XXXX 集团系统信息安全建设方案

信息安全管理体系

XXXX 集团系统信息安全建设方案

ISMS

目　　录

12 信息安全管理体系（ISMS）

12.1 信息安全管理体系概述

12.1.1 信息安全管理体系及其建立的必要性

信息安全的目的是通过预防安全事件和使安全事件的影响最小化来保证业务的连续性并使业务的损失最小化。

信息安全管理的目的就是在实现信息能够充分共享基础上，同时也能保证信息和其他资产得到保护。

信息安全有三个要素：

- 机密性：保护敏感的信息不被未授权的泄露或很容易被截获。
- 完整性：保证信息和软件的准确性和完整性;
- 可用性：保证在需要时用户可获得信息和至关重要的服务。

ISMS 就是以信息安全的三要素为目标，通过建立 ISMS 模型和管理过程，利用技术和管理的方法达到组织的业务的连续性。

实施信息安全管理原因是：

- 支撑一个组织的信息和系统、应用程序和网络都是组织的重要业务资产。这些资产的机密性、完整性、可用性对于维持组织的竞争优势、现金流动、利益、法律上的适应性和组织的声誉都是至关重要的。
- 一个组织可能会面临广泛来源的，日益增加的威胁。
- 一个组织的系统、应用程序和网络，可能成为严重威胁的目标，其中包括以计算机为基础的欺诈、间谍活动、破坏活动、破坏他人财产的行为以及失败源或灾祸源。
- 新的损害源，诸如来自不断公开报道过的计算机病毒和计算机黑客的威胁，仍在不断地出现。预计这些对信息安全的威胁会越来越广泛，越来越野心勃勃且日益向成熟的方向发展。

带格式的：项目符号和编号

基于上述原因，我们认为建立信息安全管理体系对一个组织来说是非常必要的。信息安全管理体系的建立是为了确保一个组织的信息系统全生命期的安

全。也就是说在整个信息系统的生命期内都要实施安全风险管理，并且随着技术、环境等因素的变化也要不断的改进、修正和完善。

在这种情况下，对于一个组织而言，是否采用信息安全管理体系是一个重大的战略决策。

组织的 ISMS 的设计和实现要受安全和业务需求和目标的影响，也受使用的过程以及组织的大小和结构影响。但是，这些因素及其支持系统随着时间的推移也要发生变化。我们期望，根据 XXX 电子的要求，提出一个完整、有效的信息安全管理体系（ISMS）的解决方案。

12.1.2 建立 XXX 信息系统安全管理体系的应具备条件

要建立一个完整和有效的 ISMS 系统，除了需要配备一定的资源、技术手段外，各级管理层必须：

带格式的：项目符号和编号

要认识到业务信息安全要求以及建立信息安全方针和目标的重要性

要认识到如何实现和运行管理组织的所有业务风险控制方法的重要性。

要认识到监控和评审 ISMS 的执行情况和有效性的重要性。

要认识到基于目标权衡的持续改进的重要性。

要构建一个有效和实用的信息安全管理体系首先要建立信息安全管理体系模型。我们将在下一节叙述这一过程管理的模型。

其次，要构建的管理过程是一个动态过程，每一个过程都有若干信息安全管理活动，并且在执行过程中不断循环。

应当强调的是，信息安全管理体系建立的基础是风险分析和风险评估。风险分析和评估的成败取决于所选择的方法，因此，如何选择实用的风险分析和评估方法是建立信息安全管理体系关键之所在。为了突出其重要性，我们把风险分析和评估单独作为一个文件。信息安全管理体系将利用风险分析和评估的结果作为的基础。其中不仅包括风险分析的结果，还包括安全目标、安全控制措施等。

最后，要特别强调的是：

带格式的：项目符号和编号

5、信息安全管理体系是一个过程管理体系，它突出了过程管理。

6、信息安全管理体系的运行必须得到高级领导层的理解和支持，没有他们的支持这个管理体系是无法很好运行的。

7、信息安全管理体系不仅是过程管理而且是一个动态管理过程，这个过程是一个循环过程，通过反复运行这个过程，使这个过程不断改进、修正和完善。因此，我们不能静态的执行这个管理体系，只有反复执行各阶段的活动，不断修正和改进才能达到预期的安全目标。

8、应当特别注意，运行信息安全管理体系的重要基础是人，因此对人的培训是很好运行管理体系的重要前提。对人员的培训将根据他们在信息安全管理体系中的责任分别进行。

9、信息安全管理体系建设所涉及的人员必须包括：资深的信息安全专家、组织的高层领导、涉及到信息安全管理的中层领导。

12.2 信息安全管理体系模型

正如上节所述，构造信息安全管理体系首先要建立该体系的模型。以往，信息安全管理被认为是制定一系列的安全规章制度而没有建立一个完整的体系。

1995 年英国制订的 BS 7799 第一部分为‘ 实践准则 ’，它提供了帮助各公司落实自己的信息安全系统的‘ 最佳做法 ’指导材料。

1998 年制订的 BS 7799 第二部分则为针对衡量一个组织的安全遵从情况及随后给予认证证书的一览表文件。

2000 年 12 月国际标准化组织发布了 ISO/IEC 17799 信息安全管理的第一个国际标准。这些标准都是实现目标管理，而没有实现动态的过程管理。2002 年英国标准化组织发表了信息安全管理——信息安全管理体系规范的草案。该草案最大的变化是把静态的目标管理变成动态的过程管理。这个变化也能真正体现了信息安全管理的实际。

我们参考了 BS7799-2002 的草案版本，认为 XXX 电子系统 ISM 的构成如图 12.1 所示。

图 12.1　信息安全管理体系模型

该图说明了过程连接的关系。我们把它命名为 Plan-Do-Check-Act（即 **PDCA**）过程模型。该模型可以用于所有的过程控制。

我们为 XXX 电子系统设计的 PDCA 过程模型可以简单描述如下：

计划（Plan）过程（建立 ISMS 的基本要素）：

本阶段的目标是：建立、控制和改善与信息安全相关的安全方针、安全目的、安全目标、安全过程、安全程序，以便提交与组织的所有安全方针和目标相一致的结果。

实行（Do）过程（设计和实现）：

本阶段的目标是：实现安全方针（过程和程序）

检查（Check）（监控和评审）

本阶段的目标是：对照方针、目标、实践经验来量度和评估过程的性能，并把结果报告给决策者。

行动（Act）（改善）：

本阶段的目标是：实现纠正和预防活动以便进一步改善过程的执行情况。

12.3信息安全管理体系建立程序

建立 XXXX 集团系统的 ISMS 过程要素如图 12.2 所示：

图 12.2 ISMS 过程要素

12.3.1 计划阶段

XXXX 集团系统的 ISMS 在计划阶段要执行如下活动 :确定信息安全管理体系的范围、确定信息安全管理方针、确定风险分析和评估的系统方法、用系统方法进行风险分析、识别和评估风险处理的选项、选择风险处理的安全控制目标和安全控制措施。

12.3.1.1 XXXISMS 信息安全管理体系的范围

XXXISMS 管理体系覆盖的范围包括整个 XXX 电子系统，其目的是为 XXXX 集团网络建立完善的信息安全体系框架和制定安全标准。为 XXXX 集团达到资源共享，提高办公效率和质量，提高市、局、县及集团的决策能力、管理能力、应急能力，提供安全保障。为核心业务上网、公文批发上网、集团有关告示/通知上网、服务职能上网等保驾护航。保证电子连续、可靠、安全地运行。

为 XXXX 集团专网建立完整的信息安全保障体系，首先解决填平众多“信息孤岛”间的“数字鸿沟” 及整顿“信息荒岛”中面临的安全问题，初步实现某些关键信息资源的安全共享，以及紧迫业务的安全集成。提出翔实的资源管理中心网络安全实施方案，为实现 XXX 电子专网全部资源的安全共享打下良好的基础，第一期工程争取达到如下具体的建设目标：

带格式的：项目符号和编号

建设安全的信息资源管理中心门户网站；

解决电子专网的入网身份认证，达到“ 单点登录，全网通行 ”的目标；

内部百兆安全电子邮箱问题；

选择部分影响较大、技术和协调难度较低的项目和业务上网，逐步建设安全的网上办公及应用项目；(这一段要改成概述中描述的目标)

12.3.1.2 XXXX 集团系统信息安全管理方针

12.3.1.2.1 制定信息安全方针的必要性和要求

安全方针是制定信息安全管理体系的重要的一步，也是建立 ISMS 系统的基本依据。

信息方针简要描述为什么需要信息安全、安全为什么重要以及说明什么是允许的，什么是不允许等方面的安全主题。通常情况下，方针并不要求变化频繁。方针也包含通用的行政命令，这些命令并不一定和体系结构或系统有关。方针也是强制性的，也就是说，一定要清楚的知道，当发生违反方针的时候，一定要采取强制性措施。方针一定要简明扼要，具有可操作性。

信息安全方针的制定需要考虑四种相关人员，他们是：

- XXX 集团决策相关人员，他们负责对 XXX 重大的集团运行事项做出决策，电子系统建设的重要目标就是保证集团决策的科学性和高效性；
- XXXX 集团业务系统的管理人员，他们负责各自相关专业集团业务领域的业务正常开展，并做出授权范围内相关的决策；
- XXX 业务系统的具体工作人员，这是为 XXXX 集团系统服务的、数量最大的用户群体，电子系统的建设目标之一就是保证集团业务流程高效流转、提高集团工作效率、增加透明度；
- XXXX 集团 IT 相关人员，他们的首要职责是分析 XXXX 集团对信息以

及信息技术的需求，从而建立起业务与 IT 技术的桥梁，是 IT 技术成为集团运行的有效和不可缺少的工具。IT 相关人员还负责确保 XXXX 集团信息系统的正常运行。

信息安全方针就是规定上述四类人员安全使用电子系统的基本原则，即：针对每一类人员（或细分的每一类人员）在什么时间、在何地点、使用什么手段、可以访问哪些信息，可以对信息进行哪些处理，负有哪些安全责任。

安全方针一定要有可操作性，以便相关人员的阅读、理解和执行。

成功的信息安全方针的具有以下特点：

带格式的：项目符号和编号

- 必须基于电子系统的目标和要求，并由业务管理者来指导。
- 必须有来自管理层的明确支持和承诺。
- 必须有对电子系统安全风险及其在机构内的安全程度（等级）的深刻理解。
- 安全必须对所有管理者和集团员工都是有效的。
- 安全方针和标准的综合指南必须发给所有员工和相关人员。
- 内容是全面、合理和可操作的。

12.3.1.2.2 XXXX 集团系统安全方针的构成

XXXX 集团安全方针系统是一个三维的体系，也就是说指定 XXXX 集团安全方针需要同时关注三个方面，即：业务应用领域、行政级别和方针的内容，尤其要关注不同业务领域、不同行政级别部门之间在安全方针上的差异。在具体实施时，究竟是按照行政级别还是根据业务部门来分别制定安全方针，则可根据 XXXX 集团系统的实际建设情况灵活开展，但要注意不同时期所制定方针的兼容性和可追踪性。

对于每一个具体的安全方针应包括以下内容：

- **安全方针的基本原理：**
  - 强调安全方针和安全管理的重要性使得信息共享成为可能；
  - 相关法律法规的要求；
  - 确保组织的资产不受损失。

- **信息安全定义：**
  - 总目标；
  - 信息安全的定义；
  - 支持这些目标和原则的管理意向声明；
  - 确定有关信息安全各方面的责任。
- **信息安全如何运作**
  - 特定的安全方针和要求的说明;
  - 如何对全体员工进行安全必要性的教育;
  - 业务连续性方针;
  - 向委员会和管理机构报告安全事件过程的说明;
  - 权限要求;
  - 授权委员会和管理机构;
- **其它**
  - 任何需要说明的相关信息安全基本问题、规定、规则、流程。

指定信息安全方针是 XXXX 集团实施的基础和出发点，因此必须予以高度的重视和关注，建议用户在具体实施过程中，聘请专业的、有资质的信息安全咨询服务机构提供帮助，并对方针的合理性、科学性进行评审。

12.3.1.3 XXXX 集团风险分析、评估的方法

12.3.1.3.1 必要性

XXXX 集团系统的 ISMS 是建立在信息安全分析和评估的基础之上的。

对 XXX 集团而言，保证以最低的运行成本，取得最大的效果，是进行电子系统建设决策的基本依据。同样，一个正式的风险分析文件就是研究以合理的投入获取可接受的安全水平。

风险分析帮助 XXX 集团机关了解信息系统系统带来的集团运行风险，从而为安全措施的采取提供决策依据。在采用有效风险分析过程的地方，只有实际需要的控制和保障措施才得到实施。一个组织将不再根据审计的要求去实施一些不

必要的安全控制措施。

无论任何时候，只要有资金或者资源的花费，都应进行风险分析。

大多数风险分析失败的原因是因为内部专家和相关专家没有参加。没有人比内部专家了解系统和应用，了解电子系统的运作和业务流程。

为了满足需求，风险分析和评估过程应该尽快完成，尽量不影响组织员工的工作安排。

风险分析和评估是评估当 XXXX 集团信息系统在面临安全威胁时，相关信息资产受到损害的程度，同时也对集团业务开展的影响程度作出评估。通过风险评估，决策人员可以了解信息系统在存在安全威胁的环境下，可能对电子的业务系统正常运转所造成的影响，从而在综合多方面因素后，做出信息系统安全建设的决策。

风险分析和评估使组织管理者检查现在组织关心的所有问题，排列脆弱性等级，然后选择适当的控制水平或者接受风险。

风险分析和评估的目标不是排除所有风险。风险分析只是管理的一种工具，其目的在于了解信息系统对业务系统潜在的安全威胁。

没有高层决策者的支持，风险分析和评估很难进行。风险分析为管理的决策提供信息。风险分析和评估的结果一般要定出适当的保密等级，并提供给高层管理者或者高层管理者认为合适的人。

评定风险分析和评估是否成功的可感受到的方法是看成本是否降到一个更低的范围。风险分析帮助确定必要的仅需要执行的控制措施。另一种评定风险分析和评估成功与否的方法是看管理的决策时间。管理决策越快越证明风险分析越成功。

12.3.1.3.2 风险分析和评估方法简介

风险分析和评估的方法一般有两种：定量的和定性的方法。下面分析这两种主要的方法及它们各自的优缺点。

定量风险分析

定量的风险分析通过一套方法，给出风险分析各组成部分的潜在损失的量化数值。当所有的因素都量化（资产价值、威胁频率、保护措施、有效性、保护措施成本、不确定性和可能性），定量分析的过程就完全地完成了。

定量分析的优点

- 结果主要来源于一系列方法，建立在一定的数学和理论基础。
- 大量的工作集中在资产价值的确定和减轻风险上。
- 成本利益分析是基本的。
- 结果能用管理具体术语表示。（如资金价值、比例、可能性）。
- 分析评估的结果具有一定的可比性。

定量方法的缺点

- 计算很复杂。
- 需要积累历史数据，才可能做出有意义的结果。
- 一般地，定量分析不是一个人完成，需要一定的人力投入。

定性风险分析并不给出风险分析组成部分的量化指标，而是提出“ 如果，怎么样 ”类似问题。它的主观性比较强。

定性分析优点：

- 计算很简单。
- 没必要确定资产的资金价值。
- 非安全公务员和非技术性公务员更容易加入。
- 定量分析具有灵活的方法和报告。

定性分析缺点：

- 定性分析的主观性比较强。
- 结果的准确性与风险分析评估小组人员的经验和素质关系较大。

在实际 XXX 信息系统系统的 ISMS 建设中，单独采取某一种方法，并不一定可行，尤其对于 XXXX 集团信息系统，边规划、边实施的信息系统，更是如此。一般来说，在系统的规划阶段，定性的分析和评估多一些，伴随项目建设工作的开展，尤其是开通运行一段时间后，会逐渐积累各种基础数据，从而使分析和评估更多基于所积累的量化数值。事实上，定性分析往往会成为定量分析的基础，定性与定量分析的框架基本一致，定量分析量化的内容更多一些。

带格式的：项目符号和编号

带格式的：项目符号和编号

带格式的：项目符号和编号

带格式的：项目符号和编号

风险分析和评估的最终结果是提供哪些资产是要保护的最重要的资产以及需要那些安全措施。

风险分析和评估的关键要素包括：

- 识别资产并为资产赋值
- 识别资产的脆弱性
- 识别对资产的威胁
- 识别风险对资产的影响
- 评定资产的保护等级
- 进行风险管理
- 识别安全控制措施
- 执行和降低风险
- 可接受风险分析等。

常见评估过程如图 12.4 所示。

图 12.4　风险分析和评估过程

定性风险分析的核心要素是资产、资产的价值、资产面临的威胁、资产的脆弱性、资产的破坏对业务的影响、为了避免对业务的影响提出的安全要求、满足安全要求的控制措施、控制措施对抗威胁、威胁利用资产的脆弱性对资产实施攻击。

12.3.1.3.3 XXXX 集团信息安全分析评估方法

XXX 电子系统的风险分析和评估是采用的是定性分析法，分析结果参见后续章节，详细内容参见《XXXX 集团信息安全风险分析报告》。

该信息安全风险分析法依赖下列事项：

带格式的：项目符号和编号

（1）组织的信息及其信息系统的性质

（2）组织所属信息运用范围

（3）信息系统使用及操作环境

（4）现有的安全保护措施

安全风险与其他因素的关系如图 12.5 所示。

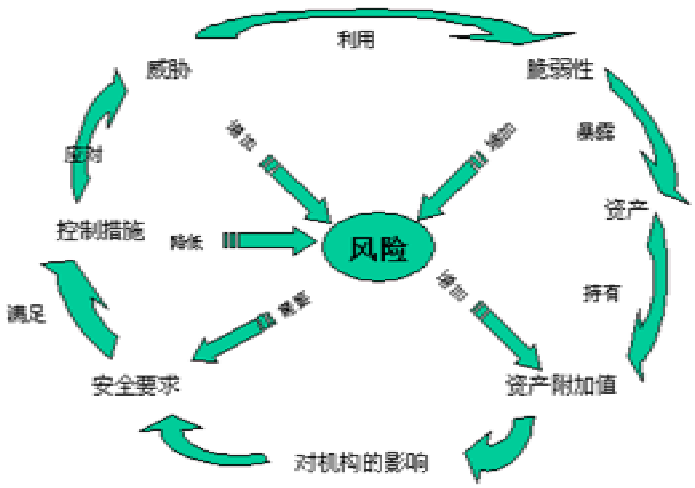

图 12.5　安全风险与其他因素的关系

在采用的定量风险分析方法中，将充分考虑图 12.5 所示的关系。

本信息安全管理体系采用的风险分析和评估的具体方法是：

风险分析过程概述

风险分析流程如图 12.6 所示。

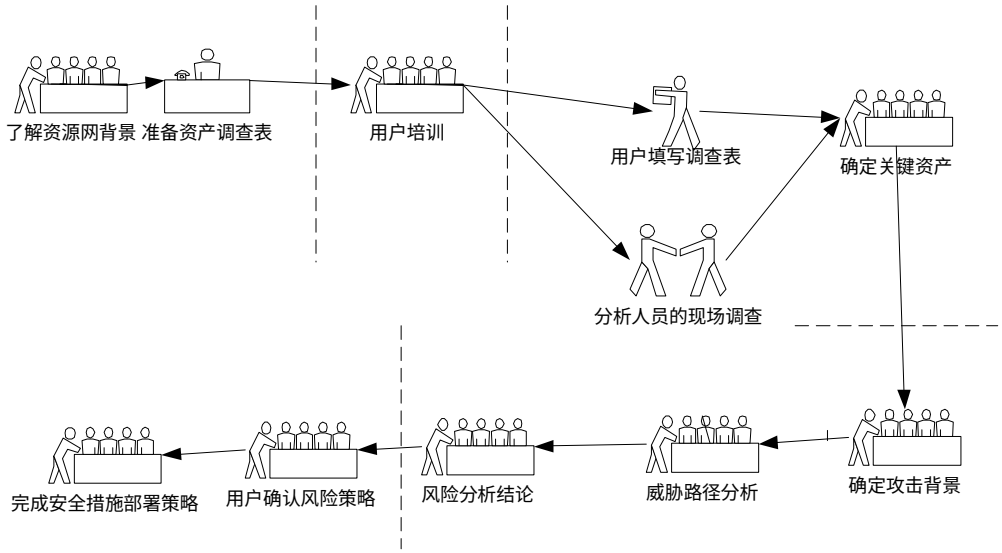

图 12.6　风险分析流程

风险分析基本分为五个阶段，即：

带格式的：项目符号和编号

- 准备阶段：风险分析人员准备各类材料、工具和表格（见附件一）；
- 培训阶段：此阶段，专业人员对用户进行培训，培训的重点在风险分析的目的、内容、方式，帮助用户建立正确的风险观念，理解和配合风险分析工作的开展。培训对象为风险分析涉及的四类人员：用户机构运行决策代表、主要业务部门管理人员代表、主要业务部门普通用户代表、信息系统运行维护责任部门代表。
- 资产确定阶段：此阶段，用户和风险分析人员共同对资源网络系统进行详细的分析，根据资源网的组成结构、功能作用等，确定资源网的关键资产、这些资产的基本安全需求、资产的价值，其中资产基本安全需求是指用户根据应用业务的实际情况，提出的对资产的最基本保护要求，此要求如果无法得到满足，资产将失去再资源网中存在和利用的价值。
- 风险评估阶段。此阶段，风险分析人员同用户一起，确定资源网络中资产面临的安全威胁背景，确定可能的威胁、后果，从而得出每一项资产

明确的风险结论。

- 风险策略阶段。此阶段，风险分析人员将同用户一起讨论，由用户确定每一项资产的风险策略，即：是接受风险还是降低风险，对于用户确定的每一项需要降低风险的资产，风险分析人员将根据威胁路径提出安全措施的部署策略，并向用户明确相应的残余风险。

风险分析方法概述

风险分析采用表格方式，对资源网内每一个识别出的资产，按照该分析法围绕资产的“机密性”、“完整性”和“可用性”三个最基本的安全需求，结合用户提出的其他基本安全需求，针对资源网内的信息流程模型，详细分析系统中可能存在的、针对信息上“三性”的潜在威胁和后果。

为便于分析，我们对每一个威胁因素逐层进行了编号，如：T1.1。

风险分析采用表格方式完成。

风险分析结论

在本方案中，我们将采用定性的方式，对每一类威胁的发生可能性及后果予以评估，并提出相应的安全需求建议。我们威胁发生的可能性分为四个级别，即：A、B、C、D，其中 A 级的可能性最大。后果分为：I、II、III、IV 四个级别，其中：I 级的损失最大。

对于一个制定的资产，其风险可能有 16 种可能，见表 12.1：

表 12.1 可能的威胁表

后果 / 威胁	I	II	III	IV	V
A					
B					
C					
D					
E					

每一种组合则表示一种风险。

12.3.1.4 用系统方法进行风险分析

在确定了系统风险分析和评估方法后，就要实施风险分析。

风险分析的第一步是资产分类，在本风险分析方案中，资产分为如下五类：

表 12.2　系统资产分类表

编号	业务领域名称	简称	简要描述
1	综合决策支持系统	ZHJC	有关领导和部门对城市规划、建设、管理的重大问题决策及城市应急指挥，提供准确、实时的信息支撑及直观、真实的可视化和互操作环境
2	信息共享系统	XXGX	实现 XXX 各机构之间安全、有序的信息资源共享
3	业务整合	ZWZH	实现跨各个信息中心的专网之上的各自业务整合
4	单点登录系统	DDDL	提供全网统一的公务员身份管理系统，实现单点登录，全网通行
5	网络基础设施系统	JCSS	专网的运行基础

在资产分类的基础上，就要对具体的资产进行调查，调查是以填表的方式进行，具体以综合决策支持系统的资产调查为例，调查表如下所示：

业务领域： 综合决策支持系统（ZHJC）

资产类型：

最高管理者资产　业务领域管理者资产　业务人员资产　IT 人员资产

表 12.3　综合决策支持系统资产调查表

编号	资源描述	基本安全需求
信息资产		
I1	**决策原始数据** 来自于各部门的原始数据，供决策人参考、分析的数据	原始数据有一些敏感数据，对机密性、完整性、可用性(准确性)的要求高
I2	**决策** 决策人做出的决策	机密性、完整性有严格要求
I3	**决策过程记录** 对决策过程中调阅数据、参与决策人、系统使用等方面的纪	机密性、完整性、可用性有严格要求

	录，是今后对决策过程合法性、科学性、公正性的检查依据	
I4	**决策系统管理、维护、记录数据** 系统维护人员所使用的数据，记录有相关的权限、配置、账号等信息，以及系统维护操作的信息，是系统正常维护、运行必需的信息	完整性最为重要，可用性其次。
物理资产		
P1	**计算机工作站**	**可用性**
P2	**投影设备**	**可用性**
P3	**后台服务器系统**	**可用性**
P4	**网络系统**	**可用性**
软件资产		
S1	**决策支持系统** 综合决策系统最重要的软件资产	**确保其可用性。** 该软件本身还应具有 :用户身份识别、用户权限控制、输入输出控制的安全功能 ;具有根据一定的安全策略和设置,自动检查和限制用户权力的功能；具有操作审计功能；系统的管理和维护应采取三权分立的原则，防止“ 超级用户 ”的出现。
S2	计算机工作站平台软件系统（包括：操作系统等）	可用性和完整性
S3	**后台服务器系统平台软件系统**（包括：操作系统、数据库系统、Web 系统等）	可用性和完整性
S4	**工具与诊断软件**（如：防病毒软件、系统引导盘等）	可用性和完整性
其它资产		
O1		
O2		
O3		

其它的四种资产也按照同样的方法和表格进行。

第二步将进行威胁分析。

威胁概述

资源网面临的信息安全威胁如下所示。首先要对威胁进行分类。

威胁分为以下几类：

- 不可抗力，由于自然、政治等因素造成的威胁；

带格式的：项目符号和编号

- 组织弱点，由于组织机构、行政制度等因素造成的安全威胁；
- 人为错误，由于人员的技能、培训等方面原因造成的安全威胁；
- 技术缺陷，由于信息技术、产品的设计、实现、配置、使用等造成的安全威胁；
- 故意行为，故意、人为造成的安全威胁；

资源网在整个规划、设计、实施、运行等过程中，都可能面临上述几方面的威胁，本章的重点在于提取出各个威胁对指定资产的可能威胁途径、方法、后果，从而为后面的风险分析打下基础。

威胁分析：

威胁分析也是以列表的方式进行。由于该表非常庞大，这里仅列出不可抗力和组织弱点两项。其他详见风险分析和评估部分。

表 12.4 安全威胁列表

威胁	备注
1、不可抗力	
T1.1 人员丧失	
T1.2 IT系统故障	
T1.3 雷电	
T1.4 火灾	
T1.5 水灾	
T1.6 电缆燃烧	
T1.7 温度和湿度异常	
T1.8 灰尘、尘土	
T1.9 强磁场造成的数据丢失	
T1.10 广域网故障	
2、组织弱点	
T2.1 缺乏信息安全规则，或规则不足	
T2.2 使用人员对安全要求的了解不足	
T2.3 缺乏的资源（如：人力、资金等）	
T2.4 对IT安全措施的监控不足	
T2.5 缺乏管理，或管理不充分	
T2.6 未经授权进入需要保护的房间	
T2.7 未授权使用权限	
T2.8 不加限制地使用资源	

T2.9 当系统使用人员、环境发生变化时，缺乏相应的调整	
T2.10 需要时，数据媒体不可用	
T2.11 带宽规划不足	
T2.22 布线系统文档不足	
T2.23 对电源配线箱的保护不足	
T2.24 对移动计算机用户缺乏管制	
T2.25 数据媒体缺乏标记	
T2.26 对数据媒体的传送处理不当	
T2.27 密钥管不足	
T2.28 用户发生变化时，交接流程考虑不足	
T2.29 审计数据缺乏处理	
T2.30 确保保护措施的网络互连	
T2.31 系统的非正常使用造成传输和执行速率的降低	如：将Win95机器用作服务器
T2.32 软件、系统测试和发布规程缺乏或不足	
T2.33 文档不足或缺乏文档	
T2.34 违反版权	
T2.35 用生成的数据对软件进行测试	生成的数据不一定真实反映实际的应用环境
T2.36 域规划不足	主要指NT的信任域
T2.37 对Windows NT系统的保护不足	
T2.38 线路带宽不足	
T2.39 Netware服务器安放在不安全的环境中	
T2.30 Netware的安全机制缺乏，或安全机制不足	
T2.31 对通信线路的使用缺乏控制	一些远程通信产品（如：modem卡）由一些用户并不清楚的远程通信功能
T2.32 数据库安全机制缺乏，或机制不足	
T2.33 DBMS的复杂度	数据库功能、性能非常复杂，正确选择数据库非常重要
T2.34 数据库访问的复杂度	数据库访问权限的设置非常复杂，正确的设置对于数据库安全非常重要
T2.35 数据库用户更换的安全考虑不足	在多个用户共享一个访问终端时，应仔细设计用户更换的安全
T2.36 NDS复杂性	Novell NDS的配置也非常复杂，正确配置NDS
T2.37 网络部件不兼容	使用不同厂家产品时，并且使用各厂家的专用协议、非标协议时，更需注意
T2.38 对网络应用变化估计不足	
T2.39 超出电缆/总线允许的长度	
T2.40 文件和数据媒体的运输缺乏安全	
T2.41 在家庭工作场所，对数据媒体和文档的处置不当	
T2.42 对远程工作者缺乏培训，培训不足	

T 2.50 由于远程工作者的原因造成的延误	
T 2.51 由于联络和交流的原因，远程工作者完全融入工作流程中	
T 2.52 远程工作人员由于IT系统崩溃而造成响应时间过长	
T 2.53 对于远程工作者的工作缺乏足够的后备人员考虑	
T 2.54 由于的隐藏数据碎片造成泄密	如：文件拷贝泄漏文件所在目录的信息；文件复制时，填充数据泄漏内存数据；……
T 2.55 电子邮件的使用缺乏控制	
T 2.56 对所传送文件的描述不足	
T 2.57 紧急事件情况下，媒体的存储不足	
T 2.59 使用没有登记的部件	
T 2.60 网络系统和管理系统缺乏战略或规划不足	
T 2.61 对个人数据进行非授权的收集	
T 2.62 对安全事故的处理不当	
T 2.64 RAS缺少保护规则	
T 2.65 SAMBA系统配置的复杂性	
T 2.66 缺乏足够的IT安全管理措施	

资产风险评估：

资产风险评估首先要界定资产损失级别，本管理体系的损失级别如表 12.5 所示：

表 12.5 资产损失级别

损失级别	划分原则
I	全系统信息系统资产都受到了损害； 关键信息系统的可用性遭受到了严重损害； 重大的泄密事故；
II	资源中心信息资产受到了严重损害；
III	重要业务系统资产和可用性遭受了损害；
IV	部门的系统资产和可用性遭受了损害；
V	个别公务员资产和可用性遭受了损害；

风险分析结论：

风险分析结论是风险分析的最重要的部分，同样这部分也用表格的方式来表达。首先，把各类威胁出现的可能性分为 A、B、C、D、E 五个等级。这五个

等级中，A 意味这种威胁出现的可能性最大，B 出现的可能性次之，依次类推，E 出现的可能性最小。

威胁对资产的影响是以对资产的机密性、完整性、可用性和其它影响来划分的。用户确认损失的程度分为五级，这五级要由最高领导层和相应的管理者最终确定。

根据威胁出现的可能性、对资产的影响程度和用户确认的的资产损失，最终确定要采取措施克服的威胁。

在本管理体系中，把要对付的威胁分成三种，这三种在以下图表中分别用红色、天蓝色和灰色来表示。

具体表格如下：

表 12.6　用户确认损失列表

威胁	可能性					影响				用户确认的损失					风险	说明
	A	B	C	D	E	保密性	完整性	可用性	其它	I	II	III	IV	V		
1、不可抗力																
T1.2 IT系统故障	V					V	V	V				V			A-III	
T1.10 广域网故障	V						V	V				V			A-III	
T2.25 数据媒体缺乏标记	V							V			V				A-II	
T2.29 审计数据缺乏处理	V					V		V			V				A-II	
T2.32 软件、系统测试和发布规程缺乏或不足	V					V	V					V			A-III	
T2.32 软件、系统测试和发布规程缺乏或不足	V							V				V			A-III	
T2.33 DBMS的复杂度	V					V	V	V			V				A-II	
T2.36 NDS复杂性	V						V		V		V				A-II	
3、人员错误																
T 3.1 由于IT用户失误造成的数据保密性/完整性丧失	V					V	V						V		A-III	
T 3.6 因清洁、外包员工带来的风险			V			V	V	V		V					C-I	
T 3.10 UNIX UNIX下不恰当地共享文件系统	V					V						V			A-III	
T 3.25 因粗心删除东西	V						V	V				V			A-III	
T 3.29 缺乏或不正确的网络分段	V					V		V				V			A-III	

T 3.38 配置和操作错误	V					V	V	V				V			A-III		
T 3.43 不恰当地处理口令字	V					V				V					A-I		
4、技术缺陷																	
T 4.1 断电	V							V		V					A-I		
T 4.7 有缺陷的数据媒体	V						V	V				V			A-III		
T 4.8 缺乏对已知软件漏洞的了解	V					V	V	V			V				A-II		
T 4.13 后备存储的数据丢失	V					V	V	V			V				A-II		
T 4.22 软件存在漏洞或错误	V					V	V	V		V					A-I		
T 4.22 软件存在漏洞或错误	V							V		V					A-I		
T 4.31 网络设备故障或丧失功能	V							V			V				A-II		
T 4.32 通过不可靠的方式传送重要信息	V					V		V		V					A-I		
T 4.39 软件设计缺陷	V					V						V			A-III		
T 4.39 软件设计缺陷	V							V				V			A-III		
5、故意行为																	
T 5.7 搭线	V					V				V					A-I		
T 5.10 滥用远程维护端口	V					V		V				V			A-III		
T 5.18 口令的强力攻击			V			V				V					C-I		
T 5.21 特洛伊木马	V					V				V					A-I		
T 5.23 计算机病毒	V					V		V		V					A-I		
T 5.28 拒绝服务攻击	V							V			V				A-II		
T 5.42 社会工程攻击	V					V	V	V			V				A-II		

威胁	可能性					影响					用户确认的损失					风险	说明
	A	B	C	D	E	保性	密性	完整性	可用性	其它	I	II	III	IV	V		
1、不可抗力																	
T1.1 人员丧失			V			V		V				V				C-II	
T1.8 灰尘、尘土				V			V	V					V			D-III	
2、组织缺陷																	
T2.1 缺乏信息安全规则，或规则不足		V				V	V	V					V			B-III	
T2.2 使用人员对安全要求的了解不足			V			V	V	V					V			C-III	
T2.6 未经授权进入需要保护的房间			V			V	V	V						V		C-IV	

T2.9 当系统使用人员、环境发生变化时，缺乏相应的调整			V			V					V					C-II	
T2.22 布线系统文档不足			V					V					V			C-IV	
T2.23 对电源配线箱的保护不足			V					V					V			C-IV	
3、人员错误																	
T 3.18 共享目录、打印机、文件等					V	V					V					E-II	
4、技术缺陷																	
T 4.3 已有物理安全措施失效			V			V	V	V			V					C-II	
T 4.4 环境因素引起线路损伤				V				V				V				D-III	
T 4.5 串扰和电子感应			V					V				V				C-III	
T 4.43对网络访问行为的审计和记录质量太差			V			V		V					V			C-IV	
5、故意行为																	
T 5.1 IT设备及附属设备被控制或破坏			V					V					V			C-IV	
T 5.3 非法进入建筑物			V			V		V				V				C-III	
T 5.4 偷窃			V			V		V				V				C-III	
T 5.5 有意破坏			V			V		V				V				C-III	
T 5.15 好奇的员工	V					V		V					V			A-IV	
T 5.17外部人员在维护工作中造成的威胁		V				V		V					V			B-IV	
T 5.19 滥用用户权限		V				V							V			B-IV	
T 5.24 信息重放			V			V		V					V			C-IV	
T 5.25 伪装		V				V							V			B-IV	
T 5.26 分析信息流		V							V			V				B-III	
T 5.27 抵赖对消息的接受/发送			V			V						V				C-III	
T 5.29 非法复制数据介质		V				V						V				B-III	

威胁	可能性					影响				用户确认的损失					风险	说明
	A	B	C	D	E	保密性	完整性	可用性	其它	I	II	III	IV	V		
1、不可抗力																
T1.3 雷电				V				V						V	D-V	
T1.4 火灾				V				V						V	D-V	
T1.5 水灾				V				V						V	D-V	
T1.6 电缆燃烧					V			V						V	E-V	
T1.7 温度和湿度异常				V			V	V					V		D-IV	
T1.9 强磁场造成的数据丢失				V			V	V				V			D-III	
T1.11 地震				V				V						V	D-V	
2、组织缺陷																
T2.3 缺乏的资源（如：人力、资金等）				V		V	V	V					V		D-IV	
T2.34 违反版权					V	V	V	V					V		E-IV	
T2.34 违反版权					V			V					V		E-IV	
3、人员错误																

T 3.34不恰当地配置网络管理系统					V		V		V			V			E-III	
4、技术缺陷																
5、故意行为																

在本管理体系中，红色所表示的风险是后果严重的风险，蓝色次之，灰色再次之。

12.3.1.5 风险管理策略

XXX 应对每一个识别的风险制定详细的风险处理计划。风险处理计划是确定减少不可接受的风险以及实现保护信息所要求的控制措施的协调一致的文档。需要识别剩余风险的接受水平并且对每一个这样的风险也要识别出相应的活动。

（1） 接受剩余风险

（2） 转移风险

（3） 降低风险到可接受的水平

并不是总能把风险降低到在一定费用范围的可接受水平，那么就需要确定是否要加更多的控制措施或接受更高的风险。

在规定可接受风险水平时，要把控制措施的强度和费用与潜在的意外事件的费用相比较。

对于 XXXX 集团系统，其风险级别如表 12.7 所示：

表 12.7 XXXX 集团系统风险级别描述

后果 / 威胁	I	II	III	IV	V
A					
B					
C					
D					
E					

我们建议的策略如下：

对于表中红色区域代表的风险，是属于后果严重的安全风险，用户必须采取措施予以应对，以保护相应的信息资产；绿色区域对应较为严重的风险，用户应予以关注，具体措施的采取可以根据工程的进展和用户投入的实际情况予以确定；灰色区域对应较轻的安全风险，用户予以关注，可不在近期的投资中考虑降低的安全措施。

附录 A 提供一些一般相关的控制措施。

12.3.1.6 选择风险处理的控制目标和控制措施

附录 A 列出了 BS7799 标准中的安全目标和控制措施，本方案据此提出了 XXXX 集团系统所需要实施的安全控制措施，具体内容参见《XXXX 集团系统信息安全风险分析评估报告》第 8 章。

本方案所选择的安全控制措施的实施要点和要求，参见 3.2 节。

12.3.1.7 定期风险分析

风险分析和评估是了解 XXX 电子系统安全现状的唯一手段，而系统的安全状态并不是一成不变的，因此，风险分析和评估必须定期进行，制定合理的风险分析计划。

我们建议 XXXX 集团系统定期进行重要资产的风险分析和评估，如每 1 年对整个系统进行系统级的风险分析。

12.3.2 执行阶段

PDCA 循环中的执行活动是为了实现符合计划阶段所做的决定，而所选择的控制措施和管理信息安全风险的相应的活动。

下面将列出本方案所选择的信息安全控制措施，以及其实现要点：

12.3.2.1 安全方针

在安全方针方面，我们重点实现的安全措施有:

- 建立安全策略宣贯体系

XXXX 集团的信息安全策略宣贯体系包括：安全策略文本的起草、发布、宣传、贯彻、监察等方面，其目的是确保所制定的信息安全策略为所有相关的责任人所了解和熟悉，并指导其日常的访问信息系统的活动。

- 建立安全策略评审与评估体系

安全策略的评审和评估应该定期进行，评审评估体系是为确保安全策略的科学性、有效性、可用性、适用性而设计实施的，其内容包括：评审评估周期、评审评估素材、评审评估流程、评审评估方法、评估评审结论认可流程、评估评审结论的发布等。

12.3.2.2 安全组织

在安全组织方面，我们重点实现下列安全措施：

- 设立信息安全的领导机构

XXXX 集团系统将按照行政级别，逐级、逐部门设置信息安全领导机构，每一级领导机构均由该级别集团机构的管理决策人负责牵头，同时每一级领导机构向上一级领导机构负责，负责执行上一级领导机构确认的安全策略在本级机构内的实施，并负责指定实施本机构进一步的安全策略和要求。

- 定期开展信息安全协调

XXXX 集团系统将建立各个级别的信息安全协调体系，该体系将设立固定的信息安全沟通方式、定期的信息安全通报（建议每周）、不定期的信息安全研讨和讨论（至少半年一次）。

- 定义信息安全责任

XXXX 集团信息系统将建立明确的信息安全责任制，明确规定信息系统系统相关的所有人员——公务员对相关信息负有的安全责任。

- 建立信息处理设施的授权过程

XXXX 集团系统将建立各级机关相应的信息处理设施授权过程，信息处理设施将涉及网内的所有物理资产、软件资产和部分的信息资产。（资产可参见《XXXX 集团信息安全风险分析报告》。

- 建立专家的咨询体系

XXXX 集团系统将建立固定的专家咨询体系，建立市级信息安全专家咨询组，同时鼓励各级机构建立自己的信息安全专家班子。XXXX 集团专家咨询组将采取商务合同的方式，明确专家咨询组的任务和职责，同时对专家组提供的咨询时间、咨询意见质量提出要求，并要求专家组对所提供的咨询意见负建议责任。

- 建立与其他安全机构的合作

XXXX 集团系统信息安全合作对象包括三个方面，即：信息安全主管部门、信息安全测评机构和信息安全专业公司。XXX 将在充分遵守主管部门规定、国家法令、法规的基础上，建立与主管部门的合作；信息安全测评机构将作为 XXX 信息安全体系的外部测评的依托对象；信息安全专业公司在做好信息安全产品供应的同时，XXX 将选择专业的服务公司，提供信息安全咨询、评估、外包服务。

- 建立信息安全的独立评审体系

XXX 将依托国家授权的信息安全测评机构作为信息系统系统的授权独立评审机构，该机构负责对 XXXX 集团系统的相关的方案、规划、策略等进行评估和评审。

- 对外部用户访问的风险进行管理

系统中将针对外部用户的访问采取安全措施，其中包括技术和管理措施。技术措施中包括：防火墙、权限控制系统等，具体内容可参见《XXXX 集团技术方案》报告相应内容。

- 与外部用户签署安全责任书

作为对外部用户访问安全风险的管理措施之一，作为统一的规定，将要求使用 XXXX 集团系统的外部用户都必须签署安全责任书（通过集团门户访问公众服务的社会公众除外），并做出相应的安全责任承诺。

- 外包合同应有信息安全条款

作为对外部用户访问安全风险的管理措施之一，作为统一的规定，XXXX 集团所有外包合同都必须包括相应的信息安全条款，以规定外包服务上的安全责任。

12.3.2.3 资产分类和控制措施

再资产分类方面拟采取以下措施：

- 建立资产清单

XXX 将建立统一的电子资产清单分类标准，并要求所有的单位按照该标准建立自己的信息资产清单。资产清单是信息安全风险分析的基础，是安全措施保护的对象。

- 建立信息分类原则

XXX 将建立统一的信息系统分类标准和原则，XXX 各级集团机关将据此对自己的信息进行分类和保护。

● 建立信息标识和处理程序

信息标识一般指用在信息存储介质上，用来表示媒体所承载信息的性质、用途、分类的标识。表示一般用人易懂的语言和方示表示。XXX 将对电子所涉及的信息媒体标识的方法、内容、建立标识流程、销毁标识流程、 标识的责任等做出明确规定。

12.3.2.4 人员安全

（1） 定义工作职责中的安全责任

XXX 将建立整个电子使用的统一的安全责任定义,对系统所涉及的所有集团人员的安全责任进行定义，其中包括：各级集团决策人员、各专业集团业务管理人员、普通公务员、IT 相关人员。

（2） 建立人员资质审查方针

对信息系统的重要管理、维护人员建立资质审查制度，其中包括：系统管理员、数据库管理员、网络管理源等；对外部服务和合作单位也建立资质管理制度；定期对所有相关的资质进行检查。

（3） 与公务员签署保密协议

（4） 建立定期的信息安全教育和培训体系

XXXX 集团信息系统应建立完整的培训体系，培训体系构成如下：

- 培训对象为 XXXX 集团相关的：决策人员、集团业务管理人员、普通集团工作人员、IT 人员；
- 培训内容：政策法规、XXXX 集团信息安全策略、基本安全规则、安全知识、专业安全技能（针对信息安全专职人员）；
- 培训计划：XXX 应确保所有公务员每年能够接受至少一次，为期半天的信息安全培训；信息安全专职人员每年接收 3 天的专业培训；系统安全管理责任人员，每年不小于 24 小时的实际操作培训；每一级部门、机构都应指定自己的信息安全培训计划；

带格式的：项目符号和编号

带格式的：项目符号和编号

带格式的：项目符号和编号

带格式的：项目符号和编号

● 建立信息安全培训评估体系，对所有培训活动的效果进行评估和评价。

（5） 建立安全事故报告制度

包括：报告的流程；报告的机构；报告的内容；报告的时间要求等。最重要的报告流程就是安全事故的报告和应急处理流程，可参见《XXXX 集团系统技术方案》中相关章节。

- 建立安全弱点报告制度

  作为信息安全协调工作的一个组成部分进行规定。

- 建立软件故障报告制度

  作为信息安全协调工作的一个组成部分进行规定。

- 建立安全事件中分析总结制度
- 建立违规处置制度

这是与处罚相关的制度，是一个非常重要的管理措施，规定对信息安全相关责任人的处罚规定。

12.3.2.5 物理和环境安全

XXX 将在以下方面做出统一的规定：

- 建立基本的物理安全边界；
- 应在重要的信息处理设备进出口设置保安设施；
- 办公室、处所等处信息设施的物理安全；
- 对所有信息设备采取物理保护措施；
- 保障电力供应；
- 保护传输电缆；
- 设备定期维护；
- 保障离开安全区域的设备安全，尤其是送修、借用、移动办公、临时办公、现场办公、联合办公设备的安全；

- 建立设备报废或再启用安全安全流程；
- 建立清桌面及屏幕制度；
- 建立资产的转移制度。

12.3.2.6 通信和运行管理

XXX 针对系统运行，将在以下方面建立相应的管理制度：

- 建立文挡制度；

将对电子系统从规划、设计、实施、验收、运行、升级等各个环节的文档种类、内容提出要求。

- 建立统一的设备操作制度；
- 书面化安全事件管理程序；
- 建立开发与运行设备、环境的隔离措施；
- 建立电子系统外设施的使用管理规定；
- 建立系统容量监控和定期规划体系；
- 建立系统验收体系；
- 采取恶意软件的防制措施（参见《技术方案》）；
- 建立数据备份体系（参见《技术方案》）；
- 建立操作者日志系统（参见《技术方案》）；
- 建立故障记录系统；
- 建立可移动计算机介质的管理体系；

此管理体系除了管理制度外，还有相应的技术手段予以支持。

- 建立介质的报废处理体系；
- 对系统文挡采取安全保护措施；
- 签订信息及软件交换协议；

XXX 将对软件和信息交换建立统一的制度，以保护版权，确保软件和信息的质量。

- 对软件、数据传递中采取安全保护措施，建立统一规定；
- 建立电子邮件的安全保护体系（参见《技术方案》）；
- 建立电子办公系统的安全保护体系；
- 建立信息公开发布制度。

12.3.2.7 访问控制

XXX 将在以下几个方面采取安全措施：

- 文档化所有资产访问控制要求；
- 建立用户注册管理系统；

XXX 将建立基于 CA 的统一公务员身份管理系统，具体细节参见《技术方案》相关章节。

- 建立特权管理体系；

与用户注册管理系统相一致，建立配套的特权和权限管理系统。

- 建立用户口令管理体系；

与用户注册管理系统相一致，建立配套的口令管理系统。

- 建立用户访问权限的审核制度；
- 无人值守的用户设备安全保护规定；
- 建立使用网络服务的策略和管理体系；

对网络使用的一些基本试想做出统一规定，如：对拨号服务使用的规定等。

- 对服务访问路径进行保护；
- 建立用户鉴别体系

XXXX 集团系统将建设统一的用户单点登录系统，参见技术方案相关章节。

- 建立网络节点鉴别体系；
- 对远程诊断端口进行保护；
- 建立适当的网络内部的隔离体系（参见《技术方案》）；
- 对网络路由进行控制和安全保护；

- 建立网络服务的安全控制和保护体系；
- 设立统一的登录程序——单点登录（参见《技术方案》）；
- 对系统应用程序进行安全保护；
- 采取终端超时保护措施；
- 采取连接时间限制措施；
- 对信息访问的采取限制措施；
- 对敏感系统的建立隔离(或专用)保护环境（参见《技术方案》）；
- 建立安全事件记录系统；

主要通过审计系统实现，参见《技术方案》。

- 对系统实施监控；

监控系统包括安全事件的监控（IDS 和审计）和安全设备的监控（安全资源管理中心），参见《技术方案》。

- 对移动计算机采取保护措施；
- 严格限制远程连网。

12.3.2.8 系统开发和维护

XXX 将在以下方面开展工作：

- 在所有系统的规划中提出安全需求和规范；
- 要求应用系统应对输入合法性进行确认；
- 要求应用系统应对处理的结果正确性进行检查；
- 采取内容完整性保护措施；
- 建立加密体系；

为电子建立完整的加密体系，实现从信道、网络、应用、存储等国层面、多级别的加密体系，有关内容参见《技术方案》。

- 对软件安装采取统一的安全措施；
- 对系统测试数据采取统一的保护措施；

- 对源程序库采取保护措施；
- 对操作系统变更的实施结果进行安全评估；
- 对已安装软件变更（如升级、重新安装等）进行安全控制；
- 对隐蔽通道和特洛伊木马采取防范措施；
- 对外包软件开发实施安全控制。

12.3.2.9 业务连续性管理

- 建立系统连续性计划

对电子系统一旦发生严重问题后，业务的开展和延续做出规划。

- 建立系统连续性计划测试、维护和评估体系

12.3.2.10 符合性安全措施

XXXX 集团系统将建立一整套的符合性安全措施，以便为相关法律活动提供依据和证据。

- 保护知识产权；
- 建立信息安全策略和技术符合性的评审体系；
- 建立系统审计体系；
- 系统审计工具的保护。

12.3.2.11 管理资源

为确保执行阶段各项安全措施的实施，XXX 要在相关资源：人力、资金等方面予以保障，并将其列入到信息系统系统投资中，需要特别指出的示：信息安全是一个动态的信息系统保护体系，是信息系统日常运行维护的一个重要促组成部分，运行阶段的安全甚至比规划和建设阶段的安全更为重要，因此，必须保证在运行阶段的相关资源投入。

12.3.3 检查阶段

12.3.3.1 定期检查的必要性

检查活动的目的是保证安全控制措施能有效工作并能达到预期目的。如果发

现这些控制措施不适当，则应及时进行纠正。

定期检查，即是对不当措施进行纠正的必要性体现在：

（1） 维护 ISMS 文档的内部的一致性。互相矛盾的文档不仅不利于确保系统的安全，而且可能引发更为严重的后果；

（2） 如果不能对安全措施及时进行纠正，会使整个系统的安全风险增加，甚至到不可承受的地步。

12.3.3.2 检查的内容

XXXX 集团安全检查，尤其是周期性的检查内容有:

（1） 各类审计数据的定期分析和检查；

（2） 各类安全措施相关文档的定期检查和分析，保证措施得到完全的贯彻和实施；

（3） 定期的安全漏洞检查和脆弱性分析；

（4） 其它需要定期检查的内容；

（5） 对合作伙伴提供信息的检查，从中获得 XXX 改进的依据；

（6） 定期对整个管理体系进行检查，确保其有效性。

所有检查和评审活动，都应按照程序，正规进行。保证定期实施正规评审。

12.3.4 行动阶段

12.3.4.1 简介

为了使 ISMS 更有效，要定期进行评审和改进。

行动阶段根据检查阶段的结论，对 ISMS 相关内容进行改进和提高。

有时可以检查结论对安全的现时状态是满意的，行动阶段注意力要集中在对 ISMS 未来可能要改变的技术、业务要求，同时对新冒出来的威胁和脆弱性予以关注，以便保证 ISMS 在未来是持续有效的。

行动阶段的主要工作内容有两项，即：对安全措施的改进和对未来趋势的分析

12.3.4.2 对安全措施的改进

根据检查阶段的结论，对识别出有问题的安全措施进行改进和提高。

根据安全策略、风险分析的要求，对已经发生的安全事件采取相应的安全措施，以确保信息安全事件不再发生。

安全措施的改进可能涉及的面非常广，也可能很少，根据系统建设、使用情况的不同而变化。

在某些情况下，行动阶段与系统的建设、实施和升级工作是整合在一起，同时进行。

12.3.4.3 对未来趋势的分析

行动阶段的重要工作之一就是对未来的趋势进行分析，分析的依据是系统当前的安全状态，以及相关 IT 技术、安全威胁等的发展趋势。趋势分析的目的是对今后 ISMS 体系的建设、完善提出工作依据，使 ISMS 能够不断提高和完善。

12.4适用性声明

作为一种选择性的标准（除安全方针外，不存在强制性控制措施）要求适用性声明是最基本的。

用户可用适用性声明来评价信息安全管理体系。

适用性声明在第三方评估时是一份关键性文件。

适用性声明是对组织选择适合其业务需求的目标和控制措施的评判。声明也记录排除在外的任何安全控制措施。

适用性声明是一份证明组织是如何控制风险的文件。声明不能详细给出有价值的信息以免由此造成安全的破坏。声明可能被潜在的贸易伙伴或者作为一个单独的文件或者作为发证组织所发证书的正式附件，因此可能成为公开的文件。

声明应当说明已经做的、可能做的和不能做的。

声明可能有一个以上，它对认证来讲是十分重要的。

从新评估系统，组织必须认识到风险评估和风险管理并不是一次性的事件，ISMS 必须清明确给出如何进行系统重新评估和升级的管理和运行程序。

13 安全目的符合性

13.1局域网计算环境安全目的符合性

13.1.1 安全目的符合性声明

为保护局域网计算环境的安全，本方案采用了如下的安全措施以达到相应的安全目的：

(a) 硬件标识身份认证系统能实现对用户主体的身份鉴别；

(b) 硬件标识身份认证系统提取的用户设备关键的、不易更换的硬件信息以识别用户硬件设备的真实性；

(c) 安全电子邮件系统支持邮件加密功能。

(d) 安全电子邮件具有邮件投递证明和邮件接收证明功能。

(e) 安全电子邮件系统支持邮件签名功能。

(f) WEB 服务器防护系统对服务器防御具有实时性。

(g) WEB 服务器防护系统能有效防御任何形式的网络攻击行为，无论是否知道攻击的特征。

(h) WEB 服务器防御系统能防止用户对系统注册表的未授权修改、对系统文件系统的未授权修改、未授权启动非法进程、未授权启动非法网络连接。

(i) WEB 服务器防御系统能在合法用户的误操作产生效果之前阻止行为的发生。

(j) 数据库对用户使用了双因子身份认证保证了用户身份和安全属性的真实性，大大增强了对用户的鉴别，能抗击用户粗心删除有用的数据。

(k) 数据库基于身份的强认证和基于属性的访问控制，大大减少用户失误造成数据完整性和机密性的丧失。

(l) 数据库对用户的基于安全属性的访问控制的保护和自动备份，并对控制文件、日志文件进行了保护，使得用户大大减少了文件损失。

(m) 数据库由于可对用户数据、文件、整个数据库进行了有效的备份，避免了由于ＩＴ故障、ＩＴ广域网故障造成用户文件、数据及数据库管

理系统造的损失明显的减少。

（n） 数据库的逻辑、物理备份，脱机和联机备份使得用户失误、粗心及ＩＴ系统故障的损坏信息的情况大大降低。

（o） 由于数据库身份认证依靠了操作系统，减少了ＤＢＭＳ的复杂性。

（p） 主机检测系统具有检测主机入侵、恶意代码驻留的能力。

（q） 主机检测系统扫描检测主机脆弱性的能力。

13.1.2 安全目的符合性对应表

威胁	风险	应对安全措施	对应章节
T 4.32 ：通过不可靠的方式传送重要信息	A-I	7.4.4	6.2.2.1.3-(3)-(a) 6.2.2.2.3-(2)-(a)
T5.10: 滥用远程维护端口	A-III	5.2.1, 7.4.5	6.2.2.1.3-(3)-(d)
T5.18: 口令的强力攻击	C-I	7.5.4, 8.3	6.2.2.1.3-(3)-(b) 6.2.2.1.3-(3)-(f)
T 5.28 拒绝服务攻击	A-II	8.1.1	6.2.2.1.3-(3)-(b)
T3.1：由于IT用户失误造成的数据保密性/完整性丧失	A-III	7.4.2, 7.4.3, 7.5.1, 7.5.3	6.2.2.2.3-(2)-(a) 6.2.2.2.3-(2)-(b) 6.2.2.2.3-(2)-(e) 6.2.2.2.3-(2)-(f)
T2.36: NDS复杂性	A-II	6.3.2	6.2.2.3.5-(3)
T 3.25 因粗心删除东西	A-III	8.2.1	6.2.2.3.5-(3) 6.2.2.3.5-(5) 6.2.2.3.5-(7)
T 3.38 配置和操作错误	A-III	8.1.1, 4.2.1,8.5.1 4.3.1,4.3.2,4.3.4	6.2.2.3.5-(3) 6.2.2.3.5-(5) 6.2.2.3.5-(7) 6.4.2.3
T 4.8 缺乏对已知软件漏洞的了解	A-II	4.2.1,4.3.2 ,4.3.1,4.3.4,6.3.2	6.2.2.3.5-(7) 6.4.2.3
T 4.22 软件存在漏洞或错误	A-I	4.3.2, 4.3.1,4.3.4,6.3.2,	6.2.2.3.5-(7) 6.4.2.3
T 4.39 软件设计缺陷	A-III	6.3.2	6.2.2.3.5-(7)
T 5.21 特洛伊木马	A-I	4.3.1,6.3.2, 4.3.4	6.2.2.3.5-(3) 6.2.2.3.5-(6) 6.4.2.1, 6.4.2.2
T 5.23 计算机病毒	A-I	4.2.1,4.3.1. 6.3.2	6.2.2.3.5-(3) 6.2.2.3.5-(6) 6.4.2.2

T2.32 软件、系统测试和发布规程缺乏或不足	A-III	4.3.2, 4.3.1,4.3.4, 6.3.2,	6.4.2.2
T2.33 DBMS的复杂度	A-II	4.3.1,4.3.4,,6.3.2,	6.4.2.3
T 3.10 UNIX下不恰当地共享文件系统	A-III	,4.3.2, 4.3.4, 4.3.1,4.3.5,6.3.2, 7.5.3, 8.5.1	6.4.2.1, 6.4.2.3
T 3.43 不恰当地处理口令字	A-I	4.2.1, 4.3.1,4.3.2,4.3.4,	6.4.2.3

威胁	风险	应对安全措施	对应章节
T2.9 当系统使用人员、环境发生变化时，缺乏相应的调整	C-II	8.1.1	6.2.2.1.3-(3)-(b)
T5.19: 滥用用户权限	B-IV	7.4.3, 7.4.4, 7.4.9, 7.5.1, 7.5.3, 8.5.4	6.2.2.1.3-(3)-(a) 6.2.2.1.3-(3)-(d) 6.2.2.3.5-(4) 6.2.2.3.5-(5) 6.2.2.3.5-(6) 6.4.2.1
T5.24: 信息重放	C-IV	8.3	6.2.2.1.3-(3)-(f) 6.2.2.2.3-(2)-(d)
T5.25: 伪装	B-IV	6.3.2, 8.3	6.2.2.1.3-(3)-(C) 6.2.2.1.3-(3)-(e) 6.2.2.1.3-(3)-(f)
T5.26：分析信息流	B-III	8.3	6.2.2.1.3-(3)-(f)
T5.27：抵赖对消息的接受/发送	C-III	6.7.4, 8.3.3, 8.3.4	6.2.2.2.3-(2)-(a) 6.2.2.2.3-(2)-(f)
T 3.18 共享目录、打印机、文件等	E-II	6.3.2,7.5.3, 8.5.1	6.4.2.3
T 5.15 好奇的员工	A-IV	5.2.5,7.5.1,7.5.3, 8.5.4,	6.4.2.1

13.2边界安全目的符合性

13.2.1 安全目的符合性声明

为保护网络边界的安全，本方案采用了如下的安全措施以达到相应的安全目的：

（1） 物理隔离安全网闸装配于内外网络边界，能实现网络级的物理隔离；

（2） 物理隔离安全网闸具有严格的失效保护功能；

（3） 物理隔离安全网闸能自主可控地实现内外数据交换，数据交换应达到

要求的速率；

(4) 物理隔离安全网闸能避免基于 TCP/IP 协议漏洞的攻击。

(5) 物理隔离安全网闸阻断了内外网络之间任何存活的连接；

(6) 物理隔离安全网闸能一定程度防止拒绝服务攻击等传统难于抵抗的攻击，如 DOS 攻击；

(7) 单硬盘物理隔离卡使用两套独立的操作系统、物理分离的两套存储和工作区，对于断电后会丢失信息的部件，如内存、处理器等暂存部件，在网络转换时能进行彻底清除处理，有效防止残留信息串网；

(8) 单硬盘物理隔离卡能阻止通过修改系统配置，植入攻击代码或破坏隔离功能；

(9) 单硬盘物理隔离卡提供强制户使用隔离功能的技术手段，使用户不能轻易旁通物理隔离功能；

(10) 防火墙可以使用双机热备，避免由于本身故障造成的网络中断；

(11) 防火墙可以避免由于用户配置不当造成系统开放无用端口或服务而给入侵者带来的方便之门；

(12) 安全远程接入系统可以保证移动用户通过拨号线路远程访问专网的安全；

(13) 防病毒软件采取对恶意软件的防制措施，建立用户口令管理体系，建立使用网络服务的策略和管理体系，对远程诊断端口进行保护；

(14) 漏洞扫描检查边界出入口的关键网络设备存在的安全隐患；

(15) 漏洞扫描检查局域网网络设施的安全隐患；

入侵检测系统可有效发现来自外部访问人员的违规行为，可探测网中不应出现的行为，包括内部人员的行为，如口令猜测等。

13.2.2 边界安全符合性对应表

威胁	风险	应对安全措施	对应章节
T1.2 IT 系统故障	A-III	5.2.4, 6.1.3, 6.2.2, 6.3.2, 6.4.2, 6.4.3, 6.6.3, 6.7.4, 6.7.5, 7.1.1, 7.2.2, 7.2.3, 7.4.2, 7.4.5, 7.4.6, 7.4.8, 7.4.9, 7.5.1, 7.5.3, 7.5.5, 7.5.7, 7.5.8, 7.6.1, 7.6.2, 7.7.1, 7.7.2, 8.2.4, 8.3, 8.3.3, 8.3.4, 8.5.4, 10.2, 10.3.1 6.1.5 ,6.6.4, 7.4.3, 10.3.2	7.2.1.1.4-(1) 7.2.1.1.4-(2) 7.2.1.1.4-(3) 7.1.2
T5.10: 滥用远程维护端口	A-III	5.2.1, 7.4.5, 5.1.1, 0.2	7.2.1.1.4-(7) 7.1.2

			7.3.1.2-9-1, 7.3.1.2-9-2, 7.3.1.2-9-4, 7.3.4.2-2
T4.8 缺乏对已知软件漏洞的了解	A-II	6.3.2, 8.1.1, 10.2 .4.1, 6.4.3	7.2.1.1.4-(5) 7.2.1.1.4-(7) 7.1.2 7.3.1.2-9-1, 7.3.1.2-9-3, 7.3.4.2-1
T4.22 软件存在漏洞或错误	A-I	6.3.2, 8.1.1, 6.1.1, 8.5.5	7.2.1.1.4-(5) 7.2.1.1.4-(7) 7.3.1.2-9-1, 7.3.1.2-9-3, 7.3.4.2-1, 7.3.4.2-2
T4.31 网络设备故障或丧失功能	A-II	7.4.9	7.2.1.1.4-(1) 7.2.1.1.4-(2)
T4.39 软件设计缺陷	A-III	6.3.2, 8.1.1	7.2.1.1.4-(5) 7.2.1.1.4-(7) 7.3.1.2-9-1, 7.3.1.2-9-3, 7.3.1.2-9-5, 7.3.1.2-9-7, 7.3.4.2-1, 7.3.4.2-3
T5.21 特洛伊木马	A-I	6.3.2	7.2.1.1.4-(5) 7.2.1.1.4-(7) 7.2.1.2.4-(3) 7.2.1.2.4-(5) 7.2.1.2.4-(6) 7.3.2.2-1，7.3.2.2-4 7.3.1.2-9-1, 7.3.1.2-9-8, 7.3.4.2-1, 7.3.4.2-3
T5.28 拒绝服务攻击	A-II	8.1.1	7.2.1.1.4-(9) 7.3.1.2-9-1, 7.3.1.2-9-4, 7.3.4.2-1, 7.3.4.2-2, 7.3.4.2-3
T5.23 计算机病毒	A-I	6.3.2, 8.1.1	7.2.1.2.4-(3) 7.2.1.2.4-(5) 7.2.1.2.4-(6) 7.3.2.2-1, 7.3.2.2-4， 7.3.2.2-3
T3.1 由于 IT 用户失误造成的数据保密性/完整性丧失	A-III	6.6.3,7.4.1,7.4.2,7.4.3,7.4.5,7.4.6,.7.4.8,7.4.9,7.5.1,7.5.3,7.5.4,7.5.5,7.5.7,7.5.8,7.6.1,7.6.2,7.7.2,7.8.2,8.3.3,8.3.4,8.5.2,8.5.4, 10.3.1,10.3.2 5.2.4,6.3.2,8.2.2,8.2.4	7.1.2，7.3.3 7.3.2.2-1，7.3.2.2-4， 7.3.1.2-9-1，7.3.1.2-9-2， 7.3.1.2-9-3，7.3.1.2-9-7, 7.3.4.2-2, 7.3.3.2-2
T3.29 缺乏或不正确的网络分段	A-III	10.2 6.6.3.,9.1.3,10.3.1,10.3.2	7.1.2 7.3.1.2-9-1, 7.3.1.2-9-2, 7.3.1.2-9-3
T3.43 不恰当地处理口令字	A-I	7.5.4,7.8.1,10.2 6.6.3,	7.1.2 7.3.1.2-9-1, 7.3.1.2-9-3, 7.3.4.2-2, 7.3.4.2-3
T4.32 通过不可靠的方式传送重要信息	A-I	7.4.2,7.4.3,7.4.4,7.4.8,7.4.9,10.2 7.4.6,7.8.2,	7.1.2 7.3.3.2-1, 7.3.3.2-2
T2.32 软件、系统测试和发布规程缺乏或不足	A-III	4.3.2,5.2.4,6.1.1,6.4.3,8.1.1,8.5.5 2.3.1,4.3.1,4.3.4,6.2.3,6.3.2,6.6.3,7.7.2,8.4.1,8.5.2	7.3.2.2-1，7.3.2.2-3 7.3.1.2-9-1，7.3.1.2-9-3 7.3.4.2-1, 7.3.4.2-2, 7.3.4.2-3
T2.33 DBMS 的复杂度	A-II	5.2.4,6.2.3,6.4.3,8.1.1, 4.3.1,4.3.4,6.1.1,6.3.2,6.6.3,8.5.2,	7.3.4.2-1, 7.3.4.2-2 7.3.1.2-9-1, 7.3.1.2-9-5,
T3.6 因清洁、外包员工带来的风险	C-I	5.2.4,6.6.3,	7.3.1.2-9-1
T3.10 UNIX 下不恰当地共享文件系统	A-III	6.2.3,6.6.3,7.4.1,5.2.4,6.3.2,7.6.1,8.5.1,	7.3.4.2-2
T3.38 配置和操作错误	A-III	8.5.1,8.5.2,	7.3.1.2-9-1, 7.3.1.2-9-2,

		4.3.1,4.3.2,4.3.4,6.6.3,7.4.5,9.1.3,	7.3.1.2-9-3, 7.3.1.2-9-7 7.3.4.2-2
T5.18 口令的强力攻击	C-I	4.3.1,6. 3.2,7.2.3,7.5.4, 4.3.2,4.3.4,	7.3.1.2-9-1, 7.3.1.2-9-5, 7.3.4.2-3
T4.32 通过不可靠的方式传送重要信息	A-I	7.4.2,7.4.3,7.4.4,7.4.9,8.1.1,7.8.2	7.3.1-2,7.3.2,7.3.3,7.3.4-1, 7.3.4-3
T5.7 搭线	A-I	5.2.1,8.1.1,8.3,8.3.3,5.1.2	7.3.1-2,7.3.2,7.3.3,7.3.4-1, 7.3.4-3

威胁	风险	应对安全措施	对应章节
T4.3 已有物理安全措施失效	C-II	6.4.2,6.4.3,8.1.1, 4.3.1,4.3.2,4.3.4,4.3.5,5.1.1,5.1.2,6.6.3,9.1.3,	7.3.3.2-1
T5.4 偷窃	C-III	4.3.1,4.3.5,5.1.1,5.1.2,5.2.5,5.2.6,6.7.4,6.7.5,7.1.1,8.1.1,8.5.5, 4.3.2,4.3.4,6.1.2,7.4.6,7.4.8,	7.3.2.2-3 7.3.1.2-9-, 7.3.4.2-1, 7.3.4.2-2
T5.5 有意破坏	C-III	4.3.1,4.3.5,5.1.2,5.2.5,5.2.6,6.4.1,6.4.2,6.7.4,6.7.5,7.1.1,8.5.5, 4.3.2,4.3.4,5.1.1,6.1.2,7.4.6,	7.3.2.2-1 7.3.1.2-9, 7.3.4.2,
T5.17 外部人员在维护工作中造成的威胁	B-IV	2.2.1,2.3.1,4.3.1,4.3.5,5.1.1,5.1.2,5.2.5,5.2.6,6.4.2,6.7.4,6.7.5,7.4.1,7.4.4,7.4.9,7.5.4,8.1.1,8.5.5, 4.3.4,6.1.1,6.1.2,7.4.6,7.4.8,8.5.4,	7.3.2.2-1 7.3.1.2-9-1, 7.3.4.2-2
T5.19 滥用用户权限	B-IV	4.3.1,4.3.5,7.4.1,7.4.4,7.4.9,7.5.4,8.1.1,8.1.4,8.5.5, 4.3.4,6.1.2,6.2.2,7.4.6,7.4.8,8.1.4,8.5.4,	7.3.1.2-9-1, 7.3.1.2-9-3, 7.3.4.2-3, 7.3.3.2-1 7.2.1.2.4-(4) 7.2.1.2.4-(7) 7.2.1.2.4-(8)
T5.25 伪装	B-IV	4.3.1,6.3.2,6.7.4,6.7.5,8.1.1, 4.3.2,7.4.1,	7.3.1.2-9-1, 7.3.1.2-9-7, 7.3.4.2-1, 7.3.4.2-3,
T5.27 抵赖对消息的接受/发送	C-III	4.3.1,4.3.5,6.7.4,6.7.5,7.4.4,8.1.1, 4.3.2,7.4.1,7.5.4,	7.3.1.2-9-1, 7.3.3.2,
T5.29 非法复制数据介质	B-III	2.3.1,4.3.1,4.3.5,6.7.4,6.7.5,7.6.1,7.6.2,8.1.1, 7.2.2,	7.3.2.2-3 7.3.1.2-9-1, 7.3.4.2,
T 4.5 串扰和电子感应	C-III	6.4.3,8.1.1	7.2.1.1.4-(1)
T 5.1 IT 设备及附属设备被控制或破坏	C-IV	5.1.1 ,5.2.1, 5.2.5	7.2.1.2.4-(3) 7.2.1.2.4-(5) 7.2.1.2.4-(6)

13.3网络与网络基础设施安全目的符合性

13.3.1 安全目的符合性声明

为保护网络与网络基层设施的安全，本方案采用了如下的安全措施以达到相应的安全目的：

a) 通过在骨干网、接入网和无线网中建立相应的安全通道，实施加密、访问控制、鉴别等安全措施，可以防止拒绝服务的攻击。

b) 为保证广域网的可用性，与其它电信服务商签署质量保证协议。结合ATM 密码机的高速、实时性特点、TCP/IP 网络密码机的安全隧道、无线网安全等措施，可以有效保证信息在发送过程中的安全。

c) ATM 加密、IP 层加密、无线网络加密措施均可抵抗数据流分析。

d) ATM 加密、IP 层加密、无线网络加密措施可以保障用户数据流的安全。

e) 与其它电信服务商签署质量保证协议可以保护网络基础设施控制信息。

13.3.2 安全目的符合性对应表

威胁	风险	应对安全措施	对应章节
T1.2 IT系统故障	A-III	6.7.2,7.4.2,7.4.4,7.4.5,7.4.8,7.4.9,7.5.1,7.5.3,7.6.1,7.6.2,7.7.1,7.7.2,8.1.1,8.3,8.3.3,8.3.4,8.4.1,8.4.2,8.4.3,9.1.1,9.1.3	8.1，8.2，8.3
T1.10 广域网故障	A-III	6.1.6,6.2.2,7.4.1,7.4.4,7.4.5,7.4.8,7.7.1,7.7.2, 8.1.1, 9.1.1	8.1，8.2，8.3，8.4
T 4.31 网络设备故障或丧失功能	A-II	7.7.2,8.1.1,9.1.1,7.4.8	8.1
T 4.32 通过不可靠的方式传送重要信息	A-I	7.4.2,7.4.3,7.4.4,7.4.8,7.4.9,8.1.1	8.1， 8.2.4-2，8.3.3-2，8.4
T 5.7 搭线	A-I	8.1.1,8.3,8.3.3,5.1.1,5.1.2,	8.2，8.3，8.4
T 5.10 滥用远程维护端口	A-III	5.1.2	8.1
T 5.18 口令的强力攻击	C-I	8.3	8.1
T 5.28 拒绝服务攻击	A-II	8.1.1	8.1

威胁	风险	应对安全措施	对应章节
T 5.24 信息重放	C-IV	8.1.1,8.3,8.3.3	8.2.4－3，8.3.3－2
T 5.25 伪装	B-IV	8.3,6.7.5,8.1.1	8.2.4－3，8.3.3－10
T 5.26 分析信息流	B-III	8.1.1,8.3,7.4.8	8.2.4－3，8.3.3－2

13.4支撑基础设施安全目的符合性

威胁	风险	应对安全措施	对应章节

T1.2 IT系统故障	A-III	5.2.4, 6.1.3, 6.2.2, 6.3.2,6.4.1,6.4.2,6.4.3, 6.6.3, 6.7.2, 6.7.4, 6.7.5,7.1.1,7.2.2,7.2.3,7.4.2,7.4.5,7.4.6,7.4.8,7.4.9,7.5.1,7.5.3, 7.5.5,7.5.7,7.5.8,7.6.1,7.6.2,7.7.1,7.7.2,8.2.4,8.3,8.3.3,8.3.4,8. 5.4,10.2,10.3.1,6.1.5,6.6.4,7.4.3,10.3.2	9.1，9.3，9.4，9.5
T 3.1 由于IT用户失误造成的数据保密性/完整性丧失	A-III	6.6.3,7.4.1,7.4.2,7.4.3,7.4.5,7.4.6,.7.4.8,7.4.9,7.5.1,7.5.3,7.5.4 ,7.5.5,7.5.7,7.5.8,7.6.1,7.6.2,7.7.2,7.8.2,8.3.3,8.3.4,8.5.2,8.5.4 ,10.3.1,10.3.2,5.2.4,6.3.2,8.2.2,8.2.4	9.2,9.3，9.4，9.5
T 3.25 因粗心删除东西	A-III	6.6.3,10.2,10.3.1,9.1.3,	9.3，9.4，9.5
T 3.43 不恰当地处理口令字	A-I	7.5.4,7.8.1,10.2,5.2.6,6.6.3,	9.1
T 4.7 有缺陷的数据媒体	A-III	5.2.3,10.2,6.6.3	9.5
T 4.13 后备存储的数据丢失	A-II	5.1.1,5.1.2,5.2.1,5.2.5,5.2.6,5.3.1,6.1.1,6.1.2,6.1.5,8.1.1,10.2 6.3.2,6.4.1,8.4.1,	9.4，9.5
T 4.31 网络设备故障或丧失功能	A-II	6.6.3,7.7.2,9.1.3,10.2,7.4.8,	9.3，9.4，9.5
T 4.32 通过不可靠的方式传送重要信息	A-I	6.1.1,7.4.2,7.4.3,7.4.4,7.4.9,8.1.1,7.4.6	9.2

威胁	风险	应对安全措施	对应章节
T 5.5 有意破坏	C-III	5.2.1,5.2.5,5.2.6,6.4.1,6.4.2,6.6.1,6.6.3,6.7.2,6.7.4,6.7.5,7.1.1, 8.3,8.3.3,10.2,7.4.6	9.4，9.5
T 5.25 伪装	B-IV	6.3.2,6.7.4,6.7.5,8.1.1,10.2,7.4.1,8.3	9.1,9.2
T 5.27 抵赖对消息的接受/发送	C-III	6.7.4,6.7.5,7.4.3,7.4.4,7.5.3,8.3,8.3.3,8.3.4,10.2,10.3.1,10.3.2, 7.5.4	9.1, 9.2
T 5.24 信息重放	C-IV	7.4.6,8.1.1,7.4.1,8.3,8.3.3	9.2
T 5.26 分析信息流	B-III	7.4.6,8.1.1,8.3,7.4.1	9.2

13.5物理安全的安全目的符合性

威胁	风险	应对安全措施	对应章节
T 4.1 断电	A-I	5.2.2,5.2.3,8.1.1,9.1.1,6.6.3,	10.2-1，10.2-4

威胁	风险	应对安全措施	对应章节

T1.8 灰尘、尘土	D-III	5.2.1,7.3.2,7.7.2,8.1.1	10.2-1，10.2-4
T2.6 未经授权进入需要保护的房间	C-IV	5.1.1,5.1.2,5.1.3,5.2.1,5.3.1,7.2.1,7.2.4	10.2-1， 10.2-2，10.4-1,10.4-2
T2.23 对电源配线箱的保护不足	C-IV	5.1.1,5.1.2,5.2.1,5.2.2,5.2.3,5.2.4,8.1.1	10.2-1，10.2-4
T 4.3 已有物理安全措施失效	C-II	8.1.1,5.1.2,5.1.3,5.2.1,6.6.3	10.2-1， 10.2-2，10.1-4
T 4.4 环境因素引起线路损伤	D-III	8.1.1,6.6.3	10.2-1， 10.2-2，10.1-3，10.2-4
T 4.5 串扰和电子感应	C-III	5.2.3,5.2.4,6.4.3,8.1.1,6.6.3	10.4-1，10.4-2
T 5.1 IT 设备及附属设备被控制或破坏	C-IV	5.1.1,5.1.2,5.2.1,5.2.5,5.2.6,5.3.1,7.7.2,8.1.1,9.1.1,6.1.5	10.1，10.2，10.3，10.4，10.5
T 5.3 非法进入建筑物	C-III	5.1.1,5.1.2,8.1.1,6.1.2	10.5
T 5.4 偷窃	C-III	5.1.1,5.1.2,5.2.1,5.2.5,5.2.6,8.1.1,8.3,6.1.2,7.4.6	10.5
T 5.5 有意破坏	C-III	5.1.2,5.2.1,5.2.5,5.2.6,6.7.2,7.3.2,8.3,8.3.3,5.1.1,7.4.6	10.5

附录 A ： 安全目的和安全控制措施

A3 安全方针

			ISO/IEC 编号
A3.1 信息安全方针（策略） 目标：为信息安全提供管理指导和支持			3.1
控制措施			
A3.1.1	信息安全方针文件	视具体情况，向机构所有职员发布机构领导制定的方针文件	3.1.1
A3.1.2	评审与评估	对方针进行定期审核；如需修正，须做到合情合理	3.1.2

A4 安全组织

			ISO/IEC 编号
A4.1 信息安全基础设施 目标：管理机构内部的信息安全。			4.1
控制措施			
A4.1.1	管理信息安全的委员会（论坛）	管理信息安全委员会的目标是确保机构在适当启动安全方面有明确的指导方针和有成效的管理支持	4.1.1
A4.1.2	信息安全协调	针对机构的规模，从机构的相应部门抽调管理代表组成跨部门的委员会（论坛），以此协调信息安全控制措施的实施	4.1.2
A4.1.3	信息安全权责分配	对各种资产保护和实施特定安全过程的职责要加以明确定义	4.1.3
A4.1.4	信息处理设施的授权过程	确立新的信息处理设施的管理授权过程	4.1.4

A4.1.5	专家的信息安全建议	寻求由机构内部提出的或专家顾问提交的信息安全建议并在整个机构内发布	4.1.5
A4.1.6	机构间合作	与执法、监管机构、信息服务提供商及电讯运营商保持适当联系	4.1.6
A4.1.7	信息安全的独立评审	对信息安全方针的实施应实施独立评审	4.1.7
A4.2 第三方访问的安全 目标：保持被第三方访问的机构的信息处理设施和信息资产的安全			4.2
A4.2.1	第三方访问的风险识别	与由第三方访问的机构的信息处理设施有关的风险要进行评估并采取适当安全控制措施	4.2.1
A4.2.2	第三方合同的安全要求	在涉及第三方访问机构信息处理设施的情况下要求签定正式合同，此合同应包含所有必要的安全要求	4.2.2
A4.3 外包 目标：当信息处理的责任委托给另外机构时，要保持信息安全			4.3
A4.3.1	外包合同的安全要求	当机构需将其信息系统、网络和/或桌面电脑环境的管理和控制部分地或全部地委托给他方实施时，此机构的安全要求要在有关各方签订的合同中加以说明	4.3.1

A5 资产分类和控制措施

			ISO/IEC 编号
A5.1 资产的责任 目标：维护机构的资产得以适当保护			5.1
控制措施			
A5.1.1	资产清单	对所有的重要资产要草拟清单并保存	5.1.1

A5.2 信息分类 目标：确保信息资产受到恰当水平的保护			5.2
A5.2.1	分类的指导方针	信息分类及相关的控制措施应符合分享信息或限制信息的业务需求以及与这些需求相关的业务影响	5.2.1
A5.2.2	信息标签及处理	根据机构采用的分类原则，制定一整套信息标识和处理程序	5.2.2

A6 人员安全

			ISO/IEC 编号
A6.1 工作职责定义及资源使用的安全 目标：降低人为错误、偷窃、欺骗或设备误用的风险			6.1
控制措施			
A6.1.1	工作职责包含的安全	机构信息安全方针中规定的安全角色和责任当在工作定义中恰当标明	6.1.1
A6.1.2	人员任用方针	在机构职员申请工作时，对其终身工作进行资格审查	6.1.2
A6.1.3	保密协议	雇员在受雇时，应和机构签署保密协议，此协议为员工守则的一部分	6.1.3
A6.1.4	员工守则	该守则应阐明员工在信息安全方面的职责	6.1.4
A6.2 用户培训 目标：确保用户了解信息安全威胁及其利害关系，并支持机构在日常工作中的安全方针			6.2
A6.2.1	信息安全的教育和培训	机构的所有职员，以及在必要情况下涉及的第三方用户，都应接受相应的培训并定期升级机构的方针和程序	6.2.1

A6.3 安全事件和故障的响应 目标：使安全事件及故障的损害降至最小、监控并掌握类似事件			6.3
A6.3.1	安全事故报告	发现安全事故后，应立即通过适当管理渠道尽快报告	6.3.1
A6.3.2	安全弱点报告	要求信息服务用户记录并回报任何其觉察或怀疑存在的安全漏洞	6.3.2
A6.3.3	软件故障报告	要求建立并遵守软件故障报告程序	6.3.3
A6.3.4	从事件中学习	要求建立相应机制，对事件或故障的类型、量级和损失程度进行量化、监控	6.3.4
A6.3.5	违规处置过程	员工如违反机构的安全方针和程序，应通过正式的违规处置过程加以处理	6.3.5

A7 物理和环境安全

			ISO/IEC 编号
A7.1 信息安全区 目标：保护企业所在地及信息免于未经授权的访问、破坏及入侵			7.1
控制措施			
A7.1.1	物理安全周边	机构应通过安全周边来保护信息处理设施的区域	7.1.1
A7.1.2	安全区进出控制	在信息安全区采取适当出入控制来确保只有经授权的人员得以进入	7.1.2
A7.1.3	信息安全办公室、处所、设施	在有特别安全要求的办公室、处所或设施处设立安全区	7.1.3
A7.1.4	安全区内工作	为进一步加强已采取物理保护措施的安全区的安全，应制定附加的控制措施和指导方针	7.1.4
A7.1.5	交接区的隔离	对交接区进行控制；如有必要，将其与	7.1.5

		信息处理设施进行隔离，并避免未经授权的进入	
A7.2 设备安全 目标：防止资产的遗失、损坏、危害并防止正常业务活动中断			7.2
A7.2.1	设备选址及防护	对设备要定位并加以保护，使其免受周围环境造成的威胁或意外损坏，并避免未经授权的进入	7.2.1
A7.2.2	电力供应	使设备避免断电或其它供电方面的问题	7.2.2
A7.2.3	传输设备安全性	保护传输数据或支持信息服务的供电信电缆，使之免于中断或损坏	7.2.3
A7.2.4	设备的维护	对设备的维护应依据制造商的指示或文挡的流程进行，确保设备的持续可用性和完整性	7.2.4
A7.2.5	脱离周边的设备安全	运用安全流程和控制手段，确保脱离机构周边的设备的安全	7.2.5
A7.2.6	设备报废或再启用安全	在设备报废后或再启用前，清除其存储的信息	7.2.6
A7.3 通用的控制措施 目标：防止信息或信息处理设施被毁坏或偷窃			7.3
A7.3.1	清除桌面及屏幕方针	机构应制定并执行桌面及屏幕清除方针，降低未经授权访问和信息遗失或损坏的风险	7.3.1
A7.3.2	资产的移动	机构所属设备、信息或软件未经授权不得移动	7.3.2

A8 通信和运行管理

			ISO/IEC 编号
A8.1 操作程序及职责			8.1

目标：确保正确、安全地操作信息处理设备			
控制措施			
A8.1.1	文挡化的操作程序	第 4.1.1.1 条安全原则中阐明的操作程序应有文件记录并加以存档	8.1.1
A8.1.2	操作变更控制	对信息处理设施和系统方面的变化加以控制	8.1.2
A8.1.3	安全事件管理程序	要建立安全事件的管理责任和程序，确保安全事故发生后作出快速、有效、有序的反应	8.1.3
A8.1.4	职责分离	权责和区域应清楚地隔离，以减少未经授权的修改或信息或服务滥用的机会	8.1.4
A8.1.5	开发与运行设备的隔离	开发及测试设施应与运行设施隔离	8.1.5
A8.1.6	外部设施管理	使用外部设施管理服务前，应识别相关风险并且与承包商协商采取适当控制措施，并将其纳入合同中	8.1.6
A8.2　系统规划及验收 目标：将系统故障风险降至最低			8.2
A8.2.1	容量规划	对容量需求要进行监控，并进行未来容量要求进行预测，确保能够得到足够的处理和存储能力	8.2.1
A8.2.2	系统验收	建立新信息系统、系统升级和新版本方面的验收标准；在验收前进行适当测试	8.2.2
A8.3　恶意软件的防护 目标：保护软件及信息的完整性			8.3
A8.3.1	防恶意软件的控制措施	要实现检测和预防恶意软件的控制措施以及相应的用户须知程序	8.3.1

A8.4 内务 目标：维护信息处理及通信服务的完整性和可用性			8.4
A8.4.1	信息备份	重要的业务信息和软件应要进行定期备份	8.4.1
A8.4.2	操作者日志	操作人员应保存其日志	8.4.2
A8.4.3	故障记录	对故障进行记录并采取纠正措施	8.4.3
A8.5 网络管理 目标：保护网络的信息及支持性基础设施			8.5
A8.5.1	网络控制	实施一系列管制措施，实现并保持网络安全	8.5.1
A8.6 介质处理及安全 目标：防止资产损失及业务活动中断			8.6
A8.6.1	可移动计算机介质的管理	对可移动计算机介质如磁带、光盘、打印的报告的管理进行控制	8.6.1
A8.6.2	介质的处理	在介质作不在需要时，应对其进行保密和安全处理	8.6.2
A8.6.3	信息处理程序	建立信息处理和存储程序，确保信息不被非法泄漏或滥用	8.6.3
A8.6.4	系统文挡的安全	系统文件未经授权不得访问	8.6.4
A8.7 信息及软件的交换 目标：进行机构间信息交换时，避免信息的遗失、篡改或误用			8.7
A8.7.1	信息及软件交换协议	机构间通过电子或手动方式交换信息或软件时，其中许多应签订正式协议	8.7.1
A8.7.2	传递中介质的安全	在传输过程中的介质，应防止被非法访问、滥用或讹误	8.7.2
A8.7.3	电子商务的安全	电子商务应防止欺诈行为、合同纠纷和信息的泄漏或修改	8.7.3

A8.7.4	电子邮件的安全	制定使用电子邮件的安全方针和控制措施，降低使用电子邮件产生的风险	8.7.4
A8.7.5	电子办公系统的安全性	准备和实现有关方针和纲领，对与电子办公系统有关的业务和安全风险进行控制	8.7.5
A8.7.6	公开发布系统	信息在公开发布前，要经过正式审批过程；应保持所发布信息的完整性以避免信息未经授权的修改	8.7.6
A8.7.7	其它形式的信息交换	制定程序和控制措施，对通过声频、传真和视频通信设备等渠道进行信息交换要进行保护	8.7.7

A9 访问控制

			ISO/IEC 编号
A9.1 访问控制的业务要求 目标：控制对信息的访问			9.1
控制措施			
A9.1.1	访问控制方针	对访问控制的业务要求进行定义并文挡化，访问只限于访问控制方针规定的范围	9.1.1
A9.2 用户访问管理 目标：。避免未经授权地访问信息系统			9.2
A9.2.1	用户注册	对准予对所有多用户信息系统和服务进行访问的用户，要有正式的用户注册和注销程序	9.2.1
A9.2.2	特权管理	对特权的分配和使用加以限制和控制	9.2.2
A9.2.3	用户口令管理	分配口令应通过正式管理过程加以控制	9.2.3
A9.2.4	用户访问权限的	通过正式过程定期对用户访问权限进行	9.2.4

	审核	审核	
A9.3 用户职责 目标：避免未经授权的用户访问			9.3
A9.3.1	口令的使用	使用者在选择和使用口令时，要求遵守良好的安全标准	9.3.1
A9.3.2	无人值守的用户设备	用户要求对无人值守设备加以适当保护	9.3.2
A9.4 网络访问控制 目标：保护网络服务			9.4
A9.4.1	使用网络服务的方针	使用者只能直接访问经过特别授权方可访问的服务	9.4.1
A9.4.2	强制路径	对用户终端到计算机服务的路径应当加以控制	9.4.2
A9.4.3	外部连接的用户鉴别	对远程用户的访问要加以鉴别	9.4.3
A9.4.4	节点鉴别	对与远程计算机系统的连接要进行鉴别	9.4.4
A9.4.5	远程诊断端口的保护	对诊断端口的访问要被安全的保护起来	9.4.5
A9.4.6	网络内部的隔离	网络内要引入把信息服务、用户、信息系统进行分组隔离的控制措施	9.4.6
A9.4.7	网络连接控制	根据 4.7.1.1 访问控制方针的规定，把用户的连接能力限制在共享网络的范围内	9.4.7
A9.4.8	网络路由控制	对共享网络进行路由控制，确保计算机连接和信息流不违反 4.7.1.1 规定的商务应用的访问控制方针	9.4.8
A9.4.9	网络服务的安全	要提供机构所用的所有网络服务安全属性的详细描述	9.4.9

A9.5　操作系统访问控制 目标：避免未经授权的计算机访问			9.5
A9.5.1	自动终端识别技术	运用自动终端辨识技术来鉴别与特定位置及移动设备的连接	A9.5.1
A9.5.2	终端登录程序	访问信息服务时，要求采用安全的登录过程。	9.5.2
A9.5.3	用户识别和鉴别	要求所有用户（无论是人和一次应用）都拥有唯一身份（标识符），使其活动能追溯到负责的个人	9.5.3
A9.5.4	口令管理系统	建立口令管理系统，以便提供一个保证高质量口令的有效、互动的工具	9.5.4
A9.5.5	系统应用程序的使用	对系统应用程序的使用加以限制并严格控制	9.5.5
A9.5.6	有安全装置的用户的强制报警	向受胁迫的用户提供强制报警	9.5.6
A9.5.7	终端超时	处在高风险区或向高风险系统提供服务的待用终端，在规定的待用时间周期后应断开，以避免被非授权的访问	9.5.7
A9.5.8	连接时间限制	在高风险应用状态下，要对连接时间进行限制提供额外的安全保护	9.5.8
A9.6　应用系统访问控制 目标：避免非法访问信息系统中的信息			9.6
A9.6.1	信息访问的限制	根据 4.7.1.1 所规定的访问控制方针，限制对信息和应用系统功能的访问	9.6.1
A9.6.2	敏感系统的隔离	敏感系统要求有隔离（专用）的计算环境	9.6.2
A9.7　监控系统的访问及使用 目标：检测未经授权的活动			9.7

A9.7.1	事件记录	要产生用于记录异常和其它有关的安全事件的审计记录并在规定的时期内加以保存，供日后调查和访问控制监控之用	9.7.1
A9.7.2	监控系统的使用	建立信息处理设施使用情况的监控程序，对监控活动进行定期评审	9.7.2
A9.7.3	时钟同步	为了精确记录计算机时钟必须保持同步	9.7.3
A9.8 移动计算及远程连网 目标：保证使用移动计算和远程连网时的信息安全			9.8
A9.8.1	移动计算机	制定正式的方针和适当管制办法，保证移动计算机的安全	9.8.1
A9.8.2	远程连网	为了认可和控制远程连网要开发远程连网的方针和控制措施	9.8.2

A10 系统开发和维护

			ISO/IEC 编号
A10.1 信息系统的安全要求 目标：确保安全融入信息系统中			10.1
控制措施			
A10.1.1	安全需求的分析和规范	无论对新系统或是对需要生计的现有系统，它们的业务要求要规定各种控制措施的具体要求	10.1.1
A10.2 应用系统的安全要求 目标：防止应用系统中的用户数据被遗失、篡改或误用			10.2
A10.2.1	输入的确认	应用系统的输入数据应进行确认以保证其正确性和恰当性	10.2.1
A10.2.2	内部处理的控制	系统中要有确认检查，以便检测数据处理的错误	10.2.2
A10.2.3	消息鉴别	消息鉴别用于需要保护消息内容完整性的应用系统	10.2.3

A10.2.4	输出数据的确认	对来自应用系统的数据输出应进行确认，确保在那种环境下储存信息处理的正确性和恰当性	10.2.4
A10.3 密码控制 目标：保护信息的机密性、真实性和完整性			10.3
A10.3.1	密码控制措施使用的方针	为了保护信息需要开发密码控制措施使用的方针并要遵守这一方针	10.3.1
A10.3.2	加密	加密用于保护敏感或关键信息的机密性	10.3.2
A10.3.3	数字签名	数字签名用于保护电子信息的真实性和完整性	10.3.3
A10.3.4	不否认服务	不否认服务用于解决关于事件或行为是否发生的争议	10.3.4
A10.3.5	密钥管理	基于一组经协商的标准、程序和办法的密钥管理体系用于支持密码技术的使用	10.3.5
A10.4 系统文件的安全 目标：确保 IT 工程和支持活动以安全方式进行			10.4
A10.4.1	操作软件控制	在操作系统上安装软件时必须应进行必要控制	10.4.1
A10.4.2	系统测试数据的保护	测试数据必须进行保护和控制	10.4.2
A10.4.3	源程序库的访问控制	对源程序库的访问进行严格控制	10.4.3
A10.5 开发和支持过程的安全 目标：维护应用软件和信息的安全			10.5
A10.5.1	变更管理程序	实施变更时，应按照正式变更控制程序加以严格控制，从而使信息系统的损害降至最低限度	10.5.1
A10.5.2	对操作系统变更	应用系统发生变更时，应对其进行评审	10.5.2

	的技术评审	和测试	
A10.5.3	对软件包变更的限制	不鼓励对软件包进行变更；重大变更需严格控制	10.5.3
A10.5.4	隐蔽通道和特洛伊木马	购买、使用和变更软件时，应对其进行严格控制和检测，防范隐蔽通道和特洛伊木马程序	10.5.4
A10.5.5	外包软件开发	建立控制措施做到安全外包软件开发	10.5.5

			ISO/IEC 编号
A11.1 业务连续性管理的若干方面 目标：避免业务活动中断以及保护关键业务过程免受重大系统故障或天灾的影响			11.1
控制措施			
A11.1.1	业务连续性管理过程	在整个机构范围内，为了开发和保持业务连续性，在合适的地方要求建立管理过程	11.1.1
A11.1.2	业务连续性和影响分析	为了使业务连续性有一个完整的方法应开发基于适当风险评估的战略计划	11.1.2
11.1.3	业务连续性计划的制定和实施	开发计划以便在关键业务过程中断或故障后能得以及时维护和恢复业务运行	11.1.3
11.1.4	业务连续性规划框架	维护一个业务连续性计划框架，确保所有计划是一致的，并识别测试和维护的优先权	11.1.4
11.1.5	业务连续性计划的测试、维护和重新评估	要定期测试和通过定期评审来维护，以确保这些计划是最新的和有效的	11.1.5
			ISO/IEC 编号
A12.1 遵守法律要求			12.1

目标：避免触犯任何刑法、民法、已成文的法令法规或其它任何安全要求			
控制措施			
A12.1.1	识别适用的法规	所有适用的法律、法规和法令对于每一个信息系统都要明确的定义并且要文挡化	12.1.1
A12.1.2	知识产权	执行适当程序，确保关于知识产权材料的使用以及专利软件产品的使用时与法律限制相一致	12.1.2
A12.1.3	保护组织记录	机构的重要记录要求避免损失、毁坏或伪造	12.1.3
A12.1.4	数据保护和个人隐私	根据相关法律，采取控制措施保护个人信息和隐私	12.1.4
A12.1.5	防止信息处理设施的滥用	管理要对信息处理设备的使用授权并采取控制手段防范设备的滥用	12.1.5
A12.1.6	密码控制措施的规则	密码控制措施的使用要确保其符合国家有关法律、法规和方针以控制密码控制措施的访问和使用	12.1.6
A12.1.7	证据收集	若某个人或机构的行动需诉诸法律，无论是诉诸刑法还是民法，在收集有关证据时，要遵守相关法律有关于证据收集的法则，不得违反任何业已公布的标准或行为规范	12.1.7
A12.2 信息安全方针和技术符合的评审 目标：确保系统与机构的安全方针和标准符合			12.2
A12.2.1	符合信息安全方针	管理者要确保其权责范围内所有安全程序都得以正确的贯彻执行并确保对机构各领域进行定期评审，确保其符合安全方针和标准	12.2.1
A12.2.2	技术符合性检查	对信息系统是否合乎安全实现标准进行定期检查	12.2.2

A12.3　系统审计考虑 目标：通过系统审计过程扩大效能，降低干扰			12.3
A12.3.1	系统审计控制	操作系统审计要进行计划并承认诸如使对业务过程的中断风险最小化	12.3.1
A12.3.2	系统审计工具的保护	对系统审计工具的访问要进行保护，防止可能的误用或滥用	12.3.2
			ISO/IEC 编号
A12.1　遵守法律要求 目标：避免触犯任何刑法、民法、已成文的法令法规或其它任何安全要求			12.1
控制措施			
A12.2　信息安全方针和技术符合的评审 目标：确保系统与机构的安全方针和标准符合			12.2
A12.3　系统审计考虑 目标：通过系统审计过程扩大效能，降低干扰			12.3