系化管理思路，为网络安全管理提供基础数据支撑。并对等保要求重点管控的工作在本系统上实现移植和集成，方面统一、便捷的管理。至少实现以下基本要求：

（1）能够通过监控采集工具收集上述网络安全设备的原始报警日志，对报警日志进行识别、归并、分类处理。支持日志过滤策略功能，负责对收集到的安全日志进行过滤，针对不同的监控采集工具可以配置不同的策略，能够根据事件等级、事件类型、事件名称、日志样本名称、关键字、日志发生源设备IP地址等条件组合对无用日志进行过滤。

（2）支持事件忽略策略，负责对误报事件自动执行忽略操作，能够根据事件等级、事件类型、事件名称、源/目的IP地址、日志发生源IP地址等条件组合对系统相关事件自动执行忽略操作，以提升人员处理效率。

（3）支持基于统计的分析策略配置功能，负责针对相关联的日志按照既定的时间周期进行聚合，可以根据事件等级、事件名称、设备种类、设备类型、日志编号、源IP、源端口、目的IP、目的端口等进行统计合并。

（4）支持自动工单策略功能，主要针对自动将系统发现的各类事件自动生成工单，能够根据事件类型、事件等级、事件名称、事件源/目的IP地址等条件生成工单，能够重新配置工单名称和工单等级；在自动生成工单时，能够通过短信、邮件等方式通知给相关负责人。

（5）能够监控安全设备的运行指标，包括：CPU使用率、内存使用率、网络接口等技术指标。

（6）能实时监测网络接口等异常情况，并根据流量异常判断触发性能告警。

3.3.4 数据库监控

数据库监控范围为各类应用系统数据库，能够对Oracle、SQL Server 、DB2等多种数据库进行监控（包括部署在虚拟机上的数据库），按照属性相关性分为数据库工作状态、数据库表空间的利用情况、数据文件和数据设备的读写命中率、数据碎片的情况、数据库的进程状态、数据库内存利用状态等属性监控组。能实现以下基本要求：

（1）实现数据库运维指标管理，能够为Oracle、DB2、SQL SERVER等数据库提供一套运维指标体系管理，其中各类指标是检查数据库性能状况的重要因素。数据库运维指标应和主机运维指标相结合，可以综合反映数据库性能和主机性能之间的相互关系。

（2）每个指标都可以根据实际情况而灵活配置，针对不同的数据库应用，对应的指标应该有不同的差异。

（3）每项指标可对应相应的报警信息，并可设置持续时间参数指标阀值，当性能参数超过相应的指标阀值时，启动（相应级别）报警功能，及时生成报警，准确通知相关责任人。

（4）数据库监控能够监控数据库服务器的活动状态，展现包括即时或特定时间段的数据库连接的运行情况，从而实现深度监控。

（5）能够对最近24小时数据库系统的运行状态进行追溯。

系统能够对数据库系统的如下指标进行监控（包括但不限于）：每个数据库实例的用户访问信息、数据库连接、数据库锁、数据库排序堆、缓冲区、内存、表空间、应用程序、数据库实例信息等。针对不同的数据库应用，对应的指标应该有不同的差异。

3.3.5 中间件监控

中间件监控范围包括应用系统中使用的各类中间件（包括部署在虚拟机上），监控中间件的基本信息和运行状态，能够支持各类主流中间件的常用版本，应实现以下基本功能（包括但不限于）：

能够全面的监控多种主流中间件，能够实现中间件集群的监控，覆盖包括中间件实例、CPU消耗、内存使用、各部件性能数据、总体响应时间、中间件及应用Log、JDBC池、Servlet、EJB事务、Web Service等重要性能指标。能够对最近24小时数据库系统的运行状态进行追溯。

系统能够对中间件系统的如下指标进行监控（包括但不限于），针对不同的中间件，对应的指标应该有不同的差异。

（1）Weblogic中间件监控指标应至少包括：打开的端口数、连接数、队列的请求数、队列状态、连接延迟时间、连接状态、消息数。

（2）Websphere中间件监控指标应至少包括：可用服务数、平均等待时长、平均利用率、Bean状态、活动进程数、各种消息数等。

（3）Tomcat监控指标应至少包括：内存信息、线程信息、类调用信息、虚拟内存信息、Mbean信息等。

3.3.6 其他设备监控

对于其他设备，如存储设备\备份\容灾设备等，能够根据设备本身管理软件的功能和相关信息采集工具，对设备的容量、性能、故障和运行状态等进行集成监控管理和报警。

3.3.7 应用系统监控

应用系统监控是根据网络安全工作要求，突出“业务全要素”、以保障业务系统稳定运行为重点，需要在本次项目中作为重点开展的一项工作。

应用系统监控主要要求如下（包括但不限于）：

（1）系统监控在基础设施监控和应用软件监控的基础上，以系统稳定运行为目标，建立体系化的系统监控体系，实现“业务-用户”全过程的“业务级”监控，包括业务可用度、业务运行效率（状态）、用户感知等。

（2）对于部分WEB模式的应用系统，能够模拟用户进行WEB登陆的方式对系统运行是否正常，能否正常响应等进行测试。

（3）能够接收重要业务系统的异常日志，对日志进行识别、解析、分析和展示。

（4）能够将分散的资源按照业务的逻辑关系进行整合，建立业务逻辑模型和拓扑，并提供多层次的视图来展现业务应用的运行情况。应提供业务应用总视图、资源运行状况视图及重要指标分析视图等，方便运维人员监控系统运行状态，定位故障问题根源。

3.4 数据安全管理

对于运维过程中的业务数据进行全方位管理，系统包括但不限于以下内容：

（1）对数据备份情况进行实时监测，包括数据备份状态，文件目录、文件大小、备份时间等；

（2）对数据操作、使用过程进行记录，并对记录进行跟踪审计；

（3）对数据权限进行分区域存储、分权限控制；

（4）对业务数据对接、使用需进行业务数据工单申请。

3.5 网段IP地址管理

根据安全运维工作的实际需求，实现IP地址管理功能，该功能能够实现对重庆中烟的网段分配和IP地址进行管理。

系统支持对服务器、网络与安全、办公、视频管理、系统测试网段的添加、修改和删除功能。在添加和修改网段时，自动将根据网段范围内包含的IP地址与资产管理的配置项进行匹配分析，从而将IP地址与配置项信息进行一一关联。该功能定期针对服务器、网络与安全网络网段的IP地址进行PING扫描，一旦发现资产管理配置项中不存在的IP地址时，及时进行告警。针对在用网段、空闲网段，实时进行统计查看。

3.6 安全策略管理

将行业网络安全工作和三全工作要求中的安全策略管理需求细化到系统功能中，针对不同等级的安全域内的安全设备数量，安全策略的合规性和有效性，进行集成，实现统一管理和检查。系统支持通过网络数据包采集、驱动仿真访问等技术实现手段，定期针对安全域内的安全策略的有效性进行验证，针对已经失效的安全策略进行及时预警。同时对于安全策略的新增、修改和删除等操作，通过规范系统操作流程，针对所有操作保留相关痕迹记录。

3.7 安全检查管理

系统能够根据行业每年安全合规、检查工作要求，形成动态指标，自动生成可供进一步填报数据的业务系统和统计表单，并具有汇总、分析功能，支持根据相关合规指标要求生成对应统计报表，并可对历年填报数据进行统计分析。同时，支持中烟公司、厂级、车间三级检查填报功能，支持填报模板、填报人员和填报时间自定义，支持上报国家局安全运维系统。

3.8 网络流量分析与回溯

网络流量分析功能主要对关键业务应用网络环境中实时发生的网络通讯数据包进行深度协议分析，要求支持现有网络内的所有业务通讯协议解析展示。支持通过设置服务器区域交换机通讯接口为监听混杂模式，系统能监听到整个网络环境中流过该接口的数据包，支持数据包被捕获后转换为格式化字节的形式并进行分析。

支持采用多线程分析技术对捕获的数据包按照所有可能的协议进行匹配，并可获得相应的信息。例如：UDP协议分析线程能够分析数据包中的源端口、目的端口、数据包长度等信息；HTTP协议分析线程能够分析数据包中的连接、请求、超时、返回值等信息。系统能够展示来源和目的IP地址的流量信息，能够按照复杂查询条件进行流量通讯数据包的信息溯源。

支持通过交换机镜像端口技术实时抓取保存关键服务区域的网络通讯数据包；支持根据需要将特定IP地址（来源和目的）、关键线索时间、通讯协议的通讯数据包从海量的数据包中提取出来，并支持完整的网络数据包重放回溯；支持将原本瞬间发生或者持续多日的异常行为，按照其发生顺序或攻击的目标IP地址等将其通讯行为进行还原重现。重现时，可以对原始IP地址、MAC地址、通讯端口等关键参数进行修改调整，例如调整IP地址和MAC地址、甚至是通讯端口，使得网络访问可以在其他模拟场景下得以重现。

网络回溯时，系统可以将原始海量数据包按照需求将需要回溯的IP地址范围提取出来，而不需要重放所有的数据包，同时可以根据数据包中按照发送源为客户端和服务器端进行区别，指定不同的网卡将数据包发送出去，形成真正的网络通讯流量回路。

通过网络回溯，可以将代表性的网络事件或者网络攻击案例更加完整生动的保存下来，通过网络流量回溯过程不断分析研判加深对于该事件的分析处置能力，测试改进后的安全设备是否可以提升防御能力。

3.9 业务系统账户登录行为安全审计

系统通过直接实时分析获取到网络通讯数据包，将其中关键业务系统的账户登录行为进行自动学习分析，实现关键业务系统如决策管理系统、财务、办公系统、邮件系统的关键账户（例如各级领导、关键业务岗位）的登录行为审计与分析。通过审计分析可以及时发现各类登录异常行为，例如短时间内多IP地址登录同一账户，同IP地址登录多账户，明显来自行业外单位和境外IP地址登录关键账户。对各类账户异常登录事件，详细记录其行为特征，及时发出预警信息。系统实时获取全网运行日志，支持对异常来源IP地址进行细粒度行为审计分析。所有系统获取到的登录行为，在系统后台至少保留2年时间，其间支持多种查询分析统计。

3.10 安全关联防御

系统能够通过采集来自监控采集工具的实时数据，完成对所管控的设备中超过阀值的资源生成报警，能够对安全设备的报警进行集中管理。实现以下基本能（包括但不限于）：

（1）根据不同的报警机制，支持对报警进行归类管理。

（2）支持对安全设备原始日志进行同类聚合、过滤等处理。

（3）支持报警级别区分，可自动将低级别报警处理为“不上报”。

（4）支持根据需求以列表方式清晰显示详细报警信息，报警内容应至少包括：报警源、报警类型、报警级别、报警发生时间、报警信息描述、报警处理状态、报警处理时间等。

（5）报警查询与统计：应提供对当前报警或者历史报警的查询和统计功能，并能够以表格、图形（直方图、曲线图、饼图等）方式显示。系统可提供对查询结果的统计功能，即按照多种条件（如报警级别、报警源、报警时间等）分别统计当前报警的数量。能够将查询结果和统计分析结果以doc/excel等格式输出。

（6）报警通知与处理：支持多种报警通知方式，包括邮件、短信、屏幕输出、声音输出等方式，支持直接将报警生成工单，进行事件处置。

（7）可通过自动漏洞扫描结果，以及安全防护措施监测数据，进行关联分析，评估网络安全状况，并可按规则进行显示和报警。

3.11 安全态势感知

安全态势感知是对安全事件进行汇总分析，从宏观的角度持续对客户的总体安全状态和趋势进行评估和展示，结合资产和应用情况进行全面诊断。安全态势要求自动学习并建立基于全网安全告警采集与系统运行状态监测数据的态势基线，可以对于突然新类型安全告警、激增日志数量、异常系统状态进行及时的态势感知并自动化研判分析。同时，安全态势感知可以针对互联网网站上的安全资源类网站，例如国内外漏洞发布网站、第三方安全态势感知网站以及安全咨询类网站的基础数据进行自动抓取，将抓取到的安全情报信息自动与行业内系统类型进行比对分析后，给出安全态势分析结果。

3.12 安全基线审计

依据等级保护管理要求、安全基础管理要求，通过建立等保等级基线库，并与配置库资源进行关联，自动检查资产安全，包括终端设备（终端计算机、外设、移动介质）安全，主机设备，网络设备，安全设备，操作系统，应用系统，数据安全，灾备安全等安全基线对标是否符合基线标准，一旦发现偏差，提前预警提示，并通过流程下发整改任务，对整改过程记录和结果跟踪等闭环管理。

3.13 安全应急管理

对于安全隐患，提供自动触发安全应急处置流程，对于应急演练等安全预防工作需在系统中进行记录、监督、跟踪的闭环管理，应急演练需要记录参与者、过程留痕、结果确认等信息。

3.14 可视化机房监控

支持浏览器访问可视化机房系统的交互操作和浏览。展示效果以2.5维或3维形式表现机房环境、机柜、空调、独立设备和架式设备，在系统中实现机房环境、机房子区域、机柜、设备和设备端口的资产信息和运行告警信息直观展示等。需要实现如下功能：

（1）系统采用B/S架构，支持利用浏览器直接通过鼠标实现可视化系统的交互操作、访问和浏览；

（2）系统展示效果要求以直观形式表现机房环境、机柜、空调、独立设备和架式设备，通过鼠标点击，在可视化系统中实现机房环境、机房子区域、机柜、机房网络连线、设备和设备端口连接情况和运行告警信息等；

（3）提供设备产品模型库，支持主流基础设施设备和IT设备模型；

（4）提供开放的数据集成接口，可以与资源配置库（CMDB）、监控系统集成关联管理。

（5）要求与现有的机房动环系统对接，实现动环数据的实时监控。

3.15 网络应用性能检测

为有效解决运维管理和信息安全管理面临的问题，需要从全网流量可视化、业务可视化、网络及应用性能检测、故障定位、风险预警、异常访问行为发现、决策数据支撑等方面，对全网流量进行检测分析，全面提高运维管理和信息安全管理能力。需要实现如下要求：

* 基本要求

（1）产品架构：软硬一体化设备，支持Windows、CentOS7、中标麒麟操作系统，采用旁路方式部署，不影响现有网络结构；支持集群部署，通过专用控制台软件进行实时数据分析展示；支持数据链路汇聚设备流量聚合与多接口聚合模式。

（2）网络接口：单台设备支持千兆流量采集口≥4个，提供千兆网络管理接口≥2个；

（3）分析能力：单台设备实时分析能力≥4Gbps；

（4）存储能力：单台设备提供数据存储空间≥24TB；流量分析数据存储时间≥6个月。

* 技术要求

（1）系统应支持远程管理设备IP地址，支持远程关机、重启系统；支持服务管理（停止，开启，重启）；支持配置备份及批量复制；支持重置系统、系统信息查看，支持3级以上权限管理功能，支持三权分立；

（2）系统应支持实时流量分析，分析指标项不少于170种（提供产品界面截图）；支持业务质量、性能评估及动态展示功能；支持自定义基于不同业务系统各自的服务依赖视图，定制包含客户端性能、网络性能、服务器性能的统一监控视图，并实时展示，同时支持对场景进行自定义及上下视图Drill-Down操作功能；

（3）系统应支持针对应用系统识别功能，自动识别多种主流业务应用，如主动/被动式的FTP、Oracle、SQL、MS Exchange、SNA、Citrix、VoIP、SAP、 NetBIOS、P2P、Voice、Video等；支持识别自定义应用系统，支持服务器IP+服务器端口的应用定义方式，以及基于多IP和多端口的复杂应用的自定义，并且支持过滤器表达式；支持基于规则的应用识别，支持按URL定义应用；支持按HTTP协议加应用服务器的IP地址方式定义应用；支持未知协议识别，支持对未知协议的流量分析，自动统计其所采用的端口；

（4）系统应支持对国家标准 GB28181《安全防范视频监控联网系统信息传输、交换、控制技术要求》的信令流和媒体流提供性能分析、故障告警、回溯取证及音视频回放。支持自动按SIP会话关联分析信令和媒体流；支持对信令和媒体数据包进行提取，解码和分析；支持对信令的请求数量，成功率和故障码进行分析，提供信令故障诊断能力；支持对媒体流的丢包，时延和抖动进行分析，自动测算音视频质量MOS值，提供信令故障诊断能力以及信令接续梯形图；支持VoIP故障告警功能，告警日志包括用户异常下线、失败的呼叫、质量较差的呼叫、告警原因、时间、详细呼叫日志等；支持回溯取证、音视频内容回放；

（5）系统应支持对WEB业务系统资源自动发现，支持从应用、服务器、资源、方法视角对交易进行统计和趋势分析，支持对交易请求数、响应数，失败响应数等进行统计，支持对基于WEB的应用响应率、响应时间、未响应、未响应百分比、慢响应、慢响应百分比，并提供按时间的趋势分析；支持对WEB的应用的返回码统计，分别统计100类、200类、300类、400类、500类返回码，并提供按时间的趋势分析；支持对请求大小、响应大小、压缩流量、条件请求等进行统计，并提供按时间的趋势分析；分析记录典型失败交易、慢交易、无响应交易，并可以提取相关交易的原始数据包；

（6）系统应支持从应用、服务器、资源、资源方法、业务组（网段）、IP主机等多个视角进行统计和趋势分析功能，支持自定义显示趋势图，并且趋势图支持通过鼠标拖拽放大或者缩小功能，支持趋势图关联分析，支持同步关联多个趋势图数据浮现；

（7）系统应针对网络数据包含的网段具备自动识别功能，支持通过界面及统一接口方式进行业务组自定义；应支持针对应用、主机、服务器及多对象自定义业务组统计；支持流量地图，以地图的形式展示各自定义业务组的流量拓扑关系，可将吞吐量、告警数量、重传百分百等关键网络指标结合地理位置进行实时展示；

（8）系统应在数据链路层对字节数、数据包数、每秒流量、每秒数据包、数据包类型（组播、广播、单播）、协议分布、MAC主机流量进行统计及趋势图展示；应对VLAN流量、ARP流量进统计，支持双层VLAN tag的识别；支持全局多视角MAC主机、VLAN、ARP的统计和趋势分析。应支持多种隧道协议，支持CAPWAP、GREv0、GREv1、GTPU、LWAPP、MPLS、PPPoE、QinQ、IP-in-IP等隧道协议及多层隧道嵌套的解析；支持IPv6分析；

（9）系统支持利用网络流量分析结果，发现网络中活动的主机、应用以及访问关系，直观的展示网络中的主要参与者及状态。主机发现支持发现网络中出现的 IP 地址以及 IP 之间的访问关系，输入目标地址网段，即可启动主机发现过程，主机发现的结果可以图形化显示在查询时间段内，目标网络内活动的主机及相互之间的访问关系，提供主机IP地址访问关系表，点击IP地址可直接跳转至回溯页面；应用发现支持图形化显示主要应用流量大小以及相互之间的关联关系，提供显示所有发现的应用以及服务器流量统计信息的应用表和访问关系表，点击应用或服务器会跳转至回溯页面；

（10）系统应支持对IP主机、自定义网段、应用、服务器进行流量统计和趋势分析，对TCP连接建立请求性能的请求数量、响应率、成功率、连接建立时间、失败原因的测量和统计，提供各指标趋势分布；应对TCP性能指标如重传、乱序、重置、零窗口和往返时延（RTT）等进行测量和统计，提供各指标趋势图分布；应支持对用户响应时间的细化分解，如客户端重传/服务器重传/客户端重置/服务器重置/客户端零窗口/服务器零窗口等；

（11）系统应具备历史数据回放功能，支持自定义时间查看历史数据，如分钟、小时、周、月；应支持对原始数据包进行精确提取，在显示的图表基础上进行数据包提取时，自动应用时间范围和过滤条件；支持历史数据回溯能力，应满足弹性时间粒度数据库特性，极速响应不同时间范围的数据回溯；

（12）系统应支持纳秒级数据包时间戳，支持NTP时钟同步；支持过滤存储功能，只存储关键业务（用户自定义）的数据包；支持数据包锁定，支持在趋势图上采用所见即所得的方式锁定关键时间段的数据包；支持数据包去重复功能；支持数据包截断功能，能按照64字节、128字节自定义保留数据包长度，擦除应用层数据内容；

（13）系统应具备自动学习环境基线功能，并根据不同环境自动建立流量、性能基线模型，用于实时态势评估告警；应提供实时态势与基线模型的详细数据对比结果，并关联相应的性能分析界面；系统应支持自定义条件告警与多项指标的复杂组合条件告警，并提供自定义告警级别设置；针对所有告警信息可以自定义其回溯查看时间段，如年、月、日、分、秒；可针对各个告警事件提取攻击的原始数据，告警信息支持以SNMP trap、Syslog和Email方式发送；

（14）系统应具备风险预警功能，支持通过自定义检测功能，编写正则表达式对木马病毒的发现能力，支持TCP SYN洪水攻击检测、TCP空闲链接攻击检测、ARP攻击检测，并及时显示出攻击源和被攻击方，可针对各个攻击事件提取攻击的原始数据；

（15）系统应支持基于Web的报表功能，提供不少于15项预置报表；支持自定义报表时间范围及报表内容，并可按天、周、月定期自动生成报告，自动寄送到设定的电子邮箱；报表支持HTML、Word、PDF、Excel和JPG等格式输出；

（16）系统应提供统一API接口，支持设备配置管理和原始数据包提取；接口中应提供根据时间段、过滤器来提取任意数据包的方法，可通过接口提取自定义业务组、应用、主机、服务器信息，以及各自对应不少于170种的分析统计数据指标结果；接口应支持Java，C++, C#, Perl, PHP, Python, Ruby等主流开发语言。

4 运维管理中心

4.1 工作流引擎

（1）系统应能够支持快速响应个性化的需求，比如改变流程，改变参数等，系统管理员在图形化的界面下更改即可实现（如：提供能够让用户在图形界面下进行灵活配置的流程管理平台）。

（2）流程表单信息项可以根据需要，灵活配置。

（3）图形化流程设计器，支持父子流程、并流、分支、汇聚、自动升级、会签、自定义条件流转等，支持与其它流程的集成。工作流需要提供版本管理功能，支持相同流程在新老版本交替时的并行运行。

（4）图形化设计器，所见即所得，可以通过图形化的方式展现当前流程所处的位置。兼容Html、aspx等多种表单格式，基于源代码级的开放性和灵活性。

（5）默认基本工作流中需要包含以下的功能：接收、通过、退回、关联、分配、收回、委托、合并。

（6）流程支持自定义流程角色，支持对流程角色人员可选择任意单人或者多人流转。

（7）支持流程实施和关闭确认环节在一个平台上操作的闭环管理。

4.2 服务目录

应采用服务目录定义提供服务的种类以及服务目标，促使与客户建立良好的服务关系。

服务目录的设计应满足以下要求：

（1）服务目录简洁、清晰，用户易于阅读；

（2）列出服务编号、服务名称、服务描述、服务流程、服务相关人等。

（3）支持服务目录与服务请求目录关联，并根据服务项对应服务价值，计算服务成本，形成服务报告。

（4）支持菜单式的维护和勾选，选择好服务项目之后能自动生成服务内容。

4.3 事件与问题管理

（1）创建事件单：服务台可以手动创建事件单，用户可以通过服务门户创建事件，系统也可以通过各种告警自动触发事件（告警接口），系统也支持移动APP快速创建服务工单。支持二维码扫码关联报单。运维人员可手动创建部分类别的事件单（如主动发现的问题处理单或巡检单）。管理人员可批量手工创建工单，以工单的形式安排工作（如制订一项工作计划，拆分目标后用工单的形式派给一个或多个人员，这些来源于同一任务的工单支持不同的紧急程度和时限要求）。

（2）分类事件单：可以对事件进行事件类别和优先级别的划分，管理员可以调整事件的分类信息；优先级根据事件的影响范围和影响程度进行计算。

（3）调查和诊断：可以通过事件的描述查找出历史中类似或者相关的事件信息，也可以通过事件关联的配置项诊断事件的影响范围。

（4）派单功能：对明确的事件分类，系统支持根据人员负荷及预定义职责自动派单

（5）分析处理事件：可以通过知识库查找解决方案，直接使用该知识对事件进行处理（知识接口）；当无法处理事件时候可以进行事件升级 1.职能性升级 2.技能性升级；事件处理过程当中，可以派发子任务请求协助处理。

（6）跟踪事件：可以查看事件的处理过程，包括事件处理每个步骤的时间、人员、活动；可对未解决或未完成的事件通过各种方式（邮件、短信、电话）进行催办。

（7）关闭事件：可以对客户的满意度评分进行记录，然后关闭事件，对某些已经解决但用户未确认的事件可以自动关闭。

（8）问题创建分析：支持从事件到问题的升级创建，可通过知识对问题进行分析（知识接口）；支持问题的分析评审，可以对问题进行故障根源的分析。

（9）问题处理跟踪：问题可以通过变更进行处理解决，已经解决的问题可以作为知识进入知识库；可以通过变更的追踪查看问题的相关信息和解决情况（知识接口）。

4.4 变更与发布管理

（1）变更申请：提出变更请求，变更需求可能来自于IT人员维护自发的、项目建设的，以及事件、问题和配置管理流程。

（2）分析评估：对变更请求进行分类分析（涉及的变更CI、变更的影响范围），对变更的合理性、影响、成本、收益进行评估，提交可行性分析报告。

（3）变更实施：根据变更请求的信息制定变更实施方案、变更回退计划；可以从知识库中查找相关的方案、计划模板进行编制。

（4）测试回退：对已经进行的变更进行测试，看看是否达到预期效果，检验变更是否有效；当测试结果失败时执行变更回退计划，并重新进行变更实施。

（5）发布测试：对发布包进行发布测试，并提交发布测试结果和发布计划进行审批；建立配置项基线，可以对配置的变更发布版本进行跟踪控制，并保留历史版本。

（6）计划评估：根据发布测试结果进行评估发布计划的可行性；业务应用部门也可以根据发布日期的时间对发布计划进行修改调整。

（7）发布实施：根据发布计划执行发布实施；可以收集项目中的任务计划进行统一管理，对计划进行评估。

（8）发布跟踪：对发布的效果进行跟踪，看看是否有新的事件发生需要发起新的变更请求；可以在发布跟踪过程中创建新的事件。

（9）源代码管理：对源码进行版本控制和管理。

（10）发布管理自动化：支持在系统中制定发布模板，包括发布日期、发布版本、发布文件、发布目录、目标设备等信息，通过发布流程驱动自动下发至目标设备，支持一键启动发布脚本自动实施，并对发布结果进行显示，对发布过程日志进行记录等功能。

（11）系统安全评估：实现系统安全评估全过程管理，如在项目立项时应预定级、系统上线时确定定级和安全测评和备案等过程管理。

4.5 计划任务管理

（1）计划作业定义：定义计划性的任务；可定义计划内容、计划执行时间、计划完成时间、计划周期等信息。

（2）自动产生计划任务：计划作业通过审批后，系统可以在计划任务中定义的周期中根据计划的信息自动产生并派发任务。

（3）计划作业模板：可定义计划作业模板，在制定计划作业时可从模板中导入；作业计划模板中可以设置不同的指标，记录指标的完成情况。

（4）任务管理跟踪：支持实际产生的任务的分派、处理、跟踪；可查看任务处理情况，可根据任务追索到对应的处理流程，查看处理进度。

（5）个人工作日历：用户可以通过日历的方式查看每天的工作任务，可以看到总体的工作任务汇总，包括项目任务、事件任务、变更任务。

（6）任务审计管理：支持随机任务抽检；可以对任务完成质量、完成时间、完成效率进行抽样审计。

（7）任务流程关联接口：不同任务可以和各种流程模块关联（事件与问题、变更与发布）；可以和各种通讯工具集成实现任务派发通知，并可以自定义派发规则和机制。

（8）对于巡检计划任务：实现与堡垒机联动管理，对巡检执行情况进行合规性比对。

4.6 人员权限集中管理

（1）运维权限集中管理：运维管理中心整合安全运维审计系统作为运维审计引擎，使中心具有运维账户权限的集中管理、动态授权访问、统一操作控制功能。密码集中管理实现服务人员与系统、设备账号之间的分离，运维服务人员通过获取授权码的方式执行技术操作。动态授权访问实现对技术操作权限进行统一管理，针对各类运维任务，发放不同的授权码，做到统一操作控制，为运维服务人员提供统一的操作控制台，对运维操作行为进行记录，并根据预先设置安全策略对违规的操作行进行告警或阻断。授权访问验证码可以通过手机短信、微信和邮件等方式，提供给授权人员，授权码可以设置有效时间，超过有效时间必须重新授权。

（2）应用系统权限集中管理：实现人员权限纳入安全运维系统中进行集中管理。通过权限申请统一在安全运维系统中进行，使单个应用系统没有授权的权限。针对超级管理员的使用进行实时监管。并直观展示人员权限列表。

4.7 日常事务运维管理

日常事务运维管理，将当前日常事务性工作，如：日常巡检、机房值班、机房出入、资产盘点、运维商例会、运维服务评价及报告等进行管理。通过在计划任务管理中定制相应的计划任务，实现日常事务性工作定时提醒，并按照标准模板执行。实现对日常事务性工作过程记录和工作痕迹存档，保障日常事务性工作常态化。

4.8 服务报告管理

（1）对于周期性运维商例会，系统支持编排运维商例会、制定例会通知、会议内容记录，以及关联运维商服务报告，服务报告内容包括：总体运维情况概述、基本运维工作情况、重点运维工作事项、工作遗留问题、下一步工作计划与改进措施、系统服务情况汇总表，以及服务绩效情况等。

（2）支持服务报告自动生成：定义了月、季、年报模板之后可以设置时间让报告自动生成并通过短信/邮件的方式通知。

（3）报告导出打印：所有的报表、报告有打印、导出功能；可以在报告上添加自定义报告的描述、说明。

（4）报表权限管理控制：可以对每个报表进行权限的访问、查看、修改、删除控制；支持报告进行修改、调整、审核之后再进行发布。

4.9 服务绩效管理

（1）服务绩效指标定义：根据供应商评价指标体系，系统支持自定义考评指标，指标分类，指标权重和计算公式等；

（2）服务绩效监控预警：通过仪表盘进行监控，便于管理人员动态、实时的查看服务KPI，并可根据偏差实时采取措施；

（3）服务指标配置：

 可以根据各种不同纬度（类别、请求人、公司、优先级）自定义服务目标；

 服务目标可以和不同模块、流程、配置项进行关联，可以自定义测量准则；

 支持服务目标分解，可以自定义分解方式（组、团队、个人）进行绩效考核。

5 服务管理中心

5.1 服务门户

（1）为用户提供统一IT 服务窗口，用户可以通过该窗口填写故障申诉和服务申请记录，以及提供统一IT服务电话受理用户请求。

（2）用户报障页面：支持简易报障和网上自助报障两种方式：为用户提供IT 服务窗口，用户可以通过该窗口直接填写故障申诉和服务申请记录。也可通过拨打IT服务电话，由服务台快速进行故障登记和分派。支持用户通过电子邮件、移动APP、短信、扫码等的方式提交投诉和服务申请。

（4）支持跟业务系统集成，如门户或OA系统（AD域和LDAP），可直接查看登陆用户处理中的故障单状态，并对故障单进行催办、评价等功能，评价的结果作为服务评价考核的重要指标项。

（5）页面支持快速配置：支持配置向导，该向导包含所有管理任务，它可以引导您流畅地完成系统运行所需的各种配置和定制操作。

（6）我的故障单：包括未处理故障,历史故障查询、我要报障3个部分：未处理故障，通过此页面可快速查询未处理的故障单记录；历史故障查询，可通过故障单号，报障日期，评价情况等快速查询历史故障；我要报障，通过点击我要报障可以快速地进入报障页面，新建报障请求。

（7）可自动识别常用报障分类并形成快速报障按钮；

（8）知识库能够提供对自动关联知识库、故障模型、历史事件、问题等的查询功能。同时通过知识库类别的树形结构展示，快速地帮助您找到相关问题的解决方案，快速恢复故障。

（9）根据管理岗位职责的不同，系统支持不同管理员制定相应的工作界面。

5.2 服务台

（1）能够支持用户通过电话、web、图片识别、语音识别等方式提交投诉和服务申请。

（2）能够提供预定义故障和申请服务的类别，自动激活不同的处理流程。

（3）根据影响范围和紧急度，自动生成优先级；并可设置条件，自动升级；所有未分配的单按照优先级自动排序，以图形直观显示，方便快速、高效的派单。

（4）用户能够通过电话咨询、网站查询等方式了解自己提交的投诉和服务申请的处理结果。

（5）直观显示服务工单的执行进度情况，从而对故障和服务申请的跟踪督办，确保所有的故障和服务申请能够以闭环方式结束。

（6）支持对服务报告和绩效的跟踪督办和统一汇编功能。

（7）能够提供对自动关联知识库、故障模型、历史事件、问题等的查询功能。

6 移动应用

信息安全运维系统移动应用作为公司移动平台的一部分，主要实现故障告警及时通知和服务流程快速办理，快速响应效果，手机端与电脑端同步建设，支持手机版（IOS/Android）移动应用。通过移动APP可以实现代办工作、运行预警、服务申请、日常巡检、资产盘点、会议签到、统计查询等。

（1）支持通过扫描二维码，根据授予权限可以查看资产信息、资产盘点等；

（2）支持用户对移动APP功能根据喜好进行自编排；

（3）支持用户通过移动APP方式服务申请、服务跟踪、服务评价和提交建议及投诉；

（4）支持直观展示信息系统运行情况、告警提示；

（5）支持通过移动APP进行流程审批和办理工作。

7 综合大屏展示

综合展示模块为整个管理系统对外的唯一出口，也是整个系统的对外展现，各管理功能模块的管理数据和管理界面均通过应用展现层（统一门户）进行统一的发布和呈现。并需要从各个维度将运维、安全及人员质量评价清晰呈现，满足管理层对综合管控的要求。需要实现如下功能：

（1）集中（多纬度）展现信息安全状况（健康指数）及IT资源管控状态，形成综合管控驾驶舱，系统性支持管理决策。

（2）针对运维管理相关工作形成科学的、规范的质量评价体系，系统性支持管理决策。

（3）提供统一事件管理、网络状态监控、系统运行状态监控、业务状态监控、拓扑管理、趋势预警分析、服务管理、系统维护、权限管理、报表管理、知识管理、故障管理、告警管理等功能。

（4）具备集中展现功能：能将各类信息分析过滤后进行显示；能够自定义生成不同的报表模板：能够提供报表引擎：报表引擎能够对系统中的数据通过各种条件的组合进行相应的统计，为公司管理人员提供分析和决策依据。

（5）应为体系提供模块化、可定制的集中统一的管理界面。通过与底层技术平台及其它系统的集成，将监控和管理流程信息在门户中进行统一展示，使各项IT服务工作通过统一管理门户顺畅地进行处理，实现自动化流程作业。

（6）能够管理门户自身的用户和用户组，针对特定用户群，创建并管理门户视图，控制管理分级授权。

**三、集成及相关要求**

（1）与终端安全管理和上网行为管理软件集成，实现IP地址统一管理、IP地址与终端设备及使用人员关联管理；

（2）与域名管理设备集成，实现域名自动收集与合规性比对；

（3）与防火墙设备集成，实现网络策略自动收集与合规性比对；

（4）与堡垒机设备集成，实现运维账号及权限统一管理、策略自动下发、运维操作合规审计；

（5）与IDS设备集成，实现安全事件统一管理；

（6）与DNZ区设备集成，实现业务系统映射到互联网基线管理；

（7）与语音识别引擎集成，实现IT服务请求语音自动申报；

（8）与投资采购系统集成，实现信息化项目信息一致性管理；

（9）与门户系统集成，实现单点登录、用户组织信息同步、运维工单统一待办，通过门户对桌面资产领借用申请，并对资产数据进行智能分析，满足用户业务需求；

（10）与资产管理系统集成，实现与财务资产信息一致性管理，包括信息化部门资产（固定资产、耗材）转固后推送至国资系统，对于固定资产由国资系统生成资产编码和二维码回传至信息安全运维系统；

（11）与短信平台集成，实现短信提醒功能；

（12）与动力环境监控系统、门禁系统、视频监控系统和存储管理系统集成，实现IT基础设施集中监控、统一管理；

（13）与泰合SOC平台集成，实现设备日志信息的统一采集；

（14）与工控安全管理系统对接，实现工控资产和安全信息的统一采集；

（15）与行业安全运维系统集成，实现单点登录、用户组织信息同步、运维工作统一办理；

（16）与CA系统集成，实现对安全责任书和安全保密协议的电子签名和签章；

（17）与虚拟化管理平台集成，实现虚拟化平台资源集中管理，实现虚拟机自动创建、注销等功能；

（18）编制系统运行的管理办法，为开展安全运维保障工作标准和操作规范提供指导。

**四、技术架构要求**

信息安全运维系统需要以先进、成熟、可靠的技术架构为基础，结合实际需求，采用组件式、模块化的方式进行核心支持组件与业务功能模块的设计开发。

系统支持X86架构、linux操作系统、DB2数据库，应用系统支持集中管理、分布式采集部署。支持在虚拟化环境下运行。

信息安全运维系统包括展示层、功能层、组件层、数据层、采集层，实现对管控资源的管控。

展示层：提供统一集中的人机交互界面，构建安全运维“业务办理大厅”。可与门户集成，实现单点登录。与数字证书认证（CA）系统对接，集成资产管理、安全管理、运维管理三个业务中心数据分析、图形展现和操作功能的接口。系统访问实现账号密码和手机进行双因子验证。

功能层：实现包括资产管理、安全管理和运维管理三个中心的各项功能。

组件层：为保证信息安全运维系统的先进可行，缩短开发周期，系统基于成熟的技术支撑组件进行二次集成整合开发。

数据层：流程库、权限库、配置库、安全策略库在公司集中部署。安全事件库、监控数据库和预警库数据量大，与用户系统集成。

采集层：通过与成熟的数据采集工具进行集成，完成安全事件、设备故障、系统日志、运行状态、资产信息等数据采集工作。同时对收集的各种信息和日志进行范式化处理，转换成统一形式，为进一步的分析处理和展示奠定基础。

管控资源：包括用户机房基础设施、网络安全设备（包括行业骨干网）、应用支撑环境、应用系统等。

**五、软件产品选型要求**

投标人需提供网络应用性能检测软件的原厂产品投标授权函和售后服务承诺函，提供原厂三年质保服务，7\*24小时免费电话服务，软件系统一年免费升级服务。产品要求详见技术要求网络应用性能检测。

**六、性能要求**

系统在管理能力、数据分析能力和处理能力方面都应具备较高的性能，具体性能设计如下所述。

1.管理能力

信息安全运维系统采用先进的技术架构，能够同时支持500用户同时并发在线登录和管理,每个用户支持创建不同权限的角色分帐号进行分权管理。

2.数据分析能力

信息安全运维系统的数据采集、分析和处理性能要求如下：

（1）系统支持基于统计的关联分析、基于规则的关联分析等关联分析能力。

（2）系统具备自定义关联分析策略功能。

（3）数据分析能力：系统的数据分析能力可达到600条/秒以上。

（4）数据入库能力：系统的数据入库能力可达到1200条/秒以上。

3.处理能力

信息安全运维系统须采用先进稳定的技术架构，保证大规模用户的并发访问，减少系统的响应时间，能够提升系统的数据查询效率、报表生成效率，从而满足系统平均业务和高峰业务的需要。实现信息安全运维系统的业务处理能力达到如下指标：

（1）用户在查询报警数据时，查询的响应速度小于3秒。

（2）用户在系统中打开新的页面时，新页面完整打开的响应速度小于3秒。

（3）用户在点击完成当前事务到达新的页面时，新页面完整打开的响应速度小于3秒。

（4）用户在生成各类运维事件月、季度报表时，系统响应时间应小于10秒。

4.存储能力

信息安全运维系统可支持分析和存储的容量要求为至少满足5年以上的有关资产基础配置统计、监控数据、运维工单等所有数据。

**七、 实施要求**

项目整体建设周期为15个月。其中9个月内完成设计、开发、实施、部署、初验，初验后进入 6个月的试运行期，试运行期结束后，进行项目终验。

**八、 安全要求**

本系统定级为等保二级系统。

信息安全运维系统拥有完整的多层次的安全保障体系，包括授权/认证机制、存取权限与执行控制、口令保护机制等多种安全保障机制，具体设计有交叉验证、访问控制、信息加密、安全审计等功能。同时系统还具有细致的权限分级管理功能。

信息安全运维系统可保证数据完整性和机密性，具备安全检查功能，系统在数据传输过程中体现身份认证及行为不可抵赖。可按照组织结构划分操作人员的操作权限，建立相应属性证书，能体现在操作过程中操作人员的不同权限，并提供与身份认证、数字证书等网络安全措施的融合。

系统可设定备份周期和备份内容，支持备份数据的转储和转出功能，能对系统的全部信息实行定期备份，以保证系统的异常情况的补救，并设有系统恢复机制。对系统开发和维护人员无意地造成数据信息破坏的情况，给予必要的防范措施，将直接操作数据库信息权限限制在最小范围。

在应用安全方面，要使用严格的代码安全编写规范，要有保证代码安全的安全控制措施，保障应用系统的安全，抵抗恶意攻击者针对应用系统攻击导致应用系统不可用、数据泄露等问题。包括但不限于以下内容：

（1）对敏感数据进行加密存储和传输。

（2）采取措施避免系统遭受到非授权访问，避免攻击者进行缓冲区溢出攻击。在所有用户可输入处进行代码过滤。

（3）对上传的文件类型进行验证，以及可进行的操作进行限制，有效防止恶意上传者通过修改文件后缀等方式规避检测。可限制上传文件的大小，避免恶意攻击者上传超大文件长期占用服务器存储空间、缓存等资源，影响系统的响应时间等。

（4）系统具备限制管理后台登录IP地址能力。

（5）要采用安全的编码，系统支持账号管理和身份认证、访问控制、安全审计、资源控制和备份恢复等安全功能。系统支持现有CA认证的应用，并与现有数字证书认证（CA）体系的集成。

（6）为了保障应用系统自身运行的数据的保存以及应用系统恢复功能，信息安全运维系统支持备份恢复功能，主要包括：支持数据备份功能，并且支持针对基础数据、配置策略、监控数据、报警数据等不同功能模块数据的分类备份功能和总体备份功能。支持分项备份数据和总体备份文件的恢复功能。

（7）支持利用通信网络将关键数据定时批量传送至备用地址，如FTP或其他方式。

（8）要依据《烟草行业信息系统运行维护工作管理办法》（国烟办综〔2010〕320号），完善运维服务流程，规范信息发布程序，保障系统安全稳定运行。

**九、 服务与运维要求**

9.1服务要求

中标方须做好以下服务：

（1）依据标书和用户的要求进行《详细设计方案》设计、《实施方案》等，项目过程中任何改进与调整须与用户方协商一致；

（2）根据用户方需要，支持与相关的原有应用系统的集成。

9.2运维要求

9.2.1项目免费维保期要求

自终验合格之日起1年。

9.2.2运维人员要求

项目在免费维保期内，要求开发商安排不少于1名工程师常驻公司现场进行运维服务, 对开发集成系统生成的报表、告警、安全事件等的情况进行归纳和日常分析，并对处置情况进行跟踪、协调，以确保系统正常工作，及运行的有效性。1名运维人员应从系统建设开始即需参加开发、集成工作。

项目在免费维保期内，有固定的维护技术支持团队，保障项目在整体正常运行。

9.2.3运维服务内容要求

自本项目通过招标人的终验验收合格后起1年，乙方需提供免费运维服务，应包括但不限于以下内容：

1.安排1名工程师在甲方现场进行5x8小时（无特殊情况一般是法定工作日的8时至17时，下同）服务；乙方人员在甲方指定工作现场工作产生的交通、食宿等一切费用由乙方自行承担。

2.负责所开发集成系统的日常运维，确保系统达到正常工作状态。对所开发集成系统生成的报表、告警、安全事件等的情况进行归纳和日常分析，并对处置情况进行跟踪、协调，以确保系统工作的有效性。

3.升级服务：维护期内出现质量问题时，提供软件升级服务、必要的相关应用系统改造支持和其它现场技术支持服务。

4.报表服务：根据要求，完成相关报表的制作。

5.响应服务：在4小时响应时间内提供维护、维修、技术支持响应服务。保证招标人可以得到实时技术支持响应，在系统出现故障的0.5小时内给予问题处理建议的响应。

6.热线服务：要有技术支持团队提供7x24小时热线电话支持服务，解答用户在系统使用中遇到的问题，及时提出解决问题的建议和操作方法。对于电话咨询解决不了的问题，经甲方授权后方可通过Internet远程登录或其它方式进入到甲方网络系统进行故障诊断和故障排除。若以上两种服务形式仍不能解决问题，乙方需指派技术人员在甲方要求的时限内赶赴现场进行故障处理。遇到重大技术问题，乙方需及时组织有关技术专家进行会诊，并在甲方要求的时限内采取相应措施以确保系统的正常运行。在提供本项服务中产生的一切费用由乙方自行承担。

7.质量跟踪：项目验收完毕后，应定期跟踪，及时了解存在的问题，并给予解决。

8.按照甲方要求编制项目相关的技术标准。

**十、项目组织及管理要求**

10.1项目建设工期要求

信息安全运维系统项目建设周期为合同签订之日起15个月。要求开发商提供合理的分阶段项目计划和建议，保证项目按时保质保量完成。

10.2项目人员要求

投标人应在充分理解本项目需求的基础上，根据本技术需求书的要求，提供项目管理人员、咨询人员、技术人员、质量控制人员和实施人员的名单。参与项目建设的主要人员(项目经理、咨询负责人、技术负责人、主要的设计人员等项目核心成员)，在项目开发过程中不得随意变更，如有特殊原因确实需要变更，要预先告知用户，并做好人员的更换和风险控制工作。

项目管理经理须具有3年以上大型同类项目管理经验。项目开发团队、质量控制团队主要人员须具有3年以上大型项目开发及测试经验。项目实施团队核心人员须具有3年以上大型项目实施推广经验。

10.3项目管理要求

1、投标人应在标书中提供详细的系统设计、开发及实施计划，应包括项目组织机构、项目开发计划、项目实施流程、项目实施进度、项目实施安排。

2、投标人应向招标方提供参与本项目所有管理、技术人员的资质情况，并指派具有实际经验或信息系统集成资质的项目经理负责项目的组织、协调和实施工作。

**十一 、培训要求**

投标方须提供相关用户培训，以提供用户学习充足的专业知识，使其能有效使用系统资源。投标方应保证提供最有经验的教员，使各类人员在培训后能够独立地对系统进行操作、管理、维护。

（1）培训计划及大纲：投标方须提供相关用户培训（含培训所需的讲义、资料、教学设施等）。投标方必须提供必要的培训课程（上课目的、内容、课时、安排等）在建议书中进行说明。

（2）培训对象：包括系统管理员和各级最终系统用户。

（3）培训类别：包括原厂培训和应用系统培训。

（4）培训时间：培训课程应安排在整个项目计划的合适时间段内。

（5）培训费用：投标人应将所有培训费用（含培训教材费、培训教师费）及各项支出列入“培训费用价格单”中，并统一纳入项目总体报价费用。