信息安全管理程序

(TFDL-ITSS-1508)

湖南同飞电力调度信息有限责任公司

国家电网
STATE GRID
国网湖南省电力有限公司
STATE GRID HUNAN ELECTRIC POWER COMPANY LIMITED

文件编制和变更履历

版本	编制/更改		发布		实施		更改记录
	作者	日期	审核	日期	批准	日期	
V1.0	李皓朴	2016.12.3	罗喜军	2016.12.23	张远明	2017.1.1	首次发布
V1.1	李皓朴	2020.1.6	罗喜军	2020.1.8	张远明	2020.1.8	修改
V1.2	周丽	2023.1.5	罗喜军	2023.1.6	张远明	2023.1.6	修改

目 录

1 目的

本程序的目的是在运维服务交付过程中有效的管理信息安全。

- 满足信息管理系统运行和客户服务中的安全性需求以及合同、法律和外部政策等外部要求；
- 提供一个满足需求的基本的信息系统安全基线；
- 确保有效的信息安全措施在公司、运维服务部门和服务人员三个层面都得到贯彻。

2 过程定义

安全管理是顺应信息安全的需要而产生的，其主要目标是确保信息的安全性。

安全管理致力于确保服务的安全性在任何时候都能达到与客户约定的级别。

安全性在服务中被视为可用性管理的一部分。安全管理已经成为现代服务管理中一个重要的问题。

安全性是指不易遭到已知风险的侵袭，并且尽可能地规避未知风险的性能。提供这种性能的工具是安全措施。

安全措施的目标是要保护信息的价值，这种价值取决于机密性、完整性和可用性三个方面。

2.1 范围

本程序适用于运维服务覆盖的所有部门。

2.2 过程负责人

安全管理负责人

2.3 主要输入

输入	来源
服务级别需求	服务级别协议。

配置管理	系统的配置项，记录和报告配置。

2.4 主要输出

输出	去向
风险评估报告	信息安全管理负责人、部门经理。
信息安全报告	信息安全管理负责人、部门经理。
变更管理	服务实施过程中，服务交付过程的主要步骤。
服务报告管理	服务实施过程中，服务交付过程的主要步骤。

2.5 职责权限

安全管理负责人负责整个安全管理流程的有效运作。

安全管理负责人职责：

1) 监控安全管理流程；

2) 根据组织安全需求，开发与维护安全计划；

3) 处理与安全相关的问题和事件；

4) 确保满足SLA中指定的安全需求；

5) 完成包含流程结果，自评估及内部审计的信息安全风险评估报告；

6) 人员组成：信息安全员管理员、部门经理等。

客户服务负责人职责：

1) 负责安排项目中的信息安全风险评估；

2) 做好用户的沟通，协调关于信息安全的问题。

2.6 过程重要控制点

风险评估报告。

信息安全管理规范。

安全事件记录。

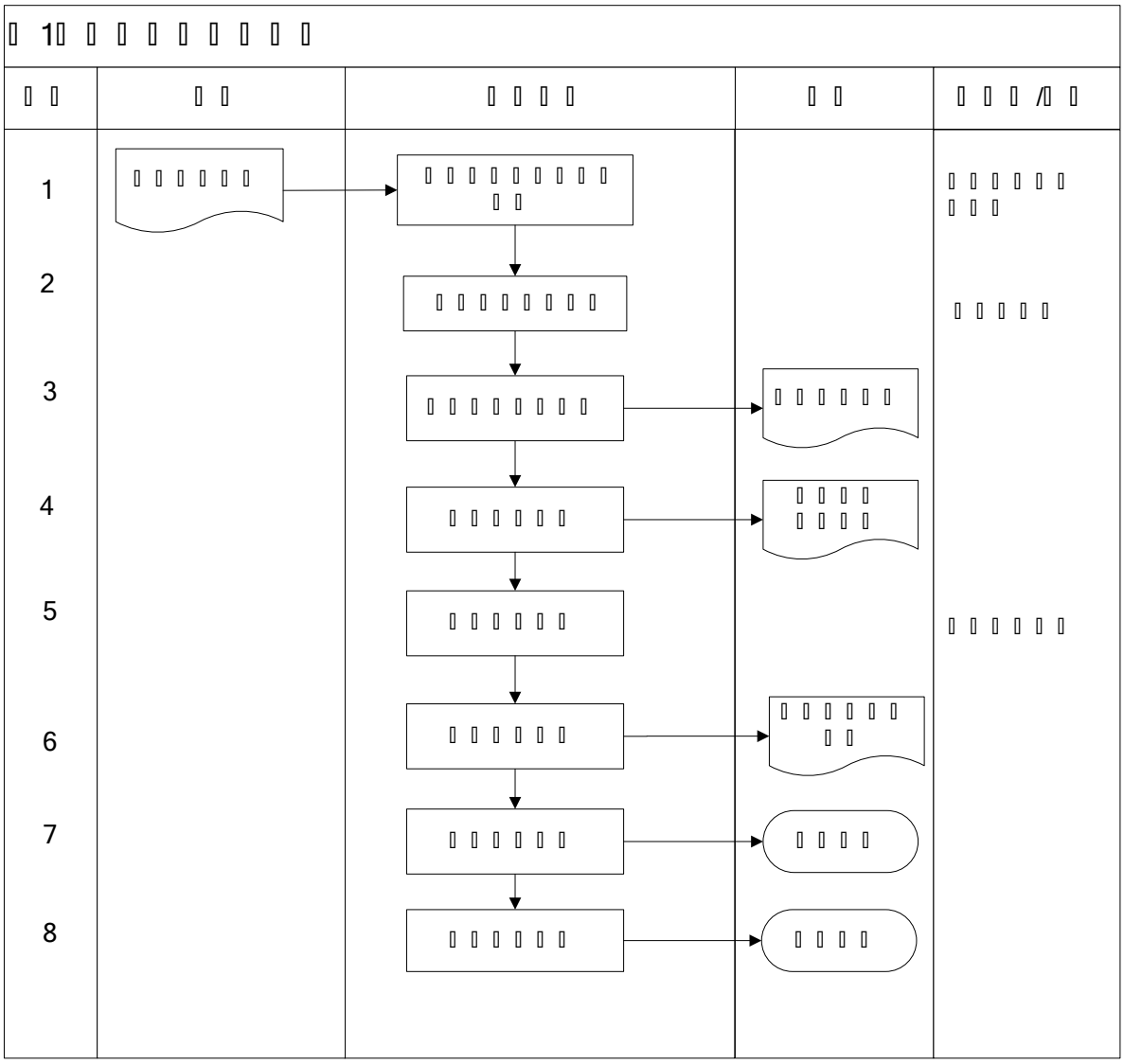
2.7 过程测量指标

安全事件次数。

3 术语

术语	定义
机密性	指保护信息免受未经授权的访问和使用。
完整性	指信息的准确性、完全性和及时性。
可用性	是信息在任何约定的时间内都可以被访问。这取决于由信息处理系统所提供的持续性。

4 流程



5 信息安全方针

公司信息安全方针为：全员参与、控制风险；积极预防、持续改进；

6 信息安全策略

为了保证信息系统安全保护工作的整体、计划性及规范性，保证各项措施和管理手段的正确实施，使信息系统信息数据的机密性、完整性及可使用性受到全面、可靠的保护，我们往往需要制定信息系统安全策略。

6.1 信息安全策略定义

信息安全策略是单位内指导本单位及其信息系统如何管理和保护包括敏感信息在内的资产的规则、指南和惯例。

信息安全策略(Information Security Policies)是组织对信息和信息处理设施进行管理，保护和分配的原则，它告诉组织成员在日常的工作中什么是可以做的，什么是必须做的，什么是不能做的，哪里是安全区，哪里是敏感区，就像交通规则之于车辆和行人，信息安全策略是有关信息安全的行为规范。

6.2 信息安全策略内容

➢ 物理安全策略

旨在保护计算机服务器、数据存贮、系统终端、网络交换等硬件设备免受自然灾害、人为破坏，确保其安全可用。

制定物理安全策略，要重点关注存放计算机服务器、数据存贮设备、核心网络交换设备的机房的安全防范。其选址与规划建设要遵循 GB9361 计算机场地安全要求和 GB2887 计算机场地技术条件，保证恒温、恒湿，防雷、防水、防火、防鼠、防磁、防静电，加装防盗报警装置，提供良好的接地和供电环境，要为核心设备配置与其功耗相匹配的稳压及 UPS 不间断电源。

➢ 网络安全策略

旨在防范和抵御网络资源可能受到的攻击，保证网络资源不被非法使用和访问，保护网内流转的数据安全。

访问控制是维护网络安全、保护网络资源的重要手段，是网络安全核心策略之一。访问控制包括入网访问控制、网络授权控制、目录级安全控制、属性安全控制、网络服务器安全控制、网络监测和锁定控制、网络端口和节点的安全控制以及防火墙控制。安全检查（身份认证）、内容检查也是保护网络安全的有效措施。

网络加密手段包括链路加密、端点加密和节点加密，链路加密是保护网络节点之间的链路数据安全，端到端加密是对从源端用户到目的端用户之间传输的数据提供保护，节点加密是对源节点到目的节点之间的传输链路提供保护。

另外，数字认证在一定程度上保证了数据交互信息的安全。

- **数据安全策略**

旨在防止数据被偶然的或故意的非法泄露、变更、破坏，或是被非法识别和控制，以确保数据完整、保密、可用。数据安全包括数据的存储安全和传输安全两个方面。

数据的存储安全系指数据存放状态下的安全，包括是否会被非法调用等，可借助数据异地容灾备份、密文存储、设置访问权限、身份识别、局部隔离等策略提高安全防范水平。

- **软件安全策略**

旨在防止由于软件质量缺陷或安全漏洞使信息系统被非法控制，或使之性能下降、拒绝服务、停机。软件安全策略分为系统软件安全策略和应用软件安全策略两类。

对通用的应用软件，可参照前款作法，通过加强与软件提供商的沟通，及时发现、堵塞安全漏洞。对量身定做的应用软件，可考虑优选通过质量控制体系认证、富有行业软件开发和市场推广经验的软件公司，加强软件开发质量控制，加强容错设计，安排较长时间的试运行等策略，以规避风险，提高安全防范水平。

- **系统管理策略**

旨在加强计算机信息系统运行管理，提高系统安全性、可靠性。

要确保系统稳健运行，减少恶意攻击、各类故障带来的负面效应，有必要建立行之有效的系统运行维护机制和相关制度。比如，建立健全中心机房管理制度，信息设备操作使用规程，信息系统维护制度，网络通讯管理制度，应急响应制度等等。

要根据分工，落实系统使用与运行维护工作责任制。

加强对相关人员的培训和安全教育，减少因为误操作给系统安全带来的冲击。要妥善保存系统运行、维护资料，做好相关记录，要定期组织应急演练，以备不时之需。

- **灾难恢复策略**

旨在趁着系统还在运行的时候，制定一个灾难恢复计划，将灾难带来的损失降低到最小，使系统安全得到保障的策略。

主要需根据本单位及信息系统的实际情况，研究系统遇到灾害后对业务的影响，设计灾后业务切换办法，如定期备份数据，根据灾难类型，制订灾难恢复流程，建立

灾难预警、触发、响应机制，组织相关培训和练习，适时升级和维护灾难恢复计划等等。

7 信息安全管理过程描述

7.1 风险评估计划和过程

7.1.1 评估计划

信息安全风险评估工作共分为 4 个阶段：即准备阶段、识别阶段、分析阶段、规划验收阶段。

准备阶段：主要完成项目组织、项目实施方案确定、组织培训、项目启动的工作。

识别阶段：主要完成大量的现场识别工作，主要有资产识别、威胁识别、脆弱性识别、安全措施识别。

分析阶段：在识别的基础上进行大量整理并分析，得出风险评估各要素的风险状况，具体有资产影响分析、威胁分析、脆弱性分析、综合风险分析。

规划验收阶段：对综合风险进行梳理分析，制定风险控制规划和改进计划，完成风险评估。

7.1.2 评估过程

现场评估工作主要分 5 个阶段：

第一阶段：网络设备资产调查和拓扑调查。获取信息系统现有网络设备资产和网络链路情况相关资料，进行现场核对，发现存在的偏差，及时和网管员沟通确认，最终根据信息资产调查的全面结果，形成网络设备资产列表和网络拓扑图。

第二阶段：对信息系统内所有服务器资产进行识别，确定评估对象外的与之相关联的资产作为最终评估对象，然后根据评估的资产在业务和应用流程中的重要程序为资产进行估价。

第三阶段：网络和安全设备测评和网络结构测评。根据资产调查结果和网络拓扑分析，确定本次项目网络和安全设备评估范围。依据确定的网络和安全设备测评范围，

开展网络设备现场测评工作。网络和安全设备测评过程中，由网络管理人员输入相关设备密码，评估人员依据测评表的内容，进行现场核查，同时记录核查结果和操作内容，为后期网络设备安全性分析提供有利依据。

第四阶段：主机系统、应用系统和存储数据备份的测评。在确定最终评估对象的资产识别和估价完成后，根据实际的系统和应用系统确定与之相应的评测表。主机测评过程中，由系统管理人员输入相关设备密码，评估人员依据测评表的内容，进行现场核查，同时记录核查结果和操作内容，为后期主机设备安全性分析提供有利依据。

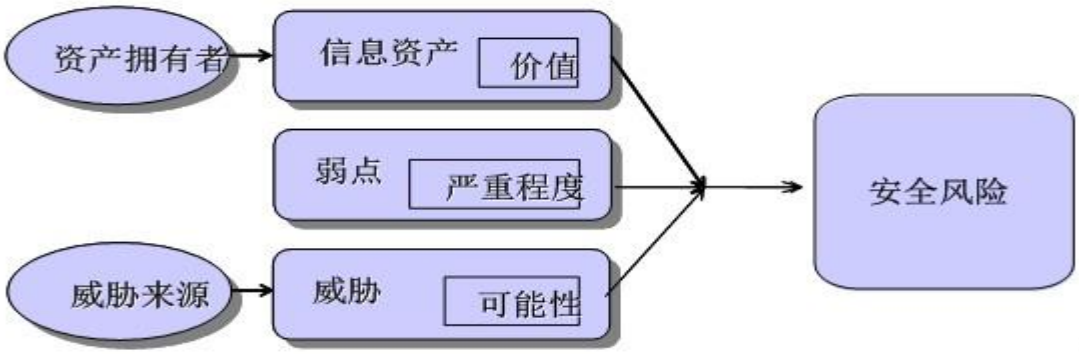
第五阶段：系统漏洞扫描，主要针对网络设备、安全设备、服务器、PC 终端的漏洞扫描，并形成漏洞扫描报告。

7.2 评估依据

- 《信息安全技术信息安全风险评估规范》（GB/T 20984-2007）
- 《信息技术安全技术信息安全管理体系要求》（GB/T22080-2008）
- 《信息技术安全技术信息安全管理实用规则》（GB/T22081-2008）
- BS7799-1《信息安全管理实施规则》和 BS7799-2《信息安全管理体系规范》
- ISO/IEC 27001, Information technology - Code of practice for information security management, 2005

7.3 评估方法和工具

我们主要参考 GBT 20984、GBT 22239、ISO27001、BS7799 等标准和指南采用最新的方法进行风险分析，表述出威胁源采用何种威胁方法，利用了系统的何种脆弱性，对哪一类资产，产生了什么样的影响，当前采取了何种安全措施进行防护，其有效性如何，描述残余风险状况，并描述采取何种对策来防范威胁，减少脆弱性。下图为风险评估模型及方法：



资产的评估主要是对资产进行相对估价，而其估价准则就是依赖于对其影响的分析，主要从保密性、完整性、可用性三方面的安全属性进行影响分析，从资产的相对价值中体现了威胁的严重程度；威胁评估是对资产所受威胁发生可能性的评估；脆弱性的评估是对资产脆弱程度的评估，安全风险评估就是通过综合分析评估后的资产信息、威胁信息、脆弱性信息，最终生成安全风险信息。

测评内容	测评方式		
管理测评	☑ 访谈	☑ 文档审核	☑ 观察现场
物理测评	☑ 访谈	☑ 文档审核	☑ 观察现场
网络状况测评	☑ 访谈	☑ 文档审核	☑ 验证
网络设备测评	☑ 验证	☑ 文档审核	☑ 漏洞扫描
主机设备测评	☑ 验证	☑ 文档审核	☑ 漏洞扫描
数据安全及备份恢复测评	☑ 访谈	☑ 验证	☑ 文档审核
应用系统测评	☑ 访谈	☑ 验证	☑ 文档审核

注：1.访谈：通过与服务事业部的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：审核服务事业部网管员提交的有关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. 验证：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；

7.4 评估内容

评估内容主要分为安全技术测评和安全管理测评，其中安全技术测评主要是针对系统所处的物理安全、网络安全、主机系统安全、应用安全、数据安全。管理测评主要是针对管理机构、安全管理制度、人员、系统建设、日常运维管理。

7.5 资产的评估和赋值

资产是风险评估的评估对象。在一个全面的风险评估中，风险的所有元素都以资产为中心，威胁、脆弱性以及风险都是针对资产而客观存在的。威胁利用资产自身的脆弱性使得安全事件的发生成为可能，从而形成了风险。因此，资产的评估是风险评估的一个重要的步骤，它被确定和分析的准确性将影响着后面所有因素的评估。

资产主要包括公司的网络设备、网络安全设备、终端、服务器、数据库、业务软件、数据等信息资产。

资产赋值的过程也就是对资产在机密性、完整性和可用性上的达成程度进行分析，并在此基础上得出综合结果的过程。

首先对机密性赋值，根据资产在机密性上的不同要求，将其分为五个不同的等级，分别对应资产在机密性上应达成的不同程度或者机密性缺失时对整个组织的影响。机密性赋值标准如下表所示：

赋值	标识	定义
5	很高	包含组织最重要的秘密，关系未来发展的前途命运，对组织根本利益有着决定性的影响，如果泄露会造成灾难性的损害
4	高	包含组织的重要秘密，其泄露会使组织的安全和利益遭受严重损害
3	中等	组织的一般性秘密，其泄露会使组织的安全和利益受到

		损害
2	低	仅能在组织内部或在组织某一部门内部公开的信息，向外扩散有可能对组织的利益造成轻微损害
1	很低	可对社会公开的信息，公用的信息处理设备和系统资源等

然后对完整性赋值，根据资产在完整性上的不同要求，将其分为五个不同的等级，分别对应资产在完整性上缺失时对整个组织的影响。完整性赋值标准如下表所示：

赋值	标识	定义
5	很高	完整性价值非常关键，未经授权的修改或破坏会对组织造成重大的或无法接受的影响，对业务冲击重大，并可能造成严重的业务中断，难以弥补。
4	高	完整性价值较高，未经授权的修改或破坏会对组织造成重大影响，对业务冲击严重，较难弥补。
3	中等	完整性价值中等，未经授权的修改或破坏会对组织造成影响，对业务冲击明显，但可以弥补。
2	低	完整性价值较低，未经授权的修改或破坏会对组织造成轻微影响，对业务冲击轻微，容易弥补。
1	很低	完整性价值非常低，未经授权的修改或破坏对组织造成的影响可以忽略，对业务冲击可以忽略。

最后对可用性赋值，根据资产在可用性上的不同要求，将其分为五个不同的等级，分别对应资产在可用性上应达成的不同程度。可用性赋值标准如下表所示：

赋值	标识	定义
5	很高	可用性价值非常高，合法使用者对信息及信息系统的可用度达到年度 99.9%以上，或系统不允许中断。
4	高	可用性价值较高，合法使用者对信息及信息系统的可用

		度达到每天 90%以上，或系统允许中断时间小于 10 分钟。
3	中等	可用性价值中等，合法使用者对信息及信息系统的可用度在正常工作时间达到 70%以上，或系统允许中断时间小于 30 分钟。
2	低	可用性价值较低，合法使用者对信息及信息系统的可用度在正常工作时间达到 25%以上，或系统允许中断时间小于 60 分钟。
1	很低	可用性价值可以忽略，合法使用者对信息及信息系统的可用度在正常工作时间低于 25%。

最终，资产价值依据资产在机密性、完整性和可用性上的赋值等级，经过综合计算评定得出一个综合数值，根据这个数值，对应下表即可分析出资产的总体价值：

等级	标识	得分	描述
5	很高	4.6-5	非常重要，其安全属性破坏后可能对组织造成非常严重的损失。
4	高	3.6-4.5	重要，其安全属性破坏后可能对组织造成比较严重的损失。
3	中	2.6-3.5	比较重要，其安全属性破坏后可能对组织造成中等程度的损失。
2	低	1.6-2.5	不太重要，其安全属性破坏后可能对组织造成较低的损失。
1	很低	1-1.5	不重要，其安全属性破坏后对组织造成导很小的损失，甚至忽略不计。

7.6 威胁评估

7.6.1 威胁概述

威胁是指可能对资产或组织造成损害事故的潜在原因。威胁可能源于对信息系统直接或间接的攻击，也可能源于偶发的或蓄意的内部、外部事件。威胁只有利用系统存在的脆弱点才能对系统造成影响和伤害，形成风险。

威胁调查主要通过调查问卷、现场观察、问询等方式对信息系统进行提取威胁评估需要的相关信息。

7.6.2 威胁识别

威胁识别的任务主要是识别可能的威胁主体（威胁源）、威胁途径和威胁方式，威胁主体是指可能会对信息资产造成威胁的主体对象，威胁方式是指威胁主体利用脆弱性的威胁形式，威胁主体会采用威胁方法利用资产存在的脆弱性对资产进行破坏。

威胁主体：分为人为因素和环境因素。根据威胁的动机，人为因素又可分为恶意和非恶意两种。环境因素包括自然灾害和设施故障。

威胁途径：分为间接接触和直接接触，间接接触主要有网络访问、语音、视频访问等形式，直接接触指威胁主体可以直接物理接触到信息资产。

威胁方式：主要有传播计算机病毒、传播异常信息(垃圾邮件、反动、色情、敏感信息)、扫描监听、网络攻击(后门、漏洞、口令、拒绝服务等)、越权或滥用、行为抵赖、滥用网络资源(P2P 下载等)、人为灾害(水、火等)、人为基础设施故障(电力、网络等)、窃取、破坏硬件、软件和数据等。

7.6.3 威胁分析

威胁识别工作完成之后，我们将对资产所对应的威胁进行评估，我们将威胁的权值分为 1-5 五个级别，等级越高威胁发生的可能性越大。

威胁的权值主要是根据多年的经验积累或类似行业的历史数据来确定。对于那些没有经验和历史数据的威胁，我们主要根据资产的吸引力、威胁的技术力量、脆弱性

被利用的难易程度等制定了一套标准对应表，以保证威胁等级赋值的有效性和一致性。

根据赋值准则，我们对威胁发生的可能性用频率来衡量赋值：

等级	标识	定义
5	很高	出现的频率很高（或≥1 次/周）；或在大多数情况下几乎不可避免；或可以证实经常发生过。
4	高	出现的频率较高（或≥ 1 次/月）；或在大多数情况下很有可能会发生；或可以证实多次发生过。
3	中	出现的频率中等（或> 1 次/半年）；或在某种情况下可能会发生；或被证实曾经发生过。
2	低	出现的频率较小；或一般不太可能发生；或没有被证实发生过。
1	很低	威胁几乎不可能发生，仅可能在非常罕见和例外的情况下发生。

7.7 脆弱性评估

脆弱性是指资产或资产组中能被威胁所利用的弱点，它包括物理环境、组织机构、业务流程、人员、管理、硬件、软件及通讯设施等各个方面，这些都可能被各种安全威胁利用来侵害一个组织机构内的有关资产及这些资产所支持的业务系统。这些表现出来的各种安全薄弱环节自身并不会造成什么危害，它们只有在被各种安全威胁利用后才可能造成相应的危害。某些目前看来不会导致安全威胁的弱点可理解为是可以容忍接受的，但它们必须被记录下来并持续改进，以确保当环境、条件发生变化时，这些弱点所导致的安全威胁不会被忽视，并能够控制在可以承受的范围内。需要注意的是，不正确的、起不到应有作用的或没有正确实施的安全保护措施本身就可能是一个安全薄弱环节。可以通过手工检查、工具扫描等方式进行脆弱性评估。

7.8 风险评估分析

- 计算安全事件发生可能性

1. 安全事件发生可能性=威胁发生频率值×脆弱性严重程度值
2. 对计算得到的安全风险事件发生可能性进行等级划分

- 计算机安全事件的损失
- 安全事件损失值=资产价值×脆弱性严重程度值
- 对计算得到的安全事件损失进行等级划分
- 计算风险值
- 安全事件风险值=安全事件发生可能性×安全事件损失
- 风险结果判定
- 根据预设的等级划分规则判定风险结果
- 依此类推，得到所有重要资产的风险值，并根据风险等级划分表，确定风险等级。

7.9 设计安全规范

根据《风险评估报告》，服务负责人制定和编写《信息安全管理程序》。并根据信息安全规范制定信息安全策略、针对个人的保密协议、岗位职责说明、机房管理制度。

7.10 实施安全规范

在设计好安全规范后，日常需按照安全规范来实施安全管理。

1) 在人员安全方面的实施：

职位说明中的任务和职责；

安全防护；

针对个人的保密协议；

2) 责任划分的实施，以及岗位分离的实施；

3) 书面的操作指示，内部规章；

4) 安全问题涉及整个生命周期，应针对系统开发、测试、验收、运营、维护和终止制定安全指南；

5) 将开发和测试环境与实际的运营环境分离开来；

6) 处理事件的程序（由事件管理负责处理）；

7) 恢复设施的实施；

8) 为变更管理提供信息输入，病毒防护措施的实施；

9) 针对计算机、操作系统、应用系统、数据、网络和网络服务的安全管理措施的实施；

10) 数据媒介的处理和安全。

7.11 监控安全状况

对安全规范实施进行监控，在工作周报、服务月报中体现。

对发生的信息安全事件按照《事件管理程序》执行。

7.12 维护安全规范

服务管理人员根据系统运行及客户服务的风险变化，必要时对《信息安全管理程序》进行修改。

由于基础架构、组织和业务流程方面的变化导致相关的风险也随着发生变化，因此安全也需要进行维护。

安全维护包括服务级别协议中安全部分的维护以及详细的安全规范的维护。

维护需要根据评估子系统流程的结果以及对风险变化的评估结果进行。这些建议既可以直接被计划子流程所采纳，也可以纳入总体的服务级别协议的维护中。

安全规范更新通过变更管理实施,参照《变更管理程序》。

7.13 风险的处置

对风险应进行处理。对可接受风险，可保持已有的安全措施；如果是不可接受风险（高风险），则需要采取安全措施以降低、控制风险。

对不可接受风险，应采取新的风险处理的措施，规定风险处理方式、责任部门和时间进度，高风险应得到优先的考虑。

风险处理方式说明

标识	描述
保持	现有控制措施完全可以应付或防止此风险的发生，控制措施保持不变
控制	现有控制措施不足或没有控制措施，必须制作重新相应的对策防止此风险 发生

接受	控制现有风险所花费的成本过高、超出公司随范围且风险发生的可能性极 小或没有适当的解决方案，公司决定接受此风险
避免	公司放弃可能涉及此风险的行为，以保证风险不会发生
转移	将风险转嫁至其他公司或第三方人员身上，公司内部不再对此风险作任何 控制措施

- 计划

导出《风险处理计划》。

- 报告

安全管理负责人导出《信息安全风险评估报告》,陈述信息安全管理现状，分析存在的信息安全风险，提出信息安全管理（控制）的建议与措施，提交信息安全管理小组进行审核。

- 审核

信息安全管理小组考虑成本与风险的关系，对《信息安全风险评估报告》及《风险处理计划》的相关内容审核，对认为不合适的控制或风险处理方式等提出说明，由风险评估小组协同相关部门重新考虑信息安全管理小组的意见，选择其他的控制或风险处理方式，并重新提交信息安全管理小组审核，由安全负责人批准实施。

- 实施

各责任部门按照批准后的《风险处理计划》的要求采取有效安全控制措施，确保所采取的控制措施是有效的。

7.14 剩余风险评估

- 再评估

对采取安全措施处理后的风险，信息安全管理小组应进行再评估，以判断实施安全措施后的残余风险是否已经降低到可接受的水平。

- 再处理

某些风险可能在选择了适当的安全措施后仍处于不可接受的风险范围内，应考虑是否接受此风险或进一步增加相应的安全措施。

➢ 审核批准

剩余风险评估完成后，导出《剩余风险评估报告》，报总经理批准。

7.15 信息安全事件管理

信息管理负责人根据信息安全管理的实施状况及日常发生的安全事件等，每季一次巡检，如发生信息安全事件则编写《信息安全服务报告》。

报告可以提供有关已实现安全绩效方面的信息，并可以了解有关的安全问题。

正确地了解有关努力（如安全措施的实施）所取得的效率以及实际被采用的安全措施。

还需要了解所有的安全事件。为报告服务级别协议中定义的安全事件，可通过服务级别管理负责人、事件管理负责人或安全管理负责人与部门经理直接的沟通渠道。

除了在特殊情形下的例外事项，报告都是通过服务级别管理负责人进行传达的。

根据信息安全管理需要报告信息安全的实施情况，并提交给《服务报告》中。

8 信息安全与其他流程的关系

主要与事件和服务请求管理流程、问题管理流程、变更与发布管理流程的接口进行维护和管理。

9 KPI 指标

指标名称	计算公式	考核周期
信息安全事件数量	全年信息安全事件发生数量	年度

10 相关文件

《事件管理程序》

《问题管理程序》

《变更管理程序》

《发布管理程序》

11 相关记录

《信息安全服务报告》

《风险评估报告》

《安全事件记录》