智慧园区

网络安全等保/密评/分保工作方案

XXX科技有限公司

2023 年 XX月 XX日

目　录

一 项目依据

1.1 实施依据

在本次项目中，我方项目组将依据国家等级保护相关标准开展工作，依据标准包括但不限于如下国家标准：

□《信息安全等级保护管理办法》（公通字[2007]43 号）；

□GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》；

□GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》；

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

□GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》；

□适用于被测评方的行业法律法规；

□其他相关法律法规要求。

1.2 实施原则

根据对业主的需求分析,在整个项目的设计与实施过程中将严格遵循国家关于信息安全等级保护测评的相关标准。同时遵循如下原则：保密性、可用性、安全性、规范性。

1)规范性

在本项目的设计与实施过程中，我方项目组将保证相关工作的规范性。测评工作将严格符合国家等级保护相关标准要求，同时符合电力行业等级保护的相关行业标准，以期能够交付一个合规、合理的优质项目。

2)保密性

对业主敏感信息保密非工作常重视，业主敏感信息视为最重要商业机密，针对本项目将实施相应的保密措施以保证业主相关敏感信息。

3)可用性

对测评过程中出具的相关建设报告中所提出的整改措施力求切实可用，对于目前网络安全领域不能实现的技术手段或因业主行业特殊原因无法实现的整改措施应进行相关说明，保证所提出的整改建议具有可用性。

4)安全性

为保证本项目的实施过程中不影响原业务系统的可用性、实时性,应在进行工具测试等环节与业主进行充分沟通,在业主许可及技术准备充分的前提下进行相关测评以保证本项目实施过程的安全性,若业主不同意进行工具测试,项目组需与业主签署《自愿放弃工具测试声明》，由业主方签字并盖章。

1.3 实施步骤

1)系统定级备案

重要信息系统的定级备案工作,是开展等级保护的首要环节,是进行信息系统建设、整改、测评、备案、监督检查等后续工作的前提。

2)差距分析

差距分析工作内容就是根据网络和信息系统的安全保护等级，根据国家等级保护相应等级的技术和管理要求,分析评价网络和信息系统当前的安全防护水平和措施与相应等级要求之间的差距。

3)等保建设整改

等级保护建设整改是根据信息系统差距分析结果，对信息系统所依赖的服务器操作系统、数据库、网络及安全设备进行配置安全加固，安装和实施各项新增安全设备，保障信息系统的安全稳定性。

4)等保管理制度建设

等级保护管理制度建设是根据信息安全等级保护安全管理的要求，编写符合等级保护要求的信息安全管理规范和制度,通过安全管理的加强来规避管理风险。

二 定级备案

2.1 工作目的

协助客户完成安全等级保护的定级与备案。依据 GBT22240-2020 《信息安全技术 网络安全等级保护定级指南》,对未定级、备案信息系统进行梳理,完成信息系统安全等级保护的定级与备案工作。

2.2 工作方式

在定级咨询过程中，咨询顾问将通过现场调研的方式来全面了解主要信息系统的基本情况，如数量、类别、名称、承载业务、服务范围、用户数量、部署方式，以进行汇总分析，初步进行系统归类、重要性划分，为下一步确定定级对象、确定级别、形成定级报告做准备。

现场信息资料收集，以及对系统管理员进行访谈及信息确认，是现场调研的

主要工作。通过现场的了解，可以较深入理解信息系统的重要程度，重要信息的分类情况，以及用户分布情况。一般系统的定级结果，不依赖于现有保护措施，所以通过现场的工作，可以基本准确理解信息系统及承载重要信息的侵害客体以及侵害程度，从而为进一步定级报告的编写打下良好基础。

2.3 工作内容

1)协助定级

如果信息系统只承载一项业务，可以直接为该信息系统确定等级，不必划分业务子系统。如果信息系统承载多项业务，应根据各项业务的性质和特点，将信息系统分成若干业务子系统，分别为各业务子系统确定安全保护等级，信息系统的安全保护等级由各业务子系统的最高等级决定。信息系统是进行等级确定和等级保护管理的最终对象。

现场调研后，咨询顾问会准备《信息系统安全等级保护定级报告模板》，给出定级报告示例。信息管理部门和业务部门依据定级报告模板，起草各信息系统安全等级保护定级报告，咨询顾问根据已经掌握的信息系统情况，对各信息系统定级报告的合理性进行初步研究和审核把关，请相关单位派人共同讨论，按照系统类别梳理定级报告，对照国家对不同等级的要求，在报告内容、行文格式、定级准确性等方面给出修改意见。根据讨论的定级报告修改意见，统一汇总、整理后，形成定级报告的专家评审稿。

2)专家评审

咨询顾问还将根据需要协助聘请等级保护专家、行业专家、主管机关领导等外部专家，召开信息系统定级评审会，对定级报告进行外部评审，形成评审意见。

咨询顾问将参考专家定级评审意见，最终协助确定信息系统等级，协助将各信息系统安全保护等级定级报告报经上级主管部门审批同意。

最后，咨询顾问将协助填写《信息系统安全等级保护备案表》，若经过专家评审目标系统为第三级，还需要提供协助客户提供《系统拓扑结构及说明》、《系统安全组织机构及管理制度》、《系统安全保护设施设计实施方案或改建实施方案》、《系统使用的安全产品清单及认证、销售许可证明》。并由咨询顾问在对

接当地公安局网安支队时提供必要的支持，了解当地公安政策，依据当地条例住准备定级资料，最终完成目标系统备案工作。

2.4 提交成果

《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》

《专家评审意见》

《系统拓扑结构及说明》（三级系统提交）

《系统安全组织机构及管理制度》（三级系统提交）

《系统安全保护设施设计实施方案或改建实施方案》（三级系统提交）

《系统使用的安全产品清单及认证、销售许可证明》（三级系统提交）

2.5 输出成果

公安局网安部门发放的《XX信息系统备案证明》

三 差距分析

根据国家等级保护政策法规和标准规范，确定安全保护等级的信息系统应该具有相应级别的安全防护能力，其中主要是根据 GBT22239-2019《网络安全技术网络安全等级保护基本要求》来分析承载于互联网和综合安防网上的业务应用系统目前的安全防护能力与基本要求中相应级别之间的差距。

3.1 工作目的

根据国家等级保护要求，对于确定了安全保护等级的信息系统规定了基本的安全保护要求，规定了应该具有的防护措施，以确保信息系统具有相当水平的安全防护能力。

差距分析就是根据 GBT22239-2019《网络安全技术网络安全等级保护基本要求》，结合本项目的业务情况和行业要求，从安全技术和安全管理两个方面，全

面分析信息系统现有防护措施和能力与相应等级基本要求之间存在的差距,用以为等级保护建设提供客观依据并指导信息系统等级保护体系设计。

3.2 工作方式

业务系统差距分析工作计划通过以下方式进行。

1)访谈

访谈是指评估人员与信息系统有关人员就差距分析所关注的问题进行有针对性的询问和交流的过程,该过程可以帮助评估者了解现状、澄清疑问或获得证据。

访谈深度(即访谈内容的详细程度)以及访谈的广度(即对被评估组织中员工角色类型以及每种类型中人数的覆盖程度)由评估人员依据不同的评估需要进行选择和判断。

2)检查

检查是指对评估对象（如规范、机制或行为）进行观察、调查、评审、分析或核查的过程。与访谈类似，该过程可以帮助评估者了解现状、澄清疑问或获得证据。

比较典型的检查行为包括：对安全配置的核查、对安全策略的分析和评审等。

3)测试

测试是指在特定环境中运行一个或多个评估对象(限于机制或行为)并将实际结果与预期结果进行比较的过程。测试的目标是判定对象是否符合预定的一组规格。测试过程可以帮助评估者获得证据。

4)调查表

根据系统业务情况和系统现状，制定详细的调查表，并由相关人员进行填写,以获得业务系统基础数据。具体包括应用信息系统调查表、物理资产调查表、软件资产调查表、各相关设备资产调查表。

按照等级保护实施要求，不同安全等级的信息系统应该具备相应等级的安全防护能力，部署相应的安全设备，制定相应的安全管理机构、制度、岗位等。差距分析就是依据等级保护技术标准和管理规范,比较分析信息系统安全防护能力与等级要求之间的差距，为等级化体系设计提供依据。

3.4 提交成果

差距分析过程中将产生众多文档,其中包括过程文档和结果文档,过程文档用以支持咨询人员进行差距分析，并形成结果文档《等级保护差距分析报告》。

信息系统等级保护差距分析报告主要内容：差距分析是以现场调查和测试所收集的信息为依据,满足等级保护要求为目标,对现有系统安全做出的一种客观的、真实的评价。报告内容包括对各信息系统现有安全防护水平与相应等级之间差距的描述和整改建议等。差距分析是制定信息系统安全等级保护体系设计方案前的一个非常关键的环节,为信息系统安全等级保护体系设计方案的撰写提供参考。

四 等保建设整改

4.1 工作目的

根据前期等级保护整改、差距分析结果，结合项目的业务需求，对信息系统的服务器、网络设备、安全设备、数据库进行安全策略加强、调优等，加强网络、系统和设备抵御攻击和威胁的能力，整体提高网络安全防护水平。

4.2 工作方式

安全加固与优化将采用如下工作方式：

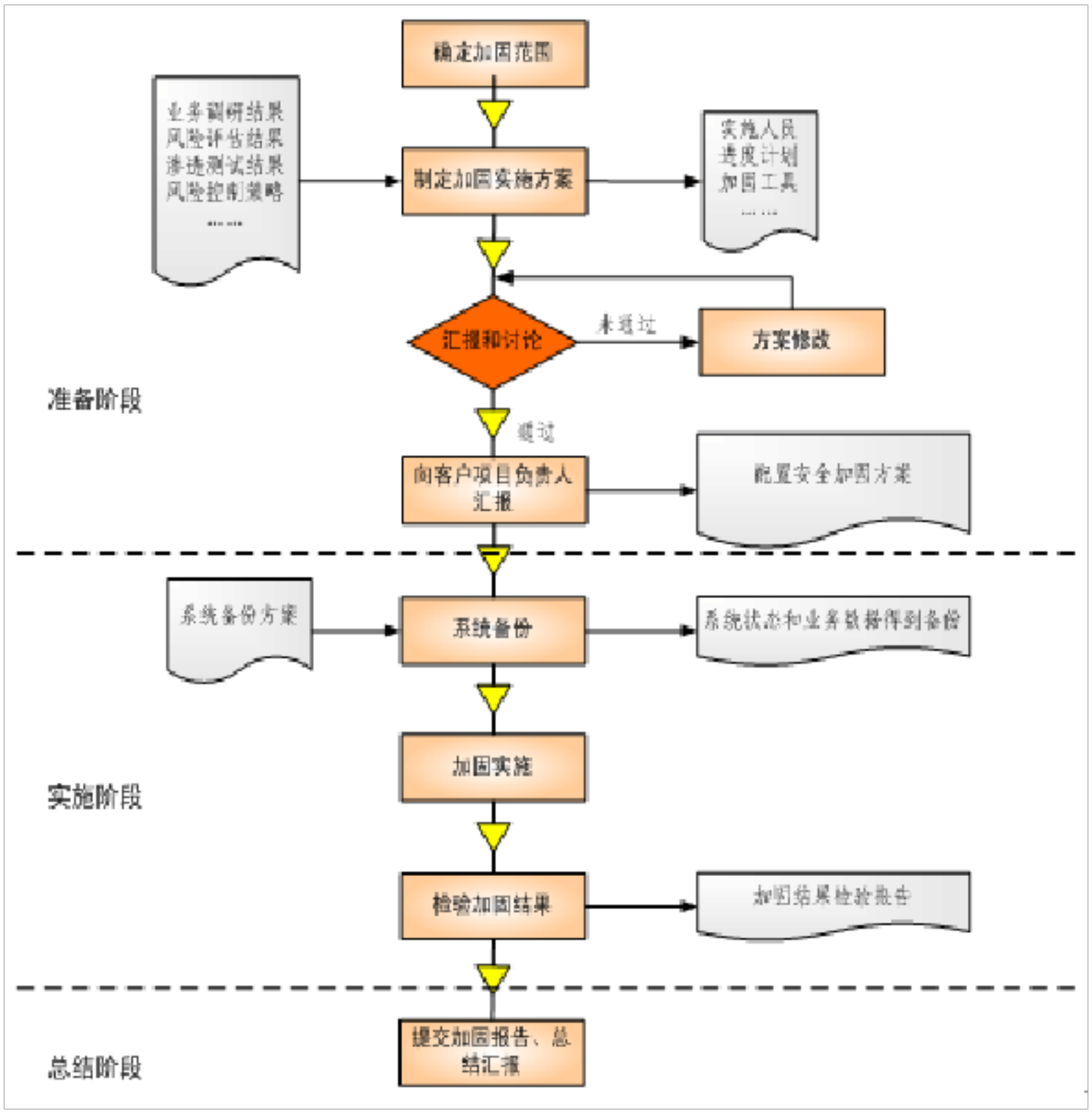
会议交流：项目组将根据脆弱性检测结果，提出安全加固与优化建议，并通

与相关负责人就每台主机、网络与安全设备的具体加固内容进行协商，明确操作风险，探讨利害关系，确定加固方式，最终确定安全加固方案；

现场实施：项目组将赴现场，以安全加固方案为依据，协助和指导系统运维人员进行加固与优化操作，逐项实施每台设备的安全加固项目。

工作流程

系统相关网络设备、安全设备、服务器操作系统以及数据库等配置安全加固与优化的工作流程如下图所示：



配置加固流程描述如下（项目实施中，可以根据实际情况需要，对流程进行调整、合并和展开等）：

制定加固实施方案：确定实施人员、加固工具、进度计划等，为实施提供指导；

向项目负责人汇报：就配置加固实施方案向项目负责人汇报，并得到同意；

系统备份：对配置加固涉及的系统和数据进行备份；

加固实施：根据配置加固实施方案进行加固实施；

检验加固结果：验证配置加固的有效性；

提交加固报告、总结汇报：总结配置加固实施情况，并进行汇报。

提交成果

《系统安全扫描人工分析报告》、《安全配置检查和加固建议报告》、《系统主机设备加固报告》、《网络设备加固实施报告》。

通过对系统相关主机、网络与安全设备配置的加固与优化，将会减少安全漏洞和设备配置策略的不合理性，提高系统抗攻击的能力，从而可有效防范攻击、限制危害蔓延，充分发挥各项安全措施的作用，增强系统的安全性和稳定性。

五 等级保护管理制度建设

5.1 工作目的

以等级保护差距分析结果为依据，依照安全保障体系设计所提及的建设内容，按照等级保护标准要求，制定等级保护管理体系框架，明确管理方针、策略，以及相应的规定、操作规程、业务流程和记录表单；从贴合业务流程的原则出发，指导系统运维方按照等级保护三级系统的管理标准，编写管理制度文件，并进行反复沟通和修订，确保所制定的文件的适用性，且满足各系统相应保护等级的安全管理要求。通过制定和完善管理制度，明确责任权力，规范操作，加强对人员、设备和业务系统的管理，完备应急响应机制，将显著提升信息安全管理水平，有效控制信息系统所面临的安全风险，从而确保业务系统的安全、稳定运行。