招标编号：（ BMCC-ZC23-0943/1 ）　　包号： 03

采　购　合　同

项目名称： 改善办学保障条件-北京信息科技大学新校区图书馆楼数字档案馆管理平台项目（新竣工楼配套）

服务名称： 等保测评服务

甲　　方（买方）： 北京信息科技大学

乙　　方（卖方）： 北京天下信安技术有限公司

签署日期：2024 年 6 月 24 日

合　　同　　书

北京信息科技大学（甲方）改善办学保障条件-北京信息科技大学新校区图书馆楼数字档案馆管理平台项目（新竣工楼配套）（项目名称）中所需　等保测评　（服务名称），经　北京明德致信咨询有限公司　（招标代理机构）以　BMCC-ZC23-0943/1　号招标文件在国内公开（公开/邀请）招标。经评审委员会评定北京天下信安技术有限公司　（乙方）为中标人。甲、乙双方同意按照下面的条款和条件，签署本合同。

1、合同文件

下列文件构成本合同的组成部分，应该认为是一个整体，彼此相互解释，相互补充。为便于解释，组成合同的多个文件的优先支配地位的次序如下：

a. 本合同书；

b. 合同专用条款；

c 合同通用条款；

d 合同附件；

e 合同补充协议（如有）；

f 中标人的投标文件　（含澄清文件）；

g 本项目招标文件（含招标文件补充通知、澄清文件）。

2、服务内容和数量

本合同服务内容及数量：　等保测评服务 1 份

3、合同总价

本合同总价：人民币　98200　元

分项价格：　详见分项报价表

4、付款方式

（1）履约保证金:本合同签订后7日内，中标人先行向采购人支付合同金额5%作为履约保证金。项目完成验收且中标人合同项下的各项义务全部妥为履行完毕后，采购人无息退还履约保证金。

（2）完成本项目网络安全等级保护测评及协助备案且验收合格，收到中标人发票后15日内，采购人支付合同总价的100%到中标人账户。

（3）特别约定

1）由于本合同价款100%来源于政府财政拨付，合同约定的付款时间以财政资金实

际到位为前提，如因采购人财政资金未到位导致采购人无法按前述付款时间节点支付款项，中标人应同意待采购人财政资金到位后，对照合同中约定的支付进度节点，按工作程序支付；（收款账户信息：1.收款供应商单位全称：北京天下信安技术有限公司；2.收款单位信用代码：91110105MA004KAB71；3.供应商收款账号：20000091782000155393159；4.供应商账户开户行：北京银行中关村科技园区支行；5.供应商收款名称：北京天下信安技术有限公司。）

（4）关于支付路径的特别约定

1）本合同项下采购人应支付给中标人的任何款项，均应通过共管账户支付。因此中标人有义务按照采购人要求在采购人指定银行开立“共管账户”，确保项目款项安全、合规支付。

2）如因中标人未能及时开立共管账户导致双方无法按照本合同约定的时间节点付款的，相关付款期限应予以顺延，直至中标人共管账户妥为设立后再行支付，在此期间未能支付款项不视为采购人违约。

5、本项目实施时间和地点

项目实施的时间：从签订合同起，至2024年10月30日前 。

项目实施的地点：北京信息科技大学清河小营校区 。

6、合同的生效。

本合同经双方全权代表签署、加盖单位印章后生效。

甲方：北京信息科技大学（印章）

2024年6月24日

授权代表(签字)：穆婉

乙方：北京天下信安技术有限公司（印章）

2024年6月24日

授权代表(签字)：

地址：北京市海淀区小营东路12号

邮政编码：100192

电话：010-82426861

地址：北京市大兴区欣雅街15号院1号楼10层1008

邮政编码：100162

电话：18831640920

开户银行：北京银行学知支行　　开户银行：中国工商银行股份有限公司北京八里庄支行

账号：0109 0375 7001 2011 1040 824　　账号：0200003809020197189

纳税人识别号：121100006908051713　　纳税人识别号：91110105MA004KAB71

合同一般条款

1　定义

本合同中的下列术语应解释为：

1.1　“合同”系指买卖双方签署的、合同格式中载明的买卖双方所达成的协议，包括所有的附件、附录和构成合同的其它文件。

1.2　“合同价”系指根据合同约定，乙方在完全履行合同义务后甲方应付给乙方的价格。

1.3　“货物”系指乙方根据合同约定须向甲方提供的设备，包括技术说明、手册等其它相关资料。

1.4　“服务”系指根据合同约定乙方承担与供货有关的安装、调试、提供技术援助、培训和其他类似的服务。

1.5　“甲方”系指与成交人签署供货合同的单位（含最终用户）。

1.6　“乙方”系指根据合同约定提供货物及相关服务的成交人。

1.7　“现场”系指合同约定货物将要实施和安装调试的地点。

1.8　“验收”系指合同双方依据强制性的国家技术质量规范和合同约定，确认合同项下的货物符合合同规定的活动。

1.9　上述术语的具体内容须与投标文件一致。

2　技术规范

2.1　本合同项下乙方提供服务所适用的技术规范应与采购文件规定的技术规范和技术规范附件(如果有的话)及其报价文件的技术规范偏差表(如果被甲方接受的话)相一致。若技术规范中无相应说明，则以国家有关部门最新颁布的相应标准及规范为准。

3　知识产权

3.1　乙方应保证甲方在使用其提供的服务全部或其中任何一部分时不受第三方提出的侵犯专利权、著作权、商标权和工业设计权等侵权纠纷的起诉。如发生第三方指控乙方提供的服务侵权的，因此给甲方造成损失的，乙方应承担赔偿责任（包括但不限于甲方已经支付或虽未实际支付但已确认需要支付的违约金、损害赔偿金、律师费、诉讼费用等）。如果任何第三方提出侵权指控，乙方须与第三方交涉并承担由此发生的一切责任、费用和经济赔偿。

4　付款条件

4.1　按合同书第四条约定执行。

5　技术资料

5.1　合同项下技术资料(除合同特殊条款规定外)将以下列方式交付：

合同生效后，乙方应按甲方要求随时提供技术方案及辅助资料、手册、图纸等文件。

6　检验和验收

6.1　乙方应严格遵照招标文件第五章采购需求中规定的各项技术要求、技术指标，对拟测评的建设项目的系统功能及相关软件等进行详细而全面的测试，并出具相关技术资料。乙方在测评完成后，将甲方提供的相关资料随测评报告一同归还甲方。

6.2　甲方有权在乙方安全测评工作完毕且提交《信息系统安全等级测评报告》后，组织验收，并制作验收备忘录，签署验收意见。

6.3　甲方有在安全测评服务过程中派员监造的权利，乙方有义务为甲方监造人员行使该权利提供方便。

7　索赔

7.1　如果乙方提供的服务与合同或招标文件、投标文件有任何不符之处，甲方有权根据有资质的权威质检机构的检验结果向乙方提出索赔。

7.2　在合同履行期内，如果乙方对甲方提出的索赔负有责任，乙方应按照甲方同意的下列方式解决索赔事宜：

7.2.1　在法定的退货期内（自买方签署验收文件之日起七日），如甲方发现乙方有任何与本合同对应的政府采购招标文件、投标文件或本合同内容不符的情形时，甲方有权单方解除合同，并要求乙方将已收取的款项全额退还给甲方，并承担由此发生的一切损失和费用。如已超过退货期，但乙方同意退货，可比照上述办法办理，或由双方协商处理。

7.3　在甲方发出索赔通知后 3 天内，乙方未作答复，上述索赔应视为已被乙方接受。如乙方未能在甲方提出索赔通知后3天内或甲方同意的更长时间内解决索赔事宜，甲方有权从合同尾款中扣除索赔金额。如果这些金额不足以补偿索赔金额，甲方有权向乙方提出不足部分的补偿。

8　延迟交付或不适当履约

8.1　乙方应按照招标文件第五章采购需求中甲方规定的时间、要求全面、适当的履行

合同义务，为甲方提供服务。

8.2 如果乙方无正当理由迟延交付或履行合同不符合合同约定、招标文件及投标文件规定的，甲方有权提出违约损失赔偿或解除合同，具体按照合同第 9 条执行。

8.3 在履行合同过程中，如果乙方遇到不能按时提供服务的情况，应及时以书面形式将不能按时交货的理由、预期延误时间通知甲方。甲方收到乙方通知后，认为其理由正当的，可酌情延长交货时间。

9 违约赔偿

9.1 除合同第 13 条规定外，如果乙方没有按照合同规定的时间提供服务，每逾期一日，应按合同总金额的 1 %向甲方支付违约金，同时乙方仍应履行交货义务。甲方有权从应向乙方支付的合同价款中扣除该违约金。逾期超过 15 天的，甲方有权单方解除本合同，乙方已收取的合同价款全部退还买方，同时还应按照合同总价款的 20 %赔偿买方的损失。如该金额不足以弥补甲方的实际损失的，甲方有权继续向卖方追偿。

10 不可抗力

10.1 如果双方中任何一方遭遇法律规定的不可抗力，致使合同履行受阻时，履行合同的期限应予延长，延长的期限应相当于不可抗力所影响的时间。

10.2 受事故影响的一方应在不可抗力的事故发生后尽快书面形式通知另一方，并在事故发生后 3 天内，将有关部门出具的证明文件送达另一方。

10.3 不可抗力使合同的某些内容有变更必要的，双方应通过协商在 3 日内达成进一步履行合同的协议，因不可抗力致使合同不能履行的，合同终止。

11 合同争议的解决

11.1 因合同履行中发生的争议，合同当事人双方可通过协商解决。协商不成的，可由买方所在地人民法院管辖。

12 税费

12.1 与本合同有关的一切税费均适用中华人民共和国法律的相关规定。

13 违约解除合同

13.1 在乙方存在下列违约的情况下，甲方可向乙方发出书面通知，主张部分或全部解除合同、停止支付合同价款，要求乙方按本合同约定总价款的 20%支付违约金，并就造成的全部损失。同时保留向乙方追诉的权利。

13.1.1 乙方未能在合同规定的限期或甲方同意延长的限期内，提供全部或部分服务，

或者提供的服务质量不合格、不符合合同约定的；

13.1.2 乙方未能履行合同规定的其它主要义务的；

13.1.3 在本合同履行过程中有腐败和欺诈行为的。

13.1.3.1 “腐败行为”和“欺诈行为”定义如下：

13.1.3.1.1“腐败行为”是指提供/给予/接受或索取任何有价值的东西来影响甲方在合同签订、履行过程中的行为。

13.1.3.1.2“欺诈行为”是指为了影响合同签订、履行过程，以谎报事实的方法，损害甲方的利益的行为。

13.1.4 未经买方同意擅自单方解除合同、擅自将合同项下的工作转包给第三方完成。

13.1.5 其它不履行或不完全履行合同约定的各项义务、履行合同义务不符合合同及招标文件、投标文件规定的情形。

13.2 在甲方根据上述第13.1条规定的全部损失，包括但不限于卖方对买方所造成的直接损失、可得利益损失、买方因卖方违约需要支付给第三方的赔偿费用/违约金/罚款、调查取证费用/公证费/鉴定费用、诉讼仲裁费用、保全费用、律师费用、维权费用以及其他合理费用。

14 破产终止合同

14.1 如果乙方破产导致合同无法履行时，甲方可以书面形式通知乙方，单方终止合同而不给乙方补偿。但甲方必须以书面形式告知同级政府采购监督管理部门。该合同的终止将不损害或不影响甲方已经采取或将要采取的任何行动或补救措施的权利。

15 转让和分包

15.1 除甲方事先书面同意外，乙方不得部分转让或全部转让其应履行的合同义务。

15.2 经甲方同意，乙方可以将合同项下非主体、非关键性工作分包给他人完成。接受分包的人应当具备相应的资格条件，并不得再次分包。分包后不能解除乙方履行本合同的责任和义务，接受分包的人与乙方共同对甲方连带承担合同的责任和义务。乙方可以将合同项下非主体、非关键性工作分包给他人完成。但必须在报价文件中载明。

16 合同修改

16.1 甲方和乙方都不得擅自变更本合同，但合同继续履行将损害国家和社会公共利益的除外。如必须对合同条款进行改动时，当事人双方须共同签署书面文件，

作为合同的补充，并报同级政府采购监督管理部门备案。

17　通知

17.1　本合同任何一方给另一方的通知，都应以书面形式发送，而另一方也应以书面形式确认并发送到对方明确的地址。

18　计量单位

18.1　除技术规范中另有规定外，计量单位均使用国家法定计量单位。

19　适用法律

19.1　本合同应按照中华人民共和国的法律进行解释。

20　合同生效和其它

20.1　本合同应在双方签字盖章后生效。

20.2　下述合同附件为本合同不可分割的部分并与本合同具有同等效力：

1）服务范围及分项价格表

2）服务方案

3）服务承诺

20.3　本合同一式10份，具有同等法律效力。

21、特别约定：

21.1 本合同的附件，为本合同的组成部分，与本合同具有同等的法律效力。

21.2 本合同附件中的未尽事宜，应当按照投标文件执行。

21.3 本合同附件载明内容如与乙方投标文件不一致的，除非甲乙双方另有约定，否则应当以投标文件为准。

合同特殊条款

合同特殊条款是合同一般条款的补充和修改。如果两者之间有抵触，应以特殊条款为准。合同特殊条款的序号将与合同一般条款序号相对应。

2、 定义

1.5 甲方：本合同甲方系指： 北京信息科技大学

1.6 乙方：本合同乙方系指： 北京天下信安技术有限公司

1.7 现场：本合同项下的服务实施地点位于：北京信息科技大学指定地点。

4、付款条件：按合同书第四条约定执行。

5、合同生效后，乙方应按照甲方要求随时提供将技术方案及辅助资料、手册、图纸等文件。

服务方式：本合同项下的服务方式为：现场服务。

6、检验和验收：【同投标文件内容一致】

甲方应在乙方安全测评工作完毕且提交《信息系统安全等级测评报告》后，组织验收，并制作验收备忘录，签署验收意见。

7、索赔：

如果在甲方发出索赔通知后 3 天内，乙方未作答复，上述索赔应视为已被乙方接受。如乙方未能在甲方提出索赔通知后 3 天内或甲方同意的更长时间内，按照本合同第 7.2 条规定的方法解决索赔事宜，甲方将从合同尾款中扣回索赔金额。如果这些金额不足以补偿索赔金额，甲方有权向乙方提出不足部分的补偿。

10、 不可抗力：

10.1 不可抗力通知送达时间：事故发生后 3 天内。

附件一　投标分项报价表

投标分项报价表

项目编号/包号：BMCC-ZC23-0943/1 项目名称：改善办学保障条件-北京信息科技大学新校区图书馆楼数字档案馆管理平台项目（新竣工楼配套）

报价单位：人民币元

序号	名称	数量	单价	总价	供应商企业类型				备注
					大型	中型	小型	微型	
1.	等级保护二级系统测评	1	65000.00	65000.00			小型企业		无
2.	网络安全建设指导	1	24000.00	24000.00			小型企业		无
3.	安全巡检服务	1	9200.00	9200.00			小型企业		无
4.	等保管理制度建设及落地辅导工作	1	0	0			小型企业		无
5.	信息安全培训、售后服务	1	0	0			小型企业		无
总价　98200.00 元									

注：1. 本表应按包分别如实填写。

2. 如果不提供分项报价将视为没有实质性响应招标文件。

3. 上述各项的详细规格（如有），可另页描述。

4. 投标人的报价的最小单位只能到“分”，否则将视未实质性响应。

投标人名称（加盖公章）：北京天下信安技术有限公司

日期：2024年　　月　　日

附件二　服务方案

北京天下信安技术有限公司本项目详细方案

2.1.北京天下信安技术有限公司技术实施方案

北京天下信安技术有限公司投标优势

北京天下信安技术有限公司非常荣幸参加北京信息科技大学的“改善办学保障条件-北京信息科技大学新校区图书馆楼数字档案馆管理平台（新竣工楼配套）”中涉及等保测评项目的投标，以及对北京天下信安技术有限公司的信任和支持，表示衷心的感谢。

北京天下信安技术有限公司是公安部认证的网络安全等级测评与检测评估认证服务机构，是常年为政府、客户、金融等行业提供信息化服务的单位，在等级保护测评服务方面的服务优势如下：

丰富的行业信息化服务经验：为国家林业和草原局、北京共青团、中国化工、中国人保等多家单位提供了等级保护咨询及测评服务；

全面专业的信息安全资质：具有 ISO9001、ISO20000、ISO27001 等国际标准认证；取得了等保测评、高新技术客户、信息安全服务、风险评估、安全运维、应急处理等服务资质；是中关村信息安全测评联盟会员、中关村网络安全与信息化产业联盟成员、中国网络空间安全协会成员、北京商用密码行业协会会员。等级测评及安全服务能力得到了国家权威认证机构的认可，服务能力覆盖本项目所涉及的各个方面，能够切实保障服务质量。

2.1.1. 项目背景

网络安全等级保护制度是国家信息安全保障工作的基本制度，开展网络安全等级保护工作不仅是加强国家信息安全保障工作的重要内容，也是一项事关国家安全、社会稳定的政治任务。

1994 年，国务院 147 号令《中华人民共和国计算机信息系统安全保护条例》规定“计算机信息系统实行安全等级保护”；2003 年《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）的出台明确提出了 “要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。为了贯彻落实 147 号令和 27 号文的要求，公安部等四部委制定了《信息安全等级保护管理办法》（公通字[2007]43 号），该文件由四部委共同会签印发，主要内容包括信息安全等级保护制度的基本内容、流程及工作要求，以及信息安全等级保护建设的几个环节，包括：信息系统定级、备案、安全风险评估及差距分析、安全建设整改、等级测评的实施与管理，信息安全产品和测评机构选择等，为开展信息安全等级保护工作提供了规范保障。2005 年发布的《关于信息安全等级保护的实施意见》（公通字 [2005] 66 号），确立了等级保护作为国家信息安全保障的基本制度，指出“信息系统安全等级保护制度是国家在国民经济和社会信息化的发展过程中，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设健康发展的一项基本制度”。

为响应国家等级保护政策及学校相关要求，落实国务院 147 号令《中华人民共和国计算机信息系统安全保护条例》和公安部《信息安全等级保护管理办法》（公通字[2007]43 号）等文件的要求，信息系统运营、使用单位或者其主管部门应定期对信息系统安全等级状况开展等级测评及安全性测试工作。

北京市信息科技大学根据北京市档案局关于转发《国家档案局关于进一步推进机关数字档案室建设的意见》（京档字[2020]14 号）的通知要求，北京信息科技大学需实现数字档案馆建设。按照《电子档案管理系统通用功能要求》对数字档案管理系统通用功能要求进行模块划分、完善，逐步实现北京信息科技大学电子档案收集、管理、存储等，校内实现公开档案数据的查询、检索；校友、离校

学生通过软件平台实现数据的一对一推送，逐步减少纸质档案，为逐步实现无纸化办公创造试点条件。利用校档案馆网站，部分开放政策性允许公开的文件资料、学校规章制度等，做好对学校档案工作的整体介绍、平台展示。

整体建设项目完成后将实现以下功能（1）建设起数字档案管理平台，提供“一站式”档案管理。（2）档案工作融入新校区智慧校园建设，并助推智慧城市建设。（3）高效合理布局新校区资源，支撑教科研和管理活动发展。

北京市信息科技大学为响应国家等级保护政策及学校相关要求，按照等保三同步原则即同步规划、同步建设、同步使用积极完善信息系统安全防护建设需求。

《中华人民共和国网络安全法》已于2017年6月1日起正式施行，其中第二十一条明确规定了网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。《网络安全法》将等级保护制度从一项基本制度、基本国策上升到了法律层面，将进一步推动等级保护制度在实际应用中的落实与执行。

为贯彻和落实国家网络安全等级保护工作的相关要求，北京信息科技大学需要委托网络安全等级测评与检测评估机构对信息系统开展等级保护测评工作，并按照等级保护的相关要求对其信息系统进行安全整改等工作，不断降低信息安全风险，保障重要业务的安全稳定运行。

2.1.2.项目服务目标和实施周期

2.1.2.1. 项目服务目标

在2024年10月30日前完成1套等保二级系统的定级备案、提供整改建设咨询及测评工作并出具被测系统的测评报告。

2.1.2.2.项目服务周期和地点

1、项目服务周期计划：

实施时间：从签订合同起，至2024年10月30日前，提供符合北京信息科技大学要求的网络安全等级保护测评服务并达到验收合格标准，并提供为期一年

的售后咨询服务。

2、服务地点：

北京信息科技大学清河小营校区。

2.1.3. 项目单位情况·

2.1.3.1.采购单位基本情况

北京信息科技大学是北京市重点支持建设的高校，是一所信息类学科齐全、信息特色鲜明，以本科、研究生教育为主体的多科性大学。学校由原机械部所属北京机械工业学院、原电子部所属北京信息工程学院合并组建而成。原北京机械工业学院源于1937年的北平市立高级商业职业学校，1958年多源汇流成立北京机械学院，1990年更名为北京机械工业学院，归机械电子工业部领导。原北京信息工程学院源于1978年创建的北京大学第二分校，1985年更名为北京信息工程学院，隶属电子工业部，1997年合并成立新的北京信息工程学院。2008年正式合并组建北京信息科技大学。

学校1958年开始大规模本科教育，1981年开始培养研究生，2018年获批设立博士后科研工作站，2021年获批成为博士学位授予单位，2023年获批仪器科学与技术学科博士后科研流动站，构建了全日制本科教育、硕博研究生教育到成人教育、留学生教育的全方位、多层次的办学格局和人才培养体系。

学校现有沙河、小营、健翔桥、金台路、酒仙桥五个校区，占地面积81万余平米，设有二级教学单位15个。现有全日制本科生11019人，全日制硕士研究生3091人，全日制博士研究生58人，留学生137人。在长达87年的办学历程中，学校始终扎根中国大地，融入国家机械工业、计算机事业的起步发展，为国防科技事业做出了不可磨灭的贡献，同时也形成了鲜明的信息特色、军工特色、行业特色，积淀了“勤以为学 信以立身”的校训精神和大学文化。

2.1.3.2.投标单位基本情况

本项目投标方为北京天下信安技术有限公司（以下简称“天下信安”）。

公司概况如下：是公安部认证的网络安全等级保护测评与检测评估认证机构（认证证书编号：SC202127130010219）。2016 年 4 月成立，是一家专业的网络安全整体解决方案咨询服务商。核心业务包括网络安全等级测评、软件测试、渗透测试、信息安全风险评估、安全运营和安全体系咨询等。

天下信安自成立以来，通过了 ISO9001 质量管理体系认证、ISO20000 信息技术服务管理体系认证、ISO27001 信息安全管理体系认证等国际标准认证；取得了高新技术企业证书、CNAS 实验室认可证书、信息安全服务资质、信息安全风险评估服务资质、信息系统安全运维服务资质、信息安全应急处理服务资质，以及多个计算机软件著作权登记证书；同时是中关村信息安全测评联盟会员、中关村网络安全与信息化产业联盟成员、中国网络空间安全协会成员、北京商用密码行业协会会员。现阶段客户已覆盖政府、事业单位、电信、金融、交通、IDC、教育、互联网等行业客户。

2.1.4.项目需求分析

2.1.4.1.服务内容分析

本项目服务内容主要包括：

1、系统定级备案

服务内容：了解北京信息科技大学新校区图书馆楼数字档案馆管理平台信息系统用途、功能、系统网络架构等基础上，依据《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020）要求，协助北京信息科技大学完成北京信息科技大学新校区图书馆楼数字档案馆管理平台 1 个新建第二级系统的定级报告和系统备案表的编写，并组织信息系统定级专家评审会，获取专家评审意见。

2、安全差距分析

服务内容：差距分析的目的是根据《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019），对确定安全保护等级的 1 个新建第二级系统（北京信息科技大学新校区图书馆楼数字档案馆管理平台信息系统），从技术和管理两方面分析其现有的安全防护措施是否达到相应保护等级的要求。包括如下两部分内容：

①技术分析：根据国家信息安全等级保护相应级别的技术要求，对物理环境、主机安全、网络安全、应用安全、数据安全开展差距分析工作。通过访谈、调研问卷、技术测试、查阅资料等多种手段，逐项分析信息系统安全防护水平与等级保护相应级别技术要求的差距。

②管理分析：根据国家信息安全等级保护相应级别的管理要求，通过访谈、调研问卷、查阅资料、要求客户举证等多种手段，逐项分析信息系统安全防护水平与等级保护相应级别技术要求的差距。

3、安全整改咨询

服务内容：供应商需要根据差距分析测评中出现的问题，结合系统实际情况，提供合理、切实可行的整改建议，并全程协助北京信息科技大学进行整改工作，使各系统达到等级保护相应级别的要求，并能通过国家相关主管部门的审核。

4、等级保护测评

服务内容：在整改工作完成后，负责对 1 个新建第二级系统（北京信息科技

大学新校区图书馆楼数字档案馆管理平台信息系统），根据《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）及《信息安全技术网络安全等级保护测评过程指南》（GB/T 28449-2018）等要求进行现场等级保护测评，出具公安部门认可的信息系统安全等级测评报告。

2.1.4.2.服务范围分析

1、1 个新建第二级系统的等级保护定级、备案、测评服务，包括：北京信息科技大学新校区图书馆楼数字档案馆管理平台信息系统。

2.1.4.3.安全需求分析

2.1.4.3.1.符合等级保护要求的需求

正如前面所述，信息系统的信息化建设必须符合国家的相关规定和要求，从安全的角度，对信息安全保障体系进行全面的规划和设计，符合相关标准，确保北京信息科技大学安全保障体系的广度和深度。从政策符合性的角度，北京信息科技大学信息安全保障体系建设必须要满足：

从信息资产划分和等级化保护设计的角度，必须符合《计算机信息系统安全保护等级划分准则》GB17859 的技术准则，对北京信息科技大学信息资产进行分级分类的设计和规划；

方案的建设原则必须以《国家信息化领导小组关于加强信息安全保障工作的意见》（中办[2003]27 号文件）的指导思想为准则，坚持“积极防御、综合防范”的建设方针，坚持“用发展的思路来解决信息安全问题，从发展中求安全，以安全保发展”的设计思路，规划并实施北京信息科技大学整体安全保障体系。

在《信息系统安全等级保护定级指南》和《信息系统安全等级保护实施指南》中规定了五个安全保护等级，已成为国家基础信息设施和实施安全等级保护的基础。完整地、正确的理解每一个安全保护等级的安全要求，并合理地确定目标系统的安全保护等级，是将安全等级保护合理地运用于具体信息系统的重要前提。五个安全保护等级指标描述如下：

第一级　自主性保护级

由公民、法人和社会组织参照国家标准自主进行保护。主要适用于一般信息系统。

第一级安全的信息系统具备对信息和系统进行基本保护的能力。

在技术方面，第一级要求设置基本的安全功能，使信息免遭非授权的泄露和破坏，能保证基本安全的系统服务。

基本安全的功能是指：

对计算机、网络的设备、环境和介质采用基本的防护措施，确保其为信息系统的安全运行提供支持，防止由于物理原因造成信息的泄漏和破坏；

通过分区域保护，采用以口令方式为主的身份鉴别、 粗粒度的自主访问控制、数据的备份和完整性保护、主机方式的病毒防护、适当的操作系统和数据库的安全配置等安全防护机制，提供对系统和信息基本的安全控制；

按照模块化结构的方法设计和实现安全子系统，并进行基本的自身安全保护，确保安全子系统的安全功能具有所要求的安全性。

在安全管理方面，自主性保护级要求“根据机构自身安全需求，为信息系统正常运行提供基本的安全管理保障”。

信息系统应根据自身安全需求，确定安全策略和防护目标，并基于安全策略在某些控制环节制订相应的管理规定；

在信息系统的工程建设中进行适当的安全管理，使建设成果达到预期设计的安全要求；

在包括机房门禁管理、设备和资源管理等方面做到事事有人管；

规定了管理员在病毒防护管理、服务器维护、用户账户维护等系统日常工作中的基本操作要求，以维护系统正常运行；

采取常用的防御性控制措施，具备基本的应急响应流程和恢复方法。

第二级　指导性保护级

在政府职能部门指导下，有公民、法人和社会组织按照国家标准自主进行保护。主要适用于企事业单位的内部信息系统。

第三级安全的信息系统具备对信息和系统进行比较完整的系统化的安全保护能力。

在技术方面，第三级要求采用系统化的设计方法（即：把各种安全机制，设计成一个安全子系统），按照木桶原理，实现比较完整的安全保护，并通过安全审计机制，使其它安全机制间接的相连接，使信息免遭非授权的泄漏和破坏，保证一定安全的系统服务。

系统化设计和比较完整的安全功能是本级安全的重要特征，主要是指：

对计算机、网络的设备、环境和介质采用一定的防护措施，确保其为信息系统的安全运行提供支持，防止由于物理原因造成信息的泄漏和破坏；

通过对区域计算环境内各组成部分采用入侵防范、安全审计、数据的备份于恢复极重要设备的冗余设计、数据的完整性保护、集中统一的病毒监控体系、高强度口令的身份鉴别、细粒度的自主访问控制、存储和传输数据的加密保护、严格的系统和数据库安全配置、重要系统的客体重用等安全机制，实现对局域计算环境内信息的安全保护和系统安全运行的支持；

采用分区域保护和边界防护（如防火墙、网络隔离部件、信息过滤、边界完整性检查等），实现不同安全等级区域之间安全互操作的控制；

按照系统化的要求和层次化结构的方法设计和实现安全子系统，在完整的系统化的安全保护基础上，采用了基本的审计、入侵防范等检测手段，使系统实现初步的动态安全性。

在安全管理方面，指导性保护级的要求“建立必要的信息系统安全管理制度，对岸”管理和执行过程进行计划、管理和跟踪。根据实际安全需求，明确机构和人员的相应责任。

“必要的信息系统安全管理”是指：

按照国家标准的要求，确定信息系统的安全方针和策略，明确机构和人员在安全方面的职责；

在机房管理、设备管理、访问控制管理、病毒防护、应急管理、工程建设管理等必要的环节，将管理意图以管理制度、操作规范、计划和流程等文件化方式加以固化；

加强对管理制度、操作规范、计划和流程的执行情况的跟踪和检查；

加强对系统以外人员的管理；

加强系统安全风险管理要求，基本实现全系统的风险管理。

第三级　监督性保护级

在政府职能部门的监督下，由信息系统主管部门运营、使用单位，按国家标准严格落实各项保护措施进行保护。

第三级安全的信息系统具备对信息和系统进行基于安全策略强制的安全保护能力。

在技术方面，第三级要求按照确定的安全策略，实施强制性的安全保护，使数据信息免遭非授权的泄漏和破坏，保证较高安全的系统服务。

完整的安全策略模型和由系统进行的强制性的安全保护是本级的重要特征，前者是从设计角度确保安全功能的安全性达到预期目标，后者是指安全策略是由系统统一执行，并加强于所有保护对象之上。

对计算机、网络的设备、环境和介质采用较严格的防护措施，确保其为信息系统的安全运行提供硬件支持，防止由于硬件原因造成信息的泄漏和破坏；

通过对局域计算环境内各组成部分采用网络安全监控、安全审计、数据、设备及系统的备份与恢复、集中统一的病毒监控体系、两种鉴别方式组合实现的强身份鉴别、细粒度的自主访问控制、满足三级要求的操作系统和数据库、较高强度密码支持的存储和传输数据的加密保护、客体重用等安全机制，实现对局域网计算环境内信息的安全保护和系统安全运行的支持；

采用分区域保护和边界防护（如应用级防火墙、网络隔离部件、信息过滤和边界完整性检查等），在不同区域边界统一制定边界访问控制策略，实现不同安全等级区域之间安全互操作的较严格控制；

按照系统化的要求和层次化结构的方法设计和实现安全子系统，增强各层面的安全防护能力，通过安全管理中心，在统一安全策略下对系统安全事件集中审计、集中监控和数据分析，并做出响应和处理，从而构建较为全面的动态安全体系。

在安全管理方面，监督性保护级要求“建立完整的信息系统安全管理体系，对安全管理过程进行规范化的定义，并对过程执行实施监督和检查。根据实际安全需求，建立安全管理机构，配备专职安全管理人员，落实各级领导及相关人员的责任。”

“完整的信息系统安全管理体系”是指：

在信息系统的安全方针和策略的指导下，在策略、组织、人员、风险、工程、运行、应急与安全事件处理等安全管理的各个环节建立相应的管理制度和工作规范；

通过建立安全管理机构，配备专职安全管理人员为安全管理提供必要组织保证和人员保证，目的在于落实各级领导及相关人员的责任；

各项管理制度明确管理目标、人员职责、关键控制点和管理手段；

具备对管理制度执行情况的监督和检查机制，加强集中统一管理，注重引入自动化的管理工具，丰富管理和监督检查手段。

第四级　强制性保护

在政府职能部门的强制监督和检查下，信息系统主管部门和运营、使用单位、按国家标准和安全需求，严格落实各项措施进行保护。

第四级安全的信息系统具备对信息和系统进行基于安全策略强制的安全保护能力。

在技术方面，第四级要求按照确定的安全策略，整体的实施强制性的安全保护。采用结构化设计方法，按照完整的安全策略模型，实现各层面相结合的强制性安全保护，使数据信息免遭非授权的泄漏和破坏，保证高安全的系统服务。

第四级的技术要求，采用以结构化设计为代表的一系列措施来保证其安全性达到所要求的目标。实现这些安全功能和提供安全保证的安全技术主要包括：

对计算机、网络的设备、环境和介质采用严格的防护措施，确保其为信息系统的安全运行提供支持，防止由于物理原因造成信息的泄漏和破坏；

通过局域计算环境内各组成部分采用网络安全监控、安全审计、全方位的备份与故障恢复、集中统一的病毒监控体系、基于密码技术或生物特征的强身份鉴别和多重鉴别、强访问控制、高强度密码支持的存储和传输数据的加密保护、严格的客体重用等安全机制，实现对局域计算环境内信息的安全保护和系统安全运行的支持；

采用分区域保护和边界防护（如高等级的防火墙、信息过滤、边界完整检查和其他隔离部件），实现不同安全等级区域之间安全互操作的严格控制；

按照结构化的方法设计和实现安全子系统，使在不同层面实现的访问控制、身份鉴别、审计、加密等安全机制的交互作用最小化，从而使复杂性降低，

充分实现系统安全设计要求。

在安全管理方面，强制性保护级要求“建立持续改进的信息系统安全管理体系，在对安全管理过程进行规范化定义，并对过程执行实施监督和检查的基础上，具有对缺陷自我发现、纠正和改正的能力。根据实际安全需求，采取安全隔离措施，限定信息系统规模和应用范围。建立安全管理机构，配备专职安全管理人员，落实各级领导及相关人员的责任。”

“持续改进的信息系统安全管理体系”是指：

在维护完整的信息系统安全管理体系的基础上，建立系统的自我完善机制，具备对不断变化的系统状态自我发现和解决问题能力：

通过采用安全隔离措施，限定信息系统的规模和应用范围，增强信息系统的安全性，以达到所要求的安全目标。

第五级　专控性保护级

由信息系统的主管部门和使用单位根据安全需求，对信息系统进行专门控制和保护，政府职能部门予以协助。主要适用于国家最重要核心部门的专用信息系统。

第五级安全的信息系统提供对信息和系统进行基于可验证安全策略强制的安全保护能力。

在技术方面，第五级要求按照的安全策略，在整体的实施强制性的安全保护的基础上，通过可验证设计增强系统的安全性，使其具有抗渗透能力，使数据信息免遭非授权的泄露和破坏，保证最高安全的系统服务。

在结构化设计的基础上，采用核心可验证设计是本级的重要特征。实现这些安全功能和提供安全保证的安全技术主要包括：

对计算机、网络的设备、环境和本质采用最严格的防护措施，确保其为信息系统的安全运行提供硬件支持，防止由于硬件原因造成信息的泄露和破坏；

通过局域计算环境内各组成部分采用网络安全监控、安全审计、全方位的备份与故障恢复、集中统一的病毒监控体系、基于密码技术或生物特征的强身份鉴别、细力度的自主访问控制、全面的强制访问控制、最高强度密码支持的全程数据和加密保护、严格的客体重用等安全机制，实现对局域计算环境内信息的安全保护和系统安全运行的支持；

采用物理隔离措施，实现最严格控制的边界保护；

用结构化的方法设计和实现安全子系统，使作为安全子系统核心的“访问监督器”和“前端过滤器”足够小，达到可验证，并具有抗渗透能力，确保安全子系统的安全功能具有所要求的安全性。

在安全管理方面，专控性保护级要求“由信息系统的主管部门和使用单位根据安全需求，建立核心部门的专用信息系统安全管理体系，对安全管理过程进行规范化的定义，并对过程执行实施监督和检查，具有对缺陷自我发现、纠正和改进的能力。采取安全隔离措施，限定信息系统规模和应用范围。建立安全管理机构，配备专职安全管理人员，落实各级领导及相关人员的责任。

“建立完善的信息系统安全管理制度，从工程管理和系统管理方面，对执行过程进行规范化的定义和管理，并严格执行：根据实际安全需求，采取安全隔离措施，限定信息系统规模和应用范围，建立安全管理机构，配备专职安全管理人员，落实各级领导及相关人员的责任。确保安全功能达到预期目标。”

“核心部门的专用信息系统安全管理体系”是指：

针对核心部分专门的安全需求，在严格限定的信息系统规模和应用范围内，制定相应的安全策略和安全管理体系；

管理体系中各项管理制度管理目标、人员职责、关键控制点和管理手段定义明确，具有良好的可操作性和可检查性；管理体系具有自我完善机制，对不断变化的系统状态具有自我发现和解决问题能力。

2.1.4.3.2.安全需求汇总

北京天下信安技术有限公司能够根据北京信息科技大学测评服务项目的实际情况，为北京信息科技大学提供全流程的等级保护测评服务。

系统定级备案

对现有信息系统的梳理，分析确定信息系统的准确级别，最终完成等级申报备案。

输出：信息系统等级保护定级报告、信息系统等级保护备案表、专家评审意见、其他定级备案材料等保相关标准文件。

安全差距分析

从技术方面和管理方面分析其现有的安全防护措施是否达到等级保护相应级别的要求。包括漏洞扫描、渗透测试安全验证手段。

输出：等级保护差距分析报告、漏洞扫描、渗透测试。

安全整改咨询

依据差距分析报告，结合实际情况，提供合理、切实可行的整改设计方案，协助完成系统的整改加固工作。

输出：等级保护整改建议方案。

等级保护测评

等级测评过程包括人员访谈、现场文档检查和现场技术测评三部分工作。我们将就这三部分工作提供具有针对性的服务。

输出：网络安全等级保护测评报告。

2.1.5.实施原则和策略

1、最小影响原则

等级保护测评工作应尽可能小的影响系统和网络的正常运行，不能对现有网络的运行和业务的正常运行产生明显影响（包括系统性能明显下降、网络拥塞、服务中断，如无法避免出现这些情况必须做出详细描述说明，并制定详细工作计划）；等级保护测评方案的设计和实施应在保证系统安全性的基础上，尽可能减小对业务系统和网络的正常使用运行影响。

2、可控性原则

实施方法和过程需要在双方认同（认可）的范围之内，各项安全服务进度要严格按照项目工作计划执行，保证北京信息科技大学对等级保护建设和风险评估项目工作的可控性。

3、整体性原则

等级保护和风险评估项目的工作内容要求做到体系完整全面。

4、标准性原则

等级保护定级备案、风险评估、等级保护测评的实施应依据国内的相关标准进行。

5、规范性原则

服务厂商实施过程和交付物文档，要求具有标准规范性，便于项目的跟踪与控制。

6、保密原则

对项目实施中产生的数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害北京信息科技大学的行为，否则北京信息科技大学有权追究其责任。

2.1.5.1.项目依据

本项目各项工作均应依据但不限于下列相关的政策条例、国家标准、行业标准：

《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发

[2003]27 号）

《关于信息安全等级保护的实施意见》（公通字[2005]66 号）

《信息安全等级保护管理办法》（公通字[2007]43 号）

《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861 号）

《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303 号）

《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429 号）

《信息安全技术网络安全等级保护测评过程指南》（GB/T 28449-2018）

《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）

《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）

《信息安全技术网络安全等级保护安全设计技术要求》（GB/T25070-2019）

《网络安全等级保护测评高风险判定指引》（T/ISEAA 001-2020）

《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020）

《网络安全等级保护测评报告模板（2021 年版）》

2.1.5.2.总体实施方案设计

等级保护的五个规定动作分别是定级、备案、建设整改、安全测评、监督检查，定级与备案属于等级保护前两个动作，定级过程中又涉及到评审，所以再分则可以理解第一个大阶段包含定级、评审与备案三个工作项。

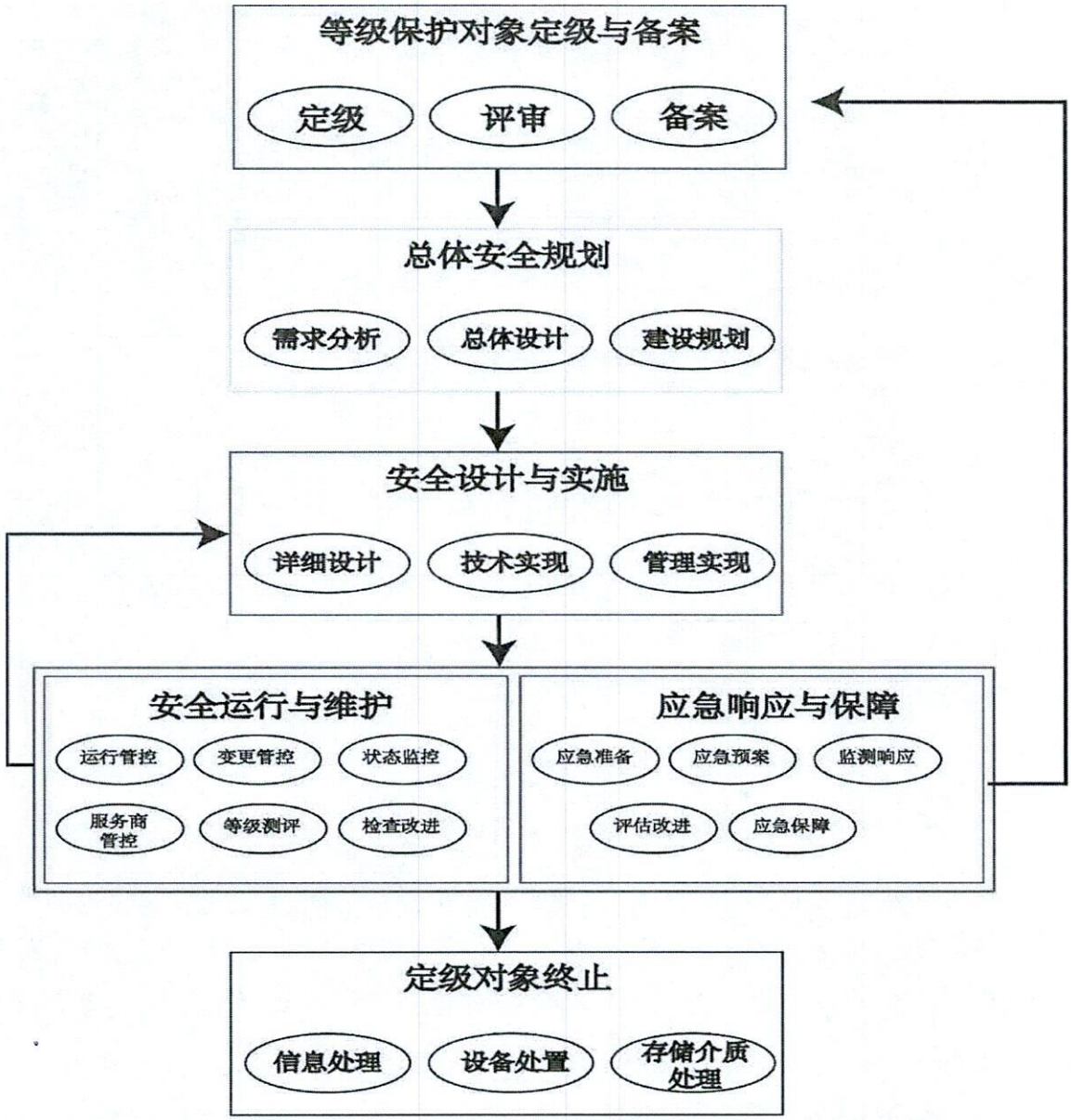


图 3-1 等级保护工作实施的基本流程框架

我们将通过以下几个步骤以及贯穿始终的项目管理，并有机融合国家网络安全等级保护要求，为本项目提供安全服务及测评。

本项目总体服务方案设计图如下：

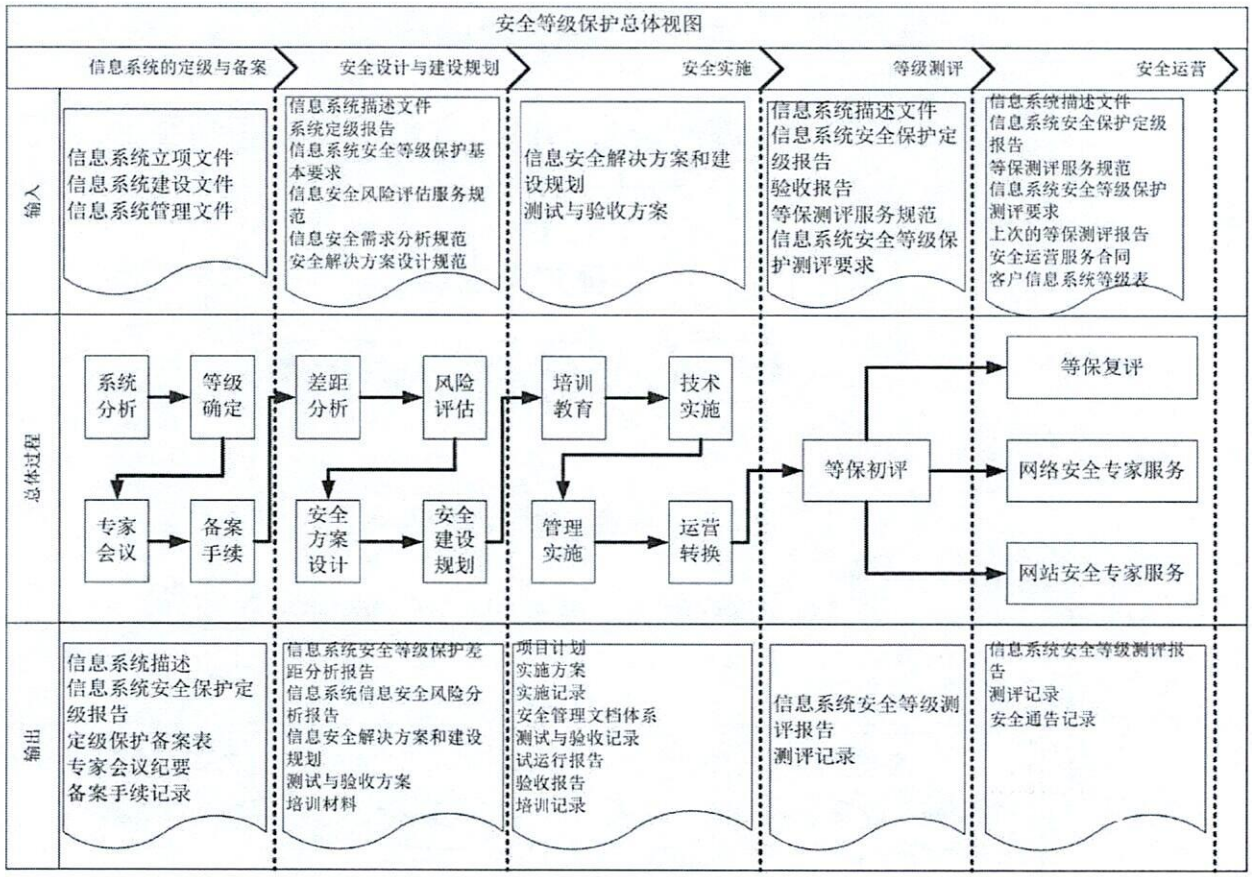


图 3-2 天下信安项目安全服务总体框架

本项目，将首先对本项目安全现状进行科学的评估和分析，以了解本项目的信息安全现状和问题，根据安全现状，进行定级备案、差距分析、整改指导，最后进行等级测评活动：测评准备活动、方案编制活动、现场测评活动、分析及报告编制。

本项目中开展的工作将包括以下内容：

定级备案

差距分析

整改指导

等级保护测评

2.1.5.3.项目总体实施方法概述

综合分析系统现状、行业相关要求及北京信息科技大学信息的安全现状，天下信安为本项目提供一站式等保合规性服务，我们将通过以下几个步骤以及贯穿

始终的项目管理对北京信息科技大学信息系统整体现状进行技术和管理体系的分析，并进行等级保护测评。

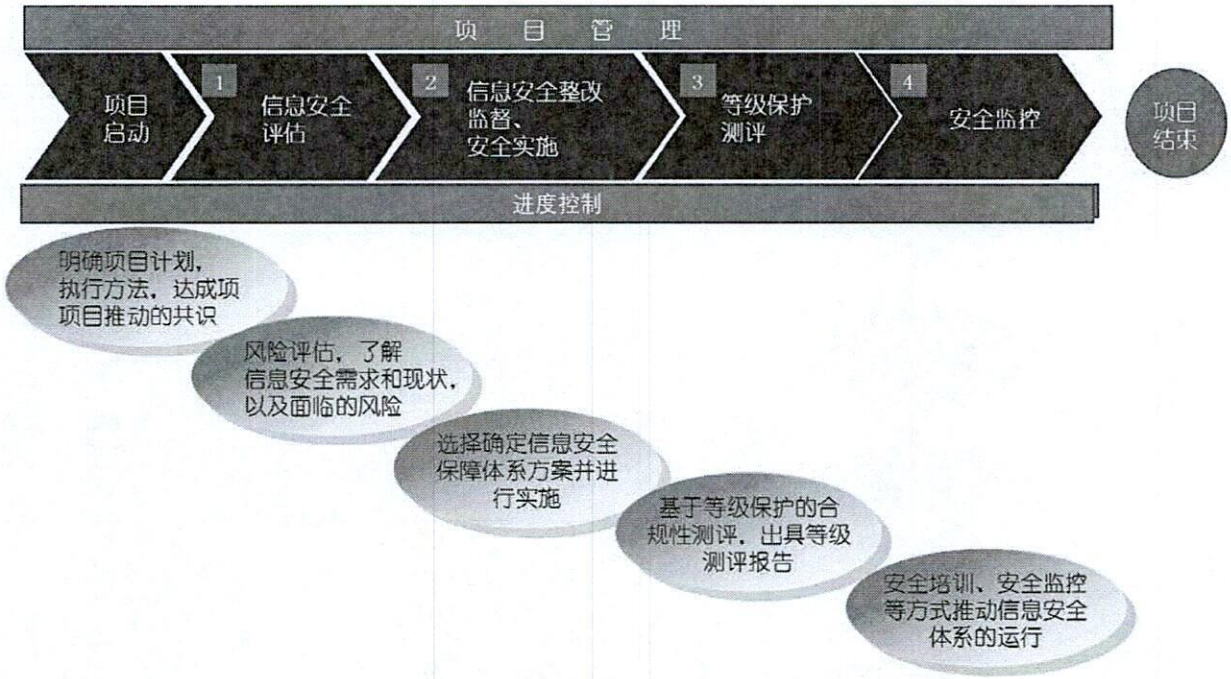


图 3-3 项目实施步骤

2.1.5.4.系统定级备案

依据上图，我们将定级与备案工作分成五个阶段。

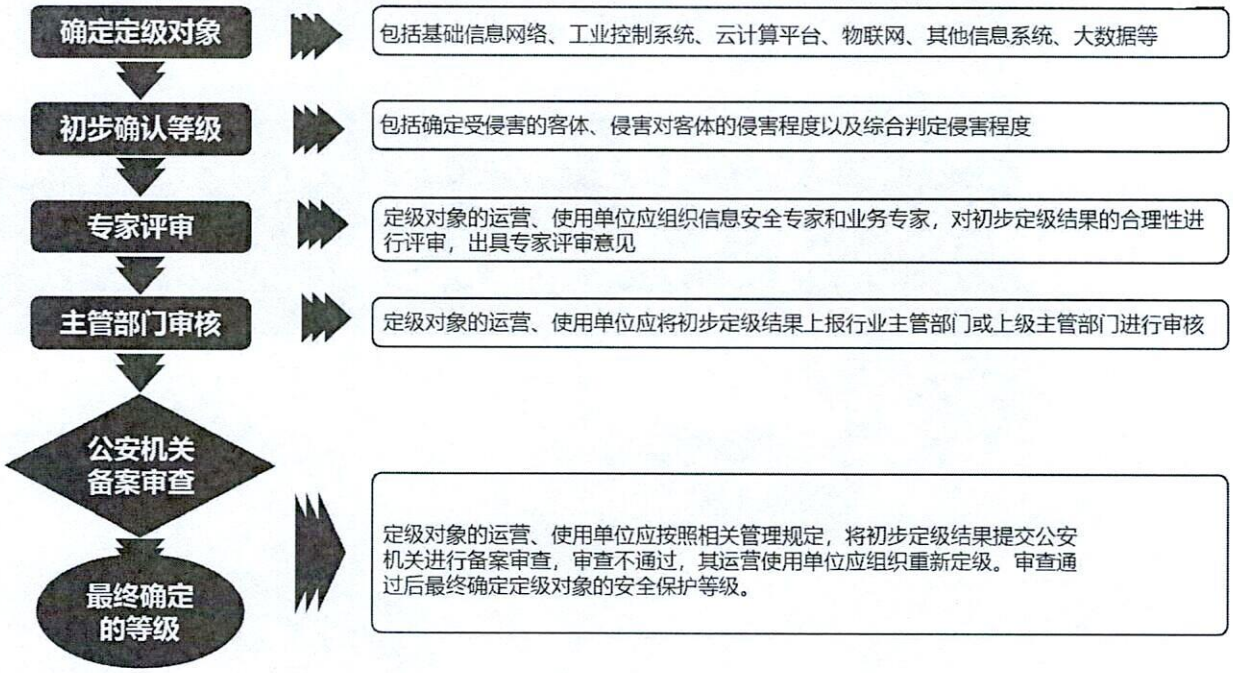


图 3-4 项目实施步骤

我方协助完成信息系统定级备案等相关工作。

1、信息系统定级资料准备：天下信安可协助北京信息科技大学准备定级备案相关资料，指导填写定级备案表及编写定级备案报告。

2、协助召开专家评审会：天下信安协助北京信息科技大学邀请专家对信息系统定级情况进行测评，指导北京信息科技大学准备汇报材料。

3、协助备案：协助北京信息科技大学进行备案，并取得备案证明。

2.1.5.5. 安全差距分析

整改与规划方案设计：根据定级和等级差距分析评估的结果，进行总体分析，结合北京信息科技大学的安全需求，然后根据公安部的等级保护基本要求，以及《信息安全等级保护安全建设整改工作指南》以及《网络安全等级保护安全设计技术要求》等标准，在满足客户信息系统在技术和管理层面的安全需求的前提下，进行安全规划和设计。

安全整改：根据整改设计方案，协助北京信息科技大学进行技术整改（安全集成、安全加固）以及管理制度整改，从而满足等级保护要求。

3.4.2.1 系统初测

现状调研：

通过访谈、走查、工具测试、渗透测试等方式对北京信息科技大学集团的信息化现状进行调研，初步了解北京信息科技大学集团的网络安全现状，为差距分析和整改方案设计提供依据。

技术单元差距分析：针对北京信息科技大学集团的信息系统，从物理安全、通讯网络、区域边界、安全计算环境、安全管理中心等五个维度进行技术差距分析。差距分析主要通过漏洞扫描、渗透测试完成。

漏洞扫描：

使用专业系统及应用漏洞扫描工具对主机、应用等进行全面的应用漏洞扫描，评估其安全策略、补丁、口令策略是否存在安全漏洞，并进行必要的漏洞分析。

渗透测试：

Web 安全测试、外网安全检测、内网安全检测、安全意识检测。

技术单元差距分析：以北京信息科技大学集团的信息系统为对象，结合现有的安全管理情况，从安全管理机构、安全管理人员、安全管理制度、安全建设管理、安全运维管理等 5 个维度进行差距分析。

初测分析和整理

通过整理风险评估结果、整理汇总分析结果、差距分析结果，形成初测差距报告，并给出整改建议。

2.1.5.6. 安全整改咨询

整改建议

整改与规划方案设计：根据定级和等级差距分析评估的结果，进行总体分析，结合采购人的安全需求，然后根据公安部的等级保护基本要求，以及《信息安全等级保护安全建设整改工作指南》以及《网络安全等级保护安全设计技术要求》等标准，在满足客户信息系统在技术和管理层面的安全需求的前提下，进行安全规划和设计。

安全整改：根据整改设计方案，协助北京信息科技大学进行技术整改（安全集成、安全加固）以及管理制度整改，从而满足等级保护要求。

2.1.5.7.等级保护测评

依据国家等级保护的相关要求，对北京信息科技大学集团总部的相关系统开展等级测评工作并出具等级测评报告，指导协助进行整改加固。

系统复测

完成对范围中的信息系统的技术测评、管理测评、综合测评。

测评报告

测评完成后，出具网络安全等级保护测评报告。

2.1.6. 工作目标

我方将协助北京信息科技大学根据项目业务需求情况，完成 1 个新建第二级系统的安全等级保护定级，并完成定级备案报告及定级备案表的编制，并协助北京信息科技大学到公安机关进行定级备案。

我方将根据信息系统承载的业务数据的重要程度及提供系统服务的重要程度，并结合项目的业务安全需求，依据国家等级保护相关政策和标准，准确划分系统边界，确定定级对象并准确定级，完成系统定级备案报告。

2.1.6.1.定级对象

在对本项目内容充分调研了解的基础上，参照《GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南》、《信息安全等级保护备案实施细则》(公信安[2007]1360 号)，结合北京信息科技大学机关的网络安全现状，协助北京信息科技大学完成 1 个新建第二级系统的定级和备案工作。

我方将根据信息系统承载的业务数据的重要程度及提供系统服务的重要程度，结合本项目业务安全需求，依据国家等级保护相关政策和标准，准确划分系统边界，确定定级对象并准确定级，完成系统定级变更备案报告。

本次项目的定级对象为 1 个新建第二级系统包括中国北京信息科技大学数字档案系统、中国北京信息科技大学作业巡检双重预防管理系统、中国北京信息科技大学应急管理系统。

2.1.6.2.定级原理

2.1.6.2.1.安全保护等级

根据参照《GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南》中的描述，等级保护对象在国家安全、经济建设、社会生活中的重要程度，以及一旦遭到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，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的侵害程度等因素，等级保护对象的安全保护等级分为以下五级：

a） 第一级，等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成一般损害，但不危害国家安全、社会秩序和公共利益；

b) 第二级，等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成严重损害或特别严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全；

c) 第三级，等级保护对象受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。；

d) 第四级，等级保护对象受到破坏后，会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害；

e) 第五级，等级保护对象受到破坏后，会对国家安全造成特别严重危害。

2.1.6.2.2.定级要素

定级要素概述

等级保护对象的定级要素包括：

a) 受侵害的客体；

b) 对客体的侵害程度。

受侵害的客体

等级保护对象受到破坏时所侵害的客体包括以下三个方面：

a)公民、法人和其他组织的合法权益；

b)社会秩序、公共利益；

c)国家安全。

对客体的侵害程度

对客体的侵害程度由客观方面的不同外在表现综合决定。由于对客体的侵害是通过对等级保护对象的破坏实现的，因此对客体的侵害外在表现为对等级保护对象的破坏，通过侵害方式、侵害后果和危害程度加以描述。

等级保护对象受到破坏后对客体造成侵害的程度归结为以下三种：

a）造成一般损害；

b)造成严重损害；

c)造成特别严重损害。

2.1.6.3.定级要素与安全保护等级的关系

定级要素与安全保护等级的关系如下表所示。

表 4-2 定级要素与安全保护等级的关系

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

2.1.6.3.1. 定级流程

等级保护对象定级工作的一般流程图如图所示。

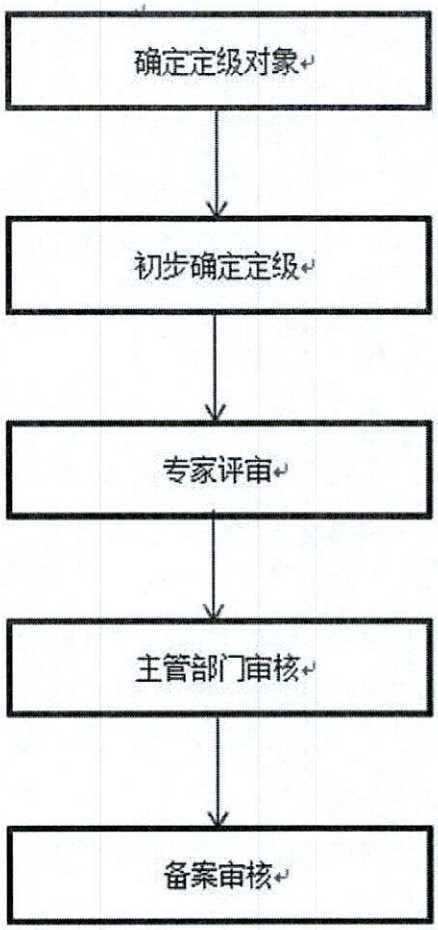


图 3-1 等级保护对象定级工作一般流程

2.1.6.4. 定级备案服务方案

2.1.6.4.1.系统识别和描述

本活动的目标是通过从北京信息科技大学相关人员处收集有关信息系统的信息，并对信息进行综合分析和整理，依据分析和整理的内容形成组织机构内信息系统的总体描述性文档。

参与角色：北京信息科技大学，天下信安。

活动输入：信息系统的立项、建设和管理文档，填好的调查表格。

活动描述：

本活动主要包括以下子活动内容：

a） 识别信息系统的基本信息

调查了解信息系统的行业特征、主管机构、业务范围、地理位置以及信息系统基本情况，获得信息系统的背景信息和联络方式。

b） 识别信息系统的管理框架

了解信息系统的组织管理结构、管理策略、部门设置和部门在业务运行中的作用、岗位职责，获得支持信息系统业务运营的管理特征和管理框架方面的信息，从而明确信息系统的安全责任主体。

c） 识别信息系统的网络及设备部署

了解信息系统的物理环境、网络拓扑结构和硬件设备的部署情况，在此基础上明确信息系统的边界，即确定定级对象及其范围。

d） 识别信息系统的业务种类和特性

了解机构内主要依靠信息系统处理的业务种类和数量，这些业务各自的社会属性、业务内容和业务流程等，从中明确支持机构业务运营的信息系统的业务特性，将承载比较单一的业务应用或者承载相对独立的业务应用的信息系统作为单独的定级对象。

e） 识别业务系统处理的信息资产

了解业务系统处理的信息资产的类型，这些信息资产在保密性、完整性和可用性等方面的重要性程度。

f） 识别用户范围和用户类型

根据用户或用户群的分布范围了解业务系统的服务范围、作用以及业务连续性方面的要求等。

g） 信息系统描述

对收集的信息进行整理、分析，形成对信息系统的总体描述文件。一个典型的信息系统的总体描述文件应包含以下内容：

- 系统概述；
- 系统边界描述；
- 网络拓扑；
- 设备部署；
- 支撑的业务应用的种类和特性；
- 处理的信息资产；
- 用户的范围和用户类型；
- 信息系统的管理框架。

活动输出：信息系统总体描述文件。

2.1.6.4.2.信息系统划分

本活动的目标是依据信息系统的总体描述文件，在综合分析的基础上将组织机构内运行的信息系统进行合理分解，确定所包含可以作为定级对象的信息系统的个数。

参与角色：北京信息科技大学，天下信安。

活动输入：信息系统总体描述文件。

活动描述：

本活动主要包括以下子活动内容：

a） 划分方法的选择

一个组织机构可能运行一个大型信息系统，为了突出重点保护的等级保护原则，应对大型信息系统进行划分，进行信息系统划分的方法可以有多种，可以考虑管理机构、业务类型、物理位置等因素，信息系统的运营、使用单位应该根据本单位的具体情况确定一个系统的分解原则。

b） 信息系统划分

依据选择的系统划分原则，将一个组织机构内拥有的大型信息系统进行划分，划分出相对独立的信息系统并作为定级对象，应保证每个相对独立的信息系统具备定级对象的基本特征。在信息系统划分的过程中，应该首先考虑组织管理的要素，然后考虑业务类型、物理区域等要素。

c） 信息系统详细描述

在对信息系统进行划分并确定定级对象后，应在信息系统总体描述文件的基础上，进一步增加信息系统划分信息的描述，准确描述一个大型信息系统中包括的定级对象的个数。

进一步的信息系统详细描述文件应包含以下内容：

- 相对独立信息系统列表；
- 每个定级对象的概述；
- 每个定级对象的边界；
- 每个定级对象的设备部署；
- 每个定级对象支撑的业务应用及其处理的信息资产类型；
- 每个定级对象的服务范围和用户类型；
- 其他内容。

活动输出：信息系统详细描述文件。

2.1.6.4.3.服务内容

基于北京信息科技大学 1 个新建第二级系统现状，天下信安参照《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020），对系统现状进行调研，根据调研结果，确定定级对象，分析定级要素，根据等级保护对象受到破坏时所侵害的客体和对客体造成的侵害程度确定系统等级，编制定级备案报告、定级备案登记表等相关材料，并组织信息系统定级专家评审会，获取专家评审意见，并协助被测评方向属地公安机关提交相关备案材料。

信息系统定级备案工作分为五个工作步骤，即信息系统调查、定级对象分析、定级要素分析、撰写定级报告和协助定级备案，相关流程如下图所示：

图 3-2 等级保护定级备案流程图

1、信息系统调查：就系统业务、承载信息、网络拓扑、相关设备、用户范围、物理边界等情况开展调研；

2、定级对象分析：就系统业务类型、包含子系统、运行环境和管理机制等方面进行分析，明确定级对象；

3、定级要素分析：就系统提供服务、承载信息的重要程度进行分析，综合两方面的分析结果，确定信息系统的安全保护等级；

4、撰写定级报告：根据调研及分析结果，撰写系统定级报告；

5、协助定级备案：协助北京信息科技大学完成信息系统的定级备案工作。

2.1.6.4.4.服务方式

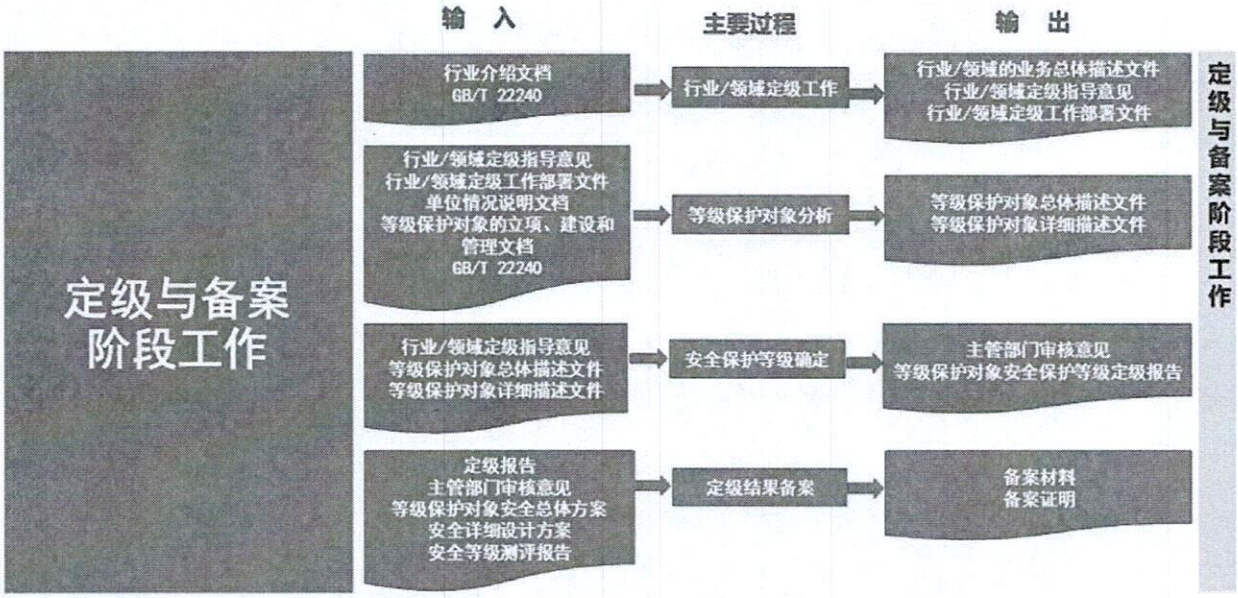


图 3-3 天下信安等级保护定级服务流程

我方信息系统进行定级及变更定级的方法如下：

1、等保 2.0 定级备案流程：确定定级对象、初步确定等级、专家评审、主管部门审核、公安机关备案审查、最终确定等级。

2、信息系统定级备案工作，我方协助北京信息科技大学完成定级备案工作。

3、定级参考《GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南》。

4、以上信息确定后，根据北京信息科技大学信息系统及机房实际情况，编写《信息系统安全等级保护备案表》、《信息系统安全等级保护定级报告》。

5、定级备案表和定级报告编写完成，下一步进行专家评审工作，专家组最低由三名信息安全专家和业务专家组成，其中一名应为等级保护高级测评师，专家现场会根据甲方负责人对公司及信息系统的介绍，提出定级是否合理相关建议并形成专家评审意见表；

6、专家评审流程：根据要求确定专家评审名单、编辑专家评审会议程、专家签到表、信息系统定级专家评审意见表、被定级单位及信息系统介绍 PPT。

7、专家评审现场工作流程：专家到现场签到入座、北京信息科技大学会议负责人将定级备案表及定级报告纸质版给专家查阅，北京信息科技大学信息安全负责人宣布会议开始，由北京信息科技大学负责人介绍公司及信息系统实际情况，专家根据公司介绍、现场访谈、备案表、定级报告等信息提出建议，专家提出建

议形成专家评审意见表，现场打印由专家签字，专家评审工作完成。

北京信息科技大学的定级备案工作主要通过以下方式进行：

1、调查表：根据北京信息科技大学的业务情况和信息系统现状，制定详细的调查表，并由北京信息科技大学相关人员进行填写，以获得业务系统基础数据，具体内容包括系统相关设备、包含的子系统或功能模块、承载信息、提供服务、与其它系统的数据交互、业务重要性等。

2、访谈：测评工程师与北京信息科技大学系统相关人员就系统定级所关注的问题进行有针对性的询问和交流，以获取足以支持分析判断、系统定级报告编写的所需依据和材料，并澄清疑问。

3、会议：召集北京信息科技大学相关的技术人员、管理人员、使用人员以及应用系统的开发厂商、运维服务商等对系统基本情况进行识别和分析，并就系统定级建议进行讨论。

2.1.6.4.5.沟通与联系

我方将协助北京信息科技大学确定本项目所辖信息系统的安全级别，帮助北京信息科技大学处理相关备案流程。

我方将提供以下的沟通保障：

1）向北京信息科技大学提供系统调研所需的材料清单。

2）对北京信息科技大学提供的信息进行分析，针对信息系统中不确定和不准确的内容，及时北京信息科技大学进行沟通和确认。

3）主动同北京信息科技大学沟通定级建议书，并向北京信息科技大学申请确认。

2.1.6.4.6. 定级和备案

为了保障本项目能够顺利通过公安机关的备案，我方将协助北京信息科技大学完成定级备案工作。

1、我方在项目中会帮助用户同系统所属的公安机关进行沟通，明确备案流程和提交物的详细构成。

2、我方在本项目中帮助用户完成定级备案所需的材料，并送交系统所属公安机关，启动备案流程。

2.1.6.4.7. 需向网安提交的材料

提交公安机关纸质版：按照纸质版文件夹内材料进行准备。

一、电子版压缩包要求：以“单位全称-系统名称”命名压缩包，将以下文件放入压缩包内，提交纸质材料的同时在钉钉内向负责民警提交电子版压缩包。原件扫描件要求，分辨率 300dpi---jpg 格式。

二、纸质版：

1. 信息系统安全等级保护备案表一式两份（封面单位名称处盖章）。应填写完整、无漏项，不得改动备案表版面格式。机打，不可手写，单面打印。

2. 信息系统安全等级保护定级报告一式两份（定级表格处盖章）。机打，单面打印。

3. 信息安全承诺书签字盖章。法人亲笔签字

4. 相关证件复印件各一份：工商营业执照(或执业许可证、事业单位证书、非盈利性机构证书等许可证明)、法人代表身份证、组织机构代码证（如三证合一，省略）。

5. 法人授权书（被授权人需携带本人身份证原件及复印件）。

6. 实际办公地的房产证或租房合同复印件。

7.主机托管合同或云主机租用合同的复印件。

8. 企业内部信息安全部门、技术部门组织架构人员登记信息表，左上角盖章（表格中确定两位 24 小时应急处置网络安全事件联系人）。

(备案面审提交时请按照以上顺序排列材料)

三、电子版压缩包要求：

以“单位全称-系统名称”命名压缩包，将以下文件放入压缩包内，提交纸质材料的同时在钉钉内向负责民警提交电子版压缩包。原件扫描件要求，分辨率 300dpi---jpg 格式。

1.备案表、定级报告和信息安全承诺书盖章扫描件

2.备案表和定级报告 word 版；

3.XX 单位 XX 系统-专家评审意见（原件扫描件）

4.《XX 单位-信息安全工作管理制度》（word 版，盖章扫描件均可）

5.XX 单位系统使用的安全产品清单及认证、销售许可证明（盖章扫描件）

6.单位拓扑图及说明（盖章扫描件）

7.三级系统需提交备案表表四全部内容。

8.信息安全部、技术部组织架构人员登记信息表，可编辑版。

9.工商营业执照副本原件扫描件(或执业许可证、事业单位证书、非盈利性机构证书等许可证明)、组织机构代码证原件扫描件（如三、五证合一，省略）

10.法人代表身份证原件扫描件；

11.备案表表一中单位负责人身份证原件扫描件。

四、工作提示

所有二级、三级系统备案，自备案证明领取之日起，30 日内提交测评报告，整改实施方案可在系统测评完成后同测评报告一同提交网安部门，三级系统每年开展一次信息系统安全等级保护测评，二级系统建议每两年开展一次信息系统安全等级保护测评。

2.1.6.4.8.交付成果

本阶段主要交付成果包括输出物：1 个新建第二级系统《信息系统安全等级保护备案表》《网络安全等级保护定级专家评审意见》，其他相关材料等。

2.1.6.5.工作目标

本项目差距分析的目的是根据《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019），对确定安全保护等级的1个新建第二级系统，从技术和管理两方面分析其现有的安全防护措施是否达到相应保护等级的要求。

2.1.6.6.工作内容

2.1.6.6.1.安全差距分析范围

本项目对1个新建第二级系统开展安全差距分析工作，包括如下两部分内容：

①技术分析：根据国家信息安全等级保护相应级别的技术要求，对物理环境、主机安全、网络安全、应用安全、数据安全开展差距分析工作。通过访谈、调研问卷、技术测试、查阅资料等多种手段，逐项分析信息系统安全防护水平与等级保护相应级别技术要求的差距。

②管理分析：根据国家信息安全等级保护相应级别的管理要求，通过访谈、调研问卷、查阅资料、要求客户举证等多种手段，逐项分析信息系统安全防护水平与等级保护相应级别技术要求的差距。

详细测评对象清单如下：

表 5-1 等级保护测评对象明细表

序号	系统范围	系统名称
1	1个第二级系统	北京信息科技大学新校区图书馆楼数字档案馆管理平台信息系统

2.1.6.6.2.安全差距分析依据

依据但不限于以下标准中相应级别安全要求，开展差距分析。如发布最新标准，应按照国家有关要求，依据最新标准开展评估测评工作。

《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）

《关于信息安全等级保护的实施意见》（公通字[2005]66 号）

《信息安全等级保护管理办法》（公通字[2007]43 号）

《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861 号）

《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303 号）

《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429 号）

《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）

《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）

《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019）

《信息安全技术网络安全等级保护安全设计技术要求》（GB/T25070-2019）

《网络安全等级保护测评高风险判定指引》（T/ISEAA 001-2020）

2.1.6.6.3.安全差距分析指标

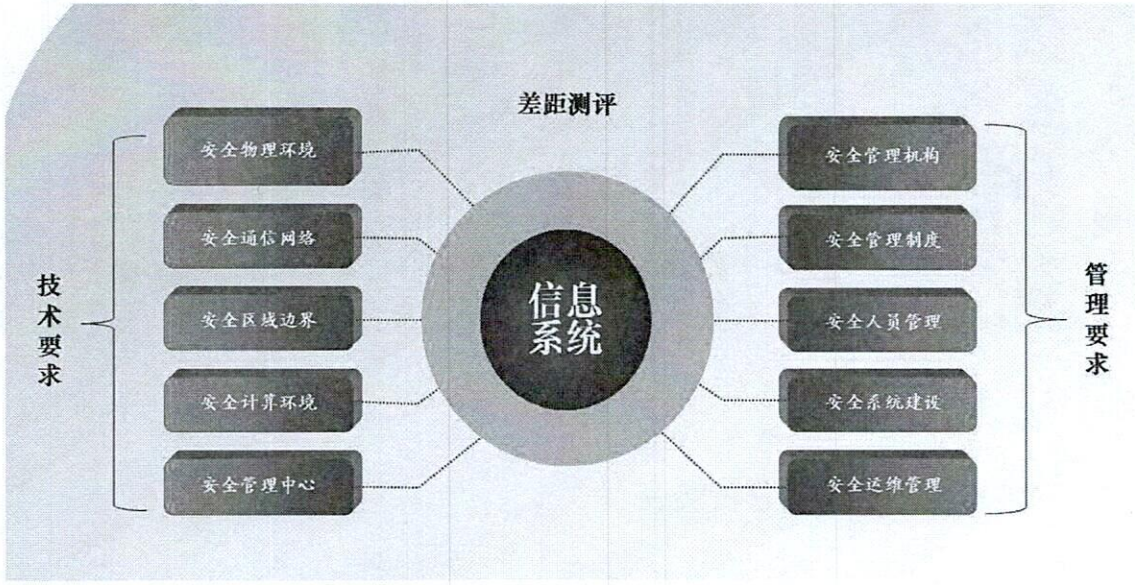
依据但不限于以下标准中相应级别安全要求，开展等级测评。如发布最新标准，应按照国家有关要求，依据最新标准开展评估测评工作。

按照《网络安全等级保护基本要求》、《网络安全等级保护测评要求》及《网络安全等级保护测评过程指南》等要求进行现场等级保护测评，出具公安部门认可的信息系统安全等级测评报告。

2.1.6.6.4.安全差距分析实施方案和计划

安全差距分析框架

安全差距分析框架如下图所示。



安全差距分析流程

为了保障等级保护差距分析的完整性和权威性，我方的差距分析工作的具体实施办法完全参考等级保护测评的要求进行组织。

安全差距分析过程分为四个基本活动：测评准备活动、方案编制活动、现场测评活动、报告编制活动。测评双方之间的沟通与洽谈贯穿整个安全差距分析测评过程。

安全差距分析工作流程如下图所示。

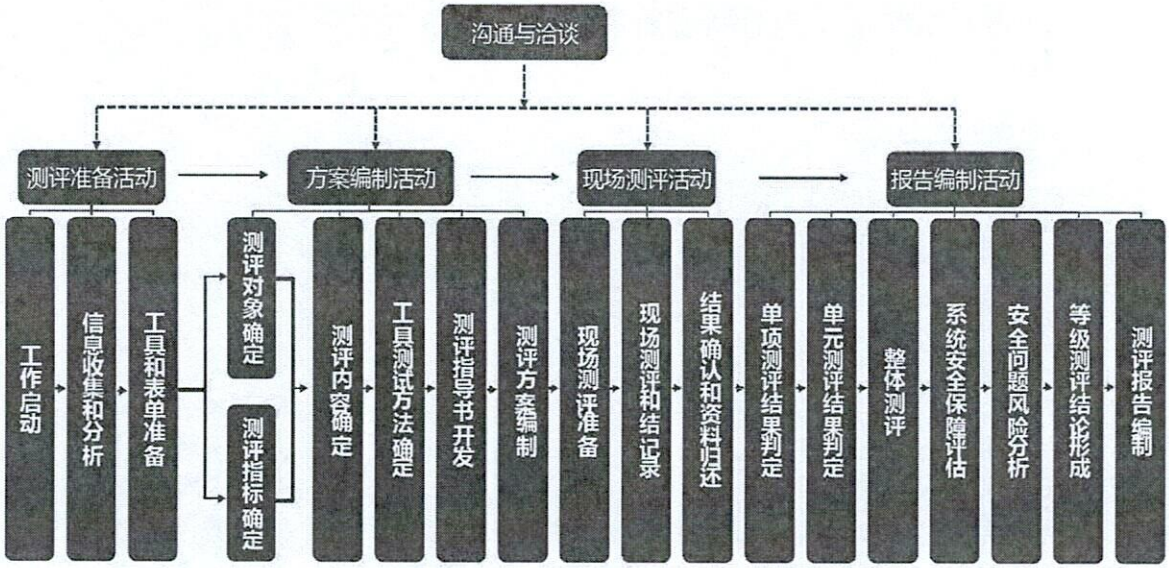


图 3-3 等级保护测评差距分析工作流程图

2.1.6.6.5.安全差距分析实施

把测评指标和测评方式结合到信息系统的具体测评对象上，就构成了可以具体测评的工作单元。具体分为安全物理环境、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、安全人员管理、安全建设管理和安全运维管理等几个方面。

5.2.5.1 安全技术差距分析

安全技术测评包括“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”五个层面。

2.1.6.6.6.安全物理环境

安全物理环境测评将通过访谈和检查的方式评测信息系统的物理安全保障情况。

在内容上，安全物理环境安全层面测评实施过程涉及 15 个指标，具体如下表：

表 5-1 物理环境安全层面测评指标表

序号	类别	测评指标	测评对象

1	安全物理环境	物理位置选择	机房场地应选择在具有防震、防风和防雨等能力的建筑内；	记录类文档和机房
2			机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	机房
3		物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。	机房电子门禁系统。
4		防盗窃和防破坏	应将设备或主要部件进行固定，并设置明显的不易除去的标记；	机房设备或主要部件
5			应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；	机房通信线缆
6		防雷击	应将各类机柜、设施和设备等通过接地系统安全接地；	机房
7		防火	机房应设置火灾自动消防系统，能够自动监测火情、自动报警，并自动灭火。	机房防火设施。
8			机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；	机房验收类文档。
9		防水和防潮	应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	机房。
10			应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；	机房
11		防静电	应安装防静电地板并采用必要的接地防静电措施；	机房。
12		温湿度控制	应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围 之内。	机房温湿度调节设施
13		电力供应	应在机房供电线路上配置稳压器和过电压防护设备；	机房供电设施
14			应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；	机房备用供电设施

15		电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。	机房线缆

配合需求：

配合项目	需求说明
陪同检查	需要陪同进入机房等现场环境检查
文档	提供相关文档

2.1.6.6.7.安全通信网络

安全通信网络安全测评将通过访谈、检查和测试的方式评测安全通讯网络安全保障情况。

评估对象：主要涉及机房的网络设备、网络安全设备以及网络拓扑结构等三大类。

在内容上，安全通信网络安全层面测评过程涉及 4 个指标，具体如下表：

表 5-2 安全通讯网络层面测评指标表

序号	类别		测评指标	测评对象
1	安全通信网络	网络架构	应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。	路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件。
2			应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可 靠的技术隔离手段。	网络拓扑图
3		通信传输	应采用校验码技术或加解密技术保证通信过程中数据的完整性；	提供加解密功能的设备或组件。
4		可	可基于可信根对通信设备的系统引导程序、系	提供可信验证的设备

		信验证	统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到 破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	或组件、提供集中审计功能的系统

配合需求

配合项目	需求说明
设备登录	登录检查设备配置
文档	提供相关文档及配置文件

2.1.6.6.8.安全区域边界

安全区域边界测评将通过访谈、检查和测试的方式评测安全区域边界安全保障情况。

评估对象：网络设备、网络安全设备以及网络拓扑结构，信息系统内的各类主机系统。

内容上，安全区域边界安全层面测评实施过程涉及 11 个指标，具体如下表：

序号	类别		测评指标	测评对象
1	安全区域边界	边界防护	应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信；	网闸、防火墙、路由器、交换机和无线接人网关设备等提供访问控制功能的设备或相 关组件。
2		访问控制	应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	网闸、防火墙、路由器和交换机等提供访问控制功能的设备或相关组件。

3			应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	网闸、防火墙、路由器和交换机等提供访问控制功能的设备或相关组件。
4			应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	网闸、防火墙、路由器和交换机等提供访问控制功能的设备或相关组件。
5			应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力	网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相 关组件。
6		入侵防范	应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为	抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件。
7		恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级 和更新。	防病毒网关和 UTM 等提供防恶意代码功能的系统或相关组件
8		安全审计	应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行 为和重要安全事件进行审计。	综合安全审计系统等
9			审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	综合安全审计系统等

10			应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	综合安全审计系统等
11		可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到 破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	提供可信验证的设备或组件、提供集中审计功能的系统

表 5-3 安全区域边界层面测评指标表

配合需求

配合项目	需求说明
设备登录	登录检查设备配置
文档	提供相关文档及配置文件

2.1.6.6.9. 安全计算环境

安全计算环境安全测评将通过访谈、检查和测试的方式评测安全计算环境安全保障情况,

评估对象：应用系统计算环境, 应用系统及数据管理人员。

在内容上，安全计算环境安全层面测评实施过程涉及 22 个评估指标，具体如下表：

表 5-4 安全计算环境层面测评指标表

序号	类别	测评指标	测评对象

1	安全计算环境	身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复 杂度要求并定期更换。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等
2			应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连 接超时自动退出等相关措施	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。
3			当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动

				终端:移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和 系统管理软件及系统设计文档等。
4		访问控制	应对登录的用户分配账号和权限。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端:移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和 系统管理软件及系统设计文档等。
5			应重命名或删除默认账户，修改默认账户的默认口令。	终端和服务器_设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和

				系统管理软件及系统设计文档等。
6			应及时删除或停用多余的、过期的账号，避免共享账号的存在。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。
7			应授予管理用户所需的最小权限，实现管理用户的权限分离。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。
8		安全审计	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进 行审	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包

			计。	括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。
9			审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。
10			应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等.	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、

				控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。
11		入侵防范	应遵循最小安装的原则，仅安装需要的组件和应用程序。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备和控制设备等。
12			应关闭不需要的系统服务、默认共享和高危端口。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备和控制设备等。
13			应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知

				节点设备、网关节点设备和控制设备等。
14			应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。	业务应用系统、中间件和系统管理软件及系统等。
15			应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞	业务应用系统、中间件和系统管理软件及系统设计文档等。
16		可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏 后进行报警，并将验证结果形成审计记录送至安全管理中心。	提供可信验证的设备或组件、提供集中审计功能的系统
17		数据完整性	应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全 保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备等
18		数据备份恢复	应提供重要数据的本地数据备份与恢复功能；	配置数据和业务数据
19			应提供异地实时备份功能，利用通信网络将重要数据实时	配置数据和业务数据

			备份至备份场地；	
20		剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	终端和服务器等设备中的操作系统、业务应用系统、数据库管理系统、中间件和系统 管理软件及系统设计文档等。
21		个人信息保护	应仅采集和保存业务必需的用户个人信息	业务应用系统和数据库管理系统等
22			应禁止未授权访问和非法使用用户个人信息	业务应用系统和数据库管理系统等。

配合需求

配合项目	需求说明
访谈	配合访谈
文档	提供相关文档及配置文件

2.1.6.6.10. 安全管理中心

安全管理中心安全测评将通过访谈、检查和测试的方式评测安全管理中心安全保障情况，

评估对象：提供集中系统管理功能的系统，业务应用系统及数据管理人员。

在内容上，安全管理中心安全层面测评实施过程涉及 4 个评估指标，具体如下表：

表 5-5 安全管理中心层面测评指标表

序号	类别		测评指标	测评对象
1	安全管理中心	系统管理	应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理 操作，并对这些操作进行审计	提供集中系统管理功能的系统

2			应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、资源 配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等	提供集中系统管理功能的系统
3		审计管理	应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计 操作，并对这些操作进行审计	综合安全审计系统、数据库审计系统等提供集中审计功能的系统。
4			应通过审计管理员对审计记录进行分析，并根据分析结果进行处理,包括根据安全 审计策略对审计记录进行存储、管理和查询等	综合安全审计系统、数据库审计系统等提供集中审计功能的系统。

配合需求

配合项目	需求说明
访谈	配合访谈
文档	提供相关文档及配置文件

5.2.5.2 安全管理差距分析

安全管理测评包括“安全管理制度、安全管理人员、安全建设管理、安全运维管理、安全物理环境”五个层面。

2.1.6.6.11. 安全管理制度

安全管理制度测评将通过访谈和检查的形式评测安全管理制度的制定、发布、评审和修订等情况。

评估对象：安全主管人员、安全管理人员、各类其它人员、各类管理制度、各类操作规程文件,相关的文件资料和工作记录等对象。

在内容上，安全管理制度测评实施过程涉及 6 个测评指标，具体如下表：

表 5-6 安全管理制度层面测评指标表

序号	类别	测评指标	测评对象

1	安全管理制度	安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、 原则和安全框架等。	总体方针策略类文档
2		管理制度	应对安全管理活动中的各类管理内容建立安全管理制度	安全管理制度类文档。
3			应对要求管理人员或操作人员执行的日常管理操作建立操作规程。	操作规程类文档。
4		制定和发布	应指定或授权专门的部门或人员负责安全管理制度的制定	部门/人员职责文件等
5			安全管理制度应通过正式、有效的方式发布，并进行版本控制。	管理制度类文档和记录表单类文档。
6		评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	信息/安全主管和管理制度类文档。

配合需求

配合项目	需求说明
访谈	配合管理访谈
文档	提供相关文档

2.1.6.6.12.安全管理机构

安全管理机构测评将通过访谈和检查的形式评测机构安全管理机构方面的情况。

评估对象：信息/网络安全主管、管理制度类文档和记录表单类文档、相关工作记录等对象。

在内容上，安全管理机构测评实施过程涉及 9 个测评指标，具体如下表：

表 5-7 安全管理机构层面测评指标表

序号	类别		测评指标	测评对象
1	安全管理机构	岗位设置	应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权	信息/网络安全主管、管理制度类文档和记录表单类文档
2			:应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。	信息/网络安全主管和管理制度类文档
3		人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。	信息/网络安全主管和管理制度类文档
4		授权和审批	应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等。	管理制度类文档和记录表单类文档
5			应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度。	操作规程类文档和记录表单类文档。
6		沟通和合作	应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题	信息/网络安全主管和管理制度类文档
7			应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通	信息/网络安全主管和管理制度类文档

8			应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	记录表单类文档
9		审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	信息/网络安全主管和管理制度类文档

配合需求

配合项目	需求说明
访谈	配合管理访谈
文档	提供相关文档

2.1.6.6.13.安全管理人员

系统安全建设管理测评将通过访谈和检查的形式评测安全管理人员过程中的安全控制情况。

评估对象：信息/网络安全主管、管理制度类文档和记录表单类文档等对象。

在内容上，系统安全建设管理测评实施过程涉及 7 个工作单元，具体如下表：

表 5-8 安全管理人员层面测评指标表

序号	类别		测评指标	测评对象
1	安全管理人员	人员录用	应指定或授权专门的部门或人员负责人员录用；	信息/网络安全主管。
2			应被录用人员的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；	管理制度类文档和记录表单类文档。
3		人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、	记录表单类文档

			钥匙、徽章等以及机构提 供的软硬件设备。	
4		安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施	管理制度类文档
5		外部人员访问管理	应确保在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案	管理制度类文档和记录表单类文档
6			应确保在外部人员接入网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案	管理制度类文档和记录表单类文档
7			外部人员离场后应及时清除其所有的访问权限	管理制度类文档和记录表单类文档

配合需求

配合项目	需求说明
访谈	配合管理访谈
文档	提供相关文档

2.1.6.6.14. 安全建设管理

安全建设管理测评将通过访谈和检查的形式评测安全建设管理过程中的安全控制情况。

评估对象：建设负责人、管理制度类文档、安全规划设计类文档、操作规程类文档和记录表单类文档、执行过程记录等对象。

在内容上，系统安全运维管理测评实施过程涉及 25 个测评指标，具体如下表：

表 5-9 安全建设管理层面测评指标表

序号	类别		测评指标	测评对象
1	安全建设管理	定级和备案	应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由。	记录表单类文档
2			应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和 审定	记录表单类文档
3			应确保定级结果经过相关部门的批准；	记录表单类文档
4			应将备案材料报主管部门和相应公安机关备案。	记录表单类文档
5		安全方案设计	应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；	安全规划设计类文档
6			应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件。	安全规划设计类文档
7			应组织相关部门和有关安全专家对总体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。	记录表单类文档
8		产品采购和使用	应确保信息安全产品采购和使用符合国家的有关规定；	记录表单类文档。
9			应确保密码产品采购和使用符合国家密码主管部门的要求；	建设负责人和记录表单类文档
10		自行软件开发	应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制	建设负责人
11			应制定软件开发管理制度，明确说明开发	管理制度类文

			过程的控制方法和人员行为准则	档
12		外包软件开发	应在软件交付前检测软件质量和其中可能存在的恶意代码；	记录表单类文档
13			应要求开发单位提供软件设计文档和使用指南；	操作规程类文档和记录表单类文档。
14		工程实施	应指定或授权专门的部门或人员负责工程实施过程的管理；	记录表单类文档
15			应制定工程实施方案控制安全工程实施过程；	记录表单类文档
16		测试验收	在制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；	记录表单类文档
17			应进行上线前的安全性测试，并出具安全测试报告。安全测试报告应包含密码应用安全性测试相关内容。	记录表单类文档
18		系统交付	应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	记录表单类文档
19			应对负责运行维护的技术人员进行相应的技能培训；	记录表单类文档
20			应提供建设过程文档和运行维护文档	记录表单类文档
21		等级测评	应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	运维负责人和记录表单类文档
22			应在发生重大变更或系统级别发生变化时进行等级测评；	运维负责人和记录表单类文档
23			应确保测评机构的选择符合国家有关规定	等级测评报告和相关资质文

				件
24		服务供应商管理	应确保服务供应商的选择符合国家的有关规定；	建设负责人
25			应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	记录表单类文档

配合需求

配合项目	需求说明
访谈	配合管理访谈
文档	提供相关文档

2.1.6.6.15.安全运维管理

安全运维管理测评将通过访谈和检查的形式评测安全运维管理过程中的安全控制情况。

评估对象：运维负责人、安全管理员、系统管理员、资产管理员、物理安全负责人、管理制度类文档、安全规划设计类文档、操作规程类文档和记录表单类文档、管理制度类文档和办公环境等对象。

在内容上，安全运维管理测评实施过程涉及 31 个测评指标，具体如下表：

表 5-10 安全运维层面测评指标表

序号	类别		测评指标	测评对象
1	安全运维管理	环境管理	应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、 空调、温湿度控制、消防等设施进行维护管理	物理安全负责人和记录表单类文档
2			应建立机房安全管理制度，对有关物理访问、物品进出和环境安全等方面的管理作 出规定。	管理制度类文档和记录表单

				类文档
3			应不在重要区域接待来访人员，不随意放置含有敏感信息的纸质文件和移动介质等。	管理制度类文档和办公环境
4		资产管理	应核查资产清单是否包括资产类别（含设备设施、软件、文档等）、资产责任部门、重 要程度和所处位置等内容。	记录表单类文档
5		介质管理	应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	资产管理员和记录表单类文档
6			应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归 档和查询等进行登记记录	资产管理员和记录表单类文档
7		设备维护管理	应对等级保护对象相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	设备管理员和管理制度类文档
8			应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等；	管理制度类文档和记录表单类文档
9		漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；	记录表单类文档

10		网络和系统安全管理	应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和 权限。	记录表单类文档
11			应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	运维负责人和记录表单类文档。
12			应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	管理制度类文档
13			应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	操作规程类文档。
14			应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；	记录表单类文档。
15		恶意代码防范管理	应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	运维负责人和管理制度类文档
16			应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	运维负责人和管理制度类文档
17			应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。	安全管理员和记录表单类文

				档
18		配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；	系统管理员
19		密码管理	应遵循密码相关的国家标准和行业标准	安全管理员
20			应使用国家密码管理主管部门认证核准的密码技术和产品	安全管理员
21		变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；	记录表单类文档
22		备份与恢复管理	应识别需要定期备份的重要业务信息、系统数据及软件系统等；	系统管理员和记录表单类文档
23			应规定备份信息的备份方式、备份频度、存储介质、保存期等；	管理制度类文档。
24			应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	管理制度类文档
25		安全事件处置	应及时向安全管理部门报告所发现的安全弱点和可疑事件	运维负责人和记录表单类文档
26			应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责	管理制度类文档

			等；	
27			应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；	记录表单类文档
28		应急预案管理	应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；	管理制度类文档
29			应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容	管理制度类文档
30		外包运维管理	应确保外包运维服务商的选择符合国家的有关规定；	运维负责人
31			应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；	记录表单类文档

配合需求

配合项目	需求说明
访谈	配合管理访谈
文档	提供相关文档

5.2.5.3 差距分析测评过程描述

1、安全差距分析测评准备

包括前期调研、数据分析、测评方案编制等。具体包括编制和配合相关单位填报信息系统基本情况调查表，开展面对面访谈进一步了解系统情况；准备评估工具，汇总和分析调研数据，确定抽测对象，完成测评工作方案编制。

2、安全差距分析现场测评

提供现场测评工作内容及配合需求说明，协同招标人做好现场测评准备工作。开展安全现状测评，对本项目中各个信息系统的物理环境、网络和通信、计算环

境、应用和数据、管理制度、管理机构和人员、建设运维等方面进行全面评估分析，查找与等级保护基本要求之间的差距。

3、出具安全差距分析报告

对本项目中各个系统出具安全差距分析报告，具体以出具报告时各信息系统的实际定级备案情况为准。报告将逐条提出具体测评中出现的差距问题。

2.1.6.6.16.漏洞扫描

对项目范围内的所有资产开展漏洞扫描工作，服务包括漏洞扫描、复检，并对高危漏洞进行人工验证，提供针对性的漏洞加固方案并全程协助进行漏洞修复，直至高危漏洞修复完毕。

漏洞扫描内容

该项服务使用绿盟极光远程安全评估系统进行漏洞扫描。能实现以下功能：

WEB 漏洞扫描：

分类		描述
WEB 漏洞检测	信息泄露	检测所有响应中的 email 地址
		检测响应中目录浏览问题
		检测密码是否开启自动填充选项
		检测响应中内部 IP 地址
		检测响应中的服务器敏感目录
		检测响应中的会话令牌
	配置安全隐患	检测 Web 应用不安全的配置项目
		检测数据库、rdp、ssh 等服务的弱密码
	SQL 注入漏洞	检测基于错误、基于时间的 SQL 注入漏洞，以及盲注漏洞等
	XSS 注入漏洞	检测反射型、存储型、DOM 型 XSS 漏洞
	XPATH 注入漏洞	检测基于错误的 XPATH 注入漏洞
	HPP 漏洞	检测参数污染漏洞
	目录遍历漏洞	检测在 URL 或参数中构造“../”，或

分类		描述
		“../”和类似的跨父目录字符串的 ASCII 编码、unicode 编码等，完成目录跳转，读取操作系统各个目录下的敏感文件
	本地文件包含漏洞	检测本地文件包含漏洞由于程序员未对用户可控的变量进行输入检查，导致用户可以控制被包含的文件，成功利用时可以使 web server 会将特定文件当成 php 执行，从而导致用户可获取一定的服务器权限。

系统漏洞扫描：

名称	一级分类	二级分类	描述
系统漏洞扫描	溢出漏洞	远程缓冲区溢出漏洞	检测远程缓冲区溢出漏洞，如：CVE 2017-9445、CVE 2017-5577 等
		栈缓冲区溢出漏洞	检测栈缓冲区溢出漏洞，如：CVE2014-9295 等
		堆缓冲区溢出漏洞	检测堆缓冲区溢出漏洞，如：CVE 2017-8287 等
	拒绝服务攻击漏洞	远程拒绝服务漏洞	检测远程拒绝服务攻击漏洞
		特定函数拒绝服务漏洞	检测多种函数造成的拒绝服务攻击漏洞
	未授权访问漏洞	未授权访问漏洞	检测未授权访问漏洞
		安全限制绕过漏洞	检测绕过安全限制漏洞进行越权访问漏洞
	代码执行漏洞	任意命令执行漏洞	检测任意命令执行漏洞，如：java 反序列化漏洞等
		远程代码执行漏洞	检测远程代码执行漏洞

弱口令检测：

实现内网信息化资产不同应用弱口令猜解，如：SMB、Mssql、Mysql、Oracle、

smtp、VNC、ftp、telnet、ssh、mysql、tomcat 等。针对不同行业提供行业密码字典，有针对性的进行内网弱口令检测，降低和减少内网弱口令的存在，为用户内网资产安全保驾护航。

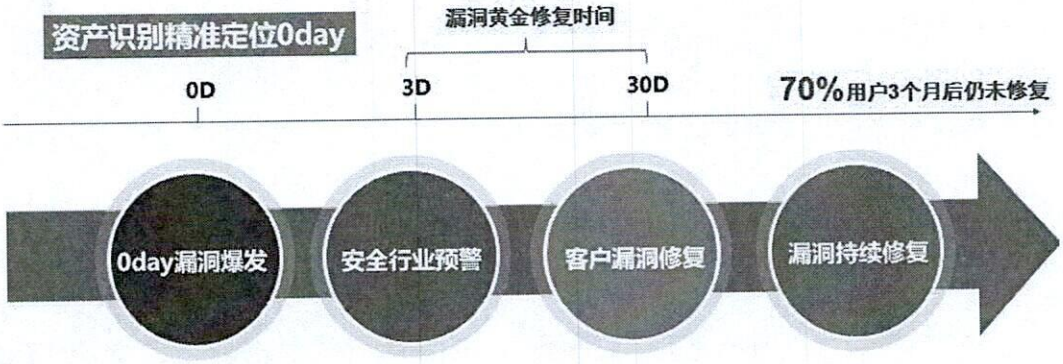
弱口令猜解提供多种字典服务方式，包括：通用弱口令字典、行业专有弱口令字典等。

通用弱口令字典，通过对百亿级社工库字典进行大数据分析，形成高发弱口令字典，通过这些字典进行弱口令猜解。

行业专有弱口令字典，通过行业内的长期积累和不断挖掘，形成强大的行业弱口令字典，每个行业字典均有不同，为不同行业用户提供行业弱口令猜解。

0day 应急响应：

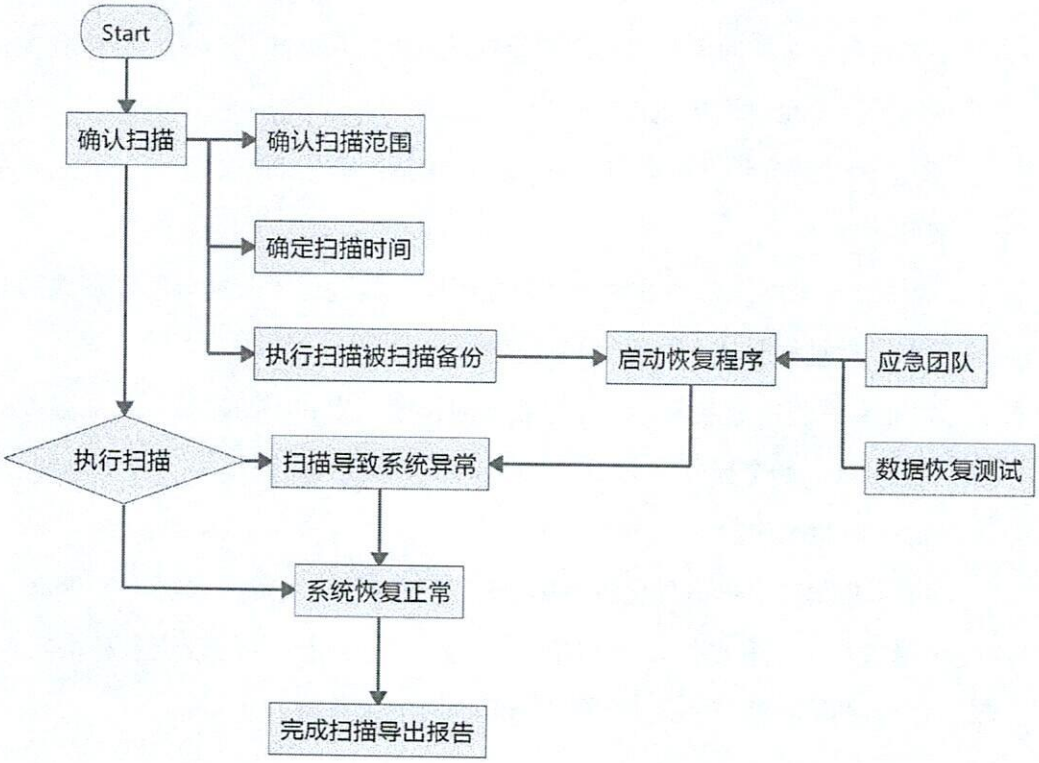
0day 爆发对用户信息化资产影响较为严重，结合资产识别，对 0day 漏洞触发环境进行识别和检测，与传统 0day 应急响应相比，能较快且精准定位 0day 漏洞，协助用户进行 0day 排查，降低内网安全风险。



漏洞扫描流程

对项目范围内的所有应用系统扫描、复检，输出《漏洞扫描报告》，并协助进行修复。扫描方式以主动发现漏洞为主。

具体实施流程如下图：



漏洞扫描工具

绿盟极光远程安全评估系统 V6.0

风险规避

- 扫描时间和策略

为减轻扫描对网络和主机的影响，扫描时间应尽量安排在业务量不大的时段或晚上。为了防止扫描造成网络和主机的业务中断，在扫描中不应使用拒绝服务等策略。

- 系统备份和恢复

为了防止在扫描过程中出现意外情况，所有评估系统最好在被评估之前做一次完整的系统备份，以便在系统发生灾难后及时恢复。

在扫描过程中，如果被评估系统没有响应或中断，应立即停止测试工作,与客户人员配合一起分析情况。确定原因后，及时恢复系统，并采取必要的预防措施，确保对系统没有影响，并经客户同意后才可继续进行。

2.1.6.6.17.渗透测试

渗透测试内容

通过模拟黑客从内、外网针对项目范围内的业务系统进行渗透。发现信息系统应用层、系统层和逻辑层的安全隐患，并出具详细的渗透测试报告，协助对已发现的安全隐患进行修复整改，修复整改后对其进行复测，直到已发现问题被真正解决。

渗透测试方法

- WEB 服务器漏洞利用

通过被披露的各种服务器操作系统及应用软件（或模块）的安全漏洞，利用这些漏洞及相关工具对 WEB 服务器和网站及其应用进行漏洞利用测试。

- SQL 注入

对网站应用程序的输入数据进行合法性检查，对客户端参数中包含的某些特殊内容进行不适当的处理，进行预判。SQL 语句注入：通过向提交给应用程序的输入数据中“注入”某些特殊 SQL 语句，最终可能获取、篡改、控制网站服务器端数据库中的内容。

• SQL Injection 定义

所谓 SQL Injection ，就是通过向有 SQL 查询的 WEB 程序提交一个 精心构造的请求，从而突破了最初的 SQL 查询限制，实现了未授权 的访问或存取。

• SQL Injection 原理

随着 WEB 应用的复杂化，多数 WEB 应用都使用数据库作为后台，WEB 程序接受用户参数作为查询条件，即用户可以在某种程度上控制查询的结果，如果 WEB 程序对用户输入过滤的比较少，那么入侵者就 可能提交一些特殊的参数，而这些参数可以使该查询语句按照自己 的意图来运行，这往往是一些未授权的操作，这样只要组合后的查询语句在语法上没有错误，那么就会被执行。

• SQL Injection 危害

SQL Injection 的危害主要包括：

1. 暴露敏感信息

2. 提升 WEB 应用程序权限

3. 操作任意文件

4. 执行任意命令

• SQL Injection 技巧

利用 SQL Injection 的攻击技巧主要有如下几种：

1. 逻辑组合法：通过组合多种逻辑查询语句，获得所需要的查询结果。

2. 错误信息法:通过精心构造某些查询语句，使数据库运行出错，错误信息中包含了敏感信息。

3. 有限穷举法：通过精心构造查询语句，可以快速穷举出数据库 中的任意信息。

4. 移花接木法：利用数据库已有资源，结合其特性立刻获得所需信息

•预防手段

要做到预防 SQL Injection,数据库管理员 (MS SQL Server)应 做到：

1. 应用系统使用独立的数据库账号，并且分配最小的库，表以及 字段权限

2. 禁止或删除不必要的存储过程

3. 必须使用的存储过程要分配合理的权限

4. 屏蔽数据库错误信息

WEB 程序员则应做到：

1. 对用户输入内容进行过滤（ ‘， “ --#%09 %20)

2. 对用户输入长度进行限制

3. 注意查询语句书写技巧

➢ XSS 跨站脚本攻击

通过跨站脚本的方式对信息系统进行测试。跨站脚本是一种向其他 Web 用

户浏览页面插入执行代码的方法。网站服务器端应用程序如果接受客户端提交的表单信息而不加验证审核，攻击者很可能在其中插入可执行脚本的代码，例如JavaScript、VBScript 等，如果客户端提交的内容不经过滤地返回给任意访问该网站的客户端浏览器，其中嵌入的脚本代码就会以该网站服务器的可信级别被客户端浏览器执行。

•漏洞成因

是因为WEB 程序没有对用户提交的变量中的HTML 代码进行过滤或转换。

•漏洞形式

这里所说的形式，实际上是指WEB 输入的形式，主要分为两种：

1. 显示输入

2. 隐式输入

其中显示输入明确要求用户输入数据，而隐式输入则本来并不要求 用户输入数据，但是用户却可以通过输入数据来进行干涉。

显示输入又可以分为两种：

1. 输入完成立刻输出结果

2. 输入完成先存储在文本文件或数据库中，然后再输出结果 注意：后者可能会让你的网站面目全非！

而隐式输入除了一些正常的情况外，还可以利用服务器或WEB 程序 处理错误信息的方式来实施。

•漏洞危害

比较典型的危害包括但不限于：

1. 获取其他用户 Cookie 中的敏感数据

2. 屏蔽页面特定信息

3. 伪造页面信息

4. 拒绝服务攻击

5. 突破外网内网不同安全设置

6. 与其它漏洞结合，修改系统设置，查看系统文件，执行系统命 令等

7. 其它

一般来说，上面的危害还经常伴随着页面变形的情况。而所谓跨站脚本执行漏洞，也就是通过别人的网站达到攻击的效果，也就是说，这种攻击能在一定程度上隐藏身份。

•解决方法

要避免受到跨站脚本执行漏洞的攻击，需要程序员和用户两方面共同努力，程序员应过滤或转换用户提交数据中的所有 HTML 代码，并限制用户提交数据的长度；而用户方则不要轻易访问别人提供的链 接，并禁止浏览器运行 JavaScript 和 ActiveX 代码。

- CRLF 注入

CRLF 注入攻击并没有像其它类型的攻击那样著名。但是，当对有安全漏洞的应用程序实施 CRLF 注入攻击时，这种攻击对于攻击者同样有效，并且对用户造成极大的破坏。

充分检测应用程序在数据执行操作之前，对任何不符合预期的数据类型的字符过滤是否符合要求。

- XPath 注入

XPath 注入攻击是指利用 XPath 解析器的松散输入和容错特性，能够在 URL，表单或其它信息上附带恶意的 XPath 查询代码，以获得权限信息的访问权并更改这些信息。XPath 注入攻击是针对 Web 服务应用新的攻击方法，它允许攻 击者在事先不知道 XPath 查询相关知识的情况下，通过 XPath 查询得到一个 XML 文档的完整内容。

- COOKIE 操纵

浏览器与服务器之间的会话信息通常存储在 Cookie 或隐藏域中，通过修改这些会话参数，来对控制会话进行测试。参数操控一般发生在数据传输之前，因

此 SSL 中的加密保护通常并不能解决这个问题。

Cookie 欺骗：修改或伪造 Cookie，达到入侵目的。

Google Hacking

使用 google 中的一些语法可以提供给我们更多的 WEB 网站信息，通过在搜索引擎中搜索 WEB 网站可能存在的敏感信息，获取有利用价值的攻击线索，并进行渗透测试攻击。

➢ 暴力猜解

对于采用口令进行用户认证的应用，将使用工具进行口令猜测以获取用户账号/密码，口令猜测使用字典攻击和蛮力攻击。

➢ 木马植入

对网站进行信息收集，查找是否存在安全漏洞，是否可以利用漏洞上传一个后门程序以取得 WEBSHELL，修改页面植入木马，对所有访问者进行木马攻击。

病毒与木马检查

根据本次渗透测试范围要求对系统进行木马检查，检查系统是否感染病毒和木马。此次检测如系统存在病毒或木马，我方将和 xx 工程师在第一时间进行彻底 的查杀和清除，并将检查结果进行汇总分析，形成报告。

病毒木马检查主要内容包括：

■启动项分析；

■隐藏文件、内核检测；

■网络异常连接检测；

■恶意文件扫描；

■注册表分析；

■清除恶意文件；

■修复系统；

■其他项；

- 溢出攻击

通过前期资料收集掌握的网站程序及各种支撑中间件进行分析、总结，利用工具与工程经验结合的方式对网站运营支撑的各种应用程序和中间件进行缓冲区溢出攻击测试，发现存在溢出的程序，充分保障网站安全运行。

- 后门

利用工具对信息系统进行彻底扫描，对异常进程、网络异常连接、异常流量、启动项等进行深入分析，查找系统是否存在后门。

- 欺骗

实时监控网络情况，对诸如网络钓鱼和其他虚假网站形成实时跟踪机制，及时发现欺骗行为，通过安全上报机制及时报告并协助加强安全防范。

通过搜索引擎对疑似钓鱼网站和错误链接进行风险排查，对重点可疑网站进行深度负面分析。一旦发现有假冒站点出现，便立刻向相关管理机构举报，关闭该虚假站点。通过这种方式，大力防范了钓鱼网站对客户的欺骗和攻击，及时抑制了欺骗对客户利益的损害，为客户打造了安全可靠的互联网环境，有效消除了客户疑虑，极大增强了客户信心。

渗透测试过程

2.1.6.7. 客户书面授权

合法性即客户书面授权委托，并同意实施方案是进行渗透测试的必要条件。渗透测试首先必须将实施方法、实施时间、实施人员等具体的实施方案提交给客户，并得到客户的相应书面委托和授权。

本次书面授权应该做到北京信息科技大学对渗透测试所有细节和风险都知晓，所有过程都在北京信息科技大学的控制下进行。这也是专业渗透测试服务与黑客攻击的本质不同。

2.1.6.8.制定实施方案

实施方案应当由我方与北京信息科技大学相关技术人员进行沟通协商。调

查了解客户对测试的基本接受情况。内容包括但不限于如下：

•目标系统介绍、重点保护对象及特性。

•是否允许数据破坏？

•是否允许阻断业务正常运行？

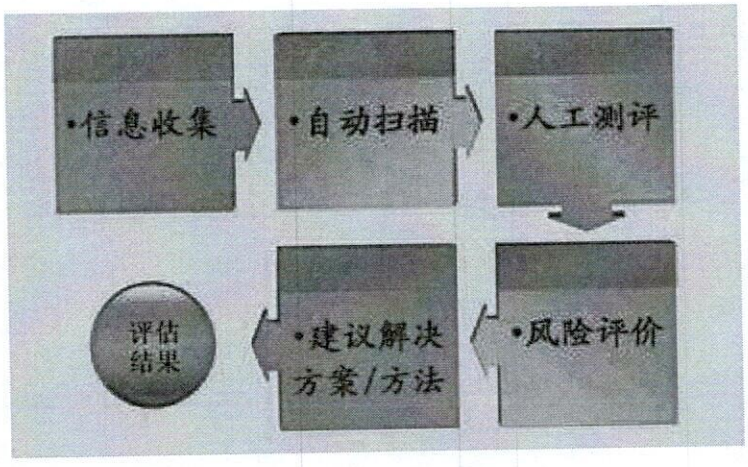
•测试之前是否应当知会相关部门接口人？

•接入方式？外网和内网？

•测试是发现问题就算成功，还是尽可能的发现多的问题？

•渗透过程是否需要考虑社会工程？

在对客户具体情况充分了解的前提下，制定相应的测试流程，安全评估步骤 如下：



图：测试流程

2.1.6.9.风险规避

- 渗透时间和策略

为减轻渗透测试对网络和主机的影响，渗透测试时间应尽量安排在业务量不大的时段或晚上。为了防止渗透测试造成网络和主机的业务中断，在渗透测试中不应使用拒绝服务等策略。

- 系统备份和恢复

为了防止在渗透测试过程中出现意外情况，所有评估系统最好在被评估之前做一次完整的系统备份，以便在系统发生灾难后及时恢复。

在渗透测试过程中，如果被评估系统没有响应或中断，应立即停止测试工作,与客户人员配合一起分析情况。确定原因后，及时恢复系统，并采取必要的预防措施，确保对系统没有影响，并经客户同意后才可继续进行。

- 沟通

在测试实施过程中，测试人员和客户方人员应当建立直接沟通渠道，并在出现难题的时候保持合理沟通。

2.1.6.10. 信息收集分析

信息收集是每一个渗透攻击的前提，通过信息收集可以有针对性的制定模拟 攻击测试计划，提高模拟攻击的成功率，同时还可以有效降低攻击测试对系统正常运行的不利影响。

- 工具收集分析

使用 nslookup. exe, super scan, x-scan, tracert, namp 等探测收集目标 主机环境及其所在的网络环境。

使用绿盟极光漏洞扫描器，对目标网络中的主机进行漏洞扫描，并对扫 描结果进行分析。

使用 ethereal、sniffer pro 等工具嗅探分析目标网络数据和私有协议交互。

- 手工收集分析

对目标主机环境及其所在网络环境，在工具分析基础上进行手工深入分析。判断是否存在远程利用漏洞和可以利用的敏感信息。

- 其他手段收集分析

可以由客户提供一些特定的资料，以便于我们查找漏洞。或者利用社会工程学或木马、间谍软件等收集有用信息。

2.1.6.11.渗透测试

根据客户设备范围和项目时间计划，并结合前一步信息收集得到的设备存活情况、网络拓扑情况以及扫描得到的服务开放情况、漏洞情况制定计划，确定无误后实施。

攻击手段大概有以下几种：

•主机存在重大安全问题，可以远程获取权限。但是这种可能性不大。

•应用系统存在安全问题，如 SSH 系统可能存在溢出、脆弱口令等问题，严重的可以获取系统权限，轻则获取普通控制权限。

•网络通信中存在加密薄弱或明文口令。

•同网段或信任主机中存在脆弱主机，通过 sniffer 监听目标服务器远程口令。

2.1.6.12. 取得权限、提升权限

通过初步的信息收集分析和攻击，存在两种可能，一种是目标系统存在重大安全弱点，测试可以直接控制目标系统，但是可能性很小；另一种是目标系统没有远程重大的安全弱点，但是可以获得普通用户权限，这时可以通过普通用户权限进一步收集目标系统信息，并努力获取超级用户权限。

渗透测试风险规避措施

渗透测试过程的最大的风险在于测试过程中对业务产生影响，为此我们在本项目采取以下措施来减少风险：

•在渗透测试中不使用含有拒绝服务的测试策略。

•渗透测试时间尽量安排在业务量不大的时段或者晚上。

•在渗透测试过程中如果出现被评估系统没有响应的情况，应当立即停止测试工作，与北京信息科技大学相关人员一起分析情况，在确定原因后，并待正确恢复系统，采取必要的预防措施（比如调整测试策略等）之后，才可以继续进行。

渗透测试工程师会与北京信息科技大学的安全管理人员保持良好沟通。随时协商解决出现的各种难题。

2.1.6.13.交付成果

本阶段主要交付成果包括输出物：《漏洞扫描报告》《渗透测试报告》。

2.1.7. 等级保护安全整改咨询服务方案工作目标

天下信安将协助北京信息科技大学根据本项目中各个信息系统根据差距分析测评中出现的问题，结合系统实际情况，提供合理、切实可行的整改建议，并全程协助北京信息科技大学进行整改工作，使各系统达到等级保护相应级别的要求，并能通过国家相关主管部门的审核。

天下信安依据信息系统安全总体方案（一个或多个文件构成）、用户单位信息化建设的中长期发展规划和北京信息科技大学的安全建设资金状况确定各个时期的安全建设目标，主要活动内容包括：

- 信息化建设中长期发展规划和安全需求调查：了解和调查单位信息化建设的现况、中长期信息化建设的目标、主管部门对信息化的投入，对比信息化建设过程中阶段状态与安全策略规划之间的差距，分析急迫和关键的安全问题，考虑可以同步进行的安全建设内容等。
- 提出信息系统安全建设分阶段目标：制定系统在规划期内所要实现的总体安全目标；制定系统短期要实现的安全目标，主要解决目前急迫和关键的问题，争取在短期内安全状况有大幅度提高。

2.1.7.1.工作内容

2.1.7.2.安全整改工作依据

- 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）
- 《关于信息安全等级保护的实施意见》（公通字[2005]66 号）
- 《信息安全等级保护管理办法》（公通字[2007]43 号）
- 《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861 号）
- 《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303 号）
- 《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安

[2009]1429 号）

- 《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）
- 《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）
- 《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019）
- 《信息安全技术 网络安全等级保护安全设计技术要求》GB/T25070-2019）
- 《网络安全等级保护测评高风险判定指引》（T/ISEAA 001-2020）

2.1.7.3.技术整改方案设计

根据前阶段的安全基础调研、差距分析工作中技术方面单元测评的结果分析以及整体测评的结论，了解到当前安全技术措施建设的不足方面，确定针对信息系统的安全需求。根据安全需求分析，形成纲领性的安全文件，包括安全工作的总体原则、安全策略等，用于指导信息系统安全技术体系和安全管理体系的构建。设计技术方案时，应以《基本要求》为基本目标，可以针对安全现状分析发现的问题进行加固改造，查漏补缺；也可以进行总体的安全技术设计，将不同区域、不同层面的安全保护措施形成有机的安全保护体系，建立总体技术框架结构，从安全物理环境，安全通信网络、安全计算环境、安全区域边界、安全管理中心等方面设计落实基本技术要求的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心的安全要求技术路线。

天下信安为被测信息系统的建设整改技术部分的方案将包含：

- **物理环境安全设计**

从安全技术设施和安全技术措施两方面来对涉及的主机房、辅助机房和办公环境等进行物理安全设计，设计内容包括《基本要求》内物理层面的各个控制点，将主要根据差距内容来描述将要补充的技术设施和措施。

- **通信网络安全设计**

对信息系统所涉及的通信网络，包括骨干网络和其他通信网络进行安全设计，设计内容包括通信过程的数据完整性、包括链路与网络设备的冗余；网络的安全配置和加固等。

- **区域边界安全设计**

对信息系统所涉及的区域网络边界进行安全设计，内容包括对边界保护、安全区域划分、身份认证、访问控制、安全审计、入侵防范、恶意代码检测和网络设备自身防护等。

- **主机系统安全设计**

对信息系统涉及的服务器和工作站进行主机系统安全设计，内容包括操作系统或数据库管理系统的选择、安装和安全配置，主机入侵防范、恶意代码检测、资源使用等情况。

- **应用系统安全设计**

对信息系统涉及的应用系统软件进行安全设计，设计内容包括身份鉴别、访问控制、安全标记、可信路径、安全审计、剩余信息保护、通信完整性、通信保密性、容错性、抗抵赖性、资源控制等。关注应用系统的安全框架、安全机制选择与实现方式、编码安全规范与代码审核。

- **备份和恢复安全设计**

针对信息系统的业务数据安全和系统服务连续性进行安全设计，设计内容包括数据备份系统、备用基础设施以及相关技术设施。针对业务数据安全的数据备份系统以考核数据备份的范围、时间间隔、实现技术与介质以及数据备份线路的速率等。

- **安全管理中心安全设计**

针对信息系统的业务数据安全和系统服务连续性进行安全设计，设计内容包括系统管理、审计管理、安全管理、集中管控等情况。

天下信安将根据建设目标和建设内容将信息系统安全总体方案中要求实现的安全策略、安全技术体系结构、安全措施和要求落实到产品功能或物理形态上，提出能够实现的产品或组件及其具体规范，并将产品功能特征整理成文档。使得在信息安全产品采购和安全控制开发阶段具有依据，主要活动内容包括：

- **结构框架设计：**

依据本次实施项目的建设内容和信息系统的实际情况，给出与总体安全规划阶段的安全体系结构一致的安全实现技术框架，内容可能包括安全防护的层次、信息安全产品的使用、网络子系统划分、IP 地址规划其他内容。

- **功能要求设计：**

对安全实现技术框架中使用到的相关信息安全产品，如防火墙、VPN、网闸、

认证网关、代理服务器、网络防病毒、PKI 等提出功能指标要求。对需要开发的安全控制组件，提出功能指标要求。

- **性能要求设计：**

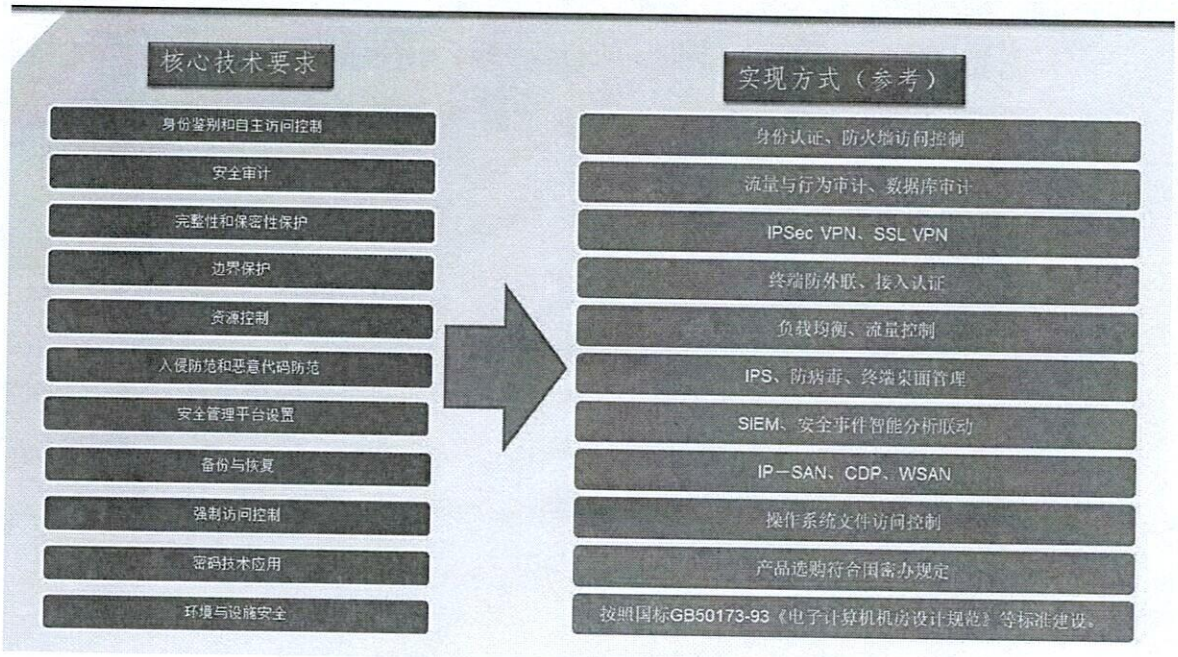
对安全实现技术框架中使用到的相关信息安全产品，如防火墙、VPN、网闸、认证网关、代理服务器、网络防病毒、PKI 等提出性能指标要求。对需要开发的安全控制组件，提出性能指标要求。

- **部署方案设计：**

结合目前信息系统网络拓扑，以图示的方式给出安全技术实现框架的实现方式，包括信息安全产品或安全组件的部署位置、连线方式、IP 地址分配等。对于需对原有网络进行调整的，给出网络调整的图示方案等。

- **制定安全策略实现计划：**

依据信息系统安全总体方案中提出的安全策略的要求，制定设计和设置信息安全产品或安全组件的安全策略实现计划。



2.1.7.4.管理整改方案设计

首先，天下信安需要通过差距测评的单元测评结果和整体测评的结论、风险评估结论提取当前安全状态下的安全管理建设需求，找到信息系统安全管理建设整改需要解决的问题，明确信息系统安全管理建设的需求。

安全管理体系的设计内容包括：

- **安全管理制度**

对北京信息科技大学开展安全建设及整改工作提供咨询指导，天下信安依据有关国家标准，审核本项目执行过程中编制的网络安全等保相关制度，对制度的规范性、合理性、准确性、可落地性进行查验和评估，并提出修改意见。使北京信息科技大学的信息安全相关管理制度满足等保相关标准的要求。

- **安全人员管理**

人员安全管理主要包括人员录用、离岗、考核、教育培训等内容。针对人员安全管理方面的差距描述整改建议和措施。

- **环境和资产管理**

明确环境（机房、办公环境）安全管理的责任部门或责任人，加强对人员录入、来访人员的控制，对有关物理访问、物品进出和环境安全等方面做出规定。针对环境和资产管理方面的差距描述整改建议和措施。

- **设备和介质安全管理**

明确配套设施、软硬件设备管理、维护的责任部门或责任人，对信息系统的各种软硬件设备采购发放、领用、维护和维修等过程的控制和管理，针对设备和

介质安全管理方面的差距描述整改建议和措施。

- **日常运维管理**

明确网络、系统日常运行维护的责任部门或责任人，对运维管理中的日常操作、账号管理、安全配置、日志管理、补丁升级、口令更新等过程进行控制和管理，针对日常运维管理方面的差距描述整改建议和措施。

- **事件处置与应急响应**

按照国家有关标准规定，确定信息安全事件等级，制定安全事件分级应急处置预案，明确应急处理策略，落实应急部门和人员，建立协调响应机制等，将针对事件处置与应急响应管理方面的差距描述整改建议和措施。

- **实时监测**

需要开展信息系统实时安全监测，实现对物理环境、通信线路、主机、网络设备、用户行为、特殊事件等的监测和报警，及时发现设备故障、病毒入侵、黑客攻击等安全事件。可建立安全运行中心机制。针对实时监测管理方面的差距描述整改建议和措施。

- **其他安全管理方面**

对运维过程中的其他管理活动，如系统变更、密码使用等进行管制和管理。或其他的安全管理内容描述整改建议和措施。

2.1.7.5. 安全整改阶段服务内容

信息安全产品采购

本阶段天下信安将协助北京信息科技大学按照安全详细设计方案中对于产品的具体指标要求进行产品采购，根据产品或产品组合实现的功能满足安全设计要求的情况来选购所需的信息安全产品，具体活动内容包括：

- **制定产品采购说明书：**信息安全产品选型过程首先依据安全详细设计方案的设计要求，制定产品采购说明书，对产品的采购原则、采购范围、指标要求、采购方式、采购流程等方面进行说明，然后依据产品采购说明书对现有产品进行比对和筛选。对于产品的功能和性能指标，可以依据国家认可的测试机构所出具的产品测试报告，也可以依据北京信息科技大学自行组织的信息安全产品功能和性能选型测试所出具的报告。

● **产品选择：**在依据产品采购说明书对现有产品进行选择时，不仅要考虑产品的使用环境、安全功能、成本（包括采购和维护成本）、易用性、可扩展性、与其他产品的互动和兼容性等因素，还要考虑产品质量和可信性。产品可信性是保证系统安全的基础，北京信息科技大学在选择信息安全产品时应确保符合国家关于信息安全产品使用的有关规定。对于密码产品的使用，应当按照国家密码管理的相关规定进行选择和使用。

6.2.4.2 安全控制集成

本阶段天下信安协助北京信息科技大学将不同的软硬件产品集成起来，依据安全详细设计方案，将信息安全产品、系统软件平台和开发的安全控制模块与各种应用系统综合、整合成为一个系统。安全控制集成的过程需要把安全实施、风险控制、质量控制等有机结合起来，遵循运营使用单位与信息安全服务机构共同参与相互配合的实施的原则，具体活动内容包括：

● **集成实施方案制定：**主要工作内容是制定集成实施方案，集成实施方案的目标是具体指导工程的建设内容、方法和规范等，实施方案有别于安全设计方案的一个显著特征之处就是它的可操作性很强，要具体落实到产品的安装、部署和配置中，实施方案是工程建设的具体指导文件。

● **集成准备：**主要工作内容是对实施环境进行准备，包括硬件设备准备、软件系统准备、环境准备。为了保证系统实施的质量，信息安全服务机构应该依据系统设计方案，制定一套可行的系统质量控制方案，以便有效地指导系统实施过程。该质量控制方案应该确定系统实施各个阶段的质量控制目标、控制措施、工程质量问题的处理流程、系统实施人员的职责要求等，并提供详细的安全控制集成进度表。

● **集成实施：**主要工作内容是将配置好策略的信息安全产品和开发控制模块部署到实际的应用环境中，并调整相关策略。集成实施应严格按照集成进度安排进行，出现问题各方应及时沟通。系统实施的各个环节应该遵照质量控制方案的要求，分别进行系统测试，逐步实现质量控制目标。例如：综合布线系统施工过程中，应该及时利用网络测试仪测定线路质量，及早发现并解决质量问题。

● **培训：**信息系统建设完成后，安全服务提供商应当向运营和使用单位提供信息系统使用说明书及建设过程文档，同时需要对系统维护人员进行必要培训，

培训效果的好坏将直接影响到今后系统能否安全运行。

- **形成安全控制集成报告：**应将安全控制集成过程相关内容文档化，并形成安全控制集成报告，其包含集成实施方案、质量控制方案、集成实施报告以及培训考核记录等内容。

6.2.4.3 系统验收

天下信安将协助北京信息科技大学中 1 个系统是否严格按照安全详细设计方案进行建设，是否实现了设计的功能和性能。在安全控制集成工作完成后，系统测试及验收是从总体出发，对整个系统进行集成性安全测试，包括对系统运行效率和可靠性的测试，也包括对管理措施落实内容的验收，具体活动内容包括：

- **系统验收准备：**安全控制开发、集成完成后，要根据安全设计方案中需要达到的安全目标，准备系统验收方案。系统验收方案应当立足于合同条款、需求说明书和安全设计方案，充分体现北京信息科技大学的安全需求。
- **组织系统验收：**由系统验收工作组按照验收计划负责组织实施，组织测试人员根据已通过评审的系统验收方案对系统进行测试。
- **验收报告：**在测试完成后形成验收报告，验收报告需要北京信息科技大学与建设方进行确认。验收报告将明确给出验收的结论，安全服务提供商应当根据验收意见尽快修正有关问题，重新进行验收或者转入合同争议处理程序。
- **系统交付：**在系统验收通过以后，要进行系统的交付，需要安全服务提供商提交系统建设过程中的文档、指导北京信息科技大学进行系统运行维护的文档、服务承诺书等。

2.1.7.6.管理措施实现

管理机构和人员的设置

本阶段天下信安将协助北京信息科技大学建立配套的安全管理职能部门，通过管理机构的岗位设置、人员的分工以及各种资源的配备，为信息系统的安全管理提供组织上的保障，具体活动内容包括：

- **安全组织确定：**识别与信息安全管理有关的组织成员及其角色，例如：操作人员、文档管理员、系统管理员、安全管理员等，形成安全组织结构表。
- **角色说明：**以书面的形式详细描述每个角色与职责，确保有人对所有的

风险负责。

管理制度的建设和修订

本阶段天下信安将协助北京信息科技大学建设或修订与信息系统安全管理相配套的、包括所有信息系统的建设、开发、运维、升级和改造等各个阶段和环节所应当遵循的行为规范和操作规程，具体活动内容包括：

- **应用范围明确：**管理制度建立首先要明确制度的应用范围，如机房管理、账户管理、远程访问管理、特殊权限管理、设备管理、变更管理等方面的内容。
- **人员职责定义：**管理制度的建立要明确相关岗位人员的责任和权利范围，并要征求相关人员的意见，要保证责任明确。
- **行为规范规定：**管理制度是通过制度化、规范化的流程和行为，来保证各项管理工作的一致性。
- **评估与完善：**制度在发布、执行过程中，要定期对其进行评估，根据实际环境和情况的变化，对制度进行修改和完善，必要时考虑管理制度的重新制定。

■ 管理制度至少包括：

表 6-1 管理制度修订表

分类		编制内容	备注
组织框架	安全管理机构	信息安全管理机构	
	岗位职责	信息安全岗岗位职责	
人员管理	人员考核	信息安全岗岗位人员培训考核	
	外部人员访问管理	第三方人员管理	
系统建设管理	系统定级制度	信息系统定级与等级保护管理	
	安全方案设计	系统安全建设工作计划	
	工程实施	安全项目和工程实施管理	
系统运维管理	日常运维	信息系统日常运行维护管理	
	环境管理	机房安全管理	
		办公环境信息安全管理	
	资产管理	资产安全管理	

分类		编制内容	备注
	介质管理	介质管理	
	设备管理	设备安全管理	
	监控管理和安全管理中心	日志审计	
	网络安全管理	网络安全管理	
	系统安全管理	系统安全管理	
	应用安全管理	应用安全管理	
	恶意代码防范管理	恶意代码防范管理	
	密码管理	密码使用管理	
	变更管理	变更管理	
	备份与恢复管理	备份和恢复管理	
	安全事件处置	安全事件报告和处置管理	
	应急预案管理	应急响应总体框架	
		应急预案	
系统安全操作	系统安全操作规程	操作系统安全操作	
		数据库系统安全操作	
		中间件系统安全操作	
网络安全操作	网络设备安全操作	网络设备安全操作	
	网络安全设备安全操作	网络安全设备安全操作	

人员安全技能培训

本阶段天下信安将协助北京信息科技大学对人员的职责、素质、意识等方面进行培训，保证人员具有与其岗位职责相适应的安全意识和管理能力，以减少人为因素给系统带来的安全风险，针对普通员工、管理员、开发人员、主管人员以及安全人员的特定安全意识培训，培训后进行考核。

2.1.7.7. 交付成果

本阶段主要交付成果包括输出物：1 个系统的《信息系统等级保护整改建议方案》等。

2.1.8.网络安全等级保护测评方案

我方将对本项目中的信息系统进行等级符合性检验，依据国家等级保护相关标准对系统的安全技术体系与安全管理体系进行整体的符合性测评，识别系统安全保护能力与国家等级保护要求之间的安全等级差距，最终出具等级测评报告，以指导后续对平台系统的等级保护差距整改工作。

我方将站在中立的第三方角度提出客观的评价及建议，并派遣具有等级保护高级测评师的专业人员作为等级测评阶段总负责人和具有等级保护中级、初级测评师的专业人员作为等级保护测评阶段的现场测评实施人员。

2.1.8.1.测评目标

本项目目标是根据《信息系统安全等级保护管理办法》等国家相关文件和标准的要求，对本项目中 1 个信息系统进行等级保护测评工作，全面分析评价系统安全等级保护情况，并给出信息安全等级保护测评报告。

2.1.8.2.测评对象

本项目中 12 个信息系统，相关明细如下。

表 7-1 等级保护测评对象明细表

序号	系统范围	系统名称
1	1 个第二级系统	北京信息科技大学新校区图书馆楼数字档案馆管理平台

2.1.8.3.等级测评内容

对本项目各系统进行等级符合性检验，依据国家等级保护相关标准对系统的

安全技术体系与安全管理体系进行整体的符合性测评，识别系统安全保护能力与国家等级保护要求之间的安全等级差距，最终出具等级测评报告，以指导后续对信息系统的等级保护差距整改工作。

根据等级保护的相关规定，等级保护测评工作分为单元测评和系统测评，工作内容描述如下：

1、单元测评：主要测评基本安全控制在信息系统中的实施配置情况；二是整体测评，主要测评分析信息系统的整体安全性。单元测评包含的内容涉及到信息系统安全技术和安全管理上的各个安全控制措施。

2、整体测评：在单元测评的基础上进行的进一步测评分析，在内容上主要包括安全控制间、层面间和区域间相互作用的安全测评以及系统结构的安全测评等。

2.1.8.4.单元测评实施

把测评指标和测评方式结合到信息系统的具体测评对象上，就构成了可以具体测评的工作单元。具体分为安全物理环境、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、安全人员管理、安全建设管理和安全运维管理等几个方面。

7.3.1.1 安全技术测评

安全技术测评包括“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”五个层面。

2.1.8.5.安全物理环境

安全物理环境测评将通过访谈和检查的方式评测信息系统的物理安全保障情况。

在内容上，安全物理环境安全层面测评实施过程涉及 15 个指标，具体如下表：

表 7-2 物理环境安全层面测评指标表

序号	类别	测评指标	测评对象

1	安全物理环境	物理位置选择	机房场地应选择在具有防震、防风和防雨等能力的建筑内；	记录类文档和机房
2			机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	机房
3		物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。	机房电子门禁系统。
4		防盗窃和防破坏	应将设备或主要部件进行固定，并设置明显的不易除去的标记；	机房设备或主要部件
5			应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；	机房通信线缆
6		防雷击	应将各类机柜、设施和设备等通过接地系统安全接地；	机房
7		防火	机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火。	机房防火设施。
8			机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；	机房验收类文档。
9		防水和防潮	应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	机房。
10			应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；	机房
11		防静电	应安装防静电地板并采用必要的接地防静电措施；	机房。
12		温湿度控制	应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围 之内。	机房温湿度调节设施
13		电力供应	应在机房供电线路上配置稳压器和过电压防护设备；	机房供电设施
14			应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；	机房备用供电设施

15		电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。	机房线缆

配合需求：

配合项目	需求说明
陪同检查	需要陪同进入机房等现场环境检查
文档	提供相关文档

2.1.8.6.安全通信网络

安全通信网络安全测评将通过访谈、检查和测试的方式评测安全通讯网络安全保障情况。

评估对象：主要涉及机房的网络设备、网络安全设备以及网络拓扑结构等三大类。

在内容上，安全通信网络安全层面测评过程涉及 4 个指标，具体如下表：

表 7-3 安全通讯网络层面测评指标表

序号	类别		测评指标	测评对象
1	安全通信网络	网络架构	应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。	路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件。
2			应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可 靠的技术隔离手段。	网络拓扑图
3		通信传输	应采用校验码技术或加解密技术保证通信过程中数据的完整性；	提供加解密功能的设备或组件。
4		可	可基于可信根对通信设备的系统引导程序、系	提供可信验证的设备

		信验证	统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到 破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	或组件、提供集中审计功能的系统

配合需求

配合项目	需求说明
设备登录	登录检查设备配置
文档	提供相关文档及配置文件

2.1.8.7. 安全区域边界

安全区域边界测评将通过访谈、检查和测试的方式评测安全区域边界安全保障情况。

评估对象：网络设备、网络安全设备以及网络拓扑结构，信息系统内的各类主机系统。

内容上，安全区域边界安全层面测评实施过程涉及 11 个指标，具体如下表：

表 7-4 安全区域边界层面测评指标表

序号	类别		测评指标	测评对象
1	安全区域边界	边界防护	应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信；	网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相 关组件。
2		访问控制	应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	网闸、防火墙、路由器和交换机等提供访问控制功能的设备或相关组件。

3			应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	网闸、防火墙、路由器和交换机等提供访问控制功能的设备或相关组件。
4			应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	网闸、防火墙、路由器和交换机等提供访问控制功能的设备或相关组件。
5			应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力	网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相 关组件。
6		入侵防范	应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为	抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保 护系统或相关组件。
7		恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级 和更新。	防病毒网关和 UTM 等提供防恶意代码功能的系统或相关组件
8		安全审计	应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行 为和重要安全事件进行审计。	综合安全审计系统等
9			审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	综合安全审计系统等

10			应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	综合安全审计系统等
11		可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到 破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	提供可信验证的设备或组件、提供集中审计功能的系统

配合需求

配合项目	需求说明
设备登录	登录检查设备配置
文档	提供相关文档及配置文件

2.1.8.8.安全计算环境

安全计算环境安全测评将通过访谈、检查和测试的方式评测安全计算环境安全保障情况，

评估对象：应用系统计算环境，应用系统及数据管理人员。

在内容上，安全计算环境安全层面测评实施过程涉及 22 个评估指标，具体如下表：

表 7-5 安全计算环境层面测评指标表

序号	类别		测评指标	测评对象
1	安全计算环	身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复 杂度要求并定期更换。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动

	境			终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等
2			应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连 接超时自动退出等相关措施	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。
3			当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端:移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和 系

				统管理软件及系统设计文档等。
4		访问控制	应对登录的用户分配账号和权限。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端:移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和 系统管理软件及系统设计文档等。
5			应重命名或删除默认账户，修改默认账户的默认口令。	终端和服务器_设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

6			应及时删除或停用多余的、过期的账号，避免共享账号的存在。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。
7			应授予管理用户所需的最小权限，实现管理用户的权限分离。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。
8		安全审计	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进 行审计。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动

				终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。
9			审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。
10			应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等.	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和

				系统管理软件及系统设计文档等。
11		入侵防范	应遵循最小安装的原则，仅安装需要的组件和应用程序。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备和控制设备等。
12			应关闭不需要的系统服务、默认共享和高危端口。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备和控制设备等。
13			应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管 理客户端、感知节点设备、网关节点设备和

				控制设备等。
14			应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。	业务应用系统、中间件和系统管理软件及系统等。
15			应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞	业务应用系统、中间件和系统管理软件及系统设计文档等。
16		可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏 后进行报警，并将验证结果形成审计记录送至安全管理中心。	提供可信验证的设备或组件、提供集中审计功能的系统
17		数据完整性	应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全 保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备等
18		数据备份恢复	应提供重要数据的本地数据备份与恢复功能；	配置数据和业务数据
19			应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	配置数据和业务数据

20		剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	终端和服务器等设备中的操作系统、业务应用系统、数据库管理系统、中间件和系统 管理软件及系统设计文档等。
21		个人信息保护	应仅采集和保存业务必需的用户个人信息	业务应用系统和数据库管理系统等
22			应禁止未授权访问和非法使用用户个人信息	业务应用系统和数据库管理系统等。

配合需求

配合项目	需求说明
访谈	配合访谈
文档	提供相关文档及配置文件

2.1.8.9.安全管理中心

安全管理中心安全测评将通过访谈、检查和测试的方式评测安全管理中心安全保障情况,

评估对象：提供集中系统管理功能的系统，业务应用系统及数据管理人员。

在内容上，安全管理中心安全层面测评实施过程涉及 4 个评估指标，具体如下表：

表 4-6 安全管理中心层面测评指标表

序号	类别		测评指标	测评对象
1	安全管理中心	系统管理	应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理 操作，并对这些操作进行审计	提供集中系统管理功能的系统

2			应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、资源 配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等	提供集中系统管理功能的系统
3		审计管理	应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计 操作，并对这些操作进行审计	综合安全审计系统、数据库审计系统等提供集中审计功能的系统。
4			应通过审计管理员对审计记录进行分析，并根据分析结果进行处理,包括根据安全 审计策略对审计记录进行存储、管理和查询等	综合安全审计系统、数据库审计系统等提供集中审计功能的系统。

配合需求

配合项目	需求说明
访谈	配合访谈
文档	提供相关文档及配置文件

7.3.1.2 安全管理测评

安全管理测评包括“安全管理制度、安全管理人员、安全建设管理、安全运维管理、安全物理环境”五个层面。

2.1.8.10.安全管理制度

安全管理制度测评将通过访谈和检查的形式评测安全管理制度的制定、发布、评审和修订等情况。

评估对象：安全主管人员、安全管理人员、各类其它人员、各类管理制度、各类操作规程文件,相关的文件资料和工作记录等对象。

在内容上，安全管理制度测评实施过程涉及 6 个测评指标，具体如下表：

表 4-7 安全管理制度层面测评指标表

序号	类别	测评指标	测评对象

1	安全管理制度	安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、 原则和安全框架等。	总体方针策略类文档
2		管理制度	应对安全管理活动中的各类管理内容建立安全管理制度	安全管理制度类文档。
3			应对要求管理人员或操作人员执行的日常管理操作建立操作规程。	操作规程类文档。
4		制定和发布	应指定或授权专门的部门或人员负责安全管理制度的制定	部门/人员职责文件等
5			安全管理制度应通过正式、有效的方式发布，并进行版本控制。	管理制度类文档和记录表单类文档。
6		评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	信息/安全主管和管理制度类文档。

配合需求

配合项目	需求说明
访谈	配合管理访谈
文档	提供相关文档

2.1.8.11. 安全管理机构

安全管理机构测评将通过访谈和检查的形式评测机构安全管理机构方面的情况。

评估对象：信息/网络安全主管、管理制度类文档和记录表单类文档、相关工作记录等对象。

在内容上，安全管理机构测评实施过程涉及 9 个测评指标，具体如下表：

表 4-8 安全管理机构层面测评指标表

序号	类别		测评指标	测评对象
1	安全管理机构	岗位设置	应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权	信息/网络安全主管、管理制度类文档和记录表单类文档
2			:应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。	信息/网络安全主管和管理制度类文档
3		人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。	信息/网络安全主管和管理制度类文档
4		授权和审批	应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等。	管理制度类文档和记录表单类文档
5			应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度。	操作规程类文档和记录表单类文档。
6		沟通和合作	应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题	信息/网络安全主管和管理制度类文档
7			应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通	信息/网络安全主管和管理制度类文档

8			应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	记录表单类文档
9		审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	信息/网络安全主管和管理制度类文档

配合需求

配合项目	需求说明
访谈	配合管理访谈
文档	提供相关文档

2.1.8.12. 安全管理人员

系统安全建设管理测评将通过访谈和检查的形式评测安全管理人员过程中的安全控制情况。

评估对象：信息/网络安全主管、管理制度类文档和记录表单类文档等对象。

在内容上，系统安全建设管理测评实施过程涉及 7 个工作单元，具体如下表：

表 4-9 安全管理人员层面测评指标表

序号	类别		测评指标	测评对象
1	安全管理人员	人员录用	应指定或授权专门的部门或人员负责人员录用；	信息/网络安全主管。
2			应被录用人员的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；	管理制度类文档和记录表单类文档。
3		人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、	记录表单类文档

			钥匙、徽章等以及机构提 供的软硬件设备。	
4		安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施	管理制度类文档
5		外部人员访问管理	应确保在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案	管理制度类文档和记录表单类文档
6			应确保在外部人员接入网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案	管理制度类文档和记录表单类文档
7			外部人员离场后应及时清除其所有的访问权限	管理制度类文档和记录表单类文档

配合需求

配合项目	需求说明
访谈	配合管理访谈
文档	提供相关文档

2.1.8.13. 安全建设管理

安全建设管理测评将通过访谈和检查的形式评测安全建设管理过程中的安全控制情况。

评估对象：建设负责人、管理制度类文档、安全规划设计类文档、操作规程类文档和记录表单类文档、执行过程记录等对象。

在内容上，系统安全运维管理测评实施过程涉及 25 个测评指标，具体如下表：

表 4-10 安全建设管理层面测评指标表

序号	类别		测评指标	测评对象
1	安全建设管理	定级和备案	应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由。	记录表单类文档
2			应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和 审定	记录表单类文档
3			应确保定级结果经过相关部门的批准；	记录表单类文档
4			应将备案材料报主管部门和相应公安机关备案。	记录表单类文档
5		安全方案设计	应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；	安全规划设计类文档
6			应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件。	安全规划设计类文档
7			应组织相关部门和有关安全专家对总体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。	记录表单类文档
8		产品采购和使用	应确保信息安全产品采购和使用符合国家的有关规定；	记录表单类文档。
9			应确保密码产品采购和使用符合国家密码主管部门的要求；	建设负责人和记录表单类文档
10		自行软件开发	应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制	建设负责人
11			应制定软件开发管理制度，明确说明开发	管理制度类文

			过程的控制方法和人员行为准则	档
12		外包软件开发	应在软件交付前检测软件质量和其中可能存在的恶意代码；	记录表单类文档
13			应要求开发单位提供软件设计文档和使用指南；	操作规程类文档和记录表单类文档。
14		工程实施	应指定或授权专门的部门或人员负责工程实施过程的管理；	记录表单类文档
15			应制定工程实施方案控制安全工程实施过程；	记录表单类文档
16		测试验收	在制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；	记录表单类文档
17			应进行上线前的安全性测试，并出具安全测试报告。安全测试报告应包含密码应用安全性测试相关内容。	记录表单类文档
18		系统交付	应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	记录表单类文档
19			应对负责运行维护的技术人员进行相应的技能培训；	记录表单类文档
20			应提供建设过程文档和运行维护文档	记录表单类文档
21		等级测评	应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	运维负责人和记录表单类文档
22			应在发生重大变更或系统级别发生变化时进行等级测评；	运维负责人和记录表单类文档
23			应确保测评机构的选择符合国家有关规定	等级测评报告和相关资质文

				件
24		服务供应商管理	应确保服务供应商的选择符合国家的有关规定；	建设负责人
25			应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	记录表单类文档

配合需求

配合项目	需求说明
访谈	配合管理访谈
文档	提供相关文档

2.1.8.14. 安全运维管理

安全运维管理测评将通过访谈和检查的形式评测安全运维管理过程中的安全控制情况。

评估对象：运维负责人、安全管理员、系统管理员、资产管理员、物理安全负责人、管理制度类文档、安全规划设计类文档、操作规程类文档和记录表单类文档、管理制度类文档和办公环境等对象。

在内容上，安全运维管理测评实施过程涉及 31 个测评指标，具体如下表：

表 4-11 安全运维层面测评指标表

序号	类别		测评指标	测评对象
1	安全运维管理	环境管理	应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、 空调、温湿度控制、消防等设施进行维护管理	物理安全负责人和记录表单类文档
2			应建立机房安全管理制度，对有关物理访问、物品进出和环境安全等方面的管理作 出规定。	管理制度类文档和记录表单

				类文档
3			应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介 质等。	管理制度类文档和办公环境
4		资产管理	应核查资产清单是否包括资产类别（含设备设施、软件、文档等）、资产责任部门、重 要程度和所处位置等内容。	记录表单类文档
5		介质管理	应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	资产管理员和记录表单类文档
6			应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归 档和查询等进行登记记录	资产管理员和记录表单类文档
7		设备维护管理	应对等级保护对象相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	设备管理员和管理制度类文档
8			应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等；	管理制度类文档和记录表单类文档
9		漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；	记录表单类文档

10		网络和系统安全管理	应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和 权限。	记录表单类文档
11			应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	运维负责人和记录表单类文档。
12			应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	管理制度类文档
13			应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	操作规程类文档。
14			应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；	记录表单类文档。
15		恶意代码防范管理	应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	运维负责人和管理制度类文档
16			应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	运维负责人和管理制度类文档
17			应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。	安全管理员和记录表单类文

				档
18		配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；	系统管理员
19		密码管理	应遵循密码相关的国家标准和行业标准	安全管理员
20			应使用国家密码管理主管部门认证核准的密码技术和产品	安全管理员
21		变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；	记录表单类文档
22		备份与恢复管理	应识别需要定期备份的重要业务信息、系统数据及软件系统等；	系统管理员和记录表单类文档
23			应规定备份信息的备份方式、备份频度、存储介质、保存期等；	管理制度类文档。
24			应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	管理制度类文档
25		安全事件处置	应及时向安全管理部门报告所发现的安全弱点和可疑事件	运维负责人和记录表单类文档
26			应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责	管理制度类文档

			等；	
27			应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；	记录表单类文档
28		应急预案管理	应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；	管理制度类文档
29			应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容	管理制度类文档
30		外包运维管理	应确保外包运维服务商的选择符合国家的有关规定；	运维负责人
31			应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；	记录表单类文档

配合需求

配合项目	需求说明
访谈	配合管理访谈
文档	提供相关文档

2.1.8.15.系统整体测评

系统整体测评涉及到信息系统的整体拓扑、局部结构，也关系到信息系统的具体安全功能实现和安全控制配置，与特定信息系统的实际情况紧密相关，内容复杂且充满系统个性。在安全控制测评的基础上，重点考虑安全控制间、层面间以及区域间的相互关联关系，测评安全控制间、层面间和区域间是否存在安全功

能上的增强、补充和削弱作用以及信息系统整体结构安全性、不同信息系统之间整体安全性等。

2.1.8.16. 综合测评分析

综合测评分析包括两个方面的内容：一是安全控制测评分析，主要分析信息安全等级保护要求的基本安全控制在信息系统中的实施配置情况；二是系统整体测评分析，主要测评分析信息系统的整体安全性。其中，安全控制测评分析是信息系统整体安全测评分析的基础。

2.1.8.17.测评方法和工具

2.1.8.17.1.确定测评指标

如何确定等级保护测评指标是本项目的重点，测评指标包括基本指标和特殊指标两部分。不同级别的信息系统的测评指标不相同，信息安全我方有丰富的等级保护测评工作经验，有多位等级保护专家，熟悉国家级传媒行业用户的安全特点，可以结合行业和系统的实际，以列表形式给出《基本要求》未覆盖或者高于《基本要求》的安全要求。

测评指标选取 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中第二级系统安全通用要求指标，包括第二级通用指标类（G2），业务信息安全性指标类（S2），系统服务保证类（A2），安全控制指标如下表：

表 7- 12 安全通用要求指标

安全类	控制点	测评项数
安全物理环境	物理位置选择	2
	物理访问控制	1
	防盗窃和防破坏	2
	防雷击	1

	防火	2
	防水和防潮	2
	防静电	1
	温湿度控制	1
	电力供应	2
	电磁防护	1
小计	10	15
安全通信网络	网络架构	2
	通信传输	1
	可信验证	1
小计	3	4
安全区域边界	边界防护	1
	访问控制	4
	入侵防范	1
	恶意代码防范	1
	安全审计	3
	可信验证	1
小计	6	11
安全计算环境	身份鉴别	3
	访问控制	4
	安全审计	3
	入侵防范	5

	恶意代码防范	1
	可信验证	1
	数据完整性	1
	数据备份恢复	2
	剩余信息保护	1
	个人信息保护	2
小计	10	23
安全管理中心	系统管理	2
	审计管理	2
小计	2	4
安全管理制度	安全策略	1
	管理制度	2
	制定和发布	2
	评审和修订	1
小计	4	6
安全管理机构	岗位设置	2
	人员配备	1
	授权和审批	2
	沟通和合作	3
	审核和检查	1
小计	5	9
安全管理人员	人员录用	2

	人员离岗	1
	安全意识教育和培训	1
	外部人员访问管理	3
小计	4	7
安全建设管理	定级和备案	4
	安全方案设计	3
	产品采购和使用	2
	自行软件开发	2
	外包软件开发	2
	工程实施	2
	测试验收	2
	系统交付	3
	等级测评	3
	服务供应商管理	2
小计	10	25
安全运维管理	环境管理	3
	资产管理	1
	介质管理	2
	设备维护管理	2
	漏洞和风险管理	1
	网络和系统安全管理	5
	恶意代码防范管理	3

	配置管理	1
	密码管理	2
	变更管理	1
	备份与恢复管理	3
	安全事件处置	3
	应急预案管理	2
	外包运维管理	2
小计	14	31
10	68	135

2.1.8.17.2.整体测评

针对测评过程中出现的“部分符合项”和“不符合项”，我方将采取逐条判定的方法，从安全控制间、层面间、区域间和系统结构进行关联关系分析，判断是否存在“弥补”该测评项的不足，或者该测评项是否会“影响”与其有关联关系的其他测评项。

2.1.8.17.3.测评方法和工具

本次等级保护测评工作将使用到以下的测评工具：

1、配置核查列表

2、工具自动化检测

3、风险评估信息库

2.1.8.17.4.配置核查列表

配置核查列表用于人工评估系统存在的各种安全弱点/脆弱性，它针对不同

的系统列出待评估的条目，以保证人工评估结果数据的完备性。下表为部分配置核查列表清单。

表 7-14 配置核查工作表单

序号	工作表单	备注
1	基本信息调查问卷	调查问卷类表单
2	《网络全局检查表》	安全核查表单
3	《防火墙检查表》	
4	《交换机检查表》	
5	《路由器检查表》	
6	《入侵检测\防御系统检查表》	
7	《主机检查表》	
8	《应用及数据检查表》	
9	《物理检查表》	
10	《安全管理机构检查表》	
11	《安全管理制度检查表》	
12	《人员安全管理检查表》	
13	《系统建设管理检查表》	
14	《系统运维管理检查表》	
15	《项目启动首次会议签到表》	其他过程表单
16	《项目启动首次会议记录表》	
17	《项目启动末次会议签到表》	
18	《项目启动末次会议记录表》	
19	《工具接入同意书》	
20	《现场测评通知函》	

2.1.8.17.5.工具自动化检测

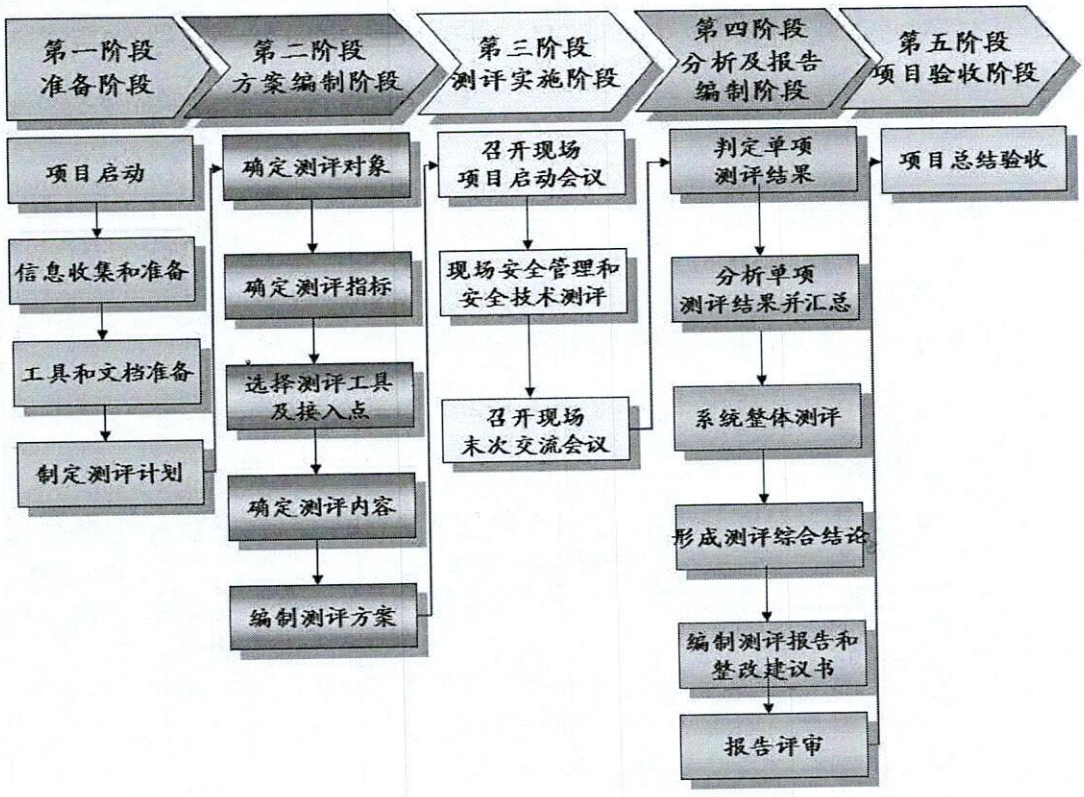
工具自动化检测是使用一个或一组自动化工具检测网络层、主机层设备以及应用层软件可能存在的漏洞。本项目中可能采用的工具如下表所示：

表 7-15 技术测试工具

序号	工具名称	工具用途分类	备注
1	绿盟远程评估系统	系统层、应用层漏洞检测	国产
2	洞鉴安全评估垂	应用渗透测试	国产
3	等保测评工具	辅助测评人员开展等保测评工作	国产
4	开源 web 检测工具	对应用进行检测，进行安全漏洞、风险分析	开源

2.1.8.17.6. 服务提供方式

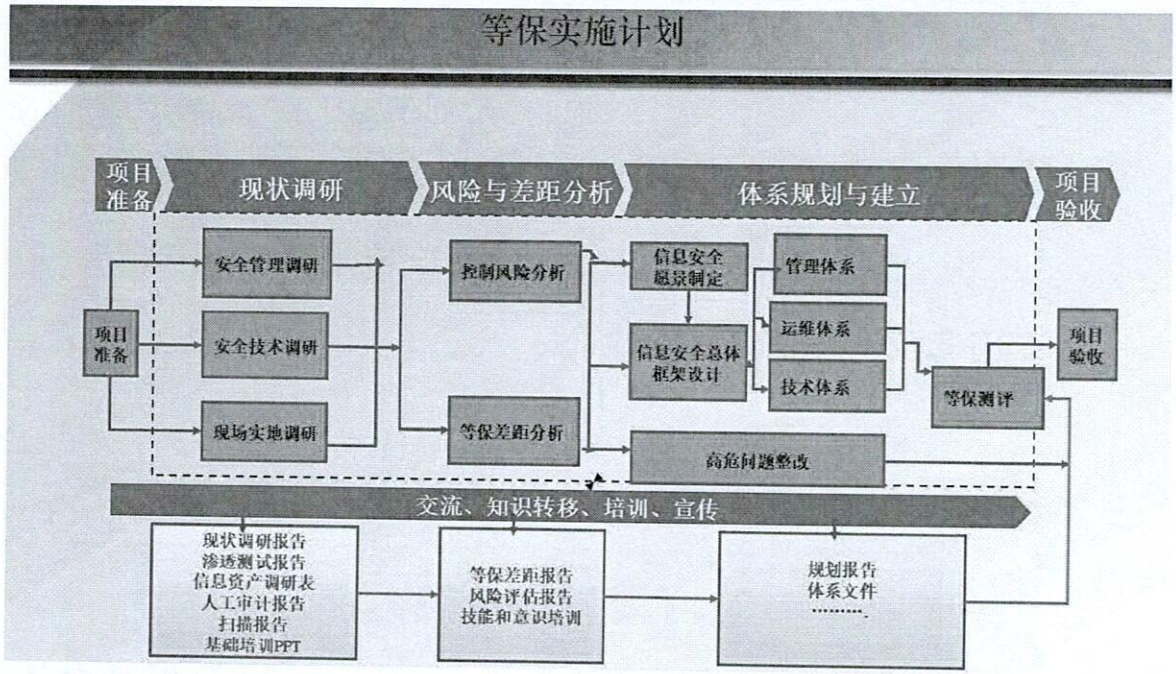
本次测评过程分为五个阶段：测评准备阶段、方案编制阶段、测评实施阶段、分析及报告编制阶段及项目验收阶段，如图所示：



图：测评实施流程

2.1.8.17.7.测评准备阶段

测评准备过程的目标是顺利启动测评项目，准备测评所需的相关资料，为顺利实施现场测评工作打下良好的基础。



7.5.1.1 项目启动

在测评过程中，不仅会涉及客户的信息管理部门，还会涉及到不同的业务部门，因此成立一个稳定、高效的测评工作项目组非常重要。组建等级测评项目组，从资料、人员、计划安排等方面为整个等级测评项目的实施做好准备。

输入：委托等级保护测评服务协议书。

任务描述：

a) 根据项目双方签订的委托等级保护测评服务协议书和系统规模，天下信安组建等级保护测评服务项目组，从人员方面做好准备，并编制项目计划书。项目计划书包含项目概述、工作依据、技术思路、工作内容和项目组织等。
b) 天下信安要求北京信息科技大学提供被测系统基本资料，包括：信息系统的立项、建设、管理相关文档以及联络方式等。

输出/产品：项目计划书。

7.5.1.2 信息收集和分析

我方通过查阅被测系统已有资料了解整个系统的构成和保护情况，为编写测评方案和开展现场测评工作奠定基础。

收集的资料包括：方针文件、规章制度及相关过程管理记录、被测系统总体描述文件、被测系统详细描述文件、被测系统安全保护等级定级报告、安全需求分析报告、被测系统安全总体方案、安全现状评价报告、被测系统安全详细设计方案、用户指南、运行步骤、网络图表、配置管理文档等。

通过与客户人员交谈，了解客户的信息化建设状况与发展，并初步了解被测系统，包括被测系统的行业特征、主管机构、业务范围以及被测系统基本情况，获得被测系统的背景信息。

输入：调查表格，信息系统的立项、建设和管理文档。

任务描述：

a) 天下信安收集等级保护测评服务需要的各种资料，包括北京信息科技大学的各种方针文件、规章制度及相关过程管理记录、被测系统总体描述文件、详细描述文件、系统设计文档、安全需求分析报告、安全总体方案、安全现状评价报告、安全详细设计方案、用户指南、运行步骤、网络图表、配置管理文档等。
b) 天下信安将调查表格提交给北京信息科技大学，督促被测系统相关人员准确填写调查表格。
c) 天下信安收回填写完成的调查表格，如果调查表格填写不准确或不完善或存在相互矛盾的地方较多，天下信安将安排现场调查，与被测系统相关人员进行面对面的沟通和了解。

输出/产品：填好的调查表格。

7.5.1.3 准备工具和文档

实施人员在进行现场测评之前，将做好各方面的准备工作。

输入：各种与被测系统相关的技术资料。

任务描述：

a) 项目人员调试本次等级保护测评服务过程中将用到的项目实施工具。
b) 项目人员模拟被测系统搭建测评环境（可选）。
c) 准备和打印表单。

输出/产品：选用的项目实施工具清单，打印的各类表单。

7.5.1.4 制定测评工作计划

我方将制定工作计划，并确认现场工作所需要的材料，包括《信息系统基本情况调查表》、《工作计划》等，确定所需要访谈的部门及人员、所需要搜集的文档列表等，并与客户沟通确认。

测评准备活动的输出文档及其内容如表 1 所示：

任务	输出文档	文档内容
项目启动	项目计划书	项目概述、工作依据、技术思路、工作内容和项目组织等
信息收集与确认	填好的调查表格	被测系统的安全情况、业务情况、数据情况、软硬件情况、管理模式和相关部门及角色等。
工具和表单准备	选用的项目实施工具清单 打印的各类表单：现场项目授权书、文档交接单、会议记录表单、会议签到表单。	现场项目授权、交接的文档名称、会议记录项目、会议签到项目。

2.1.8.18.方案编制阶段

确定测评对象

根据已经了解到的被测系统信息，分析整个被测系统和各测评业务系统，确定出本次测评的测评对象。

识别并描述被测系统的整体结构，确定被测系统的边界，确定被测系统的重要节点，分析业务系统，包括业务系统的网络边界以及边界设备。

确定测评指标

确定测评指标是本次工作的一个重点，也是一个难点，我方根据已经了解到的被测系统预定级结果，确定出本次测评的测评指标，得出被测系统应采取的安全保护措施 ASG 组合情况，从 GB/T 22239-2019 中选择相应等级的安全要求作为测评指标，包括对 ASG 三类安全要求的选择。

确定测评内容

本部分确定现场测评的具体实施内容，包括单元测评和系统测评。把各层面上的测评指标结合到具体测评对象上，并说明具体的测评方法。

表 4-15 单元测评实施内容

序号	测评指标	测评对象、测评方法、测评实施概述 （测评内容描述）

1	测评指标 1	
2	测评指标 2	
3	测评指标 3	
4	……	
5		

测评方案编制

测评方案是等级测评工作实施的基础，指导等级测评工作的现场实施过程。我方将编制测评方案，包括以下内容：

- 项目概述
- 测评对象
- 测评指标
- 测评工具的接入点
- 单元和系统测评实施
- 配置核查表等

同时，我方会根据以往测评经验以及被测系统规模，补充完善测评计划，包括现场工作人员的分工和时间安排。在进行时间计划安排时，应尽量避开被测系统的业务高峰期，避免给被测系统带来影响。同时，在测评计划中将给出具体测评所需条件以及测评需要的配合人员，便于测评实施之前双方沟通协调、合理安排。我方将测评方案提交给客户，客户签字认可方可实施。

项目方案编制活动的目标是整理项目准备活动中获取的信息系统相关资料，为项目整体活动提供最基本的文档和指导方案。

输入：项目计划书、填好的调查表格等。

任务描述：根据项目计划书和填好的调查表格编制详细的项目实施方案。项目实施方案包括项目概述、工作依据、工作内容、详细实施过程和项目管理等。

输出/产品：项目实施方案。

2.1.8.19.现场测评阶段

测评项目小组依据现场测评计划和测评方案前往信息系统运行环境现场进行实地测评。

召开现场项目启动会议

通过现场启动会议，讨论通过测评方案，确定测评配合人员和项目进度。现场启动会议标志着测评工作正式进入了现场检测阶段。

现场安全管理和安全技术测评

现场测评具体工作内容见第三章，现场测试所使用的方法包括：

- **查验文档资料**

为了获取和分析业务系统现有的安全控制措施，需要查看安全策略文档、安全管理制度、日常操作规程和其它相关文档（例如定级报告）等，查验是否按照管理要求制定了相关的文档，制定中是否定义了安全要求中的内容，是否留有制度执行的记录等。

- **人员访谈**

与有关的管理、技术员工进行逐个访谈沟通，根据相关人员的回答，获得相应信息，并可验证制定的执行情况。

通过访谈管理和技术人员，项目组成员可以收集到业务系统相关的物理、环境、安全组织结构、操作习惯等大量有用的信息，也可以了解到员工的安全意识和安全技能等自身素质。

- **现场测试**

通过现场测试，检查客户是否采取了相应要求的安全技术措施，是否配置了相应要求的安全设备，安全设备的配置是否满足要求等等，同时，也可对办公环境和机房环境作现场检查，通过观察员工的行为，获取管理制度的执行情况和物理安全状况方面的信息。

召开现场末次交流会议

通过召开现场末次会议，我方将向委托机构说明现场检测的初步情况，双方将就现场检测的初步结果达成一致，为编写信息系统综合安全测评报告提供准确证据。

当我方与北京信息科技大学相关人员对现场检测结果达成一致意见后，现场

检测阶段工作结束。

2.1.8.20.分析及报告编制阶段

判定单项测评结果

针对测评指标中的单个测评项，结合具体测评对象，我方将客观、准确地分析测评证据，形成初步单项测评结果。

分析单项测评结果并汇总

单项测评结果汇总分析是分别统计不同测评对象的单项测评结果，并以表格的形式逐一列出。

表 4-16 单项测评结果汇总表

序号	测评对象	测评指标			
		测评指标 1	测评指标 2	测评指标 3	。。。
1	对象 1	✓（或×） 符合项数/测评总项数			
2	对象 2				
3	对象 3				
4	……				
	小计	符合项数/测评总项数			
注：“✓”表示“符合”，“△”表示部分符合，“×”表示“不符合”，“N/A”表示“不适用”。					

系统整体测评

针对单项测评的不符合项，采取逐条判定的方法，从安全控制间、层面间和区域间出发考虑，给出系统整体测评的具体结果和结论，并对系统结构进行整体安全测评。

表 4-17 层面系统整体测评结果

序号	安全控制	测评对象	单项判定 不符合项	能否进行关联互补	说明
1	测评指标 1	对象 1			

		对象 2			
		……			
2	测评指标 1	对象 1			
		……			
……	……	……			
项目小计					

形成测评综合结论

我方在单项测评结果汇总分析和系统整体测评分析的基础上，找出系统保护现状与等级保护基本要求之间的差距，并形成等级测评综合结论。

编制测评报告和整改建议书

我方严格按照《网络安全等级测评报告模板（2021 年版）》编制等级保护测评报告，描述被测系统的总体情况、本次测评的主要测评目的和依据；被测系统描述、测评对象、测评指标、测评内容和方法、结果汇总、风险分析和评价及安全建设整改建议。

同时，我方将编制整改建议书，列出针对系统存在的主要安全问题提出安全建设整改建议。

项目实施报告编制活动的目标是分析和总结项目实施的整体结论，为项目整体验收做好准备。

输入：《项目计划书》、《项目实施方案》、《系统等级保护差距分析报告》、《系统安全整改建议》、《系统等级测评报告》等。

任务描述：根据项目实际实施活动做好总结。

输出/产品：项目实施报告。

报告评审

项目组将召开报告评审会，对测评报告和整改建议书进行评审，并形成评审意见评审后，项目组将参考评审意见，进一步修改，形成最终的等级保护测评报告和安全整改建议书。

2.1.8.21.交付成果

本阶段主要交付成果包括输出物：1 个系统的《网络安全等级测评报告》

2.1.9.8.1 项目组织和计划

2.1.9.1.领导和管理机构

为确保本项目的顺利实施和正常运行，圆满完成各个阶段的建设任务，实现预期目标，将成立项目建设领导小组，并按各系统不同的归属部门作为本项目的决策和协调机构，对重大的信息化建设、技术、管理、业务规范和部门关系等进行决策，对跨部门的重大问题进行协调，对全系统技术装备的采购和建设进行管理。

2.1.9.2.项目实施团队

2.1.9.2.1. 本项目实施团队情况

天下信安结合项目管理最佳实践，采用科学的项目管理组织结构是组织实施本项目的基础。项目组织结构形成不仅能使我们很好地管理项目，而且可以使我们与客户进行密切的配合，与客户建立良好的合作关系，保证项目实施过程是按照进度、计划有序执行，控制项目质量给出等级测评结论。

针对本项目，项目组织结构如图所示：

名称	职责
项目领导小组	• 审定项目方案和总体进度计划，监督协调项目进程； • 项目重大事项决策； • 定期听取项目组的工作汇报
项目总监	- 负责项目实施方案的设计，制定各阶段具体实施计划、各阶段具体资金计划、各阶段技术和管理重点、各阶段质量监控计划等。 - 负责制定总体技术方案，负责协调解决项目设计和实施过程中的各种技术问题，并做好技术把关工作。 - 审核项目实施方案。 - 负责协调项目实施进度和质量，确保各个项目按期保质推进。 - 对整体项目管理工作负总责。

质量负责人	- 负责对项目的培训计划制定，安排，沟通协调，制定项目的质量保障体系、确定可行的质量保障计划、集成质量保证方法及相关关键技术、监控开发实施手段，确保项目实施的质量，确保成果交付的质量。
定级备案组	- 负责等保备案辅助的实施协调与指导，推进项目的执行。
安全检测组	- 负责漏洞扫描、渗透测试的实施协调与指导，推进项目的执行。
整改指导组	- 负责协助安全加固、等保制度建设的实施协调与指导，推进项目的执行
等级测评组	- 负责等级保护预测评、等级保护测评的实施协调与指导，推进项目的执行。

2.1.9.2.2.人员构成和职责

天下信安目前取得测评联盟颁发的《等级测评师证书》测评人员均参加了公安部信息安全等级保护的专门培训，能够正确把握国家政策，理解和掌握相关技术标准，熟悉等级测评的方法、流程和工作规范等方面的知识及能力，能够依据测评结果做出专业判断并出具等级测评报告。

本项目工作组设立了项目领导组和项目实施组。其中项目领导组由测评机构主要领导组成，宏观监控整个项目的实施。商务负责人主要由公司销售总监指定，负责项目合同等和商务有关事务的处理。档案管理员由公司档案管理员担任。项目实施组主要按照项目经理安排、依据项目计划和项目流程开展测评工作。

项目领导组人员构成与职责

天下信安建议成立一个由测评机构和被测评方高层管理人员共同组成项目领导组。项目领导组的任务宏观监控整个项目的实施，对于项目进程中不可避免的重大变更，由项目领导组来批准这些变更的实施，从而确保项目最大限度地如期完成。

项目领导组的职责如下：

- 明确项目的总体目标、进度和实施策略；
- 跟踪国内、外信息安全的相关政策、法规及标准的发展；

- 听取项目组的工作汇报，监督项目执行情况，进行项目质量控制；
- 定期审阅有关汇报材料，例如：工作计划、进度报告、质量报告、问题清单等；
- 对项目实施过程中所出现的意外情况或重大问题（技术问题、质量问题、经费问题、关系问题等）听取汇报，做出决策；
- 对项目进程中的重大变更进行决策；
- 组织协调各种资源，支持项目；
- 组织和审核项目实施阶段性的验收以及相关重大活动；
- 指定等级测评项目经理。

项目经理人员构成和职责

天下信安领导组指派**张朋辉同志（高级测评师）**作为项目的项目经理，负责整个测评的实施与被测评单位沟通，对项目实施的全过程进行具体的实质性的组织管理，负责项目的进度、质量、成本的控制。

项目经理职责如下：

- 编制项目计划；
- 组织必要的资源；
- 负责所有的项目组成员的工作安排；
- 控制项目的总体实施进度；
- 负责项目组之间的协调和沟通；
- 召开项目例会和小组会议；
- 对单元测评和整体测评结果进行判断；
- 对测评结论进行判断，审查测评报告的完整性；
- 召开审查会议，及时解决关键问题；
- 定期地向项目领导组报告项目的实施进度；
- 做好变更控制和协调工作；
- 有效安排资源，组织、协调工作组成员的工作；
- 定期对子项目组的阶段性任务进行监督和考核，以保证整个项目按质按量按时完成；
- 保证项目按期提交验收。

项目组长构成与职责

项目组分为定级备案组、整改指导组、等级测评组和安全检测组，每个组的组长主要由天下信安经验丰富的测评师担任，保证等级测评的全面性、系统性和客观性，负责对单项测评和单元测评的结果进行正确判断，测评中遇到困难、问题及时向项目经理汇报，确保问题得到有效解决。

测评组组长职责如下：

- 现场测评活动，负责小组现场实施；
- 利用访谈、检查、测试等手段达到项目目的，符合测评力度要求；
- 搭建模拟环境进行相关技术求证，保证测评结果的真实性和可重复性；
- 按照项目经理工作计划和安排进行测评，满足测评进度要求；
- 按照测评指导书和相应表格如实填写测评记录，保证测评的全面性、系统性和客观性要求；
- 定期向项目经理汇报测评情况和项目实施进度情况；
- 对单项测评和单元测评结果进行正确判断，编写测评报告；
- 测评结果出现疑问和不完整等情况，及时向项目经理汇报并确保以上问题得到有效解决；
- 在项目总结会议中，分析测评中遇到的问题和处理方式，分享项目经验；
- 对被测评单位提出的变更，要及时回应，并以书面形式上报项目经理，并给出建议；
- 有效安排资源，组织、协调工作组成员的工作。

测评人员构成与职责

测评人员分为技术测评师和管理测评师，在等级测评中持证上岗，按照测评要求，在测评过程中需如实填写测评记录，按照测评流程卡完成工作任务，并得到被测评单位的签字确认。保证整个等级测评工作的全面性、系统性和客观性，能够对单项测评和单元测评的结果进行正确判断，测评中遇到困难、问题及时向组长汇报，确保问题得到有效解决。

测评人员职责如下：

- 测评活动的现场实施工作；
- 利用访谈、检查、测试等手段达到项目目的，符合测评力度要求；
- 搭建模拟环境进行相关技术求证，保证测评结果的真实性和可重复性；

- 按照项目经理工作计划和安排进行测评，满足测评进度要求；
- 按照测评指导书和相应表格如实填写测评记录，保证测评的全面性、系统性和客观性要求；
- 向组长汇报测评情况和项目实施进度情况；
- 对单项测评和单元测评结果进行正确判断，编写测评报告；
- 测评结果出现疑问和不完整等情况，及时向组长汇报并确保以上问题得到有效解决；
- 在项目总结会议中，分析测评中遇到的问题和处理方式，分享项目经验；
- 对被测评单位提出的变更，要及时回应，并以书面形式上报项目经理，并给出建议。

2.1.9.3. 本项目实施团队主要人员名单

具体人员安排情况如下表所示，实施过程中在征求用户许可后，项目组人员有可能进行适度调整。我方将力求保持项目组核心人员不变化。

项目组	成员	职务/职称	本项目中担任职务	资质
项目经理	张朋辉	技术负责人	项目总监	PMP/高级测评师
质量保证组组长	彭魏	质量负责人	质量负责人	高级测评师
项目实施组主要人员	**定级备案组**			
	张静威	项目经理	组长	中级测评师
	张美霞	测评工程师	实施人员	初级测评师
	安全检测组			
	朱榕庆	测评工程师	组长	中级测评师
	侯世位	测评工程师	实施人员	初级测评师
	朱勋	测评工程师	实施人员	初级测评师
	整改指导组			

	袁连彪	项目经理	组长	中级测评师
	闫军	测评工程师	实施人员	中级测评师
	张晓蕾	测评工程师	实施人员	初级测评师
	等级测评组			
	陈文超	项目经理	组长	中级测评师
	赵蓉	测评工程师	实施人员	中级测评师
	赵四杰	测评工程师	实施人员	初级测评师
	但珍	测评工程师	实施人员	初级测评师

投标人承诺：项目周期内实施人员保持稳定，项目核心人员不发生变动。

2.1.9.4. 项目实施计划

表 9-1 项目实施任务分解表

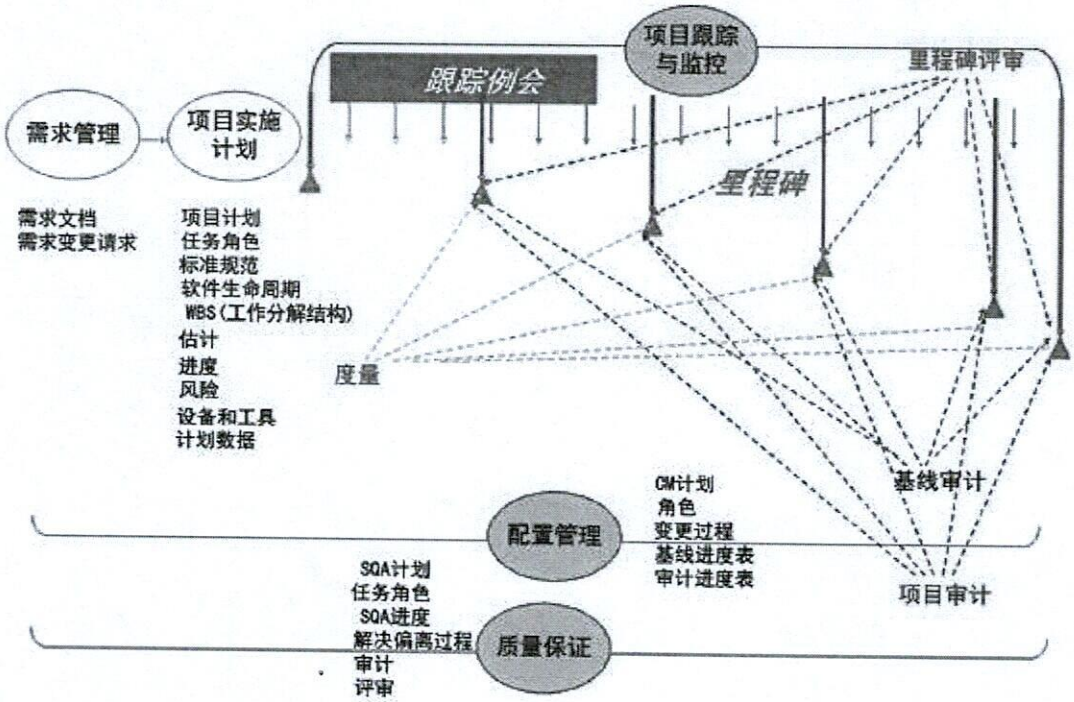
工作阶段	工作内容	日历日	交付成果
定级备案阶段	信息系统定级资料准备	10	《信息系统安全等级保护定级报告》 《信息系统安全等级保护备案表》 《网络安全等级保护定级专家评审意见》
	协助召开专家评审会		
	协助备案		
安全差距分析	前期调研	20	《信息系统等级保护差距分析报告》 《漏洞扫描报告》 《渗透测试报告》
	资产梳理		
	技术体系差距分析		
	管理体系差距分析		
	漏洞扫描		
	渗透测试		
	编写查分析报告		
安全整改咨询	技术整改方案设计	20	《信息系统等级保护整改建议方案》
	管理整改方案设计		

	编写整改建议方案		
网络安全等级保护测评	现状调研	40	《网络安全等级测评报告》
	测评指导书编制		
	测评实施方案编制		
	检查访谈		
	安全技术体系等级测评		
	安全管理体系等级测评		
	安全控制间测评		
	层面间安全测评		
	区域间安全测评		
	编写等级保护测评报告		
	预计总工期	90	
注释：合同签订并接到北京信息科技大学通知后，相关阶段工作可并行开展。			

2.1.10.项目过程管理

本项目的成功实施，不仅依靠先进、成熟的信息技术，强有力的领导支持和经验丰富的开发实施团队，更需要一套经过大型复杂项目验证的实施方法对项目实施过程进行控制与管理。

在本项目实施过程中，需要重点关注需求、设计、实施阶段的里程碑节点，把好进度质量关，控制好风险，解决好偏离等，使项目实施过程基本按照设定的轨迹进行，从而保证整个项目的实施。其大体过程如下图所示：



图：项目过程控制示意图

2.1.10.1.项目进度控制

（一）项目例会

由北京信息科技大学每周召集举行，我方汇报设计、实施工作完成情况并确定下周计划，同时在会上对提出的争议和问题进行讨论。

在实施过程中发生的临时性会议，比如专题技术协调会、高层会议等，视情况随时召集。

（二）项目状态报告

在项目实施过程中，根据项目的实际进展情况，每周二下班之前向北京信息科技大学提交项目周报，汇报项目的进度以及完成、未完成工作、存在问题、下一步的工作计划等内容。

（三）项目里程碑/阶段评估验收

在项目的方案设计、服务实施、项目验收等里程碑点，组织完成需求分析评审、设计方案评审、服务交付物评审、项目验收等工作外，我方协助业主执行对项目里程碑评审验收。

2.1.10.2.项目沟通管理

项目沟通管理包括不同情况下的沟通方式。主要包括正式会议、计划和命令下达，执行结果的汇总报告，临时情况沟通，讨论分歧并达成一致，不能达成一致问题的记录、报告和最后决策。

天下信安公司有着优秀的项目团队和丰富的 IT 项目管理经验。天下信安把客户的成功作为项目的最终目标，在项目的执行过程中始终把帮助客户实现项目的价值作为对自己的要求，并努力把项目做到最好。

在本项目中，将采用一些正规的项目沟通程序，保证参与项目的各方能够保持对项目的了解和支持。这些管理和沟通措施将对项目过程的质量和结果的质量具有重要的作用。

日常沟通、记录和备忘录

鼓励项目参加各方在项目进行过程中随时对相关问题进行沟通。所有重要的、有主题的日常沟通活动都应留下记录或形成备忘录。日常沟通的主要渠道包括：

1) 非正式会议

2) 电话

3) 电子邮件

报告

各种报告是项目各方互相沟通的最正式的渠道和证据。一些必备的项目报告包括：

1) 项目计划和进展报告

2) 项目总结报告

3) 以及在各个阶段输出的项目成果文本等

正式报告必须通过有关评审和批准之后方可发布。

会议

包括正式会议和临时会议。

正式会议是项目管理活动的重要形式，是项目各方进行正式沟通的渠道。正式会议至少有首次会议(可以和项目启动会合并一起)、调查发现报告会议和末次会议(项目总结会议)。正式会议还包括对重要提交物和重大里程碑进行确认的评审会议，以及正式通告之前通告准备会议。会议必须有签到记录和会议纪要。记录和纪要存档保留，并最后提交甲方。

临时会议是讨论临时问题所发起的会议。项目经理、技术经理和质量经理有资格发起临时会议。

分歧的处理

在项目中甲乙双方难免出现分歧，出现分歧沟通方法规定如下：

➔ 首先要记录分歧，分歧记录必须说明各个分歧方的观点和事实，事实要记录细节，不记录细节的，被认定为无效分歧；

➔ 提交项目组直接上级讨论，乙方人员的技术问题提交技术经理，管理问题提交项目经理，质量问题提交质量经理；

➔ 甲方被调查部门认为调查发现与实际不符的，向乙方安全评估人员说明情况。乙方调查人员知识确定现象是否与实际情况一致，并不做判定；

➔ 甲乙两方项目组出现分歧的，有甲乙双方项目经理讨论，其他人员进说明现象和所发现的事实。不能达成一致的，提交项目委员会做出选定。

沟通记录的管理

沟通记录一定要如实记录并向有关人员确认是否与所陈述的一致，否则为无效记录。沟通能够记录必须提交文件服务器予以保存。

2.1.10.3.项目问题及变更管理

项目问题管理

项目问题管理流程能够让团队成员及时发现、跟踪和解决对项目预计会产生重大影响的问题，避免这些问题对项目进度产生影响，该项目问题管理分成提交、

评估、汇报和解决四个阶段。

对于项目过程中影响项目实施情况、进度以及交付品质量的重大问题，项目组应按照上述项目问题管理流程对问题进行解决，同时在问题管理的不同阶段，将问题的名称、严重性、描述、提出人、提出时间、要求解决时间、影响、解决方案和情况等信息记录在问题管理表中。

问题管理表如下所示：

报告日期：			**文档编号：**
问题管理			
问题名称			
问题严重性			
问题描述			
问题提出人		问题提出时间	
问题要求解决时间			
问题评估			
影响			
解决方案			
预计完成时间			
问题解决情况			
完成人			

审阅人	

项目变更管理

项目变更管理是以一种对项目影响最小的方式改变现状，是项目组在对项目范围和进度进行合理变更时控制变更朝着良性方向发展的重要手段。遵循项目变更管理流程，项目组可以根据项目的实施情况，依据项目范围和进度管理，执行项目变更。该项目的变更管理流程分为五个阶段，各个阶段均有天下信安的人员参与。

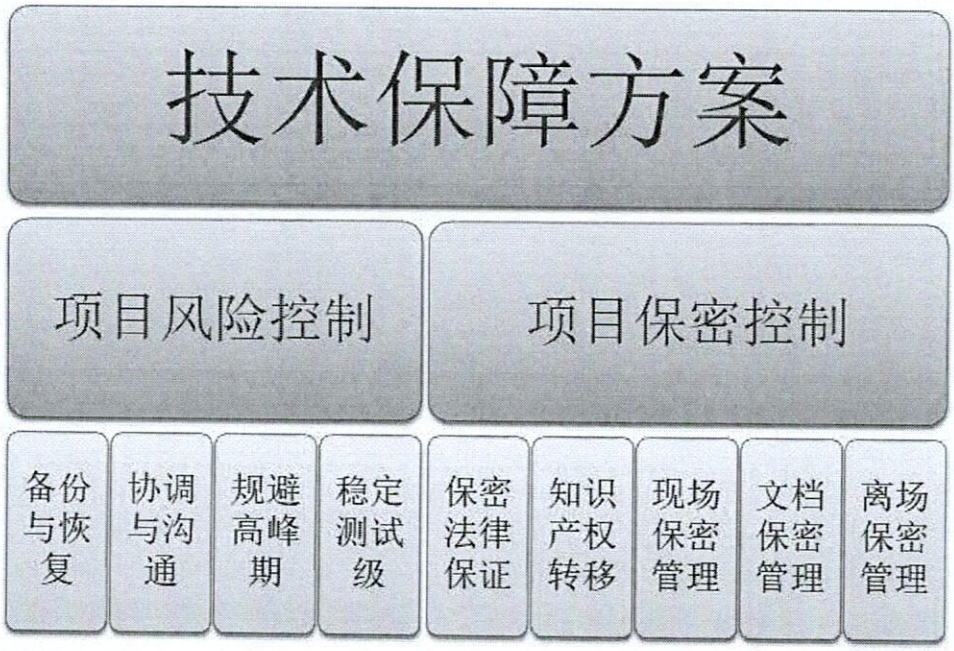
在这一阶段，项目组对项目出现的包括范围、资源、计划、交付物、关键里程碑以及其他类型的变更，应填写变更管理表以记录变更的提交、审核、分析、批准和实施过程。

变更管理表如下表所示。

报告日期：			**文档编号：**
变更申请信息			
变更申请人		变更申请日期	
变更优先级			
变更种类	□范围 □资源 □计划 □交付物 □关键里程碑 其他：_____		
变更描述			
变更方案			
申请人			
评估小组意见			

项目范围变更对项目时间和资源的影响	
项目资源的变化对项目进度的影响	
项目计划的变化对项目进展的影响	
影响到哪些交付物	
影响到哪些关键里程碑	
变更决策	
变更决策	
天下信安项目负责人	

2.1.10.4.项目质量保证



项目质量管理保证项目顺利实现预期目标的基本方法。本章从项目全过程来描述了质量控制方法，确保项目的提交物符合预期要求，项目过程符合有关要求，项目计划切实可行和可信。

为保证项目的实施质量，将从质量保证、配置管理、测试管理等方面建立相应的管理体系，从多个维度来保证项目能够按照质量要求和时间计划成功完成。

质量保证体系

在本项目中必须统一标准，明确定义保证项目质量的责任和方法。结合项目的实际情况，质量保证和责任划分方法为：

项目负责人进行项目的总体管理和控制，听取客户的意见，寻求改进的方法，自始至终负责整个项目的实施。

选派具备专业特长的项目工程师认真准备针对自己领域的工作、培训或实验环境，听取客户对培训内容的建议和意见，圆满解决客户提出的相关问题。

每一大类或一个阶段的工作内容结束后，做工作总结和定期的状态报告会，以保证客户和项目负责人能及时跟踪工作的进展。

质量保证体系严格贯彻执行

2.1.10.4.1.项目过程的定义与评审

在项目策划阶段，在充分了解客户需求的基础上，明确项目的目标、范围、工作内容和要求的基础上，依据我方《信息安全业务体系文件》中预定义的标准过程文件来裁剪出本项目的项目过程，裁剪后确定德尔项目已定义过程需要经过质量控制经理的评审确保符合组织要求，并能够满足项目需要和实现项目目标。项目过程的成熟稳定已经在整个组织中的一致性是确保项目过程、工作和工作结果满足质量要求的最有保障的基础。这种思想在信息安全工程模型中已经清晰定义，我方的信息安全业务以及本项目中得到了充分落实。

2.1.10.4.2.项目实施过程的质量监控

在项目实施过程中，需要依据先计划-执行-记录-检查和校准改进的模型进行。首次项目计划的编制，周滚动计划、项目周报和项目周例会制度的执行，技术经理的技术检查确保项目过程不仅符合预定义计划和项目已定义过程，并确保变动和变差控制及时得到了重新计划和实施控制。项目实施的过程活动和活动结果要及时记录，并把记录纳入文件管理范围。实施记录为工作任务的执行和完成结果提供了事实依据和数据，计划和记录纳入文件管理范围确保了事实依据和数据的真实性和完整性。

工程准备阶段的质量控制

目的

对工程实施的总体技术方案、实施方案、管理方案的编制提出通过评审过程进行质量管理。

质量管理流程

质管小组指定负责此阶段质管任务人员，提交质量保证计划；

依据质量保证计划和文件要求，质管组在项目经理协调支持下，组织人员对技术方案、实施方案、管理方案进行专家评审；

评审意见经项目经理认可后反馈至文档提交部门修改；

通过内部评审后，提交用户，进行文档评审。

表 9-3 质量控制内容表

质量控制点	质量控制手段	控制内容	依据标准
技术方案	内、外部评审	审查技术方案是否基本满足平台改造的业务需求	合同、总体技术方案、平台实际情况
实施方案	内、外部评审	审查实施方案的可行性、可操作性	工程总体实施方案平台实际情况
项目管理方案	内、外部评审	审查管理方案的可行性	工程总体项目管理方案及实际情况
质量保证计划	内、外部评审	审查质量保证计划的可行性、可操作性	工程总体质量保证计划和实际情况

工程实施阶段的质量控制

1、目的

对实施的质量和进度进行控制，以发现工程中存在的问题隐患，并及时进行修正，提出改正建议，对设计变更和方案的修改进行审核，并协助甲方对项目进行阶段性验收。

2、质量控制流程

质管小组指定负责此阶段各子系统的质管任务人员，依据质保工作计划开展工作；

以质量保证计划、项目计划及各类已有标准为依据，检查工程日常实施中的质量问题；

通过现场监测等质保形式，对工程实施质量问题进行记录，并形成报告，对各种问题提出质量意见；

根据不同问题发送质保报告至工程有关方，提出问题并修改建议；

跟踪提出的质保问题并记录档案，直至其符合工程质量要求。

2.1.10.4.3.项目风险管理

风险分析与控制过程是工程实施中的必经的工作内容，在本项目中天下信安

将建立完善的风险处理机制，通过有效地对项目实施中的风险预防与控制措施，在工程实施过程中对各类风险进行有效地控制。整体上达到控制、降低风险的目的。

风险分析

在项目实施过程中，或多或少会出现一些意想不到的事情发生，从而影响项目的实施。根据我们多年的项目实施经验积累，在项目 实施过程中主要存在以下几类风险：

■ **需求变更风险：**本项目技术沟通的深度和准度将影响实施服务的可靠性，沟通的不畅将有可能导致对用户环境的错误理解，从而形成错误的需求分析，影响项目实施。

■ **时间进度风险：**在实际实施过程中，可能由于安装环境不具备、人员没有到位，产品质量问题等种种原因，给项目进度控制带来压力，造成项目进度 拖延。

■ **人员组织风险：**本项目实施涉及多系统之间的对等多种类型项目内容，且在项目开展过程中互相穿插，如未对项目人员建立有效管理与责任分配机制，可能将由于任务不明确等导致的内部摩擦影响工作效率的风险。

风险控制措施

在本项目实施中，对风险过程的控制的目的是建立处理风险的策 略，而一个有效的策略应在充分分析存在的项目风险基础上，选择有效的控制措施，以降低风险带来的损失或影响。针对上述在实施过程 中可能发生的风险，采取如下规避措施来实现风险的控制。

2.1.10.4.4.规避数据采集风险

进行数据采集前，项目经理需要提前向北京信息科技大学信息提交当前工作计划，经过双方确认后，双方共同为数据采集做好相应风险规避 措施，再进行数据的采集。这样不但能够保证双方合作时间上的可靠， 同时可以防止因为采集数据(从网络产品、主机服务器上)，造成影响设备、业务、系统正常运行的可能。

当前工作计划完成后，数据采集人员需要提交工作确认单，经过双方确认数

据采集工作后，开展下一步工作。可以通过工作确认，保 证数据采集的有效性、准确性，防止进行重复性工作，同时避免工作的遗漏。

强烈建议对相关设备进行手工检查前对系统上的重要业务数据进行备份:系统包括但不限于数据库系统、涉密信息存储系统、重要业务 应用系统、网络设备等;备份数据包括但不限于数据库表、重要文档、应用配置信息、 主机设备配置文件、网络设备 IOS、网络设备配置信息、安全设备配置信息等;

建议在业务闲时对重要业务数据进行备份;备份完成后建议测试备份介质及其数据的可用性。

2.1.10.4.5.规避工作测试风险

在使用工具测试的过程中，测试人员会通过设置线程、插件数量等参数来减少其对系统的压力，同时还会去除任何可能对目标系统带来危害的插件，如:远程溢出攻击类插件、拒绝服务攻击类插件等等。

2.1.10.4.6.规避需求变更风险

双方进行需求变更确认，在需求有重大变化时，双方商定对系统 上线的时间进行适当调整，必要时双方签订补充协议或通过《项目变更申请表》进行确认。

规避时间进度风险：根据项目的总体时间进度要求，制定工程实施各个阶段时间及阶段的里程碑目标，在项目组织过程将充分考虑各种潜在因素，适当留有余地;任务分解详细度适中，便于考核;在执行过程中，强调项目 按进度执行的重要性，在考虑任何问题时，都将保持进度作为先决条件;同时，合理利用赶工及快速跟进等方法，充分利用资源。

规避人员组织风险：在此项目实施中遵循“专人负责”原则，由用户和天下信安派专人负责该项目，同时抽调天下信安骨干技术人员，在项目中承担重要的角色，保证项目对高级技术人员、高级管理人员的要求。

项目实施过程中，将参与项目人员的业绩评估与该项目实施的状况相关联，明确岗位和工作职责，制定适当的奖惩措施;确定每个项目负责人的管理权 力，提倡项目的群体观念。

2.1.10.5.其它风险规避

为保障客户系统在测评过程中稳定、安全的运转，我们将提供以下多种方式来进行风险规避。

时间：从时间安排上，测试人员将尽量避免在数据高峰时进行测试，以此来减小测评工作对被测试系统带来的压力。另外，测试人员在每 次测试前也将通过电话、邮件等方式告知相关人员，以防止测试过程 中出现意外情况。

技术手段：技术人员都具有丰富的经验和技能，在每一步测试前都会预估可能带来的后果，对于可能产生影响的测试将被记录并跳过，并在随后 与客户协商决定是否进行测试及测试方法。

2.1.10.6. 项目保密管理

保密协议

天下信安公司和甲方就本项目签订《保密协议》，双方各保存一份。

项目现场的安全保密管理规定：

所有进入工作场地的人员，均应遵守本安全保密规定。

在天下信安公司项目组所在的办公环境中，除客户提供或允许的 U 盘，不允许出现其他存储介质。

在天下信安公司项目环境，除天下信安公司顾问使用的电脑设备，不允许其他人员携带电脑进入场地环境。

沟通保密管理

沟通中所涉及的内容不经允许，不得向项目无关人员提供沟通的有关信息。沟通信息的传递必须按照规定的沟通渠道传递。

文档材料的保密管理

对需要甲方提供的文档，天下信安公司提交《文档调用单》给甲方项目接口人。

在调用单规定期限内，甲方应当提供要求的文档资料。

文档调用单上，明确文档申请人，文档使用人员等涉及此文档的人员。

对纸质文档，统一保管在指定的文件柜里。使用完后返还给甲方提供方，并

填写《文档调用单》的交回部分。

对电子文档，传递通过甲方接口人指定的u盘，保存在文档申请人及使用人员的笔记本上，项目组笔记本电脑的应设安全级别高的口令。

离场及项目结束的保密管理

天下信安公司项目组在项目离场时，笔记本交由甲方专人清理后方可带出。

所有本地提供的纸质文档，在项目结束的时候，都要返给甲方提供方，并填写《文档调用单》的交回部分。

例外情况

遇到未列明的涉及保密方面的例外情况，双方就个案单独洽谈，由项目领导小组签字确认。

2.1.10.7.培训和技术支持

2.1.10.7.1.培训目的

在项目过程中，我们将对北京信息科技大学工作人员在北京进行信息安全等级保护政策、法规、技术标准等内容的安全培训工作，使之具备一定的水平，完成信息安全等级保护政策的宣贯、提高相关工作人员的信息安全意识、信息安全技能等。

2.1.10.7.2.培训方式

在本项目的培训中，我们将采用以下方式来组织培训：

在培训方式上，采用集中培训与现场培训相结合的方式来开展我们的培训工作；其中，集中培训由北京信息科技大学提供培训场地，由专业讲师根据培训大纲的要求进行中文授课。

在培训形式上，可以分为个案讲解、系统传授、上机实践等相结合的方式。

2.1.10.7.3. 培训计划

培训时间

培训时间为：双方协商，总体时间为 1 个工作日。

培训人员

参训人员为技术、运维人员和管理人员，具体人员待定。

具体培训计划

建议的培训课程内容如下所示，具体的培训内容由双方协商后确定。

表 9-4 培训课程表

课程名称	培训内容	培训时间	培训方式	培训讲师
等级保护基本知识培训	等级保护基本规范内容包括定级政策以及相关法规培训等	0.5 天	集中培训	天下信安公司测评师
等级保护实施及测评技术培训	对实施中发生的疑难问题进行现场培训	0.5 天	现场培训	天下信安公司测评师

2.1.10.7.4.售后服务与技术支持

本次等级保护测评项目不是一朝一夕可以完结的，因此项目的售后服务与支持也是项目成功建设与应用的重要方面。在本章，我们从天下信安全面的售后服务体系出发，从项目售后服务原则，到专为项目设立的多级服务组织、服务内容、服务方式，再到服务承诺、服务监督等多方面详细的描述了天下信安的售后服务与技术支持方案。

服务内容和承诺

天下信安极其重视与北京信息科技大学的合作，为保证项目服务质量，我们针对项目制定的个性化的服务原则：

- **设立专门的项目实施服务团队，团队构成如下：**

- 资深技术专家、等保测评专家、实施项目经理；
- 建立本地化的服务团队
- 承诺在服务期内不更换项目组主要成员

■ **1年免费辅导支持服务**

- 服务的内容是针对项目提交物提供解释和说明，必要的情况下提供现场培训。
- 服务的方式是电话咨询、邮件咨询、在线咨询和现场支持。

服务方式

基于天下信安的售后服务体系，天下信安将设立北京信息科技大学项目支持服务中心，提供技术问题解答、投诉信箱，及时响应客户的服务请求，进行本地化的售后服务，保证售后服务的快速有效。售后服务中心采用以下服务方式为本项目提供售后服务支持：

1、电话、传真及网上服务：

用户可以通过电话、传真以及网络等方式提出问题，寻求技术支持。

2、远程网络支持

考虑现场支持的响应时间，天下信安提供更为快捷的远程网络支持服务，在客户允许的情况下，天下信安售后服务人员通过远程网络直接连接客户应用系统，解决问题，排除故障。

远程网络支持的前提是客户允许远程网络连接。

3、咨询服务

天下信安充分利用自身在客户架构、系统集成与信息安全等方面的综合优势，为北京信息科技大学提供技术咨询性相关的服务。客户可以通过电话、邮件、网络对话等方式对信息安全等级保护提出问题，天下信安的服务人员将给予解答。

支持服务监督

由天下信安综合管理部经理、销售部经理牵头，组成服务监督部。

负责服务制度的制定，对于涉及各部门现有规定和制度的，综合各部门意见，写出制度修订方案。

设立专门的服务投诉专线，对于在服务方面感到不满意的，可以向服务监督部投诉。服务监督部将对客户不满意的部门、服务技术人员进行及时的调查和处理，以保证不断提高服务质量。

2.1.10.7.5.验收方案

验收机构

验收机构：甲方；北京信息科技大学

配合单位：北京天下信安技术有限公司。

项目验收原则

1. 验收方案由北京信息科技大学提出，我方按北京信息科技大学要求准备相关验收材料。

2. 验收前，我方提前 5 个工作日通知北京信息科技大学，我方与北京信息科技大学在验收过程中应密切合作。

3. 北京信息科技大学对验收的认可、参加或放弃参加验收和测试，均不能减轻供应商对合同的任何责任。

4. 北京信息科技大学有权拒绝接收有缺陷的服务或要求进行改造，由此引起的一切费用应由我方负责，经改造后的服务应重新进行验收。

5. 验收依据

招标书、投标书、合同、安全服务报告、工作记录单、相关的国家标准、行业标准、规范以及检测规程等。

6. 合同验收

完成合同全部内容后，进行合同验收。

项目验收方法

1、项目节点完成时间符合合同要求

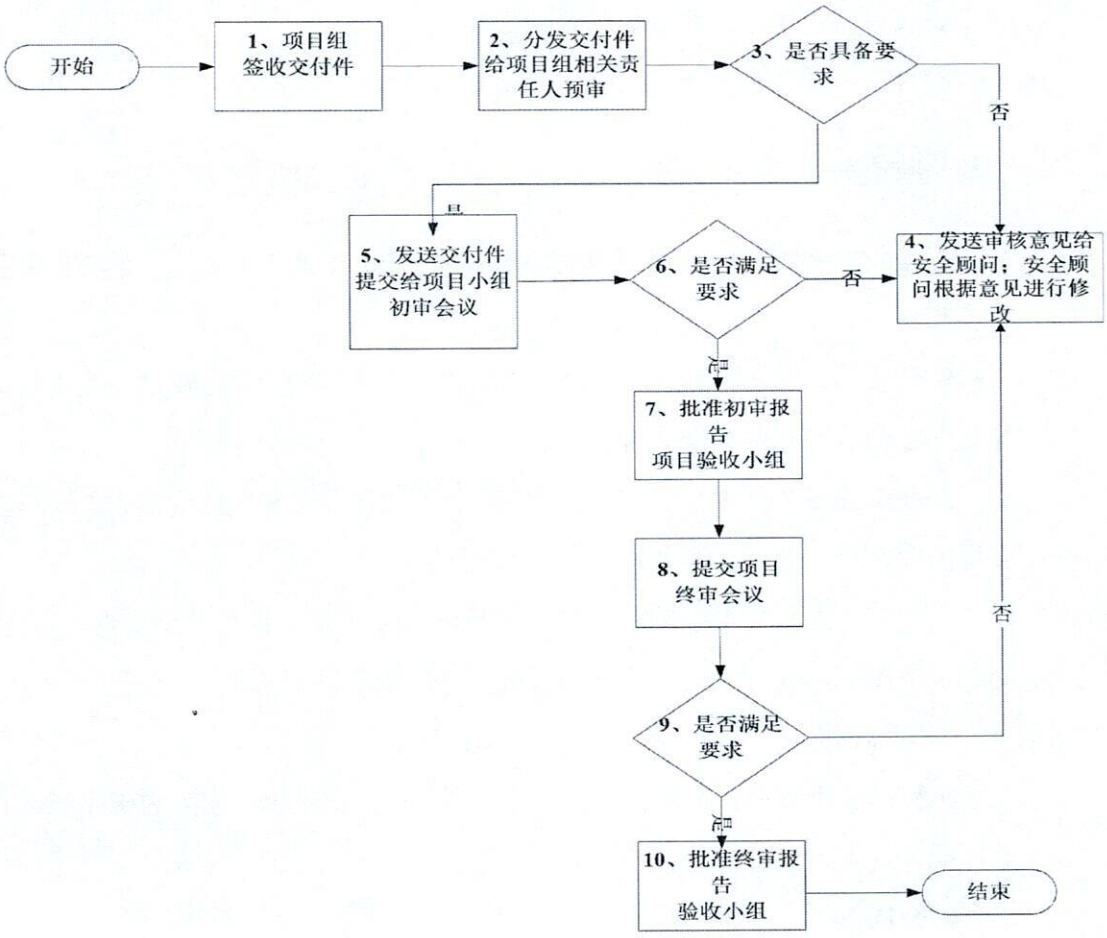
2、完成等保合规性测评及整改

3、通过等级测评

项目工作成果的评审

项目工作成果包括中间工作成果和最终提交物的工作成果，对工作成果的评审机制确保了中间工作成果和最终工作成果是满足项目预期要求的。项目工作成果的评审由项目的技术经理和甲方指定人员负责。评审结果是作为项目验收的依据之一。

交付件审视程序



图：天下信安安全服务验收程序

说明：

1、客户方项目组签收交付件

所有正式交付件在天下信安项目经理签字后，必须经过该流程提交给客户方项目组，并有客户方相关责任人进行签收。

2、把交付件分发给客户方相关责任人

交付件客户方责任人组织项目组相关人员、天下信安顾问及第三方专家审视该交付件，是否具备初审验收的条件。

3、交付件是否满足所有标准

依据双方签订的验收方法对交付件的审视，客户方交付件责任人评估是否满足初审验收的条件，并对双方的意见进行汇总和确认。

4、发送审视意见给顾问

客户方交付件责任人对交付件的问题和修改意见提交给顾问，并确定修改计划。

5、把交付件提交项目初审组会议

如果该交付件已满足初审要求，交付件客户方责任人应将该交付件提交给客户方项目验收小组，并组织初审组会议，审视交付件。

6、交付件是否满足要求

依据双方签订的验收方法对交付件的审视，客户方项目验收小组评估并确定是否满足验收方法，并对评审意见进行沟通并确认。

7、批准初审报告

项目经理签收和批准该交付件，并形成初审报告。

8、提交项目终审

项目初审后，客户方已经对报告进行了一定的消化和吸收，所有项目的输出提交项目终审。

9、交付件是否满足要求？

依据双方签订的验收方法对交付件的审视，客户方项目验收小组评估并确定是否满足验收方法，并对评审意见进行沟通并确认。

10、批准终审报告

客户方项目验收小组最终签收和批准该交付件，并形成终审报告。

文档管理

围绕本项目所产生的计划、设计方案、实施记录、项目会议记录、沟通记录和备忘录，本项目所接触到由甲方提供的资料等都属于本项目文档管理的范围。

由甲方提供文档管理服务器来集中管理文档，该文档服务器的管理由甲方负责，文档内容的管理由乙方项目组的文档工程师负责。

文档服务商的文档仅能够由项目组人员访问。非项目组人员不得直接访问，但可以向项目经理提出申请，项目经理批准后，由文档工程师转发。文档工程师需要在文档服务器上设置访问控制策略。

项目结束时，文档服务交易给甲方，甲方要取消乙方全部人员的访问权限。

在本安全项目的验收上，天下信安将和北京信息科技大学一起严格按照验收规范对项目进行验收。

安全服务类项目，目标是输出符合客户方实际的规划方案、安全策略，该项目将产生大量的文档，其中最重要的是项目的正式交付件(项目输出报告)，为有效管理这些交付件的制作、审核和归档，特制定本验收办法。

该验收办法的基本目的是：

确定所有项目正式交付件的验收方法

建立一个标准的、结构化的交付件审视办法（程序）

降低因为缺乏有效的沟通所带来的风险

降低交付件不能满足客户方信息安全实际需要的风险

本验收办法不涉及项目之外之后的交付件管理。

附件三　投标文件中所有承诺及招标文件服务要求

招标文件提出实质要求和条件响应函

北京天下信安技术有限公司对改善办学保障条件-北京信息科技大学新校区图书馆楼数字档案馆管理平台项目投标文件所提供的有关资格证明文件、商务技术证明文件，提交的投标保证金、技术规范、合同条款等与招标文件要求的其他条款、条件和规格相符，并且没有重大偏差。

可以交货日期：2024 年 10 月 30 日前按照等保二级要求，完成等保安全测评定级、测评和备案，并出具测评报告

投标人名称（盖章）：北京天下信安技术有限公司

日期：2024 年　　月　　日

服务承诺

北京天下信安技术有限公司作为公安部认证的网络安全等级测评与检测评估服务认证机构，常年为各大部委、中央客户及全国性信息系统提供等级保护及安全服务的单位，针对本次项目的承诺如下：

1.我方承诺，本项目达到国家网络安全等级保护标准的相关要求，并顺利通过测评。

2.我方承诺，在项目实施开始后不更换项目组主要成员，保证安全服务人员的稳定。

3.我方承诺，制定完善、切实可行的项目管理制度和规范，确定各项安全服务的标准流程和相关岗位设置等，使安全服务人员在制度和规范的约束下进行工作。

4.我方承诺，建立统一的项目管理体系，提高运行维护工作的效率。

5.我方承诺，遵守北京信息科技大学相关制度，安全服务人员作息时间等将与北京信息科技大学一致。

6.我方承诺，本项目所列各项国家标准和国际标准若在项目执行期间发布新版本，我方将根据国家相关规定及北京信息科技大学要求执行。

7.我方承诺，按照招标内容完成全部工作内容。我方承诺认真组织、精心部署、严格执行招标文件中所规定的以及与本工程有关的各项技术规范、标准，保证达到贵方规定的质量标准，并按期完成项目服务内容。

投标人名称（盖章）：北京天下信安技术有限公司

日期：2024年　　月　　日

保密承诺

北京天下信安技术有限公司针对本次项目，在保密方面承诺如下：

一、组织保密：

1.我方承诺，对北京信息科技大学提供的各种技术文件（软件、咨询报告、服务内容）与工作业务信息进行保密，未经北京信息科技大学书面批准不提供给第三方。如有违反，我方愿承担相应的法律责任。此保密义务不因合同的终止而免除。

2. 我方承诺，我方将与北京信息科技大学签订《安全保密协议》。如有违反，我方将承担全部责任并赔偿北京信息科技大学的一切损失，北京信息科技大学有权追究我方的法律责任并终止合同。

3. 我方承诺，遵守北京信息科技大学的各项规章制度，严格按照工作规范组织安全服务工作，制定切实可行的措施保障人员安全，设备安全，生产安全。

4. 我方承诺，制定合理的措施对服务人员进行管理和思想教育，加强保密意识，安全生产意识。

二、人员保密：

我方承诺，将负责所有参与本次项目服务的员工与北京信息科技大学、供应商签订三方保密协议，如有违反，我方将承担全部责任并赔偿北京信息科技大学的一切损失，北京信息科技大学有权追究供应商的法律责任并终止合同。

投标人名称（盖章）：北京天下信安技术有限公司

日期：2024年　　月　　日

附件四　中标通知书

中 标 通 知 书

项目名称：改善办学保障条件-北京信息科技大学新校区图书馆楼数字档案馆管理平台项目（新竣工楼配套）

项目编号：BMCC-ZC23-0943/1

03包：等保测评费

中 标 人：北京天下信安技术有限公司

中标金额：98,200.00　　元

请接到此通知书后尽快与采购人联系合同签约事宜，合同签订后2个工作日内，请将合同扫描件发送到bjmdzx@vip.163.com邮箱办理相关备案及保证金退还手续，保证金将在合同签订的5个工作日内退回来款账户。

北京明德致信咨询有限公司

2024年05月22日

北京明德致信咨询有限公司

地址：北京市海淀区学院路30号科大天工大厦B座17层1709室

电话：韩伯阳、杜畅、周经理、吕绍山，010－61192278

附件五：授权委托书

授权委托书

本人 高淑华（姓名）系 北京天下信安技术有限公司（投标人名称）的法定代表人（单位负责人），现委托 晁佳 （姓名）为我方代理人。代理人根据授权，以我方名义处理改善办学保障条件-北京信息科技大学新校区图书馆楼数字档案馆管理平台项目（新竣工楼配套）（项目名称）合同履行有关事宜，其法律后果由我方承担。

委托期限：自本授权委托书签署之日起至合同履行期届满之日止。

代理人无转委托权。

投标人名称（加盖公章）：北京天下信安技术有限公司

法定代表人（单位负责人）（签字、签章或印鉴）：高淑华

委托代理人（签字/签章）：晁佳

通讯地址：北京市大兴区欣雅街 15 号院 1 号楼 10 层 1008

固话及手机： 18831640920

日期： 2024 年 月 日

法定代表人（单位负责人）有效期内的身份证正反面扫描件：

委托代理人有效期内的身份证**正反面**扫描件：

附件六　被授权人近三个月缴纳社保证明

北京市社会保险个人权益记录(单位职工缴费信息)

社会保险登记号:91110105MA004KAB71　　校验码: 3tj4cy

统一社会信用代码(组织机构代码):91110105MA004KAB71　　查询流水号: 110115202405231115O9

单位名称:北京天下信安技术有限公司　　查询日期: 2024年02月至2024年04月

序号	姓名	社会保障号码	险种	缴费情况		本单位实际缴费月数
				起始年月	截止年月	
1	晁佳	132825199807012022	养老保险	2024年02月	2024年04月	3
			失业保险	2024年02月	2024年04月	3
			工伤保险	2024年02月	2024年04月	3
			医疗保险	2024年02月	2024年04月	3
			生育保险	2024年02月	2024年04月	3

备注:
1.如需鉴定真伪，请30日内通过登录 http://fuwu.rsj.beijing.gov.cn/bjdbhy/ggfw/，进入“社保权益单校验”，录入校验码和查询流水号进行甄别，黑色与红色印章效力相同。
2.为保证信息安全，请妥善保管个人权益记录。
3.养老、工伤、失业保险相关数据来源于社保经办机构，医疗、生育保险相关数据来源于医保经办机构。

北京市大兴区社会保险事业管理中心

日期:2024年05月23日

第1页　(共1页)