一闸三线信息化系统

网络安全技术咨询服务方案

1　项目背景分析

随着信息技术的快速发展和网络安全形势的日益严峻，保障关键信息基础设施的安全已成为国家和社会的重要任务。福建省平潭及闽江口水资源配置（一闸三线）工程作为区域水资源调配的关键项目，其信息化系统的稳定性与安全性直接关系到水资源调度的效率与安全，对区域经济社会发展具有重大意义。一闸三线信息化系统安全体系根据等级保护《GB/T 22239-2019 网络安全等级保护基本要求》，参照等级保护三级进行建设；省等保专家对信息化系统网络安全等级定级评审为第三级。依据国家相关法律法规要求，每年对该工程信息化系统需进行三级等保复评，确保系统持续高效运行、防范安全风险的关键措施。

本项目以福建省平潭及闽江口水资源配置(一闸三线)工程信息化系统网络安全等级保护复评为主线，以让信息化系统网络安全等级保护达到第三级要求。借助网络产品、安全产品、安全服务、管理制度等手段，建立全网的安全防控管理服务体系，从而全面提高一闸三线工程信息化系统的安全防护能力。

2　现状分析

福建省平潭及闽江口水资源配置(一闸三线)工程信息化系统是工业控制系统，系统部署运行于永泰莒口调度中心，系统主要实现水库、河道、泵站水务调度等功能，存储有泵站监控、闸门监控、水情监测、水质监测、鱼道信息、管道监测、隧洞安全监测及视频监控等信息数据。

2.1 待测评系统资产

2.1.1 机房

序号	机房名称	物理位置	重要程度	备注
1	主机房	福建省福州市永泰县塘前乡莒口调度中心	关键	1 间
2	备机房	福建省福州市鼓楼区东街 104 号榕水大厦	关键	1 间

2.1.2 网络设备

序	设备名称	是否虚	系统及版	品牌及型号	用途	重要	备注

号		拟设备	本			程度	
1	控制区核心交换机-主	否	5.170	华为 S5731S-AH24T4XC-A	控制区数据核心交换	关键	设备数量：1
2	控制区核心交换机-备	否	5.170	华为 S5731S-AH24T4XC-A	控制区数据核心交换	关键	设备数量：1
3	管理区核心交换机-主	否	5.170	华为 S5731S-AH24T4XC-A	控制区数据核心交换	关键	设备数量：1
4	管理区核心交换机-备	否	5.170	华为 S5731S-AH24T4XC-A	控制区数据核心交换	关键	设备数量：1
5	大顶山隧洞出口映翰通路由器	否	V1.0.0.r 20029	映翰通 IR915L	数据路由交换	一般	设备数量：1
6	高铁大桥映翰通路由器	否	V1.0.0.r 20029	映翰通 IR915L	数据路由交换	一般	设备数量：1
7	林洋支洞映翰通路由器	否	V1.0.0.r 20012	映翰通 IR915L	数据路由交换	一般	设备数量：1
8	岭斗支洞出口映翰通路由器	否	V1.0.0.r 20030	映翰通 IR915L	数据路由交换	一般	设备数量：1
9	岭脚支洞出口映翰通路申器	否	V1.0.0.r 20029	映翰通 IR915L	数据路由交换	一般	设备X数量：1
10	龙醒隧洞权出口映翰通路由器	否	V1.0.0.r 20029	映翰通 IR915L	数据路由交换	一般	设备数量：1
11	十八重溪隧洞出洞口映翰通路由	否	V1.0.0.r 20029	映翰通 IR915L	数据路由交换	一般	设备数量：1
12	石溪隧洞出洞口映翰通路由器	否	V1.0.0.r 20012	映翰通 IR915L	数据路由交换	一般	设备数量：1
13	石溪隧洞	否	V1.0.0.r	映翰通	数据路由	一般	设备

	进洞口映翰通路由器		20029	IR915L	交换		数量：1
14	炎山泵站映翰通路由器	否	V1.0.0.r20012	映翰通 IR915L	数据路由交换	一般	设备数量：1

2.1.3 安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	控制区堡垒机	否	v3.2294.30115_SAG.1	天融信 TopSAGNSAG-41108	运维管理	关键	设备数量：1
2	正向隔离网闸	否	V3	天融信 TIG-72218-R8	物理隔离	关键	设备数量 ：1
3	反向隔离网	否	V3	天融信 TIG-72218-R8	物理隔离	关键	没备数量：1
4	控制区防火墙	否	3.3.020.085F1	天融信 NGFW4000-UF	区域隔	关键	设备数量：1
5	控制区日志审计系统	否	V3.3.3Liunx	天融信 TA-LHSE-B50	日志收集分析	关键	设备数量：1
6	控制区数据库审计系统	否	V3	天融信 TA-55529-DB	数据库数据收集分析	关键	设备数量：1
7	控制区态势感知	否	V3.1125	天融信 TopSA	安全基线检查	关键	设备数量：1
8	控制区纵向加密-莒口区	不	33.010.016.1	天融信 SJJ1995-42606	数据加密	关键	设备数量1
9	控制区纵向加密-竹歧区	否	33.010.016.1	天融信 SJJ1995-42606	数据解密	关键	设备数量：1
10	控制区纵向解密-莒口区	否	33.010.016.1	天融信 SJJ1995-42606	数据加密	关键	设备数量：1
11	控制区纵向解密-竹歧	否	33.010.016.1	天融信 SJJ1995-42606	数据解密	关键	设备数量：

	区						1
12	天融信工控防火墙	否	V3	天融信 TIF-5112-NG	边界隔离	关键	设备数量：1
13	天融信终端防御 EDR	否	V1.0.2.2.14	天融信 TopEDR	终端防御	关键	设备数量：1
14	管理区 WEB 应用防火墙	否	3.2294.20128 WAF.1	天融信 TopWAF	web 应用防护	关键	设备数量：1
15	管理区堡矣机公	否	TopSAG(NSA G-41108)	天融信 TopSAG	运维管理	关键	设备数量：1
16	管理区出口防火墙	否	3.3.020085F.1	天融信 NGFW4000-UF	边界隔离	关键	设备数量：1
17	管理区边界防火墙-1	否	V3	天融信 NGFW4000-UF	。 区域间隔离	关键	设备数量：1
18	管理区边界防火墙-2	否	V3	天融信 GFW4000-UF	区域间隔离	关键	设备数量：1
19	管理区边界防火墙-3	否	V3	天融信 NGFW4000-UF	区域间隔离	关键	设备数量：1
20	管理区日志审计系统	否	V3.3.3Linux	天融信 TA-L-HSE-B50	日志收集分析	关键	设备数量 ：1
21	管理区态势感知	否	标准版	天融信 TopSA	安全基线检查	关键	设备数量：1
22	管理区终端防御 EDR	否	V1.0.2.2.14	天融信 TopEDR	终端防御	关键	设备数量：1
23	管理区准入控制系统	否	V3	天融信 TSM21128-TopNAC	准入控制	关键	设备数量：1

2.1.4 服务器/存储设备

序号	设备名称	所属业务应用系统/平台名称	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度	备注
1	BIMGIS 应用系统服务器	一闸三线工程信息化系统	是	AnolisOS 8.6	MySQL 5.7	/	关键	设备数量:1
2	POCP AFO_ AD_ Server 服务器	一闸三线工程信息化系统	是	Windows Server 2022		/	关键	设备数量:1
3	PCCP_ AFO_ Database 服务器	一闸三线工程信息化系统	是	Windows Server2022	SQL Server 16.0	/	关键	设备数量:1
4	PCCP_ AFO FTP-SERVER 服务器	一闸三线工程信息化系统	是	Windows Server 2022		/	关键	设备数量:1
5	PCCP_ AFO_ Keyclock-Server 服务器	一闸三线工程信息化系统	是	Windows Server 2022	/	/	关键	设备数量:1
6	PCCP_ AFO_ Web_ Server 服务器	一闸三线工程信息化系统	是	Windows Server 2022		/	关键	设备数量:1
7	PCCP_ AFO-Analys-Server 服务器	一闸三线工程信息化系统	是	Windows Server 2022	/	/	关键	设备数量:1
8	PCCP_ Mongo-Arbiter 服务器	一闸三线工程信息化系统	是	Ubuntu 20.04	Mongo DB 3.6.23	/	关键	设备数量:1
9	PCCP_ Mongo-Primai 服务器	一闸三线工程信息化系统	是	Ubuntu 20.04	Mongo DB 3.6.23	/	关键	设备数量:1
10	PCCP_ Mongo-Secondary 服务器	一闸三线工程信息化系统	是	Ubuntu 20.04	Mongo DB C 3.6.23	/	关键	设备数量:1
11	PCCP_ MySQL	一闸三线工程	是	Ubuntu	MySQL	/	关	设备

	服务器	信息化系统		20.04	5.7		键	数量:1
12	PCCP_ Visentl-API-service 服务器	一闸三线工程信息化系统	是	Ubuntu 20.04	/	/	关键	设备数量:1
13	PCCP_ Visentl-Detection_ Service 服务器	一闸三线工程信息化系统	是	Ubuntu 20.04	/		关键	设备数量:1
14	PCCP_ Visentl-ImporterService 服务器	一闸三线工程信息化系统	是	Ubuntu 20.04	/	/	关键	设备数量:1
15	PCCP_ Visentl-webserver 服务器	一闸三线工程信息化系统	是	Ubuntu 20.04	/	/	关键	设备数量:1
16	大坝安全监测服务器	一闸三线工程信息化系统	否	Windows Server 2012	SQL Server 11.0	/	关键	设备数量:1
17	管理区 FM_ TP 服务器	一闸三线工程信息化系统	是	Windows Server 2012		/	关键	设备数量:1
18	管理区 web 服务器	一闸三线工程信息化系统	是	凝思 6.0.80		Tomcat 9.0	关键	设备数量:1
19	管理区服务端服务器	一闸三线工程信息化系统	是	凝思 6.0.80		/	关键	设备数量:1
20	管理区接入服务器	一闸三线工程信息化系统	是	凝思 6.0.80	达梦 8		关键	设备数量:1
21	管理区数据库服务器	一闸三线工程信息化系统	是	凝思 6.0.80	达梦 8		关键	设备数量:1

22	管理区通讯服务器	一闸三线工程信息化系统	是	凝思6.0.80			关键	设备数量:1
23	管理区同步服务器	一闸三线工程信息化系统	是	凝思6.0.80			关键	设备数量:1
24	管理区应用服务器	一闸三线工程信息化系统	是	凝思6.0.80		/	关键	设备数量:1
25	管理区应用服务器2	一闸三线工程信息化系统	是	凝思6.0.80		/	关键	设备数量:1
26	海康流媒体服务器	一闸三线工程信息化系统	否	CentOS 7.6		/	关键	设备数量:1
27	控制区FM_ TP服务器	一闸三线工程信息化系统	是	Windows Server 2012		/	关键	设备数量:1
28	控制区Vsecurity服务器	一闸三线工程信息化系统	是	openEuler 22.03			关键	设备数量:1
29	控制区服务端服务器	一闸三线工程信息化系统	是	凝思6.0.80			关键	设备数量:1
30	控制区接入服务器	一闸三线工程信息化系统	是	凝思6.0.80	/	/	关键	设备数量:1
31	控制区数据库服务器	一闸三线工程信息化系统	是	凝思6.0.80	达梦8	/	关键	设备数量:1
32	控制区通镧机服务器	一闸三线工程信息化系统	是	凝思6.0.80		/	关键	设备数量:1
33	控制区同步服务器	一闸三线工程信息化系统	是	凝思6.0.80		/	关键	设备数量:1
34	控制区应用服务器1	一闸三线工程信息化系统	是	凝思6.0.80		/	关键	设备数量:1
35	控制区应用服务器2	一闸三线工程信息化系统	是	凝思6.0.80		/	关键	设备数量:1

36	数字水务管理系统服务器	一闸三线工程信息化系统	是	AnolisOS 8.6			关键	设备数量:1
37	隧洞安全监测服务器	一闸三线工程信息化系统	否	凝思 6.0.80	达梦 8	/	关键	设备数量:1
38	鱼道一期服务器	一闸三线工程信息化系统	否	Windows Server 2019	MySQL 8.0		关键	设备数量:1
39	鱼道二期服务器	一闸三线工程信息化系统	否	Ubuntu 20.04			关键	设备数量:1
40	备份一体机服务器	一闸三线工程信息化系统	否	Linux ics-backup 3.10			重要	设备数量:1

2.2 业务系统现状调研情况

1、福建省平潭及闽江口水资源配置(一闸三线)工程信息化系统共有 40 台服务器（应用服务器 30 台，数据库服务器 10 台），采用凝思、windowsever2006wdsevet 2022、ubuntu 20.04、阿里龙蜥操作系统，MySQL5.7、postgresql-11.2、MongoDB3.6 集群、SQL Server 2022、达梦 V8、MySQL8.0 数据库。

2、水务管理数据存储总量约为一亿五千万条，数据量大小约 110CB。

2.3 安全现状调研情况

1、福建省平潭及闽江口水资源配置(一闸三线)工程信息化系统横跨“控制区”、“管理区”和“外网区”，主要对控制区内的“现地层”泵站、闸站、水质站等进行监测和远程控制。

2、从网络架构来看，“控制区”各细分区域内均部署有“纵向加密装置”实现工业控制系统的安全访问控制。

3、管理区具有如下安全设备：防火墙、网闸、上网行为管理、准入控制系统、web 应用防护、SSL vpn、终端防护软件、堡垒机、威胁感知系统、日志审计、虚拟化安全防护。

4、控制区具有如下安全设备：纵向加密系统、堡垒机、威胁感知系统、日

志审计、数据库审计、虚拟化安全防护、工控安全卫士。

3 三级等保复评的必要性

1.法律法规遵循：根据《中华人民共和国网络安全法》及《信息安全技术 信息系统安全等级保护基本要求》等规定，三级等保系统需定期进行复评，以验证其是否持续满足相应安全保护要求，确保合法合规运营。

2.风险动态管理：信息技术日新月异，新的威胁和漏洞不断出现，年度复评有助于及时发现并应对这些变化，有效管理和降低安全风险。

3.系统优化升级：通过复评过程，可以评估现有安全措施的有效性，为系统的技术更新、策略调整提供依据，促进系统性能与安全性的双重提升。

4.应急响应准备：复评还包括对应急预案的审查，确保在面对突发安全事件时，系统能够迅速响应，最小化损失。

4 复评主要工作内容

1.安全现状评估：全面检查信息化系统的资产状况、安全配置、防护措施执行情况，对比上一次评测结果，识别安全状态的变化。

2.风险分析与评价：运用定量与定性相结合的方法，重新评估系统面临的安全风险，包括物理安全、网络安全、数据安全、应用安全等方面。

3.差距分析：对照国家三级等保标准，找出系统当前实施情况与标准要求之间的差距，明确改进方向。

4.整改建议制定：基于差距分析结果，提出具体的整改措施、优先级排序及实施计划，旨在消除安全隐患，增强系统抵御能力。

5.管理制度复审：审核现有的安全管理规章制度是否健全、有效，是否需要根据最新的法律法规或行业最佳实践进行调整。

6.报告编制与提交：整理复评过程中的所有发现、分析结果及建议，形成正式的复评报告，提交给相关部门审核，并根据反馈进行必要的调整。

5 等保差距分析服务

5.1 网络安全保护技术现状分析

针对三级业务系统的网络安全现状进行深度评估与三级等保标准差距分析，提供主机、数据、web 应用等维度等保差距分析，包含:目标系统漏洞扫描、渗

透测试(含 APP 应用端)，并出具等保差距分析报告，针对差距与问题指导、负责对接网络、安全、应用系统开发商对等保测评中所发现问题的整改，直至满足测评条件。

信息系统现状分析

首先得了解掌握信息系统的数量和等级、所处的网络区域以及信息系统所承载的业务应用情况，分析信息系统的边界、构成和相互关联情况，分析网络结构、内部区域、区域边界以及软、硬件资源等。具体可参照《网络安全等级保护实施指南》中“信息系统分析”的内容。

信息系统安全保护技术现状分析

在开展信息系统安全技术建设整改之前，应通过开展信息系统安全保护技术现状分析，查找信息系统安全保护技术建设整改需要解决的问题，明确信息系统安全保护技术建设整改的需求。

安全需求论证和确定

安全需求分析工作完成后，将信息系统的安全管理需求与安全技术需求综合形成安全需求报告，组织专家对安全需求进行评审论证。

5.2 网络安全建设整改方案设计

在安全需求分析的基础上，开展信息系统安全建设整改方案设计，包括总体设计和详细设计，制定工程预算和工程实施计划等，为后续安全建设整改工程实施提供依据。

1、确定安全技术策略，设计总体技术方案

1）确定安全技术策略

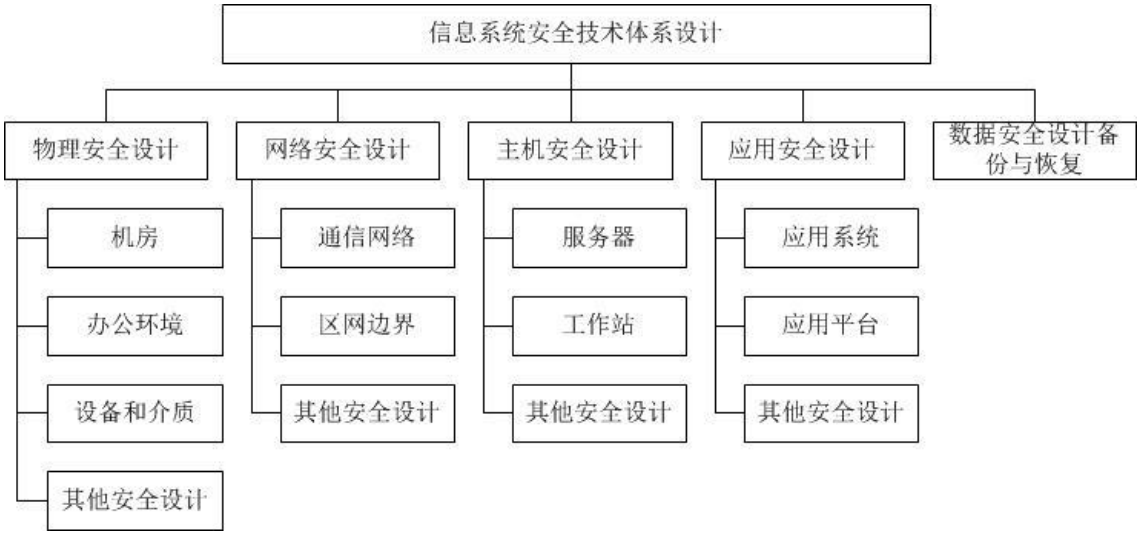
安全技术策略是基于安全需求分析形成的纲领性的安全文件，包括安全工作的总体原则，安全策略等。

2）设计总体技术方案

在进行信息系统安全建设整改技术方案设计时，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。

2、安全技术方案详细设计

信息系统安全技术体系如下图所示：



方案详细设计应包括以下方面：

1）安全物理环境设计

从安全技术设施和安全技术措施两方面对信息系统所涉及的主机房、辅助机房和办公环境等进行安全物理环境设计。

2）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、城域网络和其他通信网络（租用线路）等进行安全设计。

3）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。

4）安全计算环境

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。

5）应用系统安全设计

对信息系统涉及的应用系统软件（含应用/中间件平台）进行安全设计。

6）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。

5.3 部分整改措施说明

说明：下表为整改措施简单说明，在现场预测评工作结束后测评单位将出具详细的、可行的、务实的、有计划的、有针对性的整改建议报告。

序号	类别	整改项	测评单位提供信息	整改措施

1.	安全通信网络 安全区域边界	结构安全	Microsoft Visio、CAD 等软件，IP 地址划分建议	绘制符合要求的网络拓扑结构图，依此优化网络结构
2.		边界完整性检查	终端管理设备的品牌型号、技术需求、配置方法、设备大致价格等	部署终端管理设备
3.		入侵防范	IPS 或 IDS 设备的品牌型号、技术需求、配置方法、设备大致价格等	部署相关安全设备
4.		恶意代码防范	防病毒网关的品牌型号、技术需求、配置方法、设备大致价格等	部署相关安全设备
5.		访问控制	防火墙、核心交换机的配置方法，以文字配合图片的方式展现	优化设备的配置
6.		安全审计	安全审计设备的品牌型号、技术需求、配置方法、设备大致价格等	部署相关安全设备
7.		网络设备防护	网络设备的管理员的配置、权限划分等	配置实现网络设备管理的三权分立
8.	安全计算环境	身份鉴别	运维堡垒机的品牌型号、技术需求、配置方法、设备大致价格等，主机安全配置方法	配置实现 Windows、Linux 等主机的安全管理、双因子鉴别
9.		访问控制	服务器加固系统的品牌型号、技术需求、配置方法、大致价格等，主机安全配置方法	优化 Windows、Linux 等主机的用户权限划分
10.		安全审计	Windows 主机的详细配置步骤，提供 Linux、Aix 等主机的命令行，以文字配合图片的方式展现，安全审计系统相关信息，安全审计设备的品牌型号、技术需求、配置方法、设备大致价格等，主机安全配置方法	优化主机审计配置，部署安全审计设备
11.		剩余信息保护	Windows 主机的详细配置步骤，服务器加固系统的品牌型号、技术需求、配置方法、大致价格等，主机安全配置方法	优化主机相关配置，部署服务器加固系统
12.		入侵防范	主机版 IPS 的品牌版本、技术需求、配置方法、大致价格等	部署主机版 IPS

13.		恶意代码防范	网络版杀毒软件的品牌版本、技术需求、配置方法、大致价格等	部署网络版杀毒软件
14.		资源控制	SNMP 管理系统的品牌版本、技术需求、配置方法、大致价格等，Windows 主机的详细配置步骤，提供 Linux、Aix 等主机的命令行，以文字配合图片的方式展现，	建立 SNMP 管理系统，优化主机的配置
15.		应用软件安全	以标准化的软件开发流程形成的应用新需求报告	根据应用新需求报告进行二次开发
16.		数据完整性	常见的数据库 Oracle、DB2、MYSQL、Sybase、Microsoft、SQL、Server、Microsoft、Access 配置步骤	优化数据库的配置
17.		数据保密性	加密软件的品牌版本，SQL 命令	部署加密软件，优化配置，实现数据存储加密
18.		备份和恢复	数据备份软件的品牌版本、技术需求、配置方法、大致价格等，异地备份技术方案等	建立完善的数据备份的技术方案，建立异地备份系统
19.	安全管理中心	系统管理	提供人员岗位划分职责、制度	对人员岗位划分，并部署堡垒机限制登录方式
20.		审计管理	提供人员岗位划分职责、制度	对人员岗位划分，并部署堡垒机限制登录方式
21.		安全管理	提供人员岗位划分职责、制度	对人员岗位划分，并部署堡垒机限制登录方式
22.		集中管控	提供安全管理中品牌、版本、技术需求、配置方法、大致价格等	建立安全管理中心，对审计数据进行收集汇总和集中分析以及安全策略、恶意代码、补丁升级等安全相关事项进行集中管理
23.	安全管理制度	安全管理制度	提供一套全面的信息安全管理制度体系模板	建立全面的信息安全管理制度体系
24.		制定和发布	提供有关制度发布、制度收发文登记的相关表格	进行制度发布、制度收发文登记；负责对安全管理制度的制定和安全管理制度进行论证和审定

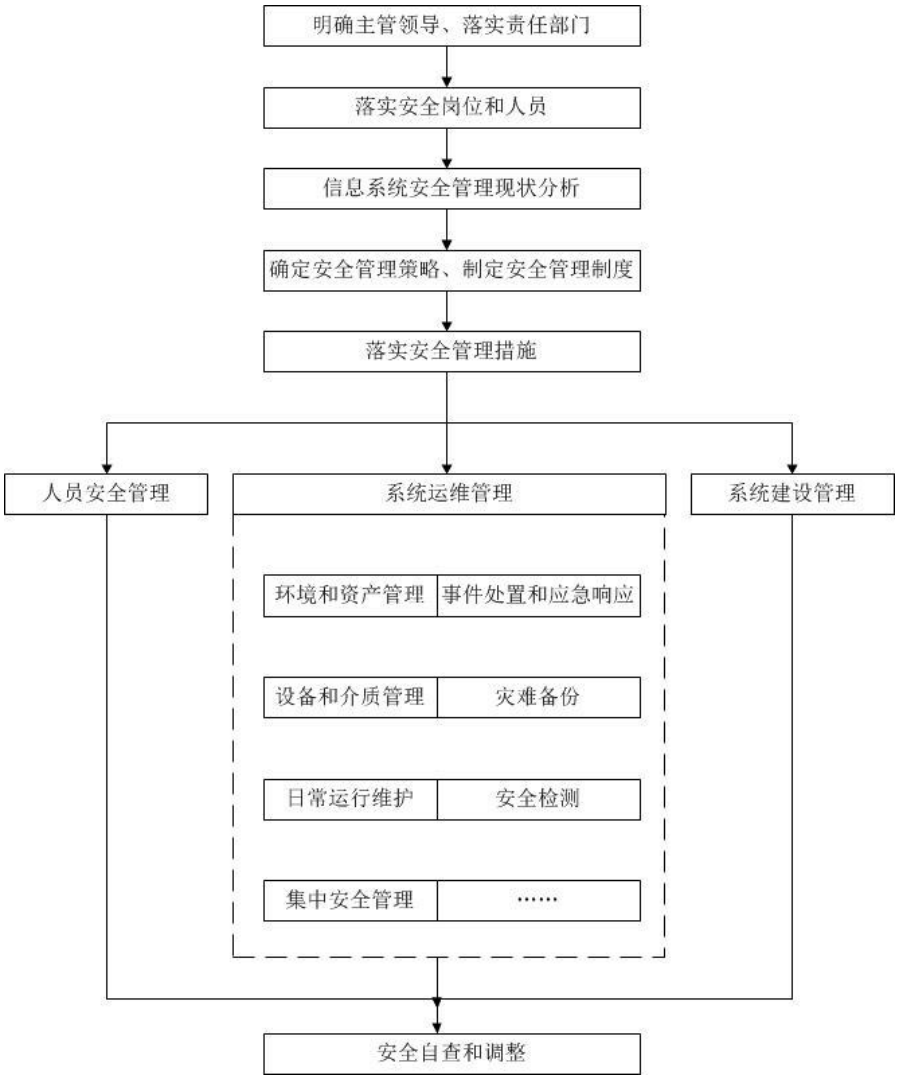
25.		评审和修订	提供相关审定表、检查表等。	对信息安全管理制度各项进行审定和检查；负责对信息安全领导小组对安全管理制度体系的合理性和适用性进行审定；对安全管理制度进行检查和修订
26.	安全管理机构	岗位设置	对安全管理机构中的岗位设置提出一些可行性建议	负责制定对各岗位职责和技能要求的说明
27.		人员配备	提供人员配备的合理化建议。	安全管理机构中配备人员合理
28.		授权和审批	提供关于各事项的审批程序以及逐级审批制度的模板。	负责制定逐级审批制度
29.		沟通与合作	提供外联列表模板以及部分外联单位	负责补全或制定外联列表
30.		审核和检查	提供安全审核和安全检查制度的模板；提供全方位的安全巡检服务	负责制定安全审核和安全检查相关制度；负责对安全管理制度的执行情况进行审核；进行全方位的安全巡检
31.	安全人员管理	人员录用	提供人员录用试题、保密协议、关键岗位安全协议的模板。	对录用人员进行考核；签署人员录用保密协议；签署关键岗位安全协议
32.		人员离岗	提供人员离岗安全承诺书的模板	人员离岗签署承诺书
33.		人员考核	提供相关安全知识和安全技能考核试题模板。	进行安全知识和安全技能考核
34.		安全意识教育和培训	提供对安全责任和惩戒措施、安全教育和培训书面规定的模板；提供安全意识教育和培训的相关课程及培训。	负责对安全责任和惩戒措施、安全教育和培训进行书面规定；进行安全意识教育和培训
35.		外部人员访问管理	提供对外部人员允许访问的区域、系统、设备、信息等内容书面规定的模板	负责对外部人员允许访问的区域、系统、设备、信息等内容进行书面规定
36.	安全建设管理	系统定级	提供系统定级咨询	负责进行系统定级工作，并配合对系统定级结果的合理性和正确性进行论证和审定

37.		安全方案设计	提供安全方案设计咨询；出具一份完整详细的信息安全规划，来指导网络安全测评之后的工作。	制定安全方案设计
38.		产品采购和使用	提供长期网络安全测评工作形成的相关产品的详细统计表	对产品进行选型
39.		自行软件开发	提供软件开发管理制度、代码编写安全规范的模板	负责对软件开发管理制度、代码编写安全规范进行补全或制定
40.		外包软件开发	提供检测的方法	负责对软件安装之前进行检测，对软件中可能存在的后门进行审查
41.		工程实施	提供包含工程实施过程的方法和人员行为准则的工程实施管理制度的模板	负责对包含工程实施过程的方法和人员行为准则的工程实施管理制度进行补全或制定
42.		测试验收	---	---
43.		系统交付	---	---
44.		系统备案	提供系统备案咨询	负责完成系统备案的工作
45.		等级测评	进行等级测评	---
46.		安全服务提供商	提供安全服务提供商列表	选择符合自己的安全服务提供商
47.	安全运维管理	环境管理	提供机房安全管理制度的模板；提供了对机房配电、空调、温湿度控制等维护的记录表格	负责对机房安全管理制度进行补充或制定；对机房配电、空调、温湿度控制等维护进行记录
48.		资产管理	提供资产安全管理制度的模板；提供资产清单表的模板。	负责对资产安全管理制度进行补充或制定；建立详细的资产清单表
49.		介质管理	提供介质安全管理制度的模板；提供包括介质归档和查询登记表、存档介质定期盘点记录表、送出维修或销毁的审批表等模板	负责对介质安全管理制度进行补充或制定；对介质归档和查询进行登记；定期盘点登记；送出维修、销毁登记
50.		设备管理	提供设备安全管理制度的模板	负责对设备安全管理制度进行补充或制定

51.		监控管理和安全管理中心	提供对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警的记录表模板	对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警并记录
52.		网络安全管理	提供网络安全管理制度的模板；测评单位还可以配合协助实现设备的最小服务配置；提供定期的漏洞扫描。	负责对网络安全管理制度进行补充或制定；实现最小服务配置；定期漏扫
53.		系统安全管理	提供系统安全管理制度的模板	负责对系统安全管理制度进行补充或制定
54.		恶意代码防范管理	提供恶意代码防范管理规定模板；配合协助进行恶意代码检测	负责对恶意代码防范管理规定进行补全和制定；对恶意代码进行检测
55.		密码管理	提供密码管理制度模板	负责对密码管理制度进行不全与制定
56.		变更管理	提供变更安全管理制度的模板；提供变更申报和审批文件、变更影响分析文档、实施过程记录、过程控制方法和人员职责文件的模板	负责对变更安全管理制度进行补充或制定；变更进行审批；变更进行影响分析；变更实施过程进行记录；变更过程控制方法和人员职责进行规定
57.		备份与恢复管理	提供备份与恢复管理制度模板；提供数据备份过程记录表、定期恢复的记录表的模板。	负责对备份与恢复管理制度进行补充或制定；对数据备份和恢复过程进行记录
58.		安全事件处理	提供安全事件处理管理制度模板	负责对安全事件处理管理制度进行补充或制定

5.4 制度建设

按照国家有关规定，依据《基本要求》，参照《信息系统安全管理要求》等标准规范要求，开展网络安全等级保护安全管理制度建设工作。工作流程如下图所示：



5.4.1 落实信息安全责任制

明确领导机构和责任部门，设立或明确信息安全领导机构，明确主管领导，落实责任部门。建立岗位和人员管理制度，根据职责分工，分别设置安全管理机构和岗位，明确每个岗位的职责与任务，落实安全管理责任制。建立安全教育和培训制度，对信息系统运维人员、管理人员、使用人员等定期进行培训和考核，提高相关人员的安全意识和操作水平。

5.4.2 信息系统安全管理现状分析

在开展信息系统安全管理建设整改之前，通过开展信息系统安全管理现状分析，查找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

设整改的需求。

对安全管理建设整改需求进行评审论证，该项工作可与安全技术建设整改需求论证工作一并进行。

5.4.3 制定安全管理策略和制度

根据安全管理需求，确定安全管理目标和安全策略，针对信息系统的各类管理活动，制定人员安全管理制度，明确人员录用、离岗、考核、教育培训等管理内容；制定系统建设管理制度，明确系统定级备案、方案设计、产品采购使用、密码使用、软件开发、工程实施、验收交付、等级测评、安全服务等管理内容；制定系统运维管理制度，明确机房环境安全、存储介质安全、设备设施安全、安全监控、网络安全、系统安全、恶意代码防范、密码防护、备份与恢复、事件处置、应急预案等管理内容；制定定期检查制度，明确检查的内容、方式、要求等，检查各项制度、措施的落实情况，并不断完善。

5.4.4 落实安全措施

人员安全管理

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。规范人员录用、离岗、过程。关键岗位签署保密协议，对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，对关键岗位的人员进行全面、严格的安全审查和技能考核。

系统运维管理

(1) 环境和资产安全管理

明确环境和资产安全管理的责任部门或责任人，加强对人员出入、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。

(2) 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、维护和维修等过程进行控制，对介质的存放、使用、维护和销毁等方面做出规定。

(3) 日常运行维护

明确网络、系统日常运行维护的责任部门或责任人，对运行管理中的日常操作、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。

(4) 集中安全管理

第三级（含）以上信息系统应按照统一的安全策略、安全管理要求，统一管理信息系统的安全运行，进行安全机制的配置与管理。

(5) 事件处置和应急响应

按照国家有关标准规定，确定信息安全事件的等级。结合信息系统安全保护等级，制定信息安全事件分级应急处置预案，明确应急处置策略，落实应急指挥部门、执行部门和技术支撑部门、建立应急协调机制。

(6) 灾难备份

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，制定数据的备份策略和恢复策略。

(7) 实时监测

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、用户行为和业务应用等的监测和报警。

(8) 其他安全管理

对系统运行维护过程中的其他活动，如系统变更、密码使用等进行控制和管理。按照国家密码管理部门的规定，对信息系统中密码算法和密钥的使用进行分级管理。

系统建设管理

系统建设管理重点是与系统建设活动相关的过程管理，由于主要的建设活动是由服务方，如集成方、开发方等完成，运营使用单位人员的主要工作是对之进行管理，应制定系统建设相关的管理制度，明确系统定级备案、方案设计、产品采购使用、工程实施、验收交付、等级测评、安全服务等内容的管理责任部门。

5.4.5 安全自查与调整

制定安全检查制度，明确检查的内容、方式、要求等，检查各项制度、措施

的落实情况，并不断完善。定期对信息系统安全状况进行自查，第三级信息系统每年自查一次。经自查，信息系统安全状况未达到安全保护等级要求的，应当进一步开展整改。

6　等保三级测评服务

6.1 等级保护测评工作

6.1.1 概述

6.1.1.1等级保护测评原则

为了提高本次项目实施专业性和分析过程客观、公正，本次信息系统等级保护测评服务项目实施将遵循以下原则：

可重复性原则:依照同样的要求，使用同样的测评方式，对每个测评实施过程的重复执行应得到相同结果。

连续性原则:确保在连续变化的环境中，在有效的服务期间内，保证相关业务系统等级备案和测评结论的准确性和及时性，保证信息系统安全测评的动态稳定性。

扩展性原则:信息系统安全测评过程要保证可扩展性，基于可持续的目标进一步加强测评结束后的安全管理有效性和可用性。

互动原则:测评过程中强调用户方的互动参与，项目各阶段都应根据用户方的要求和实际情况对测评的内容及方式做出相关调整，进而更好的开展等级测评工作。

最小影响原则:测评工作应尽可能小地影响业务系统和网络平台的正常运行，不应对业务的正常运行产生明显的影响（包括系统性能明显下降、网络阻塞、服务中断等），如无法避免，则应提前协商解决。

规范性原则:信息系统安全等级保护测评服务的实施必须由专业的测评服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，并提供完整的服务报告。

质量保障原则:必须高度重视项目质量管理，项目实施要严格按照预定方案和流程进行，并接受监理方全程监督，以便控制项目进度和质量。

保密原则：对测评的过程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福州水务水资源开发有限公司的行为，否则有权追究责任。

标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。

可控性原则：测评服务的进度要跟上进度表的安排，保证测评工作的可控性。

整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

6.1.1.2等级保护测评目的

本次等级测评的最终目的是根据一闸三线信息系统的安全等级，选择信息系统对应安全等级的安全控制要求作为本次等级测评的安全基线，对信息系统进行全面、完整地等级测评，分析现有信息系统的安全状况与《信息系统安全等级保护基本要求》及行业相关法律法规的安全要求差距，并提出科学、合理、符合实际情况的改进方法，信息系统通过合理的改进，实现重要信息系统的分等级保护与监管，信息安全事件分等级响应的目的，将信息系统的安全保护落实到点。

根据省网络安全等级保护工作协调小组有关文件要求，为切实提高一闸三线信息系统安全保障能力，开展信息系统等级保护备案和测评工作，通过项目实施，查找漏洞，整改隐患，为全面提高一闸三线信息系统稳定运行提供安全保障。主要工作目标：

（一）识别信息安全风险。通过对一闸三线工程信息化系统在安全技术和安全管理方面的备案和测评，发现信息系统在安全技术和安全管理方面与相应安全等级保护要求之间的差距，分析评估信息系统面临的风险。

（二）增强安全技术防护能力。依据安全技术等级测评结果，并结合信息化工作实际情况，制定针对性的安全技术建设整改计划，通过安全技术整改不断提高信息系统的整体安全保护水平。

（三）提高信息安全管理水平。依据安全管理等级测评结果，建立健全各项管理制度、安全策略、操作规程，落实各项管理措施，完善安全事件处置和应急预案管理，通过安全管理手段与安全技术手段相结合，进一步保证信息系统的安全性和稳定性。

6.1.1.3等级保护测评依据

在本次项目中，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和行业标准：

- GB/T 20269-2006：《信息安全技术 信息系统安全管理要求》
- GB/T 20282-2006：《信息安全技术 信息系统安全工程管理要求》
- GB/T 22081-2008：《信息技术 安全技术 信息安全管理实用规则》
- GB/T 22239-2019：《信息安全技术 网络安全等级保护基本要求》
- GB/T 22240-2020：《信息安全技术 网络安全等级保护定级指南》
- GB/T 25058-2019：《信息安全技术 网络安全等级保护实施指南》
- 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》
- 网络安全等级测评报告模版（2021 版）

6.1.2 等级保护实施整体流程

项目流程划分为以下阶段开展实施：

业务系统分类及梳理：对信息系统进行梳理，确定信息系统测评范围和类别。

制定方案：组成等保测评项目组，通过访谈、邮件、电话等方式与相关人员沟通,了解与此次项目相关的基本情况，明确测评范围。准备项目所需的测评工具、测评方法、现场实施方案和计划等内容。

现场测评：根据等级保护相关标准，从技术和管理共 10 个方面要求开展测评工作。同时针对各信息系统开展渗透测试工作，充分了解信息系统存在的安全漏洞，整理分析测评的数据。

测评编写及提交：根据现场测评数据对信息系统的安全状况进行分析，并输出《测评报告》和《整改方案》。

6.1.3 业务系统分类及梳理

通过对信息系统涉及的物理环境、网络架构、网络设备、操作系统、数据库、业务平台、中间件、数据等进行调研梳理，明确信息系统涉及的基础支撑环境和

各子系统。此外，根据前期业务系统梳理情况，从保密性、完整性、可用性三个方面对资产重要性进行分析，形成重要资产列表。

6.1.4 等级测评内容说明

6.1.4.1单元测评内容

测评单元	测评指标	测评项
安全物理环境	物理位置选择	a） 机房场地应选择在具有防震、防风和防雨等能力的建筑内； b） 机房场地应避免设在建筑物的屋顶或地下室，否则应加强防水和防潮措施。
	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。
	防盗窃和防破坏	a） 应将设备和主要部件进行固定，并设置明显的不易除去的标识； b） 应将通信缆线铺设在隐蔽安全处； **c） 应设置机房防盗报警系统或设置有专人值守的视频监控系统。**
	防雷击	a） 应将各类机柜、设施和设备等通过接地系统安全接地； **b） 应采取措施方式感应雷，例如设置防雷保安器或过压保护装置等。**
	防火	a） 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； b） 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； **c） 应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。**
	防水和防潮	a） 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； b） 应采取措施防止机房内水蒸气结雾和地下积水的转移与渗透； **c） 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。**
	防静电	a） 应采用防静电地板或地面并采用必要的接地防静电措施； **b） 应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。**
	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。
	电力供应	a） 应在机房供电线路上配置稳压器和过电压防护设备； b） 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； **c） 应设置冗余或并行的电力电缆线路为计算机系统供电。**
	电磁防护	a） 电源线和通信线缆应隔离铺设，避免互相干扰； **b） 应对关键设备实施电磁屏蔽。**

安全通信网络	网络架构	**a） 应保证网络设备的业务能力满足业务高峰期需求；** **b） 应保证网络各部分的带宽满足业务高峰期需要；** c） 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； d） 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； **e） 应提供通信线缆、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。**
	通信传输	a） 应采用校验技术或**密码技术**保证通信过程中数据的完整性； **b） 应采用密码技术保证通信过程中数据的保密性**
	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、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。
安全区域边界	边界防护	a） 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信； **b） 应能够对非授权设备私自联到内部网络的行为进行检查或限制；** **c） 应能够对内部用户非授权联到外部网络的行为进行检查或限制；** **d） 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。**
	访问控制	a） 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； b） 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； c） 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； d） 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； **e） 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。**
	入侵防范	**a） 应在关键网络节点处检查、防止或限制从外部发起的网络攻击行为；** **b） 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；** **c） 应采取技术措施对网络行为进行分析，实现对网络攻击特别是对新型网络攻击行为的分析；** d） **当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击事件，在发生严重入侵事件时应提供报警。**
	恶意代码和垃圾邮件防范	a） 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； **b） 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾**

		邮件防护机制的升级和更新。
	安全审计	a） 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； b） 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； c） 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； **d） 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。**
	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防护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。
安全计算环境	身份鉴别	a） 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性并定期更换； b） 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； c） 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。 **d） 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。**
	访问控制	a） 应对登录的用户分配账户和权限 b） 应重命名或删除默认账户，修改默认账户的默认口令； c） 应及时删除或停用多余、过期的账户，避免共享账户的存在； d） 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； **e） 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；** **f） 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；** **g） 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。**
	安全审计	a） 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； b） 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； c） 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； **d） 应对审计进程进行保护，防止未授权的中断。**
	入侵防范	a） 应遵循最小安装的原则，仅安装需要的组件和应用程序； b） 应关闭不需要的系统服务、默认共享和高危端口； c） 应通过设定终端接入方式或者网络地址范围对通过网络进行管理的管理终端进行限制；

		d) 应提供数据有效性验证功能，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； e) 应能发现可能存在的已知漏洞，并经过充分测试评估后，及时修补漏洞； **f) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。**
	恶意代码防范	**应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。**
	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。
	数据完整性	**a)** 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革新信息等；** b) **应采用校验技术或密码技术保证重要数据在存储过程中的完整性，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。**
	数据保密性	**a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；** **b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。**
	数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能； b) 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**； c) **应提供重要数据处理系统的热冗余，保证系统的高可用性。**
	剩余信息保护	a) 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； b) **应保证存有敏感数据的存储空间被释放或重新分配前得到完全的清除。**
	个人信息保护	a) 应仅采集和保存业务必需的用户个人信息； b) 应禁止未授权访问和非法使用用户个人信息。
安全管理中心	系统管理	a) 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操作系统管理操作，并对这些操作进行审计； b) 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、系统资源配置、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。
	审计管理	a) 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； b) 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。
	安全管理	a) **应对安全管理员进行申报鉴别，只允许其通过特定的命令或**

		操作界面进行安全管理操作，并对这些操作进行审计； b） **应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。**
	集中管控	a） **应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；** b） **应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；** c） **应对网络链路、安全设备、网络设备和服务器等色运行情况进行集中监测；** d） **应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；** e） **应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；** f） **应能对网络中发生的各类安全事件进行识别、报警、分析。**
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。
	管理制度	a） 应对安全管理活动中的各类管理内容建立安全管理制度； b） 应对管理人员或操作人员执行的日常管理操作建立操作规程； **c） 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。**
	制定和发布	a） 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； b） 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。
	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，对存在不足或需改进的安全管理制度进行修订。
安全管理机构	岗位设置	**a） 应成立指导和管理网络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担任或授权；** b） 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各方面的负责人岗位； c） 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
	人员配备	a） 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； **b） 应配备专职安全管理员，不可兼职。**
	授权和审批	a） 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； **b）** 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；** **c） 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。**
	沟通和合作	a） 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；

		b） 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； c） 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。
	审核和检查	a） 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； **b） 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；** c） **应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。**
安全管理人员	人员录用	a） 应指定或授权专门的部门或人员负责人员录用； b） 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，**对其所具有的技术技能进行考核；** **c） 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。**
	人员离岗	a） 应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； **b） 应办理严格的调离手续，并承诺调离后的保密义务后方可离开。**
	安全意识教育和培训	a） 应对各类人员进行安全意识教育与岗位技能培训，并告知相关的安全责任和惩戒措施； **b） 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；** c） **应定期对不同岗位的人员进行技能考核。**
	外部人员访问管理	a） 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人陪同，并登记备案； b） 应在外部人员接入受控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； c） 外部人员离场后应及时清除其所有的访问权限； **d） 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。**
安全建设管理	定级和备案	a） 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； b） 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； c） 应保证定级结果经过相关部门的批准； d） 应将备案材料报主管部门和相应公安机关报备。
	安全方案设计	a） 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； **b） 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；**

		c） **应组织相关部门和有关安全专家对安全整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。**
	产品采购和使用	a） 应确保网安安全产品采购和使用符合国家的有关规定； b） 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求； **c） 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。**
	自行软件开发	a） 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； **b） 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；** **c） 应制定代码编写安全规范，要求开发人员参照规范编写代码；** **d） 应具备软件设计的相关文档和使用指南，并对文档使用进行控制；** e） 应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测； **f） 应对程序资源的修改、更新、发布进行授权和批准，并严格进行版本控制；** g） **应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。**
	外包软件开发	a） 应在软件交付前检测其中可能存在的恶意代码； b） 应保证开发单位提供软件设计文档和使用指南； **c） 应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。**
	工程实施	a） 应指定或授权专门的部门或人员负责工程实施的管理； b） 应制定安全工程实施方案控制工程实施过程； **c） 应通过第三方工程监理控制项目的实施过程；**
	测试验收	a） 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告； b） 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**。
	系统交付	a） 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； b） 应对负责运行维护的技术人员进行相应的技能培训； c） 应提供建设过程文档和运行维护文档。
	等级测评	a） 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； b） 应在发生重大变更或级别发生变化时进行等级测评； c） 应确保测评机构的选择符合国家有关规定。
	服务供应商选择	a） 应确保服务供应商的选择符合国家的相关规定； b） 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；

		c） 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。
安全运维管理	环境管理	a） 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； **b） 应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；** c） 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。
	资产管理	a） 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容； **b） 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；** c） **应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。**
	介质管理	a） 应将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； b） 应对介质字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。
	设备维护管理	a） 应对各种设备（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； b） 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效管理，包括明确维护人员的责任、维修和服务的审批、维护过程的监督控制等； **c） 信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密；** d） **含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数和授权软件无法恢复重用。**
	漏洞和风险管理	a） 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； **b） 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。**
	网络和系统安全管理	a） 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； b） 应指定专门的部门或人员进行账户管理，对申请账户、删除账户等进行控制； c） 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； d） 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； e） 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； **f） 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；** **g） 应严格控制变更性运维，经过审批后才可以改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；** **h） 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；** **i） 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后应立即关闭接口或通道；** **j） 应保证所有与外部的连接均得到授权或批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。**
	恶意代码防范管理	a） 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； **b） 应定期验证防范恶意代码攻击的技术措施的有效性。**
	配置管理	a） 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； **b） 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。**
	密码管理	a） 应遵循密码相关国家标准和行业标准； b） 应使用国家密码管理主管部门认真核准的密码技术和产品。
	变更管理	a） 应明确变更要需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方方可实施； **b） 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；** c） **应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员的职责，必要 时对恢复过程进行演练。**
	备份与恢复管理	a） 应识别所需定期备份的重要业务信息、系统数据及软件等； b） 应规定备份信息的备份方式、备份频度、存储介质、保存期等； c） 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。
	安全事件处置	a） 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； b） 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等； c） 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； **d） 对造成系统中断或造成信息泄露的重大安全事件应采用不同的处理程序和报告程序。**
	应急预案	**a） 应规定统一的应急预案框架，包括启动预案的条件、应急组**

	管理	**织构成、应急资源保障、事后教育和培训等内容；** b） 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； c） 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练； **d） 应定期对原有的应急预案重新评估，修订完善。**
	外包运维管理	a） 应确保外包运维的选择符合国家的有关规定； b） 应与选定的外包运维签订相关的协议，明确约定外包运维的范围、工作内容； **c） 应保证选择的外包运维在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；** **d） 应在与外包运维签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。**

6.1.4.2整体测评内容

6.1.4.2.1 安全控制间测评

安全控制间的安全测评主要考虑同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。安全功能上的增强和补充可以使两个不同强度、不同等级的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。例如，应用安全层面的代码安全与访问控制，如果代码安全没有做好，很可能会使应用系统的访问控制被旁路。

如果安全控制间优势互补，使单个低等级安全控制发挥的安全功能达到信息系统相应等级的安全要求，则可认为该安全控制没有影响信息系统的整体安全保护能力。如果安全控制间存在削弱作用，使某个安全控制的功能等级降低到其安全功能已不能达到信息系统相应等级的安全要求，则可认为该安全控制影响到信息系统的整体安全保护能力。

6.1.4.2.2 层面间安全测评

层面间的安全测评主要考虑同一区域内的不同层面之间存在的功能增强、补充和削弱等关联作用。

本次测评重点考虑物理层面和网络层面、主机系统层面、应用层面之间的关联互补作用，如主机系统的身份鉴别存在的脆弱性是否可以通过物理层面和网络层面的安全控制措施得到加强弥补。

另外，网络层面、应用层面和主机系统层面与安全管理的系统运维管理之间关系密切，应关注他们之间的关联互补作用。如考虑网络层面的边界完整性检查安全功能是否通过采取恰当的安全管理措施而得到满足等等。

6.1.4.2.3 区域间安全测评

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。

6.1.4.2.4 系统结构安全测评

系统结构安全测评主要考虑信息系统整体结构的安全性和整体安全防范的合理性。

在掌握系统的物理布局、网络拓扑、业务逻辑（业务数据流）、系统实现和集成方式等基础上，结合系统的业务数据流分析物理布局与网络拓扑之间、网络拓扑与业务逻辑之间、物理布局与业务逻辑之间、不同信息系统之间存在的各种关系，明确物理、网络和业务系统等不同位置上可能面临的威胁、可能暴露的脆弱性等，综合判定系统的整体布局是否合理、主要关系是否简单、整体是否安全有效等。

在熟悉系统安全保护措施的具体实现方式和部署情况后，结合其业务数据流分析不同区域和不同边界与安全保护措施的关系、重要业务和关键信息与安全保护措施的关系等，参照纵深防御的要求，识别系统的安全防范是否突出重点、层层深入，综合判定系统的整体安全防范是否恰当合理等。

6.1.5 系统测评实施方案

等级保护测评是根据国家标准《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》要求选取安全基础指标，开展技术和管理两个方面的检测工作，并出具符合国家相关规范要求的测评报告。

6.1.5.1测评对象

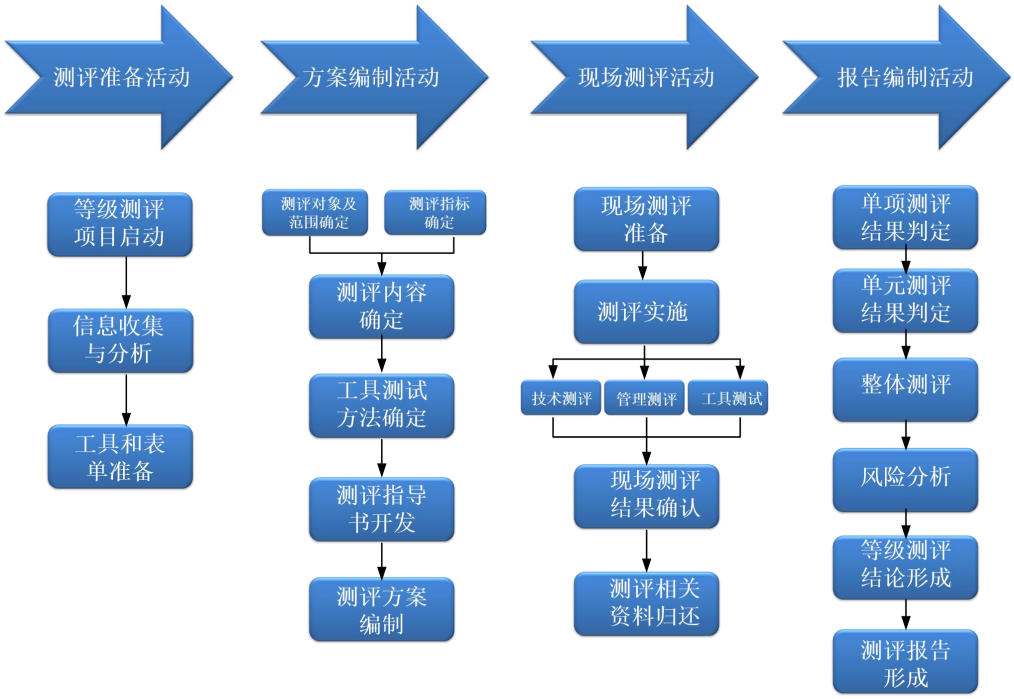
在本次测评过程中，对信息系统所涉及的物理环境、网络安全、主机安全、安全设备、应用系统、管理制度等多方面内容进行测评。针对信息系统的安全要求，本次测评的信息系统将按照《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》要求开展测评工作。

序号	被测单位	系统名称	安全等级
1			三级

表格 1- 11 测评系统范围

6.1.5.2测评流程

一闸三线工程信息系统等级保护测评服务主要采用管理员访谈、设备配置查看、渗透测试及记录查看等多种方式进行测评，对测评数据进行综合分析后，编制《信息系统等级保护测评报告》，同时提交《信息系统测评报告》、《整改方案》（信息系统基本符合）；具体工作流程图如下所示：



图表 1- 1 测评流程图

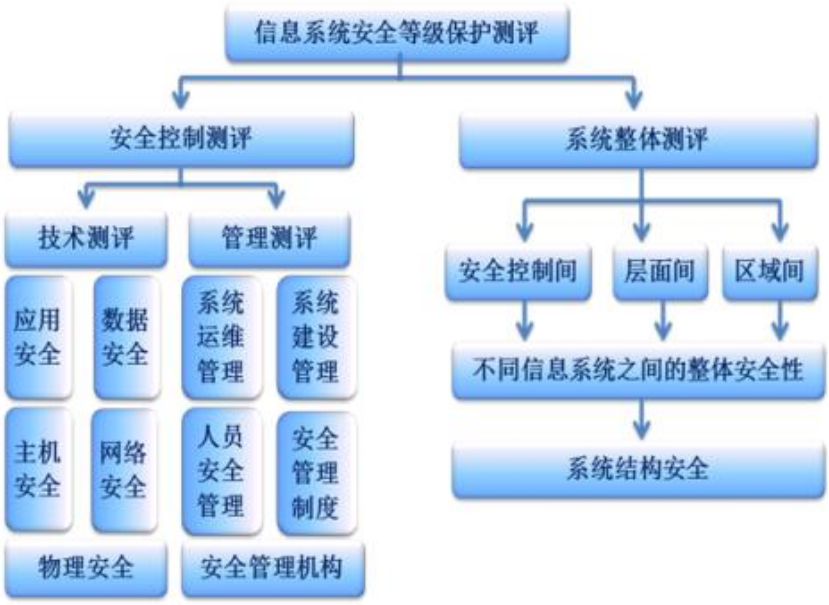
1、测评准备活动/方案编制活动：在项目开展实施前期，召开项目启动会，明确协调人员、工作内容等。项目组预先组织参与此次项目人员通过现场访谈、邮件、电话等方式与相关人员沟通，并对被测信息系统基本情况进行现场确认，初步了解和确认信息系统架构、设备数量、功能及建设投入运行时间等基础信息。根据基础调研和定级情况，项目组编写详细的《测评方案》，提交福州水务水资源开发有限公司确认。

2、现场测评活动：通过项目启动会议，准备相关材料、工具等；根据各信息系统现场调查的结果，分别对各信息系统的物理、主机、网络、应用、数据、管理等方面进行安全测评，并且通过技术手段对信息系统测评对象实施安全测试和扫描，获取信息系统最真实的数据，此外利用风险评估方法对信息系统的弱点、资产重要性、威胁等进行分析。

3、报告编制活动：根据现场测评实施获取的材料、信息、记录等进行统一汇总，并且结合标准和行业特殊需求合理分析相关数据形成最终的等级测评结论，出具符合信息系统安全等级保护要求的信息系统安全等级保护测评符合性报告（提交成果《测评报告》）及对不符合网络安全等级保护有关管理规范和技术标准出具可行的、有效的信息系统《整改方案》。

6.1.5.3等级测评整体内容

本次项目测评主要从安全控制测评和系统整体测评两个方面进行实施分析，基于以上两个方面内容开展技术、管理测评和安全控制间、层面间及区域间分析。测评结构如下所示：



图表 1- 2 等级保护测评结构图

6.1.5.4测评风险分析

6.1.5.4.1 风险分析方法

本项目依据安全事件可能性和安全事件后果对信息系统面临的风险进行分析，分析过程包括：

1）判断信息系统安全保护能力缺失（等级测评结果中的部分符合项和不符合项）被威胁利用导致安全事件发生的可能性，可能性的取值范围为高、中和低；

2）判断安全事件对信息系统业务信息安全和系统服务安全造成的影响程度，影响程度取值范围为高、中和低；

3）综合 1）和 2）的结果对信息系统面临的风险进行汇总和分等级，风险等级的取值范围为高、中和低；

4）结合信息系统的安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的风险。

6.1.5.4.2 风险分析内容

风险分析是等级保护测评工作重要方法之一，基于风险评估方法对核心业务系统的支撑环境如物理环境、网络系统、操作系统、数据库系统等进行详细的评估，可以针对测评过程中发现的业务流程安全隐患进行弱点分析以及有效弥补，更加合理、充分的去分析信息系统安全防护能力和安全风险。

6.1.5.5测评报告及整改方案

根据实际情况提供详细的《信息系统测评报告》和《整改方案》。对测评中发现的问题，依据《网络安全等级保护基本要求》相关标准分别从基础设施、安全管理制度、安全策略三个方面提供相应的针对性建议。如基础设施建议，主要针对信息系统现状存在的安全问题进行全面的需求分析，形成对物理机房环境、网络环境、边界安全、监控管理中心、双因子身份认证、设备高可靠性冗余、数据异地备份等方面的安全需求。根据安全需求形成等级保护设备扩充列表和具体的解决方案，信息系统通过硬件设施的扩充实现安全防御能力的提高。

6.1.5.6测评结论

综合现场测评与分析结果，对信息系统基本安全保护状态进行综合判断结果分为 4 类----优、良、中、差，具体判定依据及判定结论如下表：

测评结论	判别依据
优	被测对象中存在安全问题，但不会导致被测对象面临中、高等级安全风险，且系统综合得分 90 分以上（含 90 分）
良	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 80 分以上（含 80 分）
中	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 70 分以上（含 70 分）

差	被测对象中存在安全问题，而且会导致被测对象面临高等级安全风险，或被测对象综合得分低于 70 分

表格 1- 13 测评结论判定依据

6.1.6 等级测评技术实施手段

管理测评	☑ 访谈	☑ 文档审核	☑ 实地察看	
物理测评	☑ 访谈	☑ 文档审核	☑ 实地察看	☑ 工具测试
网络状况测评	☑ 访谈	☑ 文档审核	☑ 验证	☑ 工具测试
网络设备测评	☑ 访谈	☑ 文档审核	☑ 配置检查	☑ 工具测试
主机设备测评	☑ 访谈	☑ 文档审核	☑ 配置检查	☑ 工具测试
数据安全及备份恢复测评	☑ 访谈	☑ 文档审核	☑ 配置检查	
应用系统测评	☑ 访谈	☑ 文档审核	☑ 配置检查	☑ 工具测试

表格 1- 14 测评方式

注：

1.访谈：通过与相关人员进行交谈和问询，了解信息系统技术和管理方面的一些基本信息，并对一些测评内容进行确认；

2. 文档审核：审核信息系统安全的各个方面的文档，如：安全管理制度和文件、安全管理的执行过程文档、系统设计方案、网络设备的技术资料、系统和产品的实际配置说明、系统的各种运行记录文档、机房建设相关资料等。通过对这些文档的审核与分析确认测评的相关内容是否达到了等级的要求；

3. 配置检查：根据测评结果记录表格内容，利用上机验证的方式检查应用系统、主机系统、数据库系统以及网络设备的配置是否正确，是否与文档、相关设备和部件保持一致，对文档审核的内容进行核实。如果系统在输入无效命令时不能完成其功能，将要对其进行错误测试。针对网络连接，应对连接规则进行验证；

4. 实地察看：主要是对一些需要上机进行确认的信息进行核实，以及对某些面谈和文档审核的内容进行核实；

5. 工具测试：主要是根据福州水务水资源开发有限公司信息系统的实际情况，测评人员使用一些技术工具对信息系统进行测试。一般包括信息系统等级保护漏洞扫描、渗透性测试、性能测试、入侵检测、协议分析和备份测试等内容。

不同安全等级的信息系统选择的测评方法和测评深度有所差异，具体差异如下：

文档审核：

二级/三级：满足 GB/T 22239-2019 中的要求，并且所有文档之间应保持一致性，要求有执行过程记录的，过程记录文档的记录内容应与相应的管理制度和文档保持一致，与实际情况保持一致。

实地察看：

二级/三级：满足 GB/T 22239-2019 中的要求。

配置检查：

二级/三级：满足 GB/T 22239-2019 中的要求，测评其实施的正确性和有效性，检查配置的完整性，测试网络连接规则的一致性。

工具测试：

二级/三级：满足 GB/T 22239-2019 中的要求，针对主机、服务器、关键网络设备、安全设备等设备进行漏洞扫描等。

6.1.7 项目周及进度安排

本项目周期 60 个日历日。自合同签订之日起计算，在 60 天内完成三级业务系统的测评及其他相关服务。获取等保测评报告及其他相关服务报告后，提出验收申请，组织验收。

7 等保辅助测评服务

7.1 安全管理制度整改服务

负责对现有安全管理制度进行梳理，查缺补漏，进而根据等保 2.0 的安全管理制度的建设要求，完善安全管理制度的建设，主要包括以下方面的建设：

序号	制度建设
1	人员安全管理制度
2	安全工作的总体方针和安全策略
3	机构安全管理制度
4	网络安全委员会/小组职责文件
5	安全管理制度的制定发布管理制度
6	信息系统的安全检查制度
7	外部人员访问管理制度
8	产品采购管理制度
9	软件开发管理制度
10	服务供应商评价审核管理制度
11	机房安全管理制度
12	办公室安全管理制度
13	资产管理制度
14	信息分类标识文档
15	介质安全管理制度
16	设备管理制度
17	网络和系统安全管理制度
18	外部设备接入管理制度
19	恶意代码防范管理制度
20	配置信息管理制度
21	密码及密码产品的管理制度
22	系统变更管理制度
23	数据备份和恢复安全管理制度
24	数据备份和数据恢复策略
25	安全事件报告和处置管理制度

序号	制度建设
26	应急预案

提交成果包括以下五个方面：《安全管理制度》、《安全管理机构》、《安全人员管理》、《安全建设管理》、《安全运维管理》。

7.2 安全问题整改加固服务

根据差距分析结果，针对不符合项以及行业特性要求进行个性化的整改方案设计，出具一份完整的信息安全等级保护建设整改方案，方案内容包含技术策略实施、风险评估等方面的内容，即《信息系统安全加固实施方案》。

负责对系统安全进行安全策略加固，从等保 2.0 要求的技术层面，即安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心这五个方面进行加固整改，派遣专业工程师到现场根据安全加固实施方案进行边界防护安全策略优化、服务器病毒检查与清理、主机安全、数据库安全以及应用安全方面的加固等服务。

8 服务清单

序号	项目	主要技术指标
1	三级等保测评服务	1、资产调查分析：调查和统计全部网络所包含的信息资产，其中必须包括但不限于网络设备、主机、应用软件、业务系统、数据、人员、标准流程等，明确其现有状况、配置情况和管理情况，绘制信息系统的数据流图。具体的现状情况如主机系统，需明确其配置、存储空间（包括剩余空间，空间分配）操作系统平台、版本、补丁、IP 地址、开放端口、服务和进程等配置管理信息。 2、网络调查：包括对所有网络的拓扑结构进行调查，并按统一标准绘制成图。 3、信息系统定级服务：负责完成信息系统等级保护定级、备案、自查等工作，负责完成信息系统网络安全等级保护测评辅助支持工作，并根据测评结果进行相关整改工作。 4、漏洞扫描、脆弱性评估：包括网络设备评估、安全设备评估、主机系统评估、数据库安全评估、中间件安全评估、应用系统评估。 5、配置检查、威胁评估：包括网络安全设备配置检查分析以及整体威胁分析。 6、差距分析：根据网络安全等级保护基本要求，通过访谈、实地查看或配置检查等方式进行差距化分析，并记录访谈结果和查看结果，形成差距分析报告。 7、渗透测试：负责远程业务系统进行渗透测试。 8、安全加固与复查：根据等保三级要求，对系统安全评估、测评中发现的问题，配合指导完成相关安全整改加固工作。 9、策略复查：对加固前后的脆弱性进行复查。 10、网络安全制度体系建设：根据等保要求，建设安全管理制度。开展安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理制度建设。

		11、信息系统备案服务：获取测评报告后，负责将备案材料盖章、送审等工作，完成备案。 12、现场测评：联系测评机构入场对系统进行测评；负责现场测评对接，准备相关测评材料，直到获得测评报告。
2	整改服务	1、应用安全整改：对测评过程中所发现的应用系统等保安全风险问题（含数据库、中间件等应用系统运行必须的组件等）进行分析，负责对接协调应用系统开发商完成等保测评过程中所发现的问题的整改，应用系统开发商整改完成后，提交整改反馈。 2、服务器安全整改：对测评过程中所发现的服务器操作系统等保安全风险问题进行分析，负责对接协调服务器维护商完成等保测评过程中所发现的问题的整改，服务器维护商整改完成后，提交整改反馈。 3、网络安全整改：对测评过程中所发现的网络设备（交换机、路由器、负载均衡等网络设施）等保安全风险问题进行分析，负责对接协调网络设备提供商完成等保测评过程中所发现的问题的整改，网络设备提供商整改完成后，提交整改反馈。 4、安全设备整改：对测评过程中所发现的安全设备（防火墙、堡垒机、日志审计等安全设备）等保安全风险问题进行分析，负责对接协调安全设备提供商完成等保测评过程中所发现的问题的整改，安全设备提供商整改完成后，提交整改反馈。
3	咨询及技术服务	1、终端漏洞发现服务：测评服务期间使用专业安全服务工具开展终端资产的漏洞发现服务，提高终端漏洞威胁发现率，加强漏洞安全管理能力。 2、互联网攻击面检测服务：测评期间使用专业安全服务工具开展互联网攻击面检测服务，基于攻击者视角对开放在互联网的资产进行深度检测，包括端口、IP、域名、影子资产等维度。 3、安全意识培训：提供安全意识培训宣贯。 4、提供咨询及技术支撑服务。