目录

第一部分 简介和设计原理

1 目标和范围

信息安全指标体系的设计目标是以公司信息系统的实际情况和现实问题为基础，参照国际和国内的安全标准和规范，充分利用成熟的信息安全理论成果，设计出整体性好、可操作性强，并且融策略、组织、运作和技术为一体的安全指标体系。

本信息安全指标体系可分为安全技术、安全运作、安全组织和安全策略文档四个方面，涉及所有 IP 网络，包括网络系统、主机、平台、应用软件和业务数据等。

2 安全指标体系设计原理

2.1 总体设计方法

在此项目中，指标体系设计方面的三个原则如下：

整体性原则：安全指标体系设计的范围和内容应当整体全面，包括安全涉及的各个层面（应用、系统、网络、管理制度、人员等），避免由于遗漏造成未来的安全隐患。

符合性原则：符合国家 27 号文件指出的积极防御、综合防范的方针和等级保护的原则。

标准性原则：设计与实施应依据国内或国际的相关标准进行；

从而我们在设计过程中，采用体系化设计方法来满足整体性原则，采用等级化设计方法来保证满足符合性原则，采用标准化设计方法来满足标准性原则。下面分别描述这三种设计方法。

2.2 等级化设计原则

2003 年，中央办公厅、国务院办公厅转发的《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，已将信息安全等级保护作为国家信息安全保障工作的重中之重，要求各级党委、人民政府认真组织贯彻落实。《意见》中明确指出，信息化发展的不同阶段和不同的信息系统，有着不同的安全需求，必须从实际出发，综合平衡安全成本和风险，优化信息安全资源的配置，确保重点。

在国信办近期制定的《信息系统安全等级保护实施指南》中规定了 5 个等级，分别为自主性保护级、指导性保护级、监督性保护级、强制性保护级和专控型保护级。根据指南中规定的等级确定方法，将整个信息系统分为不同区域，首先确定最关键一组区域的最高等级，其他次级区域依次确定较低的等级。确认等级的依据一方面根据国家从国家安全角度的要求，主要还是依据企业自身的安全要求。根据指南中对 5 个等级的要求和适用范围的规定，公司属于国家基础信息系统，最高等级至少划分到第三级，监督性保护级，指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，具备对信息和系统进行基于安全策略的安全保护能力。

第四级强制性保护适用于政府等国家机构，指在政府职能部门的强制监督和检查下，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。第四级的要求很高，实施起来也比较困难，我们认为公司不需确认为第四级，个别系统可以视情况增加些第四级的安全要求。

第一级自主性保护级是指参照国家标准自主进行保护。主要适用于一般信息系统。第二级指导性保护级是指在政府职能部门指导下，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。第二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。

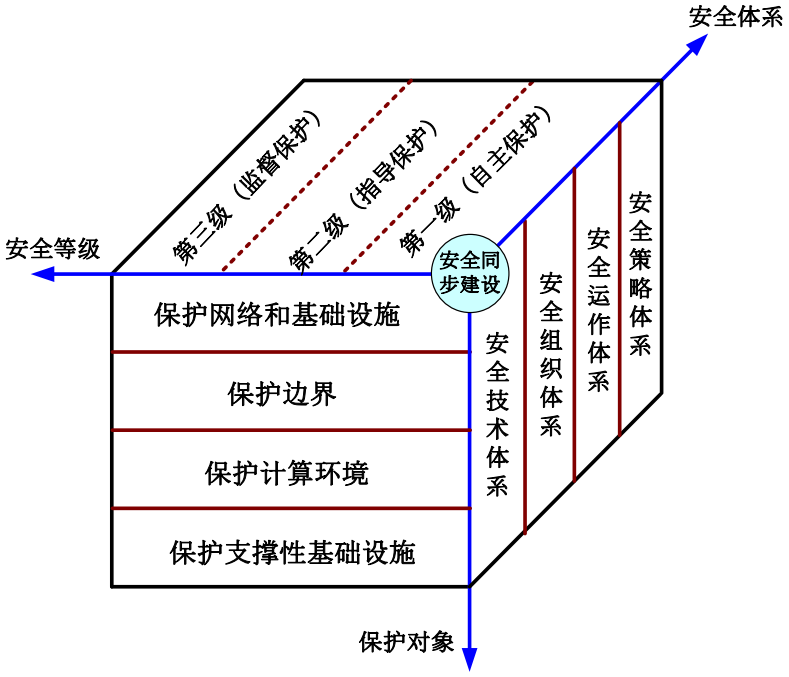
2.3 体系化设计方法

一般地，对安全体系的研究主要采用两种思路，一是模型化，它通过将要保

护的对象通过模型的方式表达，获取其安全需求；一是“最佳实施”，它通过列举安全控制来构造理想的安去体系。这两种模型都存在着一定的缺陷，模型化思路的主要难点在于难以完整和准确地表达一个信息系统，而最佳实施的主要缺陷是安全控制的不可枚举性。

鉴于这样一种情况，在设计公司安全指标体系的过程中，我们将两种思路加以综合，首先借鉴 IATF 的信息安全保障体系模型构建公司的 IP 网络安全体系模型，然后根据公司 IP 网络面临的威胁选择或设计所有可行的安全对策，然后进行纵向梳理，产生技术体系和管理体系（策略、组织和运作体系），这些体系构成所需的安全指标体系。

下图即是公司安全体系模型示意图。这个示意图说明了安全体系的构成。

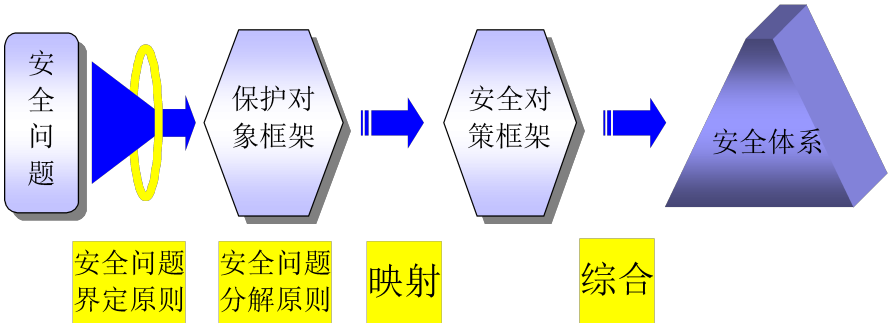


图表 1 安全体系模型

正面是公司的保护对象框架，我们将公司 IP 网络划分为若干个保护对象，将保护对象又分成计算环境、区域边界、网络和基础设施、支撑性基础设施（指 PKI/PMI/KMI 中心和应急响应中心）等，以便于威胁分析。

上面是公司 IP 网络中保护对象的安全等级，可以根据具体保护对象的重要性以及安全需求将其确定在某个等级上，其中第一级基本相当于国家标准中定义的“自主保护级”，第二级基本相当于国家标准中定义的“指导保护级”，第三级基本相当于国家标准中定义的“监督保护级”。

右面是由安全对策组件组成的策略体系、组织体系、技术体系和运作体系。准确地说，体系设计的过程如下：



图表 2 体系设计过程

✧ 界定安全问题的范围

正如前面所提，信息安全问题涉及的范围很广，有时甚至和传统安全问题牵扯在一起。这给解决安全问题带来了很大的难度。因此要科学地对待信息安全问题，首先必须明确定义信息安全问题的范围。

✧ 对安全问题进行结构化分析

当信息安全问题的范围已经被明确后，它必须按照结构化原理被不断地细分。这时整个 IP 网络已经被结构化为“保护对象框架”，而保护对象面临着诸多威胁。

✧ 编写安全对策框架

根据现有的各种安全标准和实践准则，对公司 IP 网络进行分析，编写适合公司 IP 网络的安全对策，形成安全对策框架。

✧ 细化安全对策形成 3 级安全指标体系

对公司 IP 网络面临的每一项安全威胁都从安全对策框架中选择若干安全对策，注意威胁和安全对策之间是多对多的映射关系，即每一个威胁对应若干个对策，而每一个对策对应多个威胁。将所选择的安全对策进行细化、扩展和具体化，形成策略体系、组织体系、技术体系和运作体系，再综合成 3 个基线要求就构成了公司 IP 网络的 3 级安全指标体系。

综上所述，安全指标体系的设计采用了先分析后综合的思路，而在这个过程中，框架起了至关重要的作用。

2.4 标准化设计方法

本项目参考的相关标准和文档包括：

- 美国国家安全战略
- 美国的《保护网络空间的国家战略》
- 美国银行于金融关键基础设施保护战略
- 俄罗斯联邦信息安全学说
- 欧洲信息与网络安全政策
- BS7799/ISO17799
- ISO15408/CC
- IATF
- ……

3 主要内容

公司安全体系的具体内容包括：

- 公司 IP 网络保护对象框架：公司 IP 网络保护对象框架是根据对公司 IP 网络的评估调查和普查，参照信息保障体系的建模方法，将 IP 网络划分为若干保护对象，并确定了各个保护对象的安全级别。详细内容参阅第二部分。
- IP 网络安全对策框架：公司 IP 网络安全对策框架是参照国内外先进的信息安全标准，参考业界通用的最佳实施，并结合公司的实际情况和现实问题进行定制，对大量可行的安全对策进行等级划分。详细内容参阅第三部分。
- IP 网络安全体系：公司 IP 网络安全体系是以保护对象为纬，以安全等级框架为经，对整个 IP 网络进行威胁分析，从安全框架中选择相应对策，将所选的安全对策进行细化、扩展和具体化，再综合为 3 个安全基线要求，从而形成公司 IP 网络 3 级安全指标体系。详细内容参阅第四部分。

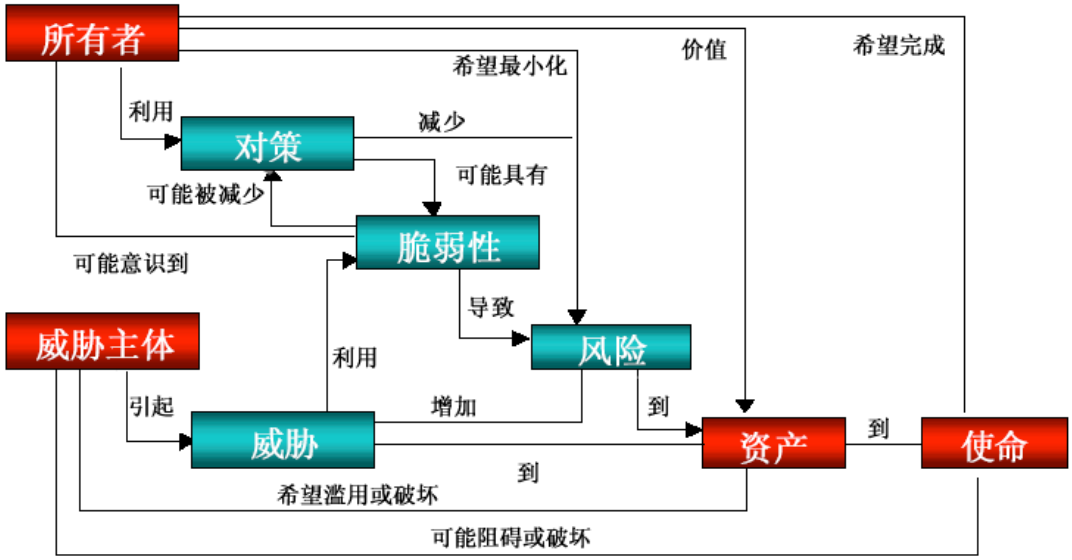
- 威胁详述：罗列了 IP 网络可能面临的所有威胁，并进行了详细阐述，标明了相应的可选对策。见附录 1。

第二部分 IP 网络安全对策框架

1 概述

公司 IP 网络安全等级化框架主要是以威胁和对策为出发点和核心，即从 IP 网络所面临的威胁出发制定安全要求，通过从技术、运作、组织和策略文档等方面提出安全对策，确保信息的机密性、完整性和可用性特征，从而将风险降低到可接受的水平，达到保护公司 IP 网络的目的，进而完成公司 IP 网络的使命——即保障公司各种业务生产正常、稳定和安全。

下图描述了资产、使命、威胁、脆弱性、风险以及安全对策之间的关系。



图表 3 安全对策框架概述

实际或假定的威胁主体希望以违背资产所有者初衷的方式滥用资产，这就是威胁。资产本身可能存在脆弱性，作为资产所有者，公司将会意识到这种威胁可能利用上述脆弱性来导致资产损坏，资产中的价值将会降低。安全性损坏一般包括以下几项：资产破坏性地暴露于未授权的接收者（失去保密性），资产由未授权的更改而损坏（失去完整性），或资产访问权被未授权的丧失（失去可用性）。

必须分析可能的威胁并确定哪些存在于公司 IP 网络中，所得出的结果就是风险。这种分析会有助于对策的选择，以应对风险并将其降低到一个可接受的水平。

安全对策用以减少公司 IP 网络的脆弱性从而降低风险。在安全对策被实施后仍会有残留的脆弱性，这些残留的脆弱性仍可以被威胁者利用，从而造成了资产的残余风险。应通过给出其它的约束来寻求最小的残余风险。

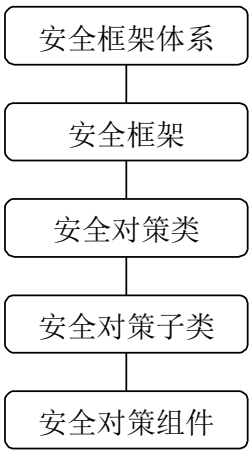
以上就是对信息安全问题以及解决方法的高度概括，其中非常重要的是进行威胁分析和选择安全对策。

本体系编写之前，已经对公司的 IP 网络进行了现状评估工作，本体系的目标就是根据公司的特点设计和定制等级化安全对策框架，并针对公司的现状选择和细化安全对策组件。

在本部分中，将公司 IP 网络可能适用的安全对策进行分类、分级，以便在第四部分中进行扩展和细化。

2 安全对策框架层次结构和分类

安全对策框架的层次结构如下图所示：

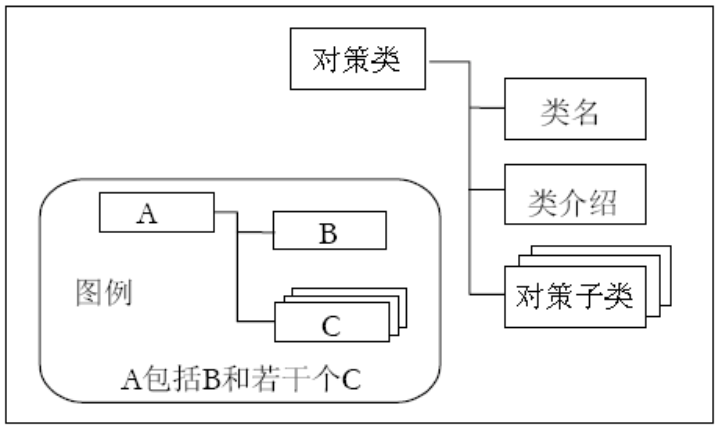


图表 4 安全框架的层次结构

安全对策框架包括安全策略文档、安全组织、安全运作和安全技术四个安全框架，这四个安全框架分别包括一系列对策类。

对策类可进一步细分对策子类，对策子类由对策组件构成。

对策类：下图阐明了对策类的结构。每个对策类包括一个类名、类介绍及一个或多个对策子类。

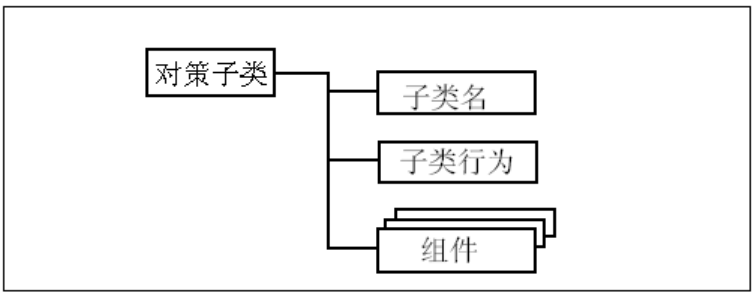


图表 5 对策类的结构

类名为对策类标识和分类提供必需的信息。每个对策类有一个唯一的名字，分类信息由三个字符的短名组成。类的短名被用于该类的子类的简名规范中。

类介绍描述了这些子类达到安全目标的通用目的和方法。对策类的定义不反映规范中的任何正式分类法。

对策子类：下图阐明了对策子类的结构。每个对策类包括一个子类名、子类介绍及至少 3 个对策组件。



图表 6 对策子类的结构

子类名部分提供了对一个功能族进行标识和分类时所必要的分类和描述性信息。每个功能族有一个唯一的名字。分类信息由七个字符的短名组成，开头三个字符与类名相同，后跟一个下划线和族名，例如 XXX_YYY。唯一的简短子类名提供了组件的主要的参考名。

子类行为叙述功能族的安全目的，对功能要求进行一般性描述。

对策组件根据其所要求的鲁棒性要求分为不同组件，每个组件使用子类名后面跟点和数字进行标识，随着数字的值的增加，其鲁棒性要求也随之增加。

3 安全对策等级划分

安全对策的等级划分，参考了 GB 17859、GB/TFORCE8336、TCSEC、SP800-53、《等级保护实施指南/评估指南》等国内外信息安全标准。不同类型的对策，参照的标准有所不同。如下表所示：

框架		主要参照标准	强度描述		
			第一级	第二级	第三级
安全策略文档框架		ISO17799	满足公司安全管理需要的安全策略文档基本要求	通过良好定义过程来提高安全策略文档管理能力	对安全策略文档管理能力进行计划和跟踪
安全组织框架			满足公司安全管理需要的安全组织基本要求	通过良好定义过程来提高安全组织管理能力	对安全组织管理能力进行计划跟踪
安全运作框架		ISO17799，ISO15408，SP800－53	满足公司安全管理需要的安全运作基本要求	通过良好定义过程来提高安全运作能力	对安全运作能力进行计划跟踪
安全技术框架	物理安全	GA/T 390 《等级保护通用技术要求》	相当于该标准基本要求	相当于该标准较高要求	相当于该标准严格要求
	网络与通信安全		为保证网络对业务的支撑能力应采取的基本措施	通过良好定义过程来提高网络的安全管理能力	对网络安全管理能力进行计划和跟踪
	边界保护	等级保护实施指南	相当于该标准中的自主保护级	相当于该标准中的指导保护级	相当于该标准中的监督保护级
	计算环境	GA/T 388 等级保护操作系统技术要求	相当于该标准中的系统审计保护级	相当于该标准中安全标记保护级	相当于该标准中的结构化保护级
		TCSEC 中的《可信数据库安全要求》	相当于该标准中C1	相当于该标准中C2	相当于该标准中B1
		GB/T 18336 (CC)	在内部管理环境下的安全保障要求	在复杂管理环境下的安全保障要求	在强对抗环境下的安全保障要求

图表 7 安全对策的等级划分

其中**第一级要求**基本相当于公安部计算机系统等级保护中的自主性保护级，主要适用于一般信息系统，要求具备对信息和系统进行基本保护的能力，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。

主要安全技术要求：

- 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；

- 通过份区域保护，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。

主要安全管理要求（包括运作、组织、策略文档）有：

- 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。

本安全对策框架中**第二级要求**基本相当于公安部计算机系统等级保护中的指导性保护级，适用于公司的重要信息系统，应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，本级要求采用系统化的设计方法（即把各种安全机制设计成单个安全子系统），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，本级的要求建立必要的信息系统安全管理制度，对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。

主要有：

- 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。

本安全对策框架中的**第三级要求**基本相当于公安部计算机系统等级保护中的监督性保护级，适用于公司的核心系统，应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，本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的。这些安全技术主要包括：

- 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，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。”

主要有：

- 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、应急与安全时间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。

4 安全技术等级化框架

4.1 TPR 类：物理环境安全

物理环境安全的总体目标是保障其所支持的业务正常运行，防止物理环境遭受外部和内部的破坏和滥用，避免和降低对其所支持的业务系统的损害。

4.1.1 防火 TPR_FIR

4.1.1.1TPR_FIR.1

关键位置的建筑材料耐火等级应符合 GBJ16-1987 中规定的二级要求；非关键位置的建筑材料的耐火等级应不低于 GBJ16-1987 中规定的三级要求；应设置灭火设备，并培训相关人员熟悉灭火设备的使用方法。

4.1.1.2TPR_FIR.2

关键位置的建筑材料耐火等级应符合 GBJ16-1987 中规定的二级要求；非关键位置的建筑材料的耐火等级应不低于 GBJ16-1987 中规定的三级要求；应设置灭火设备和**火灾报警系统**，并培训相关人员熟悉灭火设备的使用方法。**定期对灭火设备的可用性进行检查**。

4.1.1.3TPR_FIR.3

关键位置的建筑材料耐火等级应**符合 GB50045-95 中规定的二级耐火要求**；非关键位置的建筑材料的耐火等级应不低于 GBJ16-1987 中规定的**二级**要求；应设置灭火设备和火灾**自动**报警系统，并培训相关人员熟悉灭火设备的使用方法。定期对灭火设备的可用性进行检查。**并将脆弱区和危险区进行隔离**。

4.1.2 供电 TPR_SUP

4.1.2.1TPR_SUP.1

应将计算机系统供电与其它供电分开，提供短期的电力供应（如：UPS 设备），在机房电源接入处设置总开关或紧急断路器。

4.1.2.2TPR_SUP.2

应将计算机系统供电与其它供电分开，提供短期的电力供应（如：UPS 设备），在机房电源接入处设置总开关或紧急断路器。**增加设置稳压器和过电压防护设备。**

4.1.2.3TPR_SUP.3

应将计算机系统供电与其它供电分开，提供短期的电力供应（如：UPS 设备），在机房电源接入处设置总开关或紧急断路器。增加设置稳压器、过电压防护设备和**备用供电系统。**

4.1.3 空调 TPR_CON

4.1.3.1TPR_CON.1

设置必要的空调和湿度调节设施。

4.1.3.2TPR_CON.2

应有较完备的中央空调系统，保证机房温度/湿度的变化在计算机运行所允许的范围。

4.1.3.3TPR_CON.3

应有**完备的**中央空调系统（**有冗余**），保证机房**各个区域**的温度/湿度变化能

满足计算机运行、人员活动和其它辅助设备的要求。

4.1.4 防潮 TPR_WAT

4.1.4.1TPR_WAT.1

水管安装不得穿过屋顶和活动地板下，穿过墙壁和楼板的水管应使用套管，并采取可靠的密封措施；采取措施防止雨水通过屋顶和墙壁渗透、室内水蒸气结露和地下积水的转移与渗透。

4.1.4.2TPR_WAT.2

水管安装不得穿过屋顶和活动地板下，穿过墙壁和楼板的水管应使用套管，并采取可靠的密封措施；采取措施防止雨水通过屋顶和墙壁渗透、室内水蒸气结露和地下积水的转移与渗透。**还应安装对水敏感的检测仪表或元件，对机房进行防水检测、报警。**

4.1.4.3TPR_WAT.3

水管安装不得穿过屋顶和活动地板下，穿过墙壁和楼板的水管应使用套管，并采取可靠的密封措施；采取措施防止雨水通过屋顶和墙壁渗透、室内水蒸气结露和地下积水的转移与渗透。还应安装对水敏感的检测仪表或元件，对机房进行防水检测、报警。**机房应设有排水口，以便迅速排出积水。**

4.1.5 防静电 TPR_STA

4.1.5.1TPR_STA.1

控制机房温湿度，使其保持在不易产生静电的范围内。

4.1.5.2TPR_STA.2

控制机房温湿度，使其保持在不易产生静电的范围内。**人员服装采用不易产**

生静电的衣料，工作鞋选用低阻值材料制作。

4.1.5.3TPR_STA.3

控制机房温湿度，使其保持在不易产生静电的范围内。人员服装采用不易产生静电的衣料，工作鞋选用低阻值材料制作。机房内采用防静电地板。

4.1.6 防雷击 TPR_THU

4.1.6.1TPR_THU.1

构建接地系统，设置避雷地。

4.1.6.2TPR_THU.2

构建接地系统，设置避雷地。应设置安全防护地与屏蔽地，应采用阻抗尽可能小的良导体的粗线。

4.1.6.3TPR_THU.3

构建接地系统，设置避雷地。应设置安全防护地与屏蔽地，应采用阻抗尽可能小的良导体的粗线。设置交流电源地线，并将该“地线”连通机房的地线网。

4.1.7 电磁防护 TPR_TEM

4.1.7.1TPR_TEM.1

采用接地的方法防止外界电磁干扰和设备寄生耦合干扰；采用屏蔽方法，减少外部电器设备对计算机的瞬间干扰；并将计算机机房的位置选在外界电磁干扰小的地方和远离可能接收辐射信号的地方。

4.1.7.2TPR_TEM.2

采用接地的方法防止外界电磁干扰和设备寄生耦合干扰；采用屏蔽方法，减

少外部电器设备对计算机的瞬间干扰；并将计算机机房的位置选在外界电磁干扰小的地方和远离可能接收辐射信号的地方。**电源线和通信电缆隔离开，避免互相干扰。**

4.1.7.3TPR_TEM.3

采用接地的方法防止外界电磁干扰和设备寄生耦合干扰；采用屏蔽方法，减少外部电器设备对计算机的瞬间干扰；并将计算机机房的位置选在外界电磁干扰小的地方和远离可能接收辐射信号的地方。电源线和通信电缆隔离开，避免互相干扰。**采用必要措施，防止电磁泄露；对磁带、磁盘等磁介质设备的保管存放，应注意电磁感应的影响，如使用铁制柜存放。**

4.1.8 位置选择 TPR_LOC

4.1.8.1TPR_LOC.1

机房场地避免在建筑物的最高层、地下室以及用水设备的下层或隔壁。

4.1.8.2TPR_LOC.2

机房场地避免在建筑物的高层、地下室以及用水设备的下层或隔壁。**应当避开强电场、强磁场、易发生火灾、潮湿、易遭受雷击和重度环境污染的地区。**

4.1.8.3TPR_LOC.3

机房场地避免在建筑物的高层、地下室以及用水设备的下层或隔壁。应当避开强电场、强磁场、易发生火灾、潮湿、易遭受雷击和重度环境污染的地区。**应避免靠近公共区域，如运输邮件通道、停车场或餐厅等。**

4.1.9 设备安全 TPR_EQI

4.1.9.1TPR_EQI.1

设备和部件应有明显的无法除去的标记，以防更换并方便查找赃物，应安装防盗报警装置。

4.1.9.2TPR_EQI.2

设备和部件应有明显的无法除去的标记，以防更换并方便查找赃物，应安装防盗报警装置。机房报警系统有专人值守；机房外的设备，应采取加固防护措施。

4.1.9.3TPR_EQI.3

设备和部件应有明显的无法除去的标记，以防更换并方便查找赃物，应安装防盗报警装置。机房报警系统有专人值守；机房外的设备，应采取加固防护措施。应安装应急灯等应急照明设备。应利用闭路电视系统对机房的各重要部位进行监视。保安监控系统应与报警系统相连，报警系统应当与当地公安机关和公司内部的保卫部门相连。

4.1.10 防干扰和窃听 TPR _TAP

4.1.10.1 TPR _TAP.1

应有探测线路截获装置，及时发现线路截获的事件并报警；

4.1.10.2 TPR _TAP.2

应有探测线路截获装置，及时发现线路截获的事件并报警；应有定位线路截获装置，能发现线路截获窃取设备的准确位置。

4.1.10.3 TPR _TAP.3

应有探测线路截获装置，及时发现线路截获的事件并报警；应有定位线路截获装置，能发现线路截获窃取设备的准确位置。**应有对抗线路截获装置，能阻止线路截获窃取设备的有效使用。**

4.1.11 门禁 TPR_JAN

4.1.11.1 TPR_JAN.1

在系统所处环境的出入口设置专职警卫人员。

4.1.11.2 TPR_JAN.2

在系统所处环境的出入口设置专职警卫人员和**电子门禁。设置不间断视频监控手段。**

4.1.11.3 TPR_JAN.3

在系统所处环境的出入口设置专职警卫人员、电子门禁**和基于访问者生物特征身份鉴别设施。**设置不间断视频监控手段和**远红外监控手段。**

4.2 TNI 类：网络与通信安全

4.2.1 主干网可用性保护 TNI_AVI

4.2.1.1TNI_AVI.1

骨干网必须提供经过协议的响应级别、服务的连续性、抵制通信服务的意外和故意中断。必须保证充分保护的信息不拖延、误传递或不传递，和其他网络必须无缝连接。

4.2.1.2TNI_AVI.2

骨干网必须提供经过协议的响应级别、服务的连续性、抵制通信服务的意外和故意中断。必须保证充分保护的信息不拖延、误传递或不传递，和其他网络必须无缝连接。**骨干网的访问控制必须能够区分用户对数据传输的访问和管理员对网络管理与控制的访问。网络设备必须能认证从其他网络设备所有通信的来源，必须保护网络设备之间通信的完整性。**

4.2.1.3TNI_AVI.3

骨干网必须提供经过协议的响应级别、服务的连续性、抵制通信服务的意外和故意中断。必须保证充分保护的信息不拖延、误传递或不传递，和其他网络必须无缝连接。骨干网的访问控制必须能够区分用户对数据传输的访问和管理员对网络管理与控制的访问。网络设备必须能认证从其他网络设备所有通信的来源，必须保护网络设备之间通信的完整性。**骨干网必须能够安全地与其它的骨干网和当地的用户环境互操作。安全控制措施应能有效对抗网络阻塞攻击、扩散攻击、窃取攻击、网络管理通信攻击。**

4.2.2 内部网络防护 TNI_INT

4.2.2.1TNI_INT.1

内部网络结构应具有清晰的层次，所有网络端口应进行充分描述和标记。

4.2.2.2TNI_INT.2

根据各部门的工作职能、重要性、所涉及信息等级等因素，划分不同的子网或网段。不同的区域在交换机上划分不同 VLAN，不同 VLAN 之间的路由设置访问控制。按照方便管理和控制的原则为各子网、网段分配 IP 地址段。

4.2.2.3TNI_INT.3

根据各部门的工作职能、重要性、所涉及信息等级等因素，划分不同的子网

或网段。不同的区域在交换机上划分不同 VLAN，不同 VLAN 之间的路由设置访问控制。采用子网的概念进行网络逻辑和物理划分，同一子网应尽可能地只支持单一的业务、服务或流程，形成清晰的网络边界。同等安全水平的服务器应采用集中管理的方式，并与客户端工作站进行分离。

4.2.3 网络设备用户身份鉴别 TNI_IDT

4.2.3.1TNI_IDT.1

采用网络设备自身提供本地身份鉴别机制，如口令认证或者用户名/口令认证。

4.2.3.2TNI_IDT.2

采用用户集中管理方式进行用户身份鉴别，如 Radius 或者 TACACS+等，对用户的分配和管理集中在认证服务器端。

4.2.3.3TNI_IDT.3

采用用户集中管理方式进行用户身份鉴别，如 Radius 或者 TACACS+等，对用户的分配和管理集中在认证服务器端，采用多因素身份鉴别技术，如采用 Token 技术，生物特征识别，IC 卡等。

4.2.4 网络设备登录控制 TNI_TEL

4.2.4.1TNI_TEL.1

对所有设备的管理端口（vty/sc0/vlan0/aux/tty/console 等）的访问，均需要有相当认证机制。

4.2.4.2TNI_TEL.2

对设备的所有管理端口进行访问控制，对登录的记录包括通过设备自身记录

以及人工记录。

4.2.4.3TNI_TEL.3

增强设备登录的安全控制和管理，要求至少采取下列措施中的一种或者多种，以达到所需的安全需求：

a）采用带外管理方式，使得管理链路和数据交换链路隔离，通过专用内部管理网络访问管理设备

b）采用数据加密信道方式，对登录信道进行数据保护，如采用 VPN 信道，SSH 隧道等技术

c）采用一次性口令技术

d）采用动态口令技术

e）对设备的登录控制措施效能评估和审计，对审计和评估的结果进行相关处理

4.2.5 密码技术 TIN_ENC

4.2.5.1TIN_ENC.1

对称加密算法的密钥位数必须等同于 64 位 DES 算法。非对称加密算法的密钥位数必须等同于 512 位 RSA 算法；对于采用软件密码管理的系统，应提供在系统安装初始化时产生密钥种子，密钥种子不得固化在程序中。

通信过程中，至少对于敏感信息例如客户帐号、密码、金额等字段应进行加密。

4.2.5.2TIN_ENC.1

对于任何密钥，都必须设定其生命期，并提供相应的版本更替方案，对称加密算法的密钥位数必须等同于 128 位 3DES 算法。非对称加密算法的密钥位数必须等同于 1024 位 RSA 算法；系统的密码管理必须由相应硬件装置来完成。

通信过程中，应对整个报文或会话过程进行加密。

4.2.5.3TIN_ENC.1

对于任何密钥，都必须设定其生命期，并提供相应的版本更替方案，对称加密算法的密钥位数必须等同于 128 位 3DES 算法。非对称加密算法的密钥位数必须等同于 1024 位 RSA 算法；**密码运算应由相应硬件装置完成。硬件密码装置必须具备防物理攻击的功能，达到 FIPS140-2 级。**

通信过程中，应对整个报文或会话过程**以及信道**进行加密。

4.3 TEB 类：边界保护

4.3.1 网络边界访问控制 TEB_NAC

4.3.1.1TEB_NAC.1

限制用户可以建立什么样的连接以及通过网络传输什么样的数据，通过允许、拒绝经过网络访问控制设备的数据流，实现对进、出内部网络的服务和访问的控制。

4.3.1.2TEB_NAC.2

限制用户可以建立什么样的连接以及通过网络传输什么样的数据，通过允许、拒绝经过网络访问控制设备的数据流，实现对进、出内部网络的服务和访问的控制与**审计**。

4.3.1.3TEB_NAC.3

限制用户可以建立什么样的连接以及通过网络传输什么样的数据，通过允许、拒绝经过网络访问控制设备的数据流，实现对进、出内部网络的服务和访问的控制与审计。**在需要的情况下，提供专用抵御拒绝服务攻击的设备。**

4.3.2 远程访问 TEB_TEL

4.3.2.1TEB_TEL.1

所有的远程访问必须至少具备用户名/口令的身份鉴别和访问授权控制，必须对远程访问的用户进行统一集中管理，具备相关的申请登记流程和审批流程。

4.3.2.2TEB_TEL.2

远程访问接入对于内部系统的访问应当受到控制，必须采取适当的监控记录技术，记录接入时间，地址，电话，人员，访问对象等。应当建立独立的身份认证、鉴别和授权服务器，强化身份认证和鉴别能力。

4.3.2.3TEB_TEL.3

远程访问接入对于内部系统的访问应当受到控制，必须采取适当的监控记录手段，记录接入时间，地址，电话，人员，访问对象等。应当建立独立的身份认证、鉴别和授权服务器，强化身份认证和鉴别能力，**至少采用双因素认证的技术措施。**

4.3.3 防病毒网关 TEB_TVI

4.3.3.1TEB_TVI.1

设置防病毒网关对从外部网络进入用户内部网络的病毒进行过滤，一般主要针对 HTTP、HTTPS、FTP 和 SMTP 等协议进行过滤，保护用户内部网络不受病毒感染。

4.3.3.2TEB_TVI.2

设置防病毒网关对从外部网络进入用户内部网络的病毒进行过滤，一般主要针对 HTTP、HTTPS、FTP 和 SMTP 等协议进行过滤，保护用户内部网络不受病毒感染。**设置病毒集中监控中心来集中分发软件、进行病毒特征码升级。**

4.3.3.3TEB_TVI.3

设置防病毒网关对从外部网络进入用户内部网络的病毒进行过滤，一般主要针对 HTTP、HTTPS、FTP 和 SMTP 等协议进行过滤，保护用户内部网络不受病毒感染。设置病毒集中监控中心来集中分发软件、进行病毒特征码升级。**各病毒监控中心应做到集联控制。**

4.3.4 网络入侵防范 TEB_IDS

4.3.4.1.1 TEB_IDS.1

至少应包括数据收集、协议分析、行为检测、数据分析、攻击事件判断、安全报警等安全功能。

4.3.4.1.2 TEB_IDS.2

至少应包括数据收集、协议分析、行为检测、数据分析、攻击事件判断、**攻击事件的过滤规则调整、事件合并、**安全报警、**安全响应、排除响应**等安全功能。

4.3.4.1.3 TEB_IDS.3

至少应包括数据收集、协议分析、行为检测、数据分析、**流量监测、防躲避能力、事件关联、**攻击事件判断、**定制响应、阻断能力、设备联动、**攻击事件的过滤规则调整、事件合并、安全报警、安全响应、排除响应等安全功能。

4.4 TCE 类：保护计算环境

4.4.1 计算环境访问控制 TCE_TAC

4.4.1.1TCE_TAC.1

至少采用自主访问控制策略用访问控制表确定主体对客体的访问权限，阻止非授权用户读取信息。应用软件至少应实现其运行平台（主机操作系统、数据库和网络系统等）无法实施的访问权限控制。

4.4.1.2TCE_TAC.2

进行**更细粒度的自主访问控制，将自主访问控制能与身份鉴别和审计功能结合。**至少要求应用软件**独立地**实现与其运行平台（主机操作系统、数据库和网络系统等）实施的访问权限无关的访问权限控制，**支持权限的角色分离，限定资源访问路径，对访问行为进行审计。**

通过网络传输数据时，至少要**采用加密方式以确保保密性和完整性。**

4.4.1.3TCE_TAC.3

采用强制访问控制策略和功能，将访问控制能与身份鉴别和审计功能结合。至少要求应用软件独立**地**实现与其运行平台（主机操作系统、数据库和网络系统等）实施的访问权限无关的访问权限控制；支持权限的角色分离；限定资源访问路径；对访问行为进行审计。

通过网络传输数据时，至少要采用加密方式以确保保密性和完整性。

至少对从主机输入/输出的信息要进行安全属性控制和安全检测，验证其合法性、有效性和可用性；

4.4.2 身份鉴别 TCE_IDT

4.4.2.1TCE_IDT.1

至少采用用户名/口令方式进行身份鉴别，保证身份鉴别过程中口令不可见，用加密方式存储口令，保证身份鉴别的时效性，提供强制修改口令和弱口令检查的功能，记录登录失败。

分布式数据库系统中采用数据字典进行用户身份鉴别。

4.4.2.2TCE_IDT.2

至少采用用户名/口令对的方式进行身份鉴别，保证身份鉴别过程中口令不可见，**采用不可逆的加密方式存储口令**，保证身份鉴别的时效性，提供强制修改口令和弱口令检查的功能；记录登录失败和**鉴别尝试**。至少**采用两种身份验证机制。**

分布式数据库系统中采用数据字典进行用户身份鉴别，增加**操作系统和数据库系统对数据库用户标识和鉴别信息的双重保护**。

在信道中加密传输身份鉴别的用户名/口令，控制和监控用户的来源。

4.4.2.3TCE_IDT.3

采用消息摘要和数字证书等方式进行身份鉴别；IC 卡信息身份鉴别应采用密码技术；采用双因素或多因素认证机制；限制重复尝试。

分布式数据库系统中采用数据字典进行用户身份鉴别，增加操作系统和数据库系统对数据库用户标识和鉴别信息的双重保护。

在信道中加密传输身份鉴别的用户名/口令，控制和监控用户的来源。

4.4.3 安全审计 TCE_SAU

4.4.3.1TCE_SAU.1

至少能产生完整的审计数据并能提供审计数据的查阅、分析和备份。

审计功能的设计应与用户标识与鉴别、自主访问控制、标记与强制访问控制等安全功能的设计紧密结合。

4.4.3.2TCE_SAU.2

至少能产生完整的审计数据并能提供审计数据的查阅，**能以风险分析为依据进行审计事件选择，提高实时报警功能**。

审计功能的设计应与用户标识与鉴别、自主访问控制、标记与强制访问控制等安全功能的设计紧密结合。

为网络环境下运行的数据库管理系统建立分布式的审计系统。

4.4.3.3TCE_SAU.3

增强审计的精度和范围，提供审计数据的查阅，能以风险分析为依据进行审计事件选择，**运用集中审计和事件关联分析，**提高实时报警功能。

审计功能的设计应与用户标识与鉴别、自主访问控制、标记与强制访问控制等安全功能的设计紧密结合。

为网络环境下运行的数据库管理系统建立分布式的审计系统，并以审计中心进行管理和控制。

4.4.4 主机入侵防范 TCE_IDS

4.4.4.1TCE_IDS.1

至少应包括主机相关数据的收集、数据分析、行为检测、攻击事件判断、安全报警等安全功能。

4.4.4.2TCE_IDS.2

至少应包括主机相关数据收集、数据分析、行为检测、攻击事件判断、**攻击事件的过滤规则调整、事件合并**、安全报警、**安全响应、排除响应**等安全功能。

4.4.4.3TCE_IDS.3

至少应包括主机相关数据收集、数据分析、行为检测、**流量监测、防躲避能力、关联分析**、攻击事件判断、**定制响应、主动阻断、设备联动**、攻击事件的过滤规则调整、事件合并、安全报警、安全响应、排除响应等安全功能。

4.4.5 病毒和恶意代码防范 TCE_VIR

4.4.5.1TCE_VIR.1

至少在其计算环境的边界系统（如网关、电子邮件服务器）部署病毒防范系统。

4.4.5.2TCE_VIR.2

在其计算环境的边界系统（如网关、电子邮件服务器）部署病毒防范系统，**在计算环境中部署具有病毒实时防护功能计算机防病毒软件**。

4.4.5.3TCE_VIR.3

在其计算环境的边界系统（如网关、电子邮件服务器）部署病毒防范系统。在计算环境中部署具有病毒实时防护功能计算机防病毒软件。**增强病毒防范的日常管理机制和审查机制，设置合理的病毒库升级策略。**

4.4.6 数据库设计安全 TCE_DBS

4.4.6.1TCE_DBS.1

至少在数据库的系统设计中确保不留“后门”，采用分层设计，区分普通操作模式和系统维护模式。

4.4.6.2TCE_DBS.2

至少在数据库的设计中确保系统设计时不留“后门”，采用分层设计，区分普通操作模式和系统维护模式，**只为系统管理员提供修改或替换系统提供的实用程序的功能；提供识别由通信渠道接收的信息的来源者的方法。**

4.4.6.3TCE_DBS.3

至少在数据库的设计中确保系统设计时不留“后门”，采用分层设计，区分普通操作模式和系统维护模式。只为系统管理员提供修改或替换系统提供的实用程序的功能；提供识别由通信渠道接收的信息的来源者的方法。**增加系统恢复机制，**以及**为系统管理员提供一种产生安全参数值详细报告的机制。**

4.4.7 应用系统测试 TCE_APT

4.4.7.1TCE_APT.1

至少对应用系统的安全功能进行黑箱测试。

4.4.7.2TCE_APT.2

至少对应用系统的安全功能进行黑箱测试，并**对所有安全功能的白箱测试，根据应用系统的容量规划进行压力测试。**

4.4.7.3TCE_APT.3

对应用系统的安全功能进行黑箱测试，并对所有安全功能的白箱测试，根据应用系统的容量规划进行压力测试。**要求测试能够为是否具备每项安全功能提供证据。**

5 安全运作等级化框架

5.1 ORA 类：风险管理

5.1.1 资产鉴别 ORA_ASE

5.1.1.1ORA_ASE.1

应当对信息资产进行登记，维护信息资产清单，指定信息资产的责任人。

5.1.1.2ORA_ASE.2

应当对信息资产进行登记、**分类和标识**，维护信息资产清单，指定信息资产的责任人。**应根据资产的重要程度对资产进行定性赋值**。

5.1.1.3ORA_ASE.3

应当对信息资产进行登记、分类和标识，维护信息资产清单，指定信息资产的责任人。**用半定量的方法对公司的信息资产进行赋值，并用体系架构的方法描述信息资产。**

5.1.2 威胁分析 ORA_THR

5.1.2.1ORA_THR.1

应根据以往发生的安全事件、外部提供的资料和积累的经验对威胁进行分析。

5.1.2.2ORA_THR.2

在国内外标准和相关参考文档的基础上，结合业务应用、系统结构特点以及业务流程等因素，建立并维护一个较全面的威胁列表。

5.1.2.3ORA_THR.3

应采用一种系统化风险分析方法对威胁进行分析，考虑威胁源在机密性、完整性或可用性等方面造成损害，从而得到威胁值。

5.1.3 脆弱性分析 ORA_VUL

5.1.3.1ORA_VUL.1

应通过安全扫描工具来获得系统的安全弱点。

5.1.3.2ORA_VUL.2

应用**人工评估**、工具扫描、**安全访谈**等方法或工具对系统的脆弱性进行分析和评估，并形成**脆弱性列表**。

5.1.3.3ORA_VUL.3

应用人工评估、工具扫描、安全访谈、**渗透测试**等方法或工具对系统的脆弱性进行分析和评估，形成脆弱性列表。并**将定期的脆弱性评估和报告形成制度**。

5.1.4 风险分析 ORA_ANA

5.1.4.1ORA_ANA.1

应由安全管理人员和外部安全专家通过经验来判断系统弱点，形成简单的风险报告。

5.1.4.2ORA_ANA.2

应采用多层面、多角度的系统分析方法，由安全管理人员和外部安全专家对资产、威胁和脆弱性等方面进行**定性综合评价**，最终形成风险评估报告。

5.1.4.3ORA_ANA.3

应采用多层面、多角度的系统分析方法，由安全管理人员和外部安全专家对资产、威胁和脆弱性等方面进行半定量综合评价，最终形成风险评估报告。应将风险评估中的信息资产、威胁、脆弱性、防护措施等评估项综合到一个数据库中进行管理。

5.1.5 选择安全控制措施 ORA_CTR

5.1.5.1ORA_CTR.1

用信息安全领域常用的产品和服务分类列表作为基线，用基线选择的方法决定需要实施的信息安全控制措施。

5.1.5.2ORA_CTR.2

根据风险评估的结果，结合公司对于信息安全的需求选择安全控制措施。

5.1.5.3ORA_CTR.3

根据风险评估的结果，结合公司对于信息安全的需求选择安全控制措施。同时，通过定性或者半定量的方法，对相关的各种控制措施进行综合评价，以便得出紧迫性、优先级、投资比重等评价，作为落实安全控制措施的依据。

5.1.6 安全措施的实施与确认 ORA_VAD

5.1.6.1ORA_VAD.1

编写安全解决方案，进行安全控制措施的实施。

5.1.6.2ORA_VAD.2

编写安全解决方案，进行安全控制措施的实施。结合已采用的安全控制措施，

分析可能存在的残余风险，并由高层管理人员来做出风险接受的决定。

5.1.6.3ORA_VAD.3

编写安全解决方案，进行安全控制措施的实施。结合已采用的安全控制措施，分析可能存在的残余风险，并由高层管理人员来做出风险接受的决定。**采用系统化的方法实施二次风险评估，验证防护措施的有效性。**

5.2 OEN 类：工程建设安全管理

5.2.1 安全项目的立项管理 OEN_CON

5.2.1.1OEN_CON.1

信息系统的安全建设立项要符合信息系统安全建设的总体规划, 经公司安全主管部门科学论证后方可进行设计和组织实施。

5.2.1.2OEN_CON.2

信息系统的安全建设立项要符合信息系统安全建设的总体规划, 经公司安全主管部门**组织内部相关专家**科学论证后方可进行设计和组织实施。

5.2.1.3OEN_CON.3

信息系统的安全建设立项要符合信息系统安全建设的总体规划, 经公司安全主管部门组织内部和**外部**相关专家科学论证后方可进行设计和组织实施。

5.2.2 安全需求分析 OEN_REQ

5.2.2.1OEN_REQ.1

根据 ORA_THR.1、ORA_VUL.1、ORA_ANA.1、ORA_CTR.1 的要求进行安全需求分析。

5.2.2.2OEN_REQ.2

根据 **ORA_THR.2**、**ORA_VUL.2**、**ORA_ANA.2**、**ORA_CTR.2** 的要求进行安全需求分析。

5.2.2.3OEN_REQ.3

根据 **ORA_THR.3**、**ORA_VUL.3**、**ORA_ANA.3**、**ORA_CTR.3** 的要求进行安全需求分析。

5.2.3 安全功能规范 OEN_FSP

5.2.3.1OEN_FSP.1

应对系统的安全功能进行说明。

5.2.3.2OEN_FSP.2

应编写安全功能规范。

5.2.3.3OEN_FSP.3

应编写正式的安全功能规范。功能安全规范应该是内在一致的，应该完备地表示信息系统的安全属性。

5.2.4 高层安全设计 OEN_HLD

5.2.4.1OEN_HLD.1

应进行高层安全设计。

5.2.4.2OEN_HLD.2

应进行较为完整的高层安全设计，并将功能安全规范细化到子系统。

5.2.4.3OEN_HLD.3

应进行较为完整的高层安全设计，并将功能安全规范细化到子系统。高层安全设计应该标识信息系统所要求的任何基础性硬件、固件、软件、和/或通信，和在这些硬件、固件、软件、和/或通信中实现的支持性保护机制所提供的功能表示。

5.2.5 安全产品选型 OEN_PRO

5.2.5.1OEN_PRO.1

安全产品具有在国内生产、经营和销售的许可证，密码产品符合国家密码主管部门的要求，来源于国家主管部门批准的密码研制单位。

5.2.5.2OEN_PRO.2

安全产品具有在国内生产、经营和销售的许可证，密码产品符合国家密码主管部门的要求，来源于国家主管部门批准的密码研制单位。关键安全产品应获得国家相关安全认证，在选型中根据实际需要制定安全产品选型的标准。

5.2.5.3OEN_PRO.3

安全产品具有在国内生产、经营和销售的许可证，密码产品符合国家密码主管部门的要求，来源于国家主管部门批准的密码研制单位。所有安全产品或信息技术产品的安全模块应获得国家相关安全认证，在选型中根据实际需要制定安全产品选型的标准。

5.2.6 外包软件安全控制

5.2.6.1OEN_EPI.1

在软件的开发被外包时应当考虑许可安排、代码的所有权和知识产权以及质量合格证和所进行的工作的精确度。

5.2.6.2OEN_EPI.2

在软件的开发被外包时应当考虑许可安排、代码的所有权和知识产权以及质量合格证和所进行的工作的精确度。**还应进行质量审核、在安装之前进行测试以检测特洛伊代码，并要求已方提供源代码以及相关设计、实施文档。**

5.2.6.3OEN_EPI.3

在软件的开发被外包时应当考虑许可安排、代码的所有权和知识产权以及质量合格证和所进行的工作的精确度。还应进行质量审核、在安装之前进行测试以检测特洛伊代码，并要求已方提供源代码以及相关设计、实施文档。**还要对源代码进行安全审核。**

5.2.7 交付和运行 OEN_ADO

5.2.7.1OEN_ADO.1

交付过程需要系统控制以及交付设备和程序来提供保证，以确保接收方所接受的信息系统的版本正是发送者发送的，而没有任何修改。

5.2.7.2OEN_ADO.2

交付过程需要系统控制以及交付设备和程序来提供保证，以确保接收方所接受的信息系统的版本正是发送者发送的，而没有任何修改。**还需要简单的安装、生成和启动程序。**

5.2.7.3OEN_ADO.3

交付过程需要系统控制以及交付设备和程序来提供保证，以确保接收方所接受的信息系统的版本正是发送者发送的，而没有任何修改。**安装、生成和启动程序应准确描述信息系统安全地安装、生成和启动所必要的步骤。**

5.2.8 系统安全检测和验收 OEN_TES

5.2.8.1OEN_TES.1

由验收组进行安全检测和验收。验收前，应编制验收大纲；验收大纲由验收组提出。

5.2.8.2OEN_TES.2

由验收组进行安全检测和验收。验收前，应编制验收大纲；验收大纲由验收组提出。

应进行安全测试论证信息系统是否满足安全功能规范。应该论证功能规范中所描述信息系统安全功能和测试文档所标识的测试之间的对应性是完备的。并论证测试文档中所标识的测试足以论证信息系统安全功能运行和它的高层设计是一致的。

5.2.8.3OEN_TES.3

应进行安全测试论证信息系统是否满足安全功能规范。应该论证功能规范中所描述信息系统安全功能和测试文档所标识的测试之间的对应性是完备的。并论证测试文档中所标识的测试足以论证信息系统安全功能运行和它的高层设计是一致的。**还应当严格地论证功能规范所标识的信息系统的所有外部接口已经被完备测试过了。**

5.3 OPM 类：物理环境管理

5.3.1 机房管理 OPM_ROM

5.3.1.1OPM_ROM.1

机房出入应有指定人员负责，确保未经允许的人员不准进入机房；获准进入机房的来访人员，其活动范围应受到限制，并有接待人员陪同；没有指定管理人

员的明确准许，任何记录介质、文件材料及各种被保护品均不准带出机房，与工作无关的物品（如：食品、香烟等）均不准带入机房；并经常打扫机房防止灰尘以及进行灭鼠工作。

5.3.1.2OPM_ROM.2

机房出入应有**保安**人员负责，确保未经允许的人员不准进入机房；获准进入机房的来访人员，**应出示有效证件并履行严格的登记手续**，其活动范围应受到限制，并有接待人员陪同；没有指定管理人员的明确准许，任何记录介质、文件材料及各种被保护品均不准带出机房，与工作无关的物品（如：食品、香烟等）均不准带入机房；并经常打扫机房防止灰尘以及进行灭鼠工作。**禁止携带磁铁、个人计算机等电子设备进出机房；**

5.3.1.3OPM_ROM.3

机房出入应有保安人员负责，确保未经允许的人员不准进入机房；**内部人员须在门禁处使用工卡（得到指示方可进入），不允许利用别人的工卡进入（包括别人刷卡，跟随进入）**；获准进入机房的来访人员，应出示有效证件并履行严格的登记手续，**佩戴临时出入证**。其活动范围应受到限制，并有接待人员陪同；没有指定管理人员的明确准许，任何记录介质、文件材料及各种被保护品均不准带出机房，与工作无关的物品（如：食品、香烟等）均不准带入机房；并经常打扫机房防止灰尘以及进行灭鼠工作。禁止携带磁铁、个人计算机等电子设备进出机房。

5.3.2 办公环境管理 OPM_OFM

5.3.2.1OPM_OFM.1

工作人员下班后，终端计算机应关闭；存放敏感文件或信息载体的文件柜应上锁或设置密码；工作人员调离部门或更换办公室时，应立即交还办公室钥匙。禁止使用调制解调器拨号上网。

5.3.2.2OPM_OFM.2

工作人员下班后，终端计算机应关闭；存放敏感文件或信息载体的文件柜应上锁或设置密码；工作人员调离部门或更换办公室时，应立即交还办公室钥匙。禁止使用调制解调器拨号上网。**工作人员离开座位超过一定时间，应将桌面上含有敏感信息的纸件文档在抽屉或文件柜内，计算机应退出登录状态，采用屏幕保护口令加以保护或关机；**

5.3.2.3OPM_OFM.3

工作人员下班后，终端计算机应关闭；存放敏感文件或信息载体的文件柜应上锁或设置密码；工作人员调离部门或更换办公室时，应立即交还办公室钥匙。禁止使用调制解调器拨号上网。工作人员离开座位超过一定时间，应将桌面上含有敏感信息的纸件文档在抽屉或文件柜内，计算机应退出登录状态，采用屏幕保护口令加以保护或关机；**应尽可能使办公环境与机房的物理位置在一起，以便进行统一的物理保护。**

5.3.3 环境设备维护 OPM_MAI

5.3.3.1OPM_MAI.1

机房内（包括电源间）的所有环境设备（如空调、电源等），由确定的部门负责管理，并随时受理和处理这些设备的突发事故。

5.3.3.2OPM_MAI.2

机房内（包括电源间）的所有环境设备（如空调、电源等），由确定的部门负责管理，并随时受理和处理这些设备的突发事故。**机房值班员要每天到机房巡视至少一次。对各种设备的运转情况（包括电源、空调）进行必要的检查。对电源、空调进行定期（年度）检修。**

5.3.3.3OPM_MAI.3

机房内（包括电源间）的所有环境设备（如空调、电源等），由确定的部门负责管理，并随时受理和处理这些设备的突发事故。机房值班员要每天到机房巡视至少一次。对各种设备的运转情况（包括电源、空调）进行必要的检查。对电源、空调进行定期（半年）检修。

5.4 OHO 类：主机维护

5.4.1 主机设备维护 OHO_EQI

5.4.1.1OHO_EQI.1

主机设备应当由指定的专人定期维护。

5.4.1.2OHO_EQI.2

主机设备应当由指定的专人定期维护，制定明确的维护目标和要求、维护流程和操作规范，测试规范，制定相关的维护制度，维护对主机设备的维护纪录，并根据主机设备维护情况向上级管理机构报告主机设备运行状态。

5.4.1.3OHO_EQI.3

主机设备应当由指定的专人定期维护，制定明确的维护目标和要求、维护流程和操作规范，测试规范，制定相关的维护制度，维护对主机设备的维护纪录，并根据主机设备维护情况向上级管理机构报告主机设备运行状态，制定主机设备维护指标考评体系，考评主机设备的平均无故障运行时间、故障修复时间、故障发生率等。

5.4.2 账户管理 OHO_ACC

5.4.2.1OHO_ACC.1

删除或者禁用不使用的系统缺省账户。

5.4.2.2OHO_ACC.2

删除或者禁用不使用的系统缺省账户。**建立账户管理制度，记录用户的系统登录活动。**

5.4.2.3OHO_ACC.3

删除或者禁用不使用的系统缺省账户。建立账户管理制度，记录用户的系统登录活动。**对于账号管理制度的执行情况进行检查和监督，对发现的问题和异常情况进行相关处理。**

5.4.3 远程登陆管理 OHO_TEL

5.4.3.1OHO_TEL.1

应当制定远程系统管理制度，记录和分配系统账户远程系统管理的操作权限分配。

5.4.3.2OHO_TEL.2

应当制定远程系统管理制度，记录和分配系统账户远程系统管理的操作权限分配。**采用具有加密功能的远程终端和通信信道进行远程系统管理。**

5.4.3.3OHO_TEL.3

应当制定远程系统管理制度，记录和分配系统账户远程系统管理的操作权限分配。采用具有加密功能的远程终端和通信信道进行远程系统管理。**定期审计系**

统管理人员的远程系统管理情况，对审计中发现的异常和问题及时处理和报告。

5.4.4 漏洞控制 OHO_VER

5.4.4.1OHO_VER.1

定期安装系统的最新补丁程序，并根据厂家提供的可能危害计算机的漏洞进行及时修补，并在安装系统补丁前对现有的重要文件进行备份。

5.4.4.2OHO_VER.2

定期安装系统的最新补丁程序，并根据厂家提供的可能危害计算机的漏洞进行及时修补，并在安装系统补丁前对现有的重要文件进行备份，**并对补丁程序进行初步测试，以防止对现有软件的不兼容性。**

5.4.4.3OHO_VER.3

定期安装系统的最新补丁程序，并根据厂家提供的可能危害计算机的漏洞进行及时修补，并在安装系统补丁前对现有的重要文件进行备份，并对补丁程序进行初步测试，以防止对现有软件的不兼容性。**定期进行系统漏洞扫描，根据业务需求最小化系统的服务。**

5.4.5 防病毒管理 OHO_VIR

5.4.5.1OHO_VIR.1

应有指定人员检查网络内防病毒网关和主机的病毒检测情况，并保存染毒和杀毒记录，文件传输过程中应先进行病毒查杀，每周定期升级防病毒网关系统。

5.4.5.2OHO_VIR.2

应有指定人员检查网络内防病毒网关和主机的病毒检测情况，并保存染毒和杀毒记录，文件传输过程中应先进行病毒查杀，**所有网络内的计算机、**防病毒网

关上安装的防病毒软件应每周定时升级，紧急情况下应增加升级次数。

5.4.5.3OHO_VIR.3

应有指定人员检查网络内防病毒网关和主机的病毒检测情况，并保存染毒和杀毒记录，文件传输过程中应先进行病毒查杀，每周定时整体网络统一策略、统一升级、统一控制，紧急情况下增加升级次数；安全管理员每周对计算机主机防病毒产品、防病毒网关和邮件防病毒网关上截获的各种高风险病毒进行及时分析处理，并提供相应的报表；分别进行月度、季度和年度总结汇报，使主管领导和相关人员及时了解病毒防护状况。

5.5 ONE 类：网络维护

5.5.1 网络拓扑设计和规划 ONE_TOP

5.5.1.1ONE_TOP.1

具有详细和完整的网络拓扑设计需求说明、设计文档、网络拓扑、实施过程文档。

5.5.1.2ONE_TOP.2

具有详细和完整的网络拓扑设计需求说明、设计文档、网络拓扑、实施过程文档，需要强化网络拓扑/结构的变更过程和审批过程，网络拓扑图必须和当前实际运行情况保持一致。

5.5.1.3ONE_TOP.3

具有详细和完整的网络拓扑设计需求说明、设计文档、网络拓扑、实施过程文档，需要强化网络拓扑/结构的变更过程和审批过程，网络拓扑图必须和当前实际运行情况保持一致。需要对网络的设计、变更和审批进行定期的复核和审计。

5.5.2 IP 地址管理 ONE_IPM

5.5.2.1ONE_IPM.1

具有 IP 地址管理规定，应当具有统一的 IP 地址管理机构/人员，由该机构/人员负责对外部和内部各个部门人员的 IP 地址进行登记、维护和分配。

5.5.2.2ONE_IPM.2

具有 IP 地址管理规定，应当具有统一的 IP 地址管理机构/人员，由该机构/人员负责对外部和内部各个部门人员的 IP 地址进行登记、维护和分配。**实现对地址使用情况的实时动态监控，维护记录地址的使用情况，及时关闭被废止的地址，具有对 IP 地址的容量规划设计，确保各个部门有一定的地址容量冗余供扩展使用。**

5.5.2.3ONE_IPM.3

具有 IP 地址管理规定，应当具有统一的 IP 地址管理机构/人员，由该机构/人员负责对外部和内部各个部门人员的 IP 地址进行登记、维护和分配。实现对地址使用情况的实时动态监控，维护记录地址的使用情况，及时关闭被废止的地址，具有对 IP 地址的容量规划设计，确保各个部门有一定的地址容量冗余供扩展使用。**防止地址的伪造和欺骗。及时发现违反使用 IP 事件，并进行相关处理。应当实现对 IP 地址使用情况的审计功能。**

5.5.3 网络可靠性管理 ONE_REL

5.5.3.1ONE_REL.1

应当制定网络可靠性保障需求，制定相关的 SLA，并指定专门的内部部门或者外部部门维护和保证。

5.5.3.2ONE_REL.2

针对各个内部/外部部门的不同需求，制定相应的 SLA，并与这些部门签署这些 SLA。并对这些 SLA 的执行情况进行跟踪监控，对出现违反 SLA 的情况进行相关处理。

5.5.3.3ONE_REL.3

针对各个内部/外部部门的不同需求，制定相应的 SLA，并与这些部门签署这些 SLA。并对这些 SLA 的执行情况进行跟踪监控，对出现违反 SLA 的情况进行相关处理。建立网络可靠性监控系统，及时发现并处理可靠性中断/降低故障，对故障处理结果进行教训总结。对 SLA 的执行情况进行定期的审计。

5.5.4 路由管理 ONE_ROU

5.5.4.1ONE_ROU.1

应当具有路由设计和规划，明确在网络的各个部分的选择和使用恰当的路由协议，具备基本的路由 SLA，保证网络的互联互通。

5.5.4.2ONE_ROU.2

应当具有路由设计和规划，明确在网络的各个部分的选择和使用恰当的路由协议，具备基本的路由 SLA，保证网络的互联互通。对网络中使用的路由协议运行情况进行监控，对于动态路由，应当在满足互联互通的前提条件下实现可靠安全的认证交换制度，实现有效的防止路由欺骗功能。

5.5.4.3ONE_ROU.3

应当具有路由设计和规划，明确在网络的各个部分的选择和使用恰当的路由协议，具备基本的路由 SLA，保证网络的互联互通。对网络中使用的路由协议运行情况进行监控，对于动态路由，应当在满足互联互通的前提条件下实现可靠安全的认证交换制度，实现有效的防止路由欺骗功能。对路由协议的变更进行管理

和审批，对路由中断情况进行实时发现和处理、经验教训总结。

5.5.5 安全域规划 ONE_SED

5.5.5.1ONE_SED.1

针对公司内部不同的业务部门需求对其进行安全域规划。

5.5.5.2ONE_SED.2

针对公司内部不同的业务部门需求对其进行安全域规划。需要对安全域的保护功能进行详细的安全功能设计。

5.5.5.3ONE_SED.3

针对公司内部不同的业务部门需求对其进行安全域规划。需要对安全域的保护功能进行详细的安全功能设计。对安全域的使用和划分情况进行管理、审计和维护。

5.5.6 网络设备管理授权 ONE_ADV

5.5.6.1ONE_ADV.1

采用网络设备自身提供的普通/特权两级授权管理机制管理设备。

5.5.6.2ONE_ADV.2

采用设备提供的多级用户管理授权，对每一个不同的用户授予不同的设备管理权限。

5.5.6.3ONE_ADV.3

采用集中统一设备管理授权。

5.6 OCO 类：配置和变更管理

配置和变更管理通过在细化和修改信息系统的过程中进行规范和控制，确保网络系统的完整性。配置和变更管理阻止对信息系统进行非授权的修改、添加或删除。

5.6.1 配置管理计划 OCO_PLA

5.6.1.1OCO_PLA.1

应制定配置管理计划，并且每年进行审查和升级，以保证配置管理计划的可行性以及组织具有完成配置管理计划的能力。

5.6.1.2OCO_PLA.2

应制定配置管理计划，并且**每半年**进行审查和升级，以保证配置管理计划的可行性以及组织具有完成配置管理计划的能力。

5.6.1.3OCO_PLA.3

应制定配置管理计划，并且**每季度**进行审查和升级，以保证配置管理计划的可行性以及组织具有完成配置管理计划的能力。

5.6.2 配置管理自动化 OCO_AUT

5.6.2.1OCO_AUT.1

应该有措施来控制信息处理设备和系统的改变。应在关键的设备上采用半自动的配置管理工具，并使用半自动的方法对计算机进行升级，并对相关人员进行配置管理的培训。

5.6.2.2 OCO_AUT.2

应该有措施来控制信息处理设备和系统的改变。应在关键的设备上采用半自动的配置管理工具，并使用半自动的方法对计算机进行升级，并对相关人员进行配置管理的培训。**应确保网络系统的实现表示是通过自动方式控制的，并确保这些变化是已授权的行为所产生的。并且先对所有的配置变更进行测试，方能正式执行。**

5.6.2.3OCO_AUT.3

应该有措施来控制信息处理设备和系统的改变。应在关键的设备上采用半自动的配置管理工具，并使用半自动的方法对计算机进行升级，并对相关人员进行配置管理的培训。应确保网络系统的实现表示是通过自动方式控制的，并确保这些变化是已授权的行为所产生的。并且先对所有的配置变更进行测试，方能正式执行。**还要能自动确定网络系统版本间的变化，并标识出哪个配置项会因其余配置项的修改而受到影响。**

5.6.3 配置管理能力 OCO_CAP

5.6.3.1OCO_CAP.1

要求开发者所使用的版本号与所应表示的网络系统样本应完全对应，没有歧义。要求配置项应有唯一的标识。

5.6.3.2OCO_CAP.2

要求开发者所使用的版本号与所应表示的网络系统样本应完全对应，没有歧义。要求配置项应有唯一的标识。**配置管理计划应描述系统是如何使用的，并说明运行中的配置管理系统与配置管理计划的一致性，配置管理文档应足以说明已经有效地维护了所有的配置项。**

5.6.3.3OCO_CAP.3

要求开发者所使用的版本号与所应表示的网络系统样本应完全对应，没有歧义。要求配置项应有唯一的标识。配置管理计划应描述系统是如何使用的，并说明运行中的配置管理系统与配置管理计划的一致性，配置管理文档应足以说明已经有效地维护了所有的配置项。**配置管理系统应确保对配置项只进行授权修改。**

5.6.4 变更控制 OCO_CHA

5.6.4.1OCO_CHA.1

系统的变更应有相关责任人对其控制。

5.6.4.2OCO_CHA.2

系统的变更应有相关责任人对其控制。**应该制订正式的管理责任和程序以确保满足对设备、软件或程序的所有改变的控制。可行的情况下，应把操作和应用的变更控制程序整合起来。**

5.6.4.3OCO_CHA.3

系统的变更应有相关责任人对其控制。应该制订正式的管理责任和程序以确保满足对设备、软件或程序的所有改变的控制。可行的情况下，应把操作和应用的变更控制程序整合起来。**在程序变更时，应该保留包括所有相关信息的审计日志。**

5.6.5 密钥管理 OCO_KEY

5.6.5.1 OCO_KEY.1

存储密钥的介质必须严加保护，应以加密形式存储密钥，密钥必须由纯随机源产生，有关密钥存储方式和地方的信息不应被非授权人员获得。

5.6.5.2 OCO_KEY.2

存储密钥的介质必须严加保护，应以加密形式存储密钥，有关密钥存储方式和地方的信息不应被非授权人员获得。**应根据密钥的种类、系统的要求确定密钥更换周期；会话密钥应在每次会话后更换；主密钥更换时间间隔可视具体情况而定；**密钥必须由纯随机源产生，**并应经过随机性检验，生成密钥时不能降低密码算法设计中所规定的密钥空间；**

5.6.5.3 OCO_KEY.3

存储密钥的介质必须严加保护，应以加密形式存储密钥，有关密钥存储方式和地方的信息不应被非授权人员获得。应根据密钥的种类、系统的要求确定密钥更换周期；会话密钥应在每次会话后更换；主密钥更换时间间隔可视具体情况而定；密钥必须由纯随机源产生，并应经过随机性检验，生成密钥时不能降低密码算法设计中所规定的密钥空间。**密钥传送要有专门的密钥传送机制，密钥分发应专门设计密钥分发设备，用于现场加密信息的密钥，应注入加密算法或加密设备中，长期驻留的密钥及其变形必须加物理保护。当密钥定期更换时，旧密钥必须安全归档，并在规定的时间内，在安全管理负责人的严密监督下，由管理责任人销毁。**

5.7 OBA 类：备份与恢复

5.7.1 数据备份和恢复 OBA_DAT

5.7.1.1OBA_DAT.1

进行数据的备份和恢复，应有相关规范明确说明需定期备份重要业务信息、系统数据、软件、重要业务信息的保存期等。每周做一次包括数据和应用环境的全备份。

5.7.1.2OBA_DAT.2

进行数据的备份和恢复，应有相关规范明确说明需定期备份重要业务信息、系统数据、软件、重要业务信息的保存期等。**应定期检查备份介质，测试恢复程序。采用磁盘或磁带进行离线备份或在线备份方案，每日进行增量备份，每周做一次包括数据和应用环境的全备份。**

5.7.1.3OBA_DAT.3

进行数据的备份和恢复，应有相关规范明确说明需定期备份重要业务信息、系统数据、软件、重要业务信息的保存期等。**磁盘或磁带进行离线备份或在线备份方案，小时级增量备份，每天做一次包括数据和应用环境的全备份。每日的备份数据应异地保存。**

5.7.2 设备和系统冗余 OBA_EQI

5.7.2.1OBA_EQI.1

系统内重要服务器，如重要的应用服务器和数据库服务器，应采用冷备、温备或热备的方式进行冗余设置，支持重要应用的网络设备应有冗余设置。

5.7.2.2OBA_EQI.2

系统内重要服务器，如重要的应用服务器和数据库服务器，应采用冷备、温备或热备的方式进行冗余设置，支持重要应用的网络设备应有冗余设置。**采用技术措施保证服务器出现故障经更换或修复后，能够自动安装操作系统、应用软件，并恢复数据，采用支持数据快照，文件系统检查点等技术，提供高速的数据恢复手段。**

5.7.2.3OBA_EQI.3

系统内重要服务器，如重要的应用服务器和数据库服务器，应采用冷备、温备或热备的方式进行冗余设置，支持重要应用的网络设备应有冗余设置。采用技

术措施保证服务器出现故障经更换或修复后，能够自动安装操作系统、应用软件，并恢复数据，采用支持数据快照，文件系统检查点等技术，提供高速的数据恢复手段。采用高可用性软件，应提供二节点或更多节点的集群，支持高可用性和数据库并行应用。

5.8 ORM 类：存储介质管理

5.8.1 存储介质的保护 ORM_PRO

5.8.1.1ORM_PRO.1

重要介质应储存在安全的环境中防止损坏和防盗。

5.8.1.2ORM_PRO.2

重要介质应储存在安全的环境中防止损坏和防盗。根据所承载的数据和软件的重要程度对介质加贴标识并进行分类，各种处理过程应登记在册。

5.8.1.3ORM_PRO.3

重要介质应储存在安全的环境中防止损坏和防盗。根据所承载的数据和软件的重要程度对介质加贴标识并进行分类，各种处理过程应登记在册。重要介质应加密存储，经常检查介质的完整性和可用性。

5.8.2 存储介质的访问控制 ORM_ACO

5.8.2.1ORM_ACO.1

对借阅和复制的存储介质，要进行使用登记。

5.8.2.2ORM_ACO.2

对借阅和复制的存储介质，要进行使用登记。存储介质使用管理中，应该有

冗余保护措施。

5.8.2.3ORM_ACO.3

对借阅和复制的存储介质，要进行使用登记。存储介质使用管理中，应该有冗余保护措施。对高安全等级的存储介质原则上不借阅和复制。确因工作需要借阅、复制存储介质要履行申请、审批、登记、归档等手续。

5.8.3 存储介质的传输管理 ORM_TRA

5.8.3.1ORM_TRA.1

应该授权使用可靠的运输和速递公司，并按生产商的规格使用可靠的包装保护运输时不会物理破坏存储介质的内容。

5.8.3.2ORM_TRA.2

应该授权使用可靠的运输和速递公司，并按生产商的规格使用可靠的包装保护运输时不会物理破坏存储介质的内容。定期检查确实是使用统一安排的速递公司。

5.8.3.3ORM_TRA.3

应该授权使用可靠的运输和速递公司，并按生产商的规格使用可靠的包装保护运输时不会物理破坏存储介质的内容。定期检查确实是使用统一安排的速递公司。使用加锁的装运箱、防篡改的包装。

5.8.4 存储环境管理 ORM_CIR

5.8.4.1ORM_CIR.1

介质存储室必须符合物理环境安全要求（TPR 类）。

5.8.4.2ORM_CIR.2

介质存储室必须符合物理环境安全要求（TPR 类）。介质存储室管理必须制定存储室、管理员、入库、转储、使用、销毁等管理制度和办法，明确执行各项制度和办法的责任人。

5.8.4.3ORM_CIR.3

介质存储室必须符合物理环境安全要求（TPR 类）。介质存储室管理必须制定存储室、管理员、入库、转储、使用、销毁等管理制度和办法，明确执行各项制度和办法的责任人。应设立入库、转储、使用、销毁登记记录。

5.8.5 存储介质的备份 ORM_BAC

5.8.5.1ORM_BAC.1

纸介质和电子介质之间实行交叉备份。

5.8.5.2ORM_BAC.2

纸介质和电子介质之间实行交叉备份。经常需要使用的存储介质，应有双份备份。

5.8.5.3ORM_BAC.3

纸介质和电子介质之间实行交叉备份。对业务系统至关重要的、不可替代的、毁坏后不能立即恢复的存储介质，必须双重和异地备份。

5.8.6 存储介质的分类和归档 ORM_CLA

5.8.6.1ORM_CLA.1

按纸介质和电子介质分别集中分类管理、编制目录、造册登记。

5.8.6.2ORM_CLA.2

按纸介质和电子介质分别集中分类管理、编制目录、造册登记。**系统一旦投入运行，应由项目负责人把完整的存储介质归档入库。归档入库的存储介质应完整、协调、准确。**

5.8.6.3ORM_CLA.3

按纸介质和电子介质分别集中分类管理、编制目录、造册登记。系统一旦投入运行，应由项目负责人把完整的存储介质归档入库。归档入库的存储介质应完整、协调、准确。**对电子介质存储介质，要定期转储，并进行转储登记记录。**

5.8.7 存储介质的销毁 ORM_DES

5.8.7.1ORM_DES.1

不再需要的的存储介质，应该安全地予以清除。

5.8.7.2ORM_DES.2

应制订正式的清除程序，把风险减到最低。有敏感信息的存储介质应选择专业服务商进行安全地清除。

5.8.7.3ORM_DES.3

应制订正式的清除程序，把风险减到最低。有敏感信息的存储介质应选择专业服务商进行安全地清除。**应记录敏感信息的清除。**

5.9 OBC 类：应急响应

5.9.1 应急响应计划的制定 OBC_EST

5.9.1.1OBC_EST.1

应制定包括应急响应组织架构、应急响应程序、人员职责的应急响应计划。

5.9.1.2OBC_EST.2

应制定包括应急响应组织架构、应急响应程序、人员职责、**启动条件、后备程序、恢复程序**的应急响应计划。

5.9.1.3OBC_EST.3

应制定包括应急响应组织架构、应急响应程序、人员职责、启动条件、后备程序、恢复程序的应急响应计划，**并定期对应急响应内容的完备性进行检查。**

5.9.2 应急响应计划的测试和演练 OBC_TES

5.9.2.1OBC_TES.1

应对应急响应计划进行纸面模拟测试。

5.9.2.2OBC_TES.2

应该对所涉及到的人员进行应急响应计划培训，并且对应急响应计划进行桌面模拟测试。

5.9.2.3OBC_TES.3

应该对所有的员工进行应急响应计划培训，并且对应急响应计划进行完全排练（测试机构、人员、设备及处理可以应付业务停顿的情况）。

6 安全组织等级化框架

6.1 OOR 类：安全组织和职责

6.1.1 安全管理组织 OOR_MNG

6.1.1.1OOR_MNG.1

由相关部门兼管信息安全工作，配备兼职安全管理员。

6.1.1.2OOR_MNG.2

成立信息安全管理部门负责信息安全工作，设立专职的信息安全人员。

6.1.1.3OOR_MNG.3

成立信息安全管理部门负责信息安全工作，设立专职的信息安全人员。成立信息安全领导小组或者安全管理委员会对信息安全工作进行领导、决策、协调和监督。成立专项的安全小组为信息安全工作的开展提供支持和组织保障。

6.1.2 安全管理人员能力 OOR_CAP

6.1.2.1OOR_CAP.1

安全管理人员应该具有 基本的专业安全技术水平，掌握安全管理基本知识。

6.1.2.2OOR_CAP.2

安全管理人员应该具有 基本的专业安全技术水平，掌握安全管理基本知识，能够进行基本的系统安全弱点分析。

6.1.2.3OOR_CAP.3

安全管理人员应该具有 基本的专业安全技术水平，掌握安全管理基本知识，能够进行基本的系统安全风险分析和评估。

6.1.3 岗位安全职责 OOR_STA

6.1.3.1OOR_STA.1

明确各岗位的信息安全责任。

6.1.3.2OOR_STA.2

明确各岗位的信息安全责任，安全管理人员要通过相关安全资质认证。

6.1.3.3OOR_STA.3

明确各岗位的信息安全责任，安全管理人员要通过相关安全资质认证。依据“权限分散，不得交叉覆盖”的原则设置，严格规定要害岗位的职责和权限。

6.1.4 关键岗位安全管理 OOR_KST

6.1.4.1OOR_KST.1

关键岗位工作人员，应当采取严格的背景调查和管理控制措施。

6.1.4.2OOR_KST.2

关键岗位工作人员，应当采取严格的背景调查和管理控制措施，重要工作应当双人临岗，互相监督。

6.1.4.3OOR_KST.3

关键岗位工作人员，应当采取严格的背景调查和管理控制措施，重要工作应

当双人临岗，互相监督。关键的岗位应该有人员储备计划，并根据实际情况实行强制休假制度和人员轮岗制度。

6.1.5 合作与沟通 OOR_COM

6.1.5.1.1 OOR_COM.1

加强组织内部的合作与沟通，共同协助处理信息安全问题。

6.1.5.1.2 OOR_COM.2

加强与其他部门、兄弟单位、公安机关、供应商、业界专家、专业的安全公司、安全组织的合作与沟通，以便在发生安全事件时能够得到及时的支持。

6.1.5.1.3 OOR_COM.3

加强与其他部门、兄弟单位、公安机关、供应商、业界专家、专业的安全公司、安全组织的合作与沟通，以便在发生安全事件时能够得到及时的支持。聘请信息安全专家，作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。

6.2 OPE 类：人员管理

6.2.1 人员录用 OPE_EMP

6.2.1.1 OPE_EMP.1

对应聘者的个人简历、道德行为和人品进行检查和确认。

6.2.1.2 OPE_EMP.2

对应聘者的个人简历、道德行为和人品进行检查和确认，雇佣条款和条件应该阐明雇员对信息安全的责任，新招聘的员工需要签署保密协议。

6.2.1.3OPE_EMP.3

对应聘者的个人简历、道德行为和人品进行检查和确认，雇佣条款和条件应该阐明雇员对信息安全的责任，新招聘的员工需要签署保密协议。**人员上岗前必须经单位人事部门进行政治审查。**

6.2.2 人员离岗 OPE_DIM

6.2.2.1OPE_DIM.1

对准备离岗人员应该进行核实检查。

6.2.2.2OPE_DIM.2

对准备离岗人员应该进行核实检查和**安全处理。**

6.2.2.3OPE_DIM.3

对准备离岗人员应该进行核实检查和安全处理，**对保密协议进行审查，必要时重新签署保密协议。**

6.2.3 安全培训 OPE_TRA

6.2.3.1OPE_TRA.1

要给予普通职员有关信息安全责任方面的指导，为安全管理人员提供安全培训。

6.2.3.2OPE_TRA.2

应对组织中**所有**职员进行适当的信息安全培训。

6.2.3.3OPE_TRA.3

应对组织中所有职员进行完整的信息安全培训。邀请或雇用信息安全专家，吸取他们对于组织信息安全活动的建议。

6.2.4 第三方访问 OPE_OTT

6.2.4.1OPE_OTT.1

第三方人员访问安全区域（例如机房、办公区域）时需要进行审批。

6.2.4.2OPE_OTT.2

第三方人员访问安全区域（例如机房、办公区域）时需要进行审批，第三方访问需要由接待人或指定专人陪同。

6.2.4.3OPE_OTT.3

第三方人员访问安全区域（例如机房、办公区域）时需要进行审批，第三方访问需要由接待人或指定专人陪同。与第三方人员签署保密协议，除非必要，禁止第三方人员访问网络、操作重要的主机和设备。

7 安全策略文档等级化框架

安全策略文档是指为规范安全管理而制定的安全管理规章制度。安全管理规章制度通常以文档形式存在，因此统称为安全策略文档。安全策略文档是安全管理的依据，安全策略文档体系的完善程度代表了安全管理的完善程度。安全策略文档的安全目标是：建立严谨科学的安全策略文档体系，并在组织范围内正式发布，落实执行，维护更新。

7.1 PIN 类：安全策略制定与执行

7.1.1 安全策略范围 PIN_SCO

7.1.1.1PIN_SCO.1

应根据公司的总体方针和实际需求组织相关部门和人员建立常用的信息安全管理规程和制度。

7.1.1.2PIN_SCO.2

要根据机构的实际情况，由信息系统使用单位的相关部门制定信息安全工作所涉及和需要的**必要**的策略和制度文件。

7.1.1.3PIN_SCO.3

应当建立**正式的信息安全的策略和制度体系。**

7.1.2 安全策略执行 PIN_EXE

7.1.2.1PIN_EXE.1

应当有明确的规定，要求所有人员必须遵守安全策略文档。

7.1.2.2PIN_EXE.2

应当有明确的规定，要求所有人员必须遵守安全策略文档，**并定期检查安全策略文档的执行情况。**

7.1.2.3PIN_EXE.3

应当有明确的规定，要求所有人员必须遵守安全策略文档，并定期检查安全策略文档的执行情况。**制定奖惩措施，明确违反安全策略文档的处罚措施，将安**

全策略文档的执行情况与员工的绩效考核结合。

7.2 PCO 类：安全策略发布与更新

7.2.1 策略发布 PCO_PUB

7.2.1.1PCO_PUB.1

安全策略文档应该进行发布，使安全策略文档能够及时发布到所有相关人员手上。

7.2.1.2PCO_PUB.2

安全策略文档应该通过**正式有效**的发布渠道进行发布。

7.2.1.3PCO_PUB.3

安全策略文档应该通过正式有效的发布渠道进行发布。**对正式发布的策略进行培训和考评**，以保证相关人员理解安全策略文档。

7.2.2 策略更新 PCO_UPD

7.2.2.1PCO_UPD.1

当发现安全策略文档有不适用或不合理的条款，进行更新。

7.2.2.2PCO_UPD.2

当发现安全策略文档有不适用或不合理的条款，**立即**进行更新。**并定期对安全策略文档进行评审和修订。**

7.2.2.3PCO_UPD.3

当发现安全策略文档有不适用或不合理的条款，立即进行更新。并定期对安

全策略文档进行评审和修订。把安全策略更新制度化，指定安全策略文档的责任人，要求员工对安全策略不适用或不合理以及缺少的条款向责任人报告。

第三部分 IP 网络安全指标体系

1 概述

本部分针对公司的一级、二级、三级系统（系统的安全等级确定参见第二部分第 2 章），分别提出了基线（Baseline）安全要求。

这些安全基线都是在分析了公司整个 IP 网络可能面临的**所有威胁**后，结合系统的安全等级，从第三部分中选取了相应的对策组件（选取的方法参加附录 1）。而后对第三部分中这些抽象的、粗略的安全对策组件进行了细化、扩展和具体化，从而形成了三个基线要求。

需要注意的是，某一级的系统并不一定要达到此级基线安全要求中的每一个对策组件，即基线要求中的某些对策组件可能对于个别具体系统而言是不需要的，因为这些安全基线是对应于整个 IP 网络面临的威胁的，而可能某个具体系统并不面临这样多的威胁。那么在具体设计或者维护某个系统时，如何裁减下面这三个基线安全要求呢？附录 1 给出了威胁详述，可以首先对具体系统进行威胁分析，当发现某些威胁不可能对此系统起作用时，则可以排除此威胁所对应的对策组件，但需要注意某些对策组件可能对应多个威胁，排除的时候应确保这些组件对应的威胁全都不起作用。同理，当某个威胁严重影响此系统时，则可以增强此威胁对应的对策。

例如环境动力系统，此系统是个独立的本地系统，与其他任何系统都没有连接，那么滥用远程维护端口、拒绝服务这两种威胁就不会对其起作用，相应的这两种威胁所对应的两个安全对策：远程登陆管理 OHO_TEL、网络边界访问控制 TEB_NAC 就不需要，而这两种威胁所对应的其他对策则因为与其他的威胁相关，而不能删除。

以下是公司 IP 网络面临的常见威胁：

威胁标号	威胁简单描述	对策
TFORCE.PEOP	关键人员损失	关键岗位安全管理OOR_KST 安全培训OPE_TRA
TFORCE.FAIL	IT 系统故障	主干网可用性保护 TNI_AVI 主机设备维护 OHO_EQI 网络可靠性管理 ONE_REL 供电 TPR_SUP 安全培训 OPE_TRA OBC 类：应急响应 OOR 类：安全组织和职责
TFORCE.THU	雷击和闪电	防雷击 TPR_THU
TFORCE.FIR	火灾	防火 TPR_FIR
TFORCE.WAT	水灾	防潮 TPR_WAT
TFORCE.CON	温度和湿度超范围	空调 TPR_CON
TFORCE.DUST	灰尘的积累	机房管理 OPM_ROM
TFORCE.MAG	强磁场导致数据丢失	电磁防护 TPR_TEM
TLIMIT.DIS	安全管理规则和制度缺乏或不足	安全管理组织 OOR_MNG 安全管理人员能力 OOR_CAP 岗位安全职责 OOR_STA 合作与沟通 OOR_COM 安全策略范围 PIN_SCO 安全策略执行 PIN_EXE 策略发布 PCO_PUB 策略更新 PCO_UPD
TLIMIT.REQ	需求文档不明	岗位安全职责 OOR_STA 人员录用 OPE_DIM 安全培训 OPE_TRA
TLIMIT.COMP	资源缺乏兼容性和适用性	安全产品选型 OEN_PRO 应用系统测试 TCE_APT
TLIMIT.SUP	对 IT 安全措施监控不足	存储介质的保护 ORM_PRO 帐户管理 OHO_ACC 存储介质的销毁 ORM_DES 变更控制 OCO_CHA 策略发布 PCO_PUB
TLIMIT.MAI	缺乏维护或维护不足	安全策略范围 PIN_SCO

威胁标号	威胁简单描述	对策
		账户管理 OHO_ACC 安全策略执行 PIN_EXE 安全产品选型 OEN_PRO 变更控制 OCO_CHA
TLIMIT.ROOM	未经允许进入需要保护的房间	门禁 TPR_JAN 机房管理 OPM_ROM 办公环境管理 OPM_OFM
TLIMIT.PUR	未经许可使用权限	存储介质的保护 ORM_PRO 环境设备维护 OPM_MAI 账户管理 OHO_ACC 岗位安全职责 OOR_STA 配置管理计划 OCO_PLA 配置管理能力 OCO_CAP 网络设备管理授权 ONE_ADV 脆弱性分析 ORA_VUL 网络边界访问控制 TEB_NAC
TLIMIT.ERR	系统的变更错误	账户管理 OHO_ACC 岗位安全职责 OOR_STA 安全策略范围 PIN_SCO 配置管理计划 OCO_PLA 变更控制 OCO_CHA 存储介质的分类和归档 ORM_CLA 配置管理自动化 OCO_AUT 病毒和恶意代码防范 TCE_VIR 系统安全检测和验收 OEN_TES 存储介质的保护 ORM_PRO 数据备份和恢复 OBA_DAT
TLIMIT.AVI	数据存储介质在需要时不可用	存储介质的传输管理 ORM_TRA 存储介质的访问控制 ORM_ACO 存储介质的分类和归档 ORM_CLA 存储介质的备份 ORM_BAC 存储介质的销毁 ORM_DES 变更控制 OCO_CHA 病毒和恶意代码防范 TCE_VIR 办公环境管理 OPM_OFM
TLIMIT.BW	带宽规划不足	安全项目的立项管理 OEN_CON 安全需求分析 OEN_REQ

威胁标号	威胁简单描述	对策
TLIMIT.CABL	布线文档不足	交付和运行 OEN_ADO 电磁防护 TPR_TEM
TLIMIT.COND	由于工作条件不佳有损 IT 使用	位置选择 TPR_LOC 门禁 TPR_JAN 机房管理 OPM_ROM
TLIMIT.UNIX	UNIX 系统敏感数据失去机密性	远程访问 TEB_TEL 计算环境访问控制 TCE_TAC 身份鉴别 TCE_IDT 安全审计 TCE_SAU 主机入侵防范 TCE_IDS 账户管理 OHO_ACC 漏洞控制 OHO_VER
TLIMIT.CHA	对便携电脑用户的变更不进行控制	办公环境管理 OPM_OFM 账户管理 OHO_ACC 漏洞控制 OHO_VER 防病毒管理 OHO_VIR 设备和系统冗余 OBA_EQI 安全培训 OPE_TRA
TLIMIT.MARK	数据存储介质标识不足	存储介质的分类和归档 ORM_CLA 存储介质的访问控制 ORM_ACO
TLIMIT.HAND	数据存储介质移交方式不当	存储介质的传输管理 ORM_TRA 存储介质的访问控制 ORM_ACO 存储介质的分类和归档 ORM_CLA 存储介质的传输管理 ORM_TRA 密钥管理 OCO_KEY 存储介质的备份 ORM_BAC
TLIMIT.KEY	密钥管理不当	密钥管理 OCO_KEY 安全培训 OPE_TRA 人员录用 OPE_EMP 岗位安全职责 OOR_STA
TLIMIT.REX	调换用户管理不当	计算环境访问控制 TCE_TAC 岗位安全职责 OOR_STA
TLIMIT.AUD	缺乏对审计数据的评估	安全审计 TCE_SAU 安全产品选型 OEN_PRO
TLIMIT.CONF	被保护网络的敏感数据丧失机密性	网络边界访问控制 TEB_NAC 网络入侵防范 TEB_IDS

威胁标号	威胁简单描述	对策
TLIMIT.DOC	文档缺乏或不足	配置管理能力 OCO_CAP 变更控制 OCO_CHA
TLIMIT.DOMAIN	域规划不足	安全域规划 ONE_SED
TLIMIT.CTRL	通讯线路的使用失控	办公环境管理 OPM_OFM
TLIMIT.DATA	数据库安全机制实现不够	数据库设计安全 TCE_DBS 主机设备维护 OHO_EQI
TLIMIT.COM	网络组件不兼容	安全需求分析 OEN_REQ 安全功能规范 OEN_FSP 系统安全检测和验收 OEN_TES 应用系统测试 TCE_APT
TLIMIT.BUG	网络设计缺陷	安全需求分析 OEN_REQ 安全功能规范 OEN_FSP 安全项目的立项管理 OEN_CON 网络拓扑设计和规划 ONE_TOP 安全域规划 ONE_SED 网络可靠性管理 ONE_REL 主干网可用性保护 TNI_AVI
TLIMIT.DIM	超过线缆/总线长度或环的尺寸	网络拓扑设计和规划 ONE_TOP 安全需求分析 OEN_REQ 安全功能规范 OEN_FSP 主干网可用性保护 TNI_AVI
TLIMIT.TRANS	文件和数据存储介质的不安全传递	存储介质的传输管理 ORM_TRA 存储介质的备份 ORM_BAC 数据备份和恢复 OBA_DAT
TLIMIT.HOM	数据存储介质和文档在家里的办公环境中放置不当	应急响应计划的制定 OBC_EST 存储环境管理 ORM_CIR 办公环境管理 OPM_OFM 数据备份和恢复 OBA_DAT
TLIMIT.TRA	远程工作人员培训不足	人员录用 OPE_EMP 安全培训 OPE_TRA 安全策略执行 PIN_EXE 安全管理组织 OOR_MNG 应急响应计划的制定 OBC_EST
TLIMIT.DEL	临时远程工作人员引发的延迟	人员录用 OPE_EMP 安全培训 OPE_TRA 安全策略执行 PIN_EXE

威胁标号	威胁简单描述	对策
		安全管理组织 OOR_MNG 合作与沟通 OOR_COM
TLIMIT.TEL	远程工作人员被较差地集成到工作流中	人员录用 OPE_EMP 安全培训 OPE_TRA 安全策略执行 PIN_EXE 安全管理组织 OOR_MNG 合作与沟通 OOR_COM
TLIMIT.RES	当 IT 系统崩溃时响应时间比较长	应急响应计划的制定 OBC_EST 应急响应计划的测试和演练 OBC_TES 安全策略执行 PIN_EXE 安全策略范围 PIN_SCO
TLIMIT.SUB	远程工作人员更替制度不当	安全策略范围 PIN_SCO 安全策略执行 PIN_EXE 应急响应计划的制定 OBC_EST
TLIMIT.CON	部分隐藏数据导致机密性丧失	存储介质的传输管理 ORM_TRA 存储介质的访问控制 ORM_ACO 存储介质的销毁 ORM_DES
TLIMIT.MED	用于应急的介质存储量不足	应急响应计划的制定 OBC_EST 应急响应计划的测试和演练 OBC_TES 设备和系统冗余 OBA_EQI 存储介质的备份 ORM_BAC
TLIMIT.REG	未注册组件操作	安全管理人员能力 OOR_CAP 安全策略执行 PIN_EXE 岗位安全职责 OOR_STA 安全培训 OPE_TRA
TLIMIT.POL	网络和管理系统的策略不足或没落实	安全需求分析 OEN_REQ 安全项目的立项管理 OEN_CON 安全功能规范 OEN_FSP 安全策略范围 PIN_SCO 策略发布 PCO_PUB 策略更新 PCO_UPD 安全管理组织 OOR_MNG 安全策略执行 PIN_EXE
TLIMIT.PRI	未经授权收集私人信息	安全策略范围 PIN_SCO 策略发布 PCO_PUB 策略更新 PCO_UPD 安全审计 TCE_SAU

威胁标号	威胁简单描述	对策
		账户管理 OHO_ACC 身份鉴别 TCE_IDT 网络设备用户身份鉴别 TNI_IDT 安全需求分析 OEN_REQ 高层安全设计 OEN_HLD
TLIMIT.EME	安全事件处理不当	应急响应计划的制定 OBC_EST 选择安全控制措施 ORA_CTR 安全策略执行 PIN_EXE 安全策略范围 PIN_SCO 策略发布 PCO_PUB 策略更新 PCO_UPD 安全管理组织 OOR_MNG
TLIMIT.SAMBA	SAMBA 配置复杂	配置管理计划 OCO_PLA 变更控制 OCO_CHA 选择安全控制措施 ORA_CTR 安全管理人员能力 OOR_CAP
TLIMIT.SEC	IT 安全缺乏或不足	安全需求分析 OEN_REQ 安全项目的立项管理 OEN_CON 安全功能规范 OEN_FSP 安全管理组织 OOR_MNG 安全策略执行 PIN_EXE 选择安全控制措施 ORA_CTR 人员录用 OPE_EMP 安全培训 OPE_TRA 岗位安全职责 OOR_STA 安全管理人员能力 OOR_CAP 安全策略范围 PIN_SCO 策略发布 PCO_PUB 策略更新 PCO_UPD
THUMAN.MIST	IT 用户错误导致数据机密性/完整性丢失	应急响应计划的制定 OBC_EST 选择安全控制措施 ORA_CTR 安全培训 OPE_TRA 岗位安全职责 OOR_STA 安全策略执行 PIN_EXE 安全管理组织 OOR_MNG 存储介质的访问控制 ORM_ACO 存储介质的销毁 ORM_DES

威胁标号	威胁简单描述	对策
THUMAN.NEG	因疏忽大意破坏设备或数据	安全培训 OPE_TRA 安全策略执行 PIN_EXE 岗位安全职责 OOR_STA 安全管理组织 OOR_MNG 安全管理人员能力 OOR_CAP 数据备份和恢复 OBA_DAT 应急响应计划的制定 OBC_EST
THUMAN.EXE	不执行 IT 安全措施	人员录用 OPE_EMP 安全培训 OPE_TRA 岗位安全职责 OOR_STA 安全管理组织 OOR_MNG 安全管理人员能力 OOR_CAP 安全策略执行 PIN_EXE 应急响应计划的制定 OBC_EST 选择安全控制措施 ORA_CTR
THUMAN.PER	未经许可的电缆连接	安全需求分析 OEN_REQ 安全功能规范 OEN_FSP 电磁防护 TPR_TEM 位置选择 TPR_LOC
THUMAN.CAB	因疏忽造成的电缆损害	位置选择 TPR_LOC 防火 TPR_FIR 防潮 TPR_WAT 第三方访问 OPE_OTT
THUMAN.CLE	清洁人员或外来人员带来的危害	选择安全控制措施 ORA_CTR 第三方访问 OPE_OTT 安全策略范围 PIN_SCO 数据备份和恢复 OBA_DAT 存储环境管理 ORM_CIR 存储介质的备份 ORM_BAC
THUMAN.ITU	IT 系统使用不当	安全培训 OPE_TRA 人员录用 OPE_EMP 第三方访问 OPE_OTT 安全策略执行 PIN_EXE 安全管理组织 OOR_MNG 安全管理人员能力 OOR_CAP 账户管理 OHO_ACC 身份鉴别 TCE_IDT

威胁标号	威胁简单描述	对策
		网络设备用户身份鉴别 TNI_IDT 应急响应计划的制定 OBC_EST
THUMAN.ITS	IT 系统管理不当	配置管理计划 OCO_PLA 数据备份和恢复 OBA_DAT 变更控制 OCO_CHA 配置管理能力 OCO_CAP 安全管理人员能力 OOR_CAP 安全策略执行 PIN_EXE 安全管理组织 OOR_MNG 安全培训 OPE_TRA 应急响应计划的制定 OBC_EST 安全策略范围 PIN_SCO 策略发布 PCO_PUB 策略更新 PCO_UPD
THUMAN.UNIX	UNIX 文件系统的错误输出	账户管理 OHO_ACC 身份鉴别 TCE_IDT 安全审计 TCE_SAU 安全策略执行 PIN_EXE 应急响应计划的制定 OBC_EST 数据备份和恢复 OBA_DAT
THUMAN.MAIL	邮件发送系统配置不当	防病毒网关 TEB_TVI 病毒和恶意代码防范 TCE_VIR 应用系统测试 TCE_APT 系统安全检测和验收 OEN_TES 安全需求分析 OEN_REQ 安全功能规范 OEN_FSP
THUMAN.LOSE	传递过程中数据存储介质丢失	存储介质的访问控制 ORM_ACO 存储介质的传输管理 ORM_TRA 存储介质的备份 ORM_BAC
THUMAN.TRANS	错误或非预期的数据传输	存储介质的保护 ORM_PRO 存储介质的访问控制 ORM_ACO 存储介质的传输管理 ORM_TRA 存储环境管理 ORM_CIR 存储介质的销毁 ORM_DES 密码技术 TNI_ENC
THUMAN.PUR	站点和数据访问权限管理不当	人员录用 OPE_EMP 安全培训 OPE_TRA

威胁标号	威胁简单描述	对策
		岗位安全职责 OOR_STA 账户管理 OHO_ACC 身份鉴别 TCE_IDT 网络设备用户身份鉴别 TNI_IDT 安全审计 TCE_SAU 安全域规划 ONE_SED 选择安全控制措施 ORA_CTR 安全策略执行 PIN_EXE
THUMAN.CHA	PC 用户的错误变更	账户管理 OHO_ACC 身份鉴别 TCE_IDT 安全审计 TCE_SAU 网络设备管理授权 ONE_ADV 远程登陆管理 OHO_TEL 变更控制 OCO_CHA 安全策略执行 PIN_EXE 安全管理组织 OOR_MNG 安全培训 OPE_TRA 岗位安全职责 OOR_STA
THUMAN.SHA	共享目录、打印机或剪贴版	账户管理 OHO_ACC 身份鉴别 TCE_IDT 安全审计 TCE_SAU
THUMAN.REG	注册表修改不当	变更控制 OCO_CHA 配置管理能力 OCO_CAP 安全培训 OPE_TRA 安全管理人员能力 OOR_CAP 安全策略执行 PIN_EXE 应急响应计划的制定 OBC_EST 选择安全控制措施 ORA_CTR
THUMAN.DBMS	DBMS 系统管理不当	数据备份和恢复 OBA_DAT 安全功能规范 OEN_FSP 数据库设计安全 TCE_DBS 身份鉴别 TCE_IDT 账户管理 OHO_ACC 安全审计 TCE_SAU
THUMAN.UNC	无意中对数据操作	安全培训 OPE_TRA 安全管理人员能力 OOR_CAP 安全审计 TCE_SAU

威胁标号	威胁简单描述	对策
		账户管理 OHO_ACC 身份鉴别 TCE_IDT 数据备份和恢复 OBA_DAT
THUMAN.CONF	网络组件的配置不当	安全域规划 ONE_SED 网络可靠性管理 ONE_REL 网络拓扑设计和规划 ONE_TOP IP 地址管理 ONE_IPM 路由管理 ONE_ROU
THUMAN.VLAN	未进行网络划分或网络划分不当	安全域规划 ONE_SED 网络可靠性管理 ONE_REL 网络拓扑设计和规划 ONE_TOP 安全需求分析 OEN_REQ 应急响应计划的制定 OBC_EST
THUMAN.ACC	私人未经授权使用远程工作站	选择安全控制措施 ORA_CTR 应急响应计划的制定 OBC_EST 远程登陆管理 OHO_TEL 安全审计 TCE_SAU 防病毒网关 TEB_TVI 病毒和恶意代码防范 TCE_VIR 主机入侵防范 TCE_IDS 网络入侵防范 TEB_IDS 人员录用 OPE_EMP 第三方访问 OPE_OTT 数据备份和恢复 OBA_DAT
THUMAN.FRA	数据库未结构化	安全培训 OPE_TRA 存储介质的保护 ORM_PRO 存储介质的备份 ORM_BAC 存储介质的分类和归档 ORM_CLA 存储介质的传输管理 ORM_TRA
THUMAN.ENC	加密模块使用不当	密码技术 TNI_ENC 密钥管理 OCO_KEY
THUMAN.CON	管理系统配置不当	应急响应计划的制定 OBC_EST 配置管理计划 OCO_PLA 配置管理自动化 OCO_AUT 配置管理能力 OCO_CAP
THUMAN.SER	操作过程中服务器失效	选择安全控制措施 ORA_CTR 应急响应计划的制定 OBC_EST

威胁标号	威胁简单描述	对策
		数据备份和恢复 OBA_DAT 设备和系统冗余 OBA_EQI
THUMAN.MIS	事件的误解	安全培训 OPE_TRA 安全策略执行 PIN_EXE 安全管理组织 OOR_MNG 安全管理人员能力 OOR_CAP
THUMAN.CONFIG	配置和操作中的错误	安全管理组织 OOR_MNG 安全管理人员能力 OOR_CAP 安全策略执行 PIN_EXE 安全培训 OPE_TRA 身份鉴别 TCE_IDT 网络设备用户身份鉴别 TNI_IDT 账户管理 OHO_ACC
THUMAN.PW	口令处理不当	账户管理 OHO_ACC 身份鉴别 TCE_IDT 网络设备用户身份鉴别 TNI_IDT 选择安全控制措施 ORA_CTR 安全策略执行 PIN_EXE 安全培训 OPE_TRA 安全管理组织 OOR_MNG
THUMAN.INF	信息处理草率	安全培训 OPE_TRA 岗位安全职责 OOR_STA 安全策略执行 PIN_EXE 安全管理组织 OOR_MNG 安全管理人员能力 OOR_CAP
THUMAN.VAL	对通讯对象验证不足	安全培训 OPE_TRA 安全策略执行 PIN_EXE
TFAIL.BRE	电源中断	供电 TPR_SUP 数据备份和恢复 OBA_DAT 应急响应计划的制定 OBC_EST
TFAIL.SUP	内部补给网络故障	供电 TPR_SUP 防火 TPR_FIR 空调 TPR_CON 防潮 TPR_WAT 防静电 TPR_STA 防雷击 TPR_THU 电磁防护 TPR_TEM

威胁标号	威胁简单描述	对策
		位置选择 TPR_LOC 数据备份和恢复 OBA_DAT 应急响应计划的制定 OBC_EST
TFAIL.UNAV	安全措施不可用	位置选择 TPR_LOC 电磁防护 TPR_TEM 安全培训 OPE_TRA 岗位安全职责 OOR_STA 数据备份和恢复 OBA_DAT 应急响应计划的制定 OBC_EST
TFAIL.COND	因环境因素损害线路	电磁防护 TPR_TEM 位置选择 TPR_LOC 防火 TPR_FIR
TFAIL.DIM	串话干扰	防干扰和窃听 TPR _TAP 电磁防护 TPR_TEM
TFAIL.VOL	电压变化/过高/过低	
TFAIL.DEST	数据存储介质的毁坏	存储介质的保护 ORM_PRO 存储介质的访问控制 ORM_ACO 存储介质的传输管理 ORM_TRA 存储环境管理 ORM_CIR 存储介质的备份 ORM_BAC 存储介质的分类和归档 ORM_CLA 数据备份和恢复 OBA_DAT
TFAIL.LEAK	出现软件漏洞	漏洞控制 OHO_VER 应用系统测试 TCE_APT 系统安全检测和验收 OEN_TES 数据备份和恢复 OBA_DAT 应急响应计划的制定 OBC_EST
TFAIL.POW	内部电源的毁坏	供电 TPR_SUP 数据备份和恢复 OBA_DAT 应急响应计划的制定 OBC_EST
TFAIL.NIS	NIS 服务器和 NIS 客户端之间缺乏认证能力	身份鉴别TCE_IDT 账户管理OHO_ACC 安全审计TCE_SAU 计算环境访问控制TCE_TAC 远程登陆管理OHO_TEL 远程访问 TEB_TEL

威胁标号	威胁简单描述	对策
TFAIL.XAUT	X 服务器和 X 客户端间缺乏认证能力	身份鉴别TCE_IDT 账户管理OHO_ACC 安全审计TCE_SAU 计算环境访问控制TCE_TAC 远程登陆管理OHO_TEL 远程访问 TEB_TEL
TFAIL.LOSE	存储数据丢失	存储介质的保护 ORM_PRO 存储介质的传输管理 ORM_TRA 存储环境管理 ORM_CIR 存储介质的备份 ORM_BAC 数据备份和恢复 OBA_DAT 防火 TPR_FIR 防潮 TPR_WAT 防静电 TPR_STA 电磁防护 TPR_TEM 存储介质的保护 ORM_PRO 存储介质的传输管理 ORM_TRA 存储环境管理 ORM_CIR 存储介质的备份 ORM_BAC 数据备份和恢复 OBA_DAT 防潮 TPR_WAT 防静电 TPR_STA 电磁防护 TPR_TEM 病毒和恶意代码防范 TCE_VIR 防病毒网关 TEB_TVI 防病毒网关 TEB_TVI
TFAIL.EXH	因存储介质耗尽引起的信息丢失	设备和系统冗余 OBA_EQI 存储介质的保护 ORM_PRO 病毒和恶意代码防范 TCE_VIR
TFAIL.ELE	屏蔽区域的瞬间电流	电磁防护 TPR_TEM 数据备份和恢复 OBA_DAT
TFAIL.BUG	软件漏洞或错误	漏洞控制 OHO_VER 数据备份和恢复 OBA_DAT
TFAIL.DBFN	数据备份中文件名的转换	存储介质的保护 ORM_PRO 数据备份和恢复 OBA_DAT
TFAIL.DBF	数据库故障	数据库设计安全 TCE_DBS 资产鉴别 ORA_ASE 应用系统测试 TCE_APT

威胁标号	威胁简单描述	对策
		系统安全检测和验收 OEN_TES
TFAIL.ODBC	通过 ODBC 进行访问控制欺骗	数据库设计安全 TCE_DBS 资产鉴别 ORA_ASE 威胁分析 ORA_THR 脆弱性分析 ORA_VUL 应用系统测试 TCE_APT 系统安全检测和验收 OEN_TES 计算环境访问控制 TCE_TAC 数据备份和恢复 OBA_DAT 应急响应计划的制定 OBC_EST
TFAIL.DATA	数据库中数据的丢失	数据库设计安全 TCE_DBS 资产鉴别 ORA_ASE 威胁分析 ORA_THR 脆弱性分析 ORA_VUL 计算环境访问控制 TCE_TAC 系统安全检测和验收 OEN_TES 数据备份和恢复 OBA_DAT 应急响应计划的制定 OBC_EST
TFAIL.SROR	存储空间缺乏引起的数据库中数据丢失	设备和系统冗余 OBA_EQI 存储介质的保护 ORM_PRO 存储介质的备份 ORM_BAC 数据备份和恢复 OBA_DAT
TFAIL.INTE	数据库完整性/一致性丢失	数据库设计安全 TCE_DBS 应用系统测试 TCE_APT 系统安全检测和验收 OEN_TES 数据备份和恢复 OBA_DAT
TFAIL.DEF	网络组件的失败或故障	网络可靠性管理 ONE_REL
TFAIL.SEND	信息发送失败	网络可靠性管理 ONE_REL
TFAIL.AUTH	认证性能差或缺失	身份鉴别 TCE_IDT 网络设备用户身份鉴别 TNI_IDT 安全审计 TCE_SAU
TFAIL.ENCM	加密模块的故障	密码技术 TNI_ENC 密钥管理 OCO_KEY
TFAIL.ENCY	加密算法不可靠	密码技术 TNI_ENC
TFAIL.ENC	加密数据的错误	密码技术 TNI_ENC

威胁标号	威胁简单描述	对策
TFAIL.MAIL	E-mail 缺乏时间真实性	主机入侵防范 TCE_IDS 选择安全控制措施 ORA_CTR 病毒和恶意代码防范 TCE_VIR 漏洞控制 OHO_VER
TFAIL.TRB	网络管理系统或系统管理系统组件故障	网络可靠性管理 ONE_REL 应急响应计划的制定 OBC_EST
TMALICE.BREK	IT 设备或附件被操纵或被破坏	设备安全 TPR_EQI 门禁 TPR_JAN 机房管理 OPM_ROM 存储介质的保护 ORM_PRO 第三方访问 OPE_OTT 安全策略执行 PIN_EXE
TMALICE.DBCT	数据或软件被操纵	机房管理 OPM_ROM 存储介质的访问控制 ORM_ACO 账户管理 OHO_ACC 网络设备管理授权 ONE_ADV 计算环境访问控制 TCE_TAC 身份鉴别 TCE_IDT 网络设备用户身份鉴别 TNI_IDT 安全审计 TCE_SAU 变更控制 OCO_CHA 人员离岗 OPE_DIM
TMALICE.BUI	未经授权进入建筑	设备安全 TPR_EQI 门禁 TPR_JAN 机房管理 OPM_ROM 环境设备维护 OPM_MAI
TMALICE.STE	偷窃	设备安全 TPR_EQI 门禁 TPR_JAN 机房管理 OPM_ROM 存储介质的保护 ORM_PRO 第三方访问 OPE_OTT
TMALICE.DES	恶意破坏行为	设备安全 TPR_EQI 机房管理 OPM_ROM 存储介质的保护 ORM_PRO 办公环境管理 OPM_OFM 第三方访问 OPE_OTT 安全培训 OPE_TRA

威胁标号	威胁简单描述	对策
		岗位安全职责 OOR_STA 安全策略执行 PIN_EXE
TMALICE.ATT	攻击行为	门禁 TPR_JAN 办公环境管理 OPM_OFM 合作与沟通 OOR_COM 机房管理 OPM_ROM 安全策略执行 PIN_EXE 第三方访问 OPE_OTT
TMALICE.INTER	线路侦听	设备安全 TPR_EQI 防干扰和窃听 TPR _TAP 远程登陆管理 OHO_TEL
TMALICE.COMM	通讯线路被操纵	设备安全 TPR_EQI 防干扰和窃听 TPR _TAP 主干网可用性保护 TNI_AVI 内部网络防护 TNI_INT 人员离岗 OPE_DIM
TMALICE.AUIT	未经授权使用 IT 系统	身份鉴别 TCE_IDT 网络设备用户身份鉴别 TNI_IDT 账户管理 OHO_ACC 网络设备管理授权 ONE_ADV 计算环境访问控制 TCE_TAC 安全审计 TCE_SAU 网络边界访问控制 TEB_NAC
TMALICE.TELM	滥用远程维护端口	远程登陆管理OHO_TEL 网络设备管理授权ONE_ADV 身份鉴别TCE_IDT 网络设备用户身份鉴别TNI_IDT 账户管理OHO_ACC 安全审计TCE_SAU 远程访问 TEB_TEL
TMALICE.INS	内部员工在维护/系统管理工作中造成的威胁	人员录用 OPE_EMP 安全培训 OPE_TRA 安全策略执行 PIN_EXE 岗位安全职责 OOR_STA 关键岗位安全管理 OOR_KST
TMALICE.EXT	外部人员在维护/系统管理工作中造成的威胁	机房管理 OPM_ROM 第三方访问 OPE_OTT

威胁标号	威胁简单描述	对策
TMALICE.CRACK	系统地进行口令破解	身份鉴别 TCE_IDT 网络设备用户身份鉴别 TNI_IDT 账户管理 OHO_ACC 网络设备管理授权 ONE_ADV
TMALICE.USER	滥用用户权限	网络设备管理授权 ONE_ADV 远程登陆管理 OHO_TEL 安全培训 OPE_TRA 人员离岗 OPE_DIM 安全策略执行 PIN_EXE 岗位安全职责 OOR_STA 关键岗位安全管理 OOR_KST
TMALICE.ADM	滥用系统管理员权限	网络设备管理授权 ONE_ADV 岗位安全职责 OOR_STA 关键岗位安全管理 OOR_KST
TMALICE.TROY	特洛伊木马	病毒和恶意代码防范 TCE_VIR 主机入侵防范 TCE_IDS 变更控制 OCO_CHA
TMALICE.MOV	偷窃可移动 IT 系统	设备安全 TPR_EQI 资产鉴别 ORA_ASE 威胁分析 ORA_THR 存储介质的备份 ORM_BAC 计算环境访问控制 TCE_TAC 远程访问 TEB_TEL 安全策略执行 PIN_EX
TMALICE.VIRUS	计算机病毒	防病毒网关 TEB_TVI 病毒和恶意代码防范 TCE_VIR 存储介质的备份 ORM_BAC 数据备份和恢复 OBA_DAT
TMALICE.REP	信息重放	防干扰和窃听 TPR _TAP 设备安全 TPR_EQI 主干网可用性保护 TNI_AVI 安全域规划 ONE_SED 网络可靠性管理 ONE_REL 安全审计 TCE_SAU
TMALICE.POSE	伪装	身份鉴别 TCE_IDT 网络设备用户身份鉴别 TNI_IDT 网络设备管理授权 ONE_ADV

威胁标号	威胁简单描述	对策
		安全审计 TCE_SAU 防干扰和窃听 TPR _TAP
TMALICE.FLUX	信息流分析	密码技术 TNI_ENC 防干扰和窃听 TPR _TAP 主干网可用性保护 TNI_AVI 安全域规划 ONE_SED 网络可靠性管理 ONE_REL
TMALICE.DOS	拒绝服务	主干网可用性TNI_AVI 网络设备登录控制TNI_TEL 网络边界访问控制TEB_NAC 计算环境访问控制TCE_TAC 防病毒网关TEB_TVI.3 病毒和恶意代码防范TCE_VIR 安全域规划ONE_SED 网络可靠性管理ONE_REL 设备和系统冗余 OBA_EQI
TMALICE.COPY	未经授权进行数据拷贝	存储介质的访问控制 ORM_ACO 存储介质的保护 ORM_PRO 存储介质的传输管理 ORM_TRA 存储环境管理 ORM_CIR 存储介质的备份 ORM_BAC 存储介质的分类和归档 ORM_CLA
TMALICE.UUDP	滥用带有 UUDP 功能的 UNIX 系统	身份鉴别TCE_IDT 账户管理OHO_ACC 远程访问TEB_TEL 网络设备管理授权ONE_ADV 网络设备登录控制TNI_TEL
TMALICE.ARP	IP 欺骗	计算环境访问控制TCE_TAC 网络边界访问控制TEB_NAC 主机入侵防范TCE_IDS 网络入侵防范TEB_IDS 网络可靠性管理ONE_REL IP 地址管理 ONE_IPM
TMALICE.FROU	源路由的滥用	网络边界访问控制TEB_NAC 主机入侵防范TCE_IDS 网络入侵防范TEB_IDS

威胁标号	威胁简单描述	对策
TMALICE.ICMP	滥用 ICMP 协议	网络边界访问控制TEB_NAC 主机入侵防范TCE_IDS 网络入侵防范 TEB_IDS
TMALICE.OSPF	滥用路由协议	网络边界访问控制TEB_NAC 网络入侵防范TEB_IDS 路由管理 ONE_ROU
TMALICE.ADMIN	滥用 Windows 系统管理员权限	身份鉴别TCE_IDT 安全审计TCE_SAU 账户管理OHO_ACC 计算环境访问控制TCE_TAC
TMALICE.SNIF	网络分析工具	网络设备管理授权 ONE_ADV 防干扰和窃听 TPR _TAP 远程登陆管理 OHO_TEL 主干网可用性保护 TNI_AVI 内部网络防护 TNI_INT
TMALICE.ROUT	滥用远程访问路由的管理功能	网络边界访问控制 TEB_NAC 路由管理 ONE_ROU 远程访问 TEB_TEL 远程登陆管理OHO_TEL
TMALICE.TEL	通过远程 IT 系统滥用资源	网络边界访问控制TEB_NAC 网络设备登录控制TNI_TEL 远程登陆管理OHO_TEL 远程访问TEB_TEL
TMALICE.MANI	操纵数据库系统中数据或软件	数据库设计安全 TCE_DBS 身份鉴别 TCE_IDT 安全审计 TCE_SAU 计算环境访问控制 TCE_TAC 数据备份和恢复 OBA_DAT
TMALICE.DBDOS	数据库系统的拒绝服务	数据库设计安全 TCE_DBS 主机入侵防范 TCE_IDS 网络入侵防范 TEB_IDS 数据备份和恢复 OBA_DAT 设备和系统冗余 OBA_EQI
TMALICE.CONN	未经授权将 IT 系统连接到网络	网络可靠性管理 ONE_REL 远程登陆管理 OHO_TEL 网络设备登录控制 TNI_TEL 设备和系统冗余 OBA_EQI

威胁标号	威胁简单描述	对策
		安全培训 OPE_TRA 选择安全控制措施 ORA_CTR 应急响应计划的制定 OBC_EST 安全策略执行 PIN_EXE
TMALICE.NETM	未经授权执行网络管理功能	网络可靠性管理 ONE_REL 远程登陆管理 OHO_TEL 网络设备登录控制 TNI_TEL 安全审计 TCE_SAU 安全策略执行 PIN_EXE
TMALICE.ACNET	未经授权访问网络组件	远程登陆管理 OHO_TEL 网络设备登录控制 TNI_TEL 安全审计 TCE_SAU 安全策略执行 PIN_EXE 账户管理 OHO_ACC
TMALICE.CONFI	保密信息机密性丢失	人员录用 OPE_EMP 安全培训 OPE_TRA 安全策略执行 PIN_EXE 岗位安全职责 OOR_STA 设备安全 TPR_EQI 门禁 TPR_JAN 机房管理 OPM_ROM 存储介质的保护 ORM_PRO 存储介质的访问控制 ORM_ACO 存储介质的传输管理 ORM_TRA 存储环境管理 ORM_CIR 存储介质的销毁 ORM_DES 主机设备维护 OHO_EQI
TMALICE.MAIL	滥用 e-mail 服务	账户管理 OHO_ACC 身份鉴别 TCE_IDT 安全审计 TCE_SAU 安全策略执行 PIN_EXE 存储介质的访问控制 ORM_ACO 网络可靠性管理 ONE_REL 安全域规划 ONE_SED
TMALICE.CAM	伪装发件人	账户管理 OHO_ACC 身份鉴别 TCE_IDT 安全审计 TCE_SAU

威胁标号	威胁简单描述	对策
TMALICE.DNS	DNS 欺骗	主机入侵防范TCE_IDS 网络入侵防范TEB_IDS IP地址管理ONE_IPM
TMALICE.WIN	未经授权获取 Windows NT 系统管理员权限	账户管理OHO_ACC 身份鉴别TCE_IDT
TMALICE.DUPE	愚弄信息	安全培训OPE_TRA 安全策略执行PIN_EXE 选择安全控制措施ORA_CTR
TMALICE.AUTH	未经授权使用加密模块	应用系统测试TCE_APT 系统安全检测和验收OEN_TES 计算环境访问控制TCE_TAC 密码技术TIN_ENC 账户管理OHO_ACC 身份鉴别TCE_IDT 网络设备用户身份鉴别TNI_IDT 安全审计TCE_SAU
TMALICE.ENCM	加密模型被操纵	应用系统测试TCE_APT 系统安全检测和验收OEN_TES 计算环境访问控制TCE_TAC 账户管理OHO_ACC 身份鉴别TCE_IDT 网络设备用户身份鉴别TNI_IDT 安全审计TCE_SAU
TMALICE.KEY	危及密钥安全	密钥管理OCO_KEY 安全培训OPE_TRA 岗位安全职责OOR_STA 安全策略执行PIN_EXE 存储介质的保护ORM_PRO 存储介质的访问控制ORM_ACO 密码技术TIN_ENC
TMALICE.INTE	应被保护的信息的完整性缺失	网络拓扑设计和规划 ONE_TOP 网络可靠性管理 ONE_REL 防病毒管理 OHO_VIR 防病毒网关 TEB_TVI 病毒和恶意代码防范 TCE_VIR 数据库设计安全 TCE_DBS 主机入侵防范 TCE_IDS

威胁标号	威胁简单描述	对策
		网络入侵防范 TEB_IDS 存储介质的保护 ORM_PRO 存储介质的访问控制 ORM_ACO 存储介质的备份 ORM_BAC
TMALICE.CTRL	管理参数被操纵	账户管理 OHO_ACC 岗位安全职责 OOR_STA 配置管理计划 OCO_PLA 安全审计 TCE_SAU 选择安全控制措施 ORA_CTR 安全策略执行 PIN_EXE
TMALICE.WEB	web 欺骗	主机入侵防范TCE_IDS 网络入侵防范TEB_IDS 身份鉴别TCE_IDT
TMALICE.SCR	滥用脚本内容	主机入侵防范TCE_IDS 计算环境访问控制TCE_TAC 网络边界访问控制TEB_NAC
TMALICE.HIJ	网络连接的被劫持（控制）	防干扰和窃听TPR _TAP 网络可靠性管理ONE_REL 安全审计TCE_SAU 安全策略执行PIN_EXE

图表 8 公司 IP 网络面临的常见威胁

2 一级系统基线安全要求（Baseline）

2.1 安全技术要求

2.1.1 TPR 类：物理环境安全

2.1.1.1供电 TPR_SUP

a) 应该保护设备以防电力中断和其他与电力供应有关的异态。应该根据设备制造商的说明提供合适的电力；
b) 紧急电源开关应位于设备室的紧急出口附近，以便在紧急情况下迅速切断电源。在主电源发生故障时，应该提供应急照明；
c) 供电系统应将动力、照明用电与网络系统供电线路分开，并配备应急照明装置；
d) 应使用双回路或多回路供电；
e) 提供紧急情况供电，配置 UPS 设备，以备常用供电系统停电时启用。

2.1.1.2防雷击 TPR_THU

a) 重要的主机系统和网络系统，以及办公场所应当有防雷击措施。
b) XXX 所在的大厦要有避雷针等避雷设备，大厦应当具有符合要求的接地条件。
c) 应采用地桩、水平栅网、金属板、建筑物基础钢筋等构建接地系统，确保接地体良好的接地；
d) 设置信号地与直流电源地，应注意不造成额外耦合，保障去耦、滤波等的良好效果；

e) 设置避雷地，应以深埋地下、与大地良好相通的金属板作为接地点，至避雷针的引线则应采用粗大的紫铜条，或者使整个建筑的钢筋自地基以下焊连成钢筋网作为“大地”与避雷针相连。

f) 接地电阻〈4Ω，电源的地线与计算机设备的地线必须分别设置。

2.1.1.3防火 TPR_FIR

a) 建筑材料防火：要求机房和记录介质存放间，其建筑材料的耐火等级，应符合 GBJ45-1987 中规定的二级耐火等级；机房相关的其余基本工作房间和辅助房，其建筑材料的耐火等级应不低于 TJ16-1987 中规定的三级耐火等级。

b) 报警和灭火系统：要求设置火灾报警系统，由人来操作灭火设备，并对灭火设备的效率、毒性、用量和损害性有一定的要求。

c) 必须按面积和设备数量配备适合计算机设备使用的灭火器（不得使用干粉、泡沫灭火器），有条件的可以安装配备感温、感烟探测器的固定灭火系统。

2.1.1.4防潮 TPR_WAT

1) 防止空调冷凝水、暖气漏水等事故引发水患造成网络系统、文档和介质的损坏。

2) 水管安装，不得穿过屋顶和活动地板下。穿过墙壁和楼板的水管应使用套管，并采取可靠的密封措施；

3) 计算机设备应放在工作台上，并备有防水罩；

4) 对工作人员进行防水害教育，并使其了解机房进水管关闭阀的准确位置，做到人人会用；

5) 采取一定措施，防止雨水通过屋顶和墙壁渗透、室内水蒸气结露和地下积水的转移与渗透。

2.1.1.5空调 TPR_CON

a) 应有必要的空调设备，使机房温度/湿度达到所需的基本要求。

2.1.1.6电磁防护 TPR_TEM

1) 应采用接地的方法防止外界电磁干扰和设备寄生耦合干扰；
2) 应采用屏蔽方法，对信号线、电源线进行电屏蔽，减少外部电器设备对计算机的瞬间干扰；
3) 应采用距离防护的方法，将计算机机房的位置选在外界电磁干扰小的地方和远离可能接收辐射信号的地方。

2.1.1.7门禁 TPR_JAN

1) 规模较大的物理区域，应向所有的工作人员（包括来自外单位的长期工作人员）发放带有照片的身份证件，并定期进行检查或更换。
2) 短期工作人员或维修人员的证件，应注明有效日期，届时收回。
3) 参观人员必须由主管部门办理参观手续，参观时必须有专人陪同。
4) 因系统维修或其他原因需外国籍人进入办公区时，必须始终有人陪同。
5) 在无警卫的场合，必须保证室内无人时，关锁所有出入口。
6) 应该通过门禁系统对于出入进行控制。这种控制可能不仅仅限于进入，还可能包括离开，控制措施可以具体增加出示有效证件、登记姓名等。
7) 物理环境/机房的出入口应有专人负责，未经允许的人员不准进入机房；
8) 未经许可，不得在场所内拍照或摄影。

2.1.1.8位置选择 TPR_LOC

a) 按一般建筑物的要求进行机房场地选择。

2.1.1.9防静电 TPR_STA

1) 采用接地与屏蔽措施，使网络系统有一套合理的接地与屏蔽系统；
2) 人员服装应采用不易产生静电的衣料，工作鞋选用低阻值材料制作；
3) 控制机房温湿度，使其保持在不易产生静电的范围内。

2.1.1.10 设备安全 TPR_EQI

a) 网络系统的设备和部件应有明显的无法除去的标记，以防更换和方便查找赃物；
b) 物理区域中应安装防盗报警装置，防止夜间从门窗进入的盗窃行为以及对系统的非法访问。

2.1.1.11 防干扰和窃听 TPR _TAP

a) 如有可能，接入信息处理设备的电源和通信线路应该铺设在地下，或者采取足够的可替代的保护。
b) 应该保护网络电缆以防未经授权的窃听或损坏，并保护电力电缆不受损坏。例如，通过使用电缆管道和避免通过公共区域，并有防鼠害的措施。
c) 电力电缆应该与通信电缆隔离，以防干扰。
d) 应采取一定措施，预防线路截获，使线路截获设备难以工作；应有探测线路截获装置，及时发现线路截获事件并报警。

2.1.2 TNI 类：网络与通信安全

2.1.2.1 主干网可用性保护 TNI_AVI.1

为保证骨干网的可用性，应满足以下原则：

1） 对骨干网的核心设备应采用冗余设计，包括设备模块冗余、设备热备等。

2）对骨干网的链路采用冗余设计，采用如以太通道等技术，达到提高链路带宽、负载均衡、链路备份的目的。

3）对冗余的方案/设备/线路等的测试方案，并定期（至少三个月一次）进行验证测试，以判别是否满足冗余要求，并对发生的问题进行及时处理和备案。

4）制定网络可靠性保障需求，制定相关的 SLA，并指定专门的内部部门或者外部部门维护和保证。建立网络可靠性监控系统，及时发现并处理可靠性中断/降低故障，对故障处理结果进行教训总结。对 SLA 的执行情况进行定期的审计和计划，应当重点考虑以下问题：

- ✓ SLA 的执行效率
- ✓ SLA 维护情况
- ✓ 内部/外包商执行情况和问题
- ✓ SLA 的违反情况
- ✓ SLA 的改进建议
- ✓ 可靠性的改进建议

2.1.2.2 内部网络防护 TNI_INT.1

在网段划分上，提出了“同一子网支持单一业务”的原则，以形成清晰的边界。

1) 根据各组的工作职能、重要性、所涉及信息等级等因素，划分不同的子网或网段。不同的区域在交换机上划分不同 VLAN，不同 VLAN 之间的路由设置访问控制。

2) 按照方便管理和控制的原则为各子网、网段分配 IP 地址段。例如，地址规划应便于路由汇总以方便路由管理、提高路由广播效率以及简化访问控制列表的配置。

2.1.2.3 网络设备登录控制 TNI_TEL.1

对所有设备的管理端口（vty/sc0/vlan0/aux/tty/console 等）的访问，均需要有相当认证机制。要求至少采取下列措施中的一种或者多种，以达到所需的安全需求：

1) 采用带外管理方式，使得管理链路和数据交换链路隔离，通过专用内部管理网络访问管理设备，防止威胁主体通过对数据交换链路的监听获取密码和管理信息。

2.1.2.4 网络设备用户身份鉴别 TNI_IDT.1

采用网络设备自身提供本地身份鉴别机制，如口令认证或者用户名/口令认证。

维护对设备用户的记录。

2.1.2.5 密码技术 TIN_ENC.1

1) 对称加密算法的密钥位数必须等同于 64 位 DES 算法。

2) 非对称加密算法的密钥位数必须等同于 512 位 RSA 算法；

3) 对于采用软件密码管理的系统，应提供在系统安装初始化时产生密钥种子，密钥种子不得固化在程序中。

4) 通信过程中，至少对于敏感信息例如客户帐号、密码、金额等字段应进行加密。

2.1.3 TEB 类：边界保护

2.1.3.1 网络边界访问控制 TEB_NAC.1

网络边界的访问控制机制主要是限制用户可以建立什么样的连接以及通过网络传输什么样的数据。网络访问控制的目的就是在各网络连接之间建立一个安全控制点，通过允许、拒绝经过网络访问控制设备的数据流，实现对进、出内部网络的服务和访问的审计和控制。

有数据交换的不同网络之间的边界处都需要网络访问控制。一般来说，采用防火墙，路由器访问控制列表等方式对边界进行保护，保护对象为任何向外部系统提供信息发布的设备/系统，至少包括：

- 路由交换信息

- 主机
- 网络设备
- 应用服务

在本级要求在 OSI 模型的 3 到 7 层上检查数据包，并具有对应用层协议中的命令、格式、内容进行过滤的功能，具体的技术功能要求包括：

1) 防火墙应该提供一个默认策略，保证所有经过防火墙的数据包都有相对应的安全策略进行控制。这个默认策略可以是允许，也可以是拒绝。

2) 防火墙应该具有透明应用代理功能，能对信息流的内容按照一定方式进行过滤。支持 HTTP、FTP、TELNET、SMTP、POP3、NNTP、流媒体等各种常见应用协议；实现对 URL 的过滤；实现对 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制，实现对文件级的过滤。

3) 按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要业务数据主机进行通讯。

访问控制中的一个重要的步骤是对参与通信的一个或多个团体或个人进行授权，即定义其访问权限。授权将一组权限赋予一个实体。实体的访问权限通常与其真实身份相关，身份不同，工作的内容、性质、所在的部门就不同，因此所应关注的系统操作也不同，授予的权限也就不同。如系统管理员与普通用户的访问权限就有很大的差别。

访问权限的定义内容包括定义哪些用户能登录到系统并获取网络资源；哪些用户对网络有什么样的操作权限；哪些用户对目录、文件或设备有什么样的操作权限（如读权限、写权限、创建权限、删除权限、修改权限、查找权限等）等。总之，凡是需要进行网络访问控制的地方都应该先定义访问权限。

定义访问权限可以通过访问控制列表、为应用系统数据流建立的调查表、设备接入检查等技术来实现。

4) 访问授权与拒绝：

- 此类产品应能根据数据包的源地址、目的地址、源端口号、目的端口号、协议、出入的接口等，提供明确的访问保障能力和拒绝访问能力，并支持地址通配符的使用。
- 过滤表的大小应能满足用户的实际需求。
- 具有抵御常见的端口扫描的能力。

5) 支持静态 NAT（网络地址转换）功能。

6) 从外部接入专用网络必须经过鉴别（包括回叫设备，动态口令，智能卡等）、认证、授权，对号码进行身份识别。

7) 支持属性修改，此类产品自身的安全功能应(仅向授权管理员)提供修改下述（包含但不仅限于）参数的能力：源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性）；增加、修改或删除管理员帐号。

8) 支持属性查询：此类产品自身的安全功能应(仅向授权管理员)提供以下查询：源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性）。

9) 通过防火墙传送信息的用户名、主机名。

10) 具有抵御常见的端口扫描和攻击的能力：包括 IP 地址欺骗、DoS 攻击（如 TCP SYN Flood 等）、中间人攻击、碎片攻击等，能过滤异常分段、分段过小、源路由等异常包；能进行流量检测过滤等。

11) 支持多种告警方式，设置告警策略。

12) 硬件 MTBF（平均无故障运行时间）不低于 2400 小时（3 月）。

2.1.3.2 远程访问 TEB_TEL.1

应监控远程访问接入对于内部系统的访问，必须采取适当的监控记录手段，记录接入时间，地址，电话，人员，访问对象等。

1）对远程访问进行监控的主要技术功能要求

✓ 实施安全监控，由操作员负责监视以采集网络中的流量，设备运行情况等信息。

在远程访问中应当建立独立的身份认证、鉴别和授权服务器，强化身份认证和鉴别能力。

2）对远程访问中身份鉴别的具体技术功能要求

✓ 必须采用用户名/口令对的方式进行身份鉴别。

✓ 应当保证在身份鉴别过程中口令不可见。

✓ 采用加密方式存储口令。

✓ 应当保证身份鉴别的时效性，在登录或者注销时，应当对相关的身份鉴别状态进行标记，以便指示新的过程。

✓ 所有的远程访问必须具备身份鉴别和访问授权控制，只有通过适当的身份鉴别和访问授权，才能允许远程访问。

✓ 用户每次登录系统时应当进行身份鉴别，并对此过程进行记录。

✓ 不允许系统管理人员直接以具备系统管理权限的账户远程访问登录系统，必须通过中转的方式，即先以普通权限用户身份登录系统，然后通过系统用户身份切换功能变换为系统管理员。

✓ 对远程系统管理应当限定登录访问的地址范围，绝对不允许没有来源控制的远程系统管理。

✓ 必须对远程访问的用户进行统一集中管理，具备相关的申请登记流程和审批流程，其中应当至少包括人员背景调查等方面。

✓ 必须对用户的操作过程进行记录，至少保证前 1000 条操作被正确纪录，供审计分析。

3）其他技术功能要求

✓ 远程访问必须只允许来自可信信道的连接，对与其他信道则不允许。

电话拨号等（包括模拟电话/公共交换电话网 PSTN 和综合服务数字网 ISDN）经接入服务器联入用户网，当拨号用户通过认证后，接入服务器将为之分配用户网范围内的地址，远程用户在逻辑上就成为网络内部用户。

拨入方式远程访问的技术功能要求（接入服务器的功能要求）

✓ 按用户需求支持模拟 modem/公共交换电话网 PSTN 拨号接入。

✓ 按用户需求支持 ISDN 拨号接入。

✓ 具有对拨号接入用户的严格认证功能。

✓ 具有对拨号接入用户的网络访问授权功能。

2.1.3.3 防病毒网关 TEB_TVI.1

防病毒网关是网络安全的重要组成部分，其主要功能是对从外部网络进入用户内部网络的病毒进行过滤，一般主要针对 HTTP、HTTPS、FTP 和 SMTP 等协议进行过滤，保护用户内部网络不受病毒感染。

对防病毒网关的主要技术功能要求有：

1）防止病毒进出内部网络。

2）支持对常见格式压缩文件的病毒检测。

3）至少对基于 http、ftp、socks/mms、telnet、gopher、smtp、imap、pop3 等主要网络协议的事件进行检测，剥离 ActiveX 和 Java Script、Java Applet 等恶意代码。

4）支持对宏病毒和可疑宏的高效检查功能。

5）代理内容过滤。基于网页标题和内容，设置过滤规则和规则库，实现对浏览网页的过滤。过滤垃圾和违规邮件侵扰，至少可对标题、文本、html、附件（文本、html、常见压缩包）等进行内容过滤、病毒过滤及恶意代码过滤，允许管理员定制过滤规则，以符合企业或各机关单位内部网络的需要。

6）支持自动定时升级。

7）防病毒网关不能影响原有的网关系统。

8）硬件 MTBF（平均无故障运行时间）不低于 8760 小时（1 年）。

2.1.3.4 网络入侵防范 TEB_IDS.1

基于网络的入侵检测产品通过对计算机网络中的若干关键点收集信息并对其进行分析，以发现网络中是否有违反安全策略的行为和被攻击的迹象。

在一个网络环境中，有很多配置点可以考虑设置网络 IDS。IDS 设置在防火墙之外，可以观察到未被防火墙过滤的原始的外部网络通信；设置在防火墙的内部，提供了对目的地是内部网络的外部流量或目的地是外部网络的内部流量的监测，而并不监测仅在内部网络中流动的通信。在内部网络环境中，网络 IDS 通常被设置在客户机与服务器、通信路径的中间，可以监测所有通信层次上的数据。本节主要介绍在边界处的入侵防范。

在确定 IDS 配置点和数目的时候，需要考虑的因素包括：操作员对每一个 IDS 发出的报警进行分析和划分的工作负担；对多个监测器监测到同一事件的报警进行关联分析的复杂性以及不同配置点的选择所带来的系统采购、安装、运行和维护的成本。

具体技术功能要求为：

1） 数据检测功能要求

✓ 数据收集：应具有实时获取受保护网段内的数据包的能力。获取的数据包应足以进行检测分析。

✓ 协议分析：至少应监视基于以下协议的事件：HTTP、FTP、TFTP、TCP、UDP、IP、ICMP、IMAP、SNMP、TELNET、DNS、SMTP、POP3、NETBIOS、NFS、NNTP、ARP、RIP、RPC 等。

✓ 行为监测：至少应监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫攻击等。

2)入侵分析功能要求

✓ 数据分析：应对收集的数据包进行分析，发现攻击事件。

3)入侵响应功能要求

✓ 安全报警：当产品检测到入侵时，应自动采取相应动作以发出安全警告。

✓ 响应方式：可对检测到的攻击行为采取告警、记录日志、会话阻断等响应方式。告警可以采取屏幕实时提示、E-mail 告警、声音告警等几种方式。

4)管理控制功能要求

✓ 图形界面：产品应提供友好的用户界面用于管理、配置网络安全监控报警产品。管理配置界面应包含配置和管理产品所需的所有功能。

✓ 事件数据库：产品的事件数据库应包括事件定义和分析、详细的漏洞修补方案、可采取的对策等。

✓ 事件分级：产品应按照事件的严重程度将事件分级，以使授权管理员能从大量的信息中捕捉到危险的事件。

✓ 策略配置：应提供方便、快捷的网络安全监控报警策略配置方法和手段。

✓ 升级能力：产品应具有及时更新、升级产品和事件库的能力。

5)检测结果处理要求

✓ 事件记录：产品应记录并保存检测到的入侵事件。入侵事件信息应至少包含事件发生时间、源地址、目的地址、危害等级、事件详细描述以及解决方案建议等内容。

✓ 事件查看：用户应能通过管理界面实时清晰地查看入侵事件。

✓ 事件可视化：产品应提供具有统计、查询等功能的工具，供用户阅读入侵事件数据。

✓ 事件导出：产品应具有导出入侵事件数据的功能。

✓ 报告生成：产品应能生成详尽的检测结果报告。

✓ 报告查阅：产品应具有全面、灵活地浏览检测结果报告的功能。

✓ 报告输出：检测结果报告可输出成标准格式（如 HTML、文本文件等）。

6)产品灵活性要求

✓ 窗口定义：产品可提供有效的手段支持用户自定义窗口显示的内容和显示方式。

✓ 报告定制:产品应支持授权管理员按照自己的要求修改和定制报告内容。

✓ 事件定义：产品应允许授权管理员自定义事件，或者对开发商提供的事件作修改，并应提供方便、快捷的定义方法。

7)性能指标要求

✓ 稳定性：在产品设计适应的带宽下，入侵检测产品应能长期稳定工作。

✓ 网络影响：产品不应对原网络的正常运行产生明显影响。

✓ 平均响应时间：当背景数据流达到网络的有效带宽时，入侵检测产品应保证有足够快的响应时间。

2.1.4 TCE 类：保护计算环境

2.1.4.1应用系统测试 TCE_APT

通过监控系统辅助人工实现对系统运行状态、性能、资源和容量进行监控，并可设定报警阀值。

2.1.4.2病毒和恶意代码防范 TCE_VIR

在其运行网络环境的边界系统（如网关、电子邮件服务器）部署病毒防范系统。

2.1.4.3计算环境访问控制 TCE_TAC

a) 采用自主访问控制策略，可以用访问控制表及其相应的访问规则所组成的访问控制策略，确定相应的访问权限。
b) 无论采用何种访问控制策略所实现的自主访问控制功能，都要求能够：
   1) 了解掌握当前资源的访问控制能力。
   2) 允许命名用户以用户和/或用户组的身份规定并控制共享方式，并阻止非授权用户获取或者篡改敏感信息。
   3) 对访问是跨网络的情况，如果在物理上分隔（如内存与磁盘）间传递用户数据时，应严格执行访问控制策略，以防止信息的泄漏、篡改和丢失。也可以根据数据属性，按照密码支持第一级的要求保证数据在通过网络传输时的保密性和完整性。
   4) 对访问是非注册用户，如通用匿名访问的情况，应重点考虑对其获取信息的控制、写访问的严格控制以及相关必须的审计策略。

2.1.4.4身份鉴别 TCE_IDT

c) 必须采用用户名/口令对的方式进行身份鉴别；
d) 应当保证在身份鉴别过程中口令不可见；
e) 采用加密方式存储口令；
f) 应当保证身份鉴别的时效性，在登录或者注销时，应当对相关的身份鉴别状态进行标记，以便指示新的过程；

2.1.4.5安全审计 TCE_SAU

a) 要求产生完整的审计数据。
b) 提供审计数据的查阅。

2.1.4.6数据库设计安全 TCE_DBS

a) 系统在设计时不应留有“后门”，即不应以维护、支持或操作需要为借口，设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口。
b) 安全结构应是一个独立的、严格定义的软件系统子集，并应防止外部干扰和破坏，如修改其代码或数据结构；
c) 数据库管理系统应进行分层设计，并将数据库管理系统进程与和用户进程进行隔离；
d) 应提供设置和升级配置参数的安装机制，在初始化和对与安全有关的数据结构进行保护之前，应对用户和管理员的安全策略属性应进行定义；
e) 应区分普通操作模式和系统维护模式，全系统操作恢复的启动、配置系统内部的数据库和表等动作应在维护模式中执行。

2.2 安全管理要求

2.2.1 安全运作

2.2.1.1ORA 类：风险管理

2.2.1.1.1 资产鉴别 ORA_ASE.1

应该清晰识别每项资产、其拥有权、责任人以及资产现在的位置等，形成资产清单。

2.2.1.1.2 威胁分析 ORA_THR.1

应根据以往发生的安全事件、外部提供的资料和积累的经验对威胁进行粗略的分析。

威胁的分析应考虑机构所处的威胁环境及以下几方面：

a) 过去已经发生的安全事件的威胁原因分析；

b) 参考外部资料提供的威胁统计数据和报告。

2.2.1.1.3 脆弱性分析 ORA_VUL.1

采用脆弱性工具扫描，可以（但不限于）从以下几方面考虑：

a) 网关设备的脆弱性扫描；

b) 网络设备的脆弱性扫描；

c) 主机设备的脆弱性扫描；

d) 安全设备的脆弱性扫描；

2.2.1.1.4 风险分析 ORA_ANA.1

应由安全管理人员和外部安全专家通过经验来判断系统弱点，形成简单的风险报告。

2.2.1.1.5 选择安全控制措施 ORA_CTR.1

用信息安全领域常用的产品和服务分类列表作为基线，用基线选择的方法决定需要实施的信息安全控制措施。

2.2.1.1.6 安全措施的实施与确认 ORA_VAD.1

根据选择的安全控制措施，编写安全解决方案从管理手段和技术手段来实现安全控制措施。

2.2.1.2OEN 类：工程建设安全管理

2.2.1.2.1 安全项目的立项管理 OEN_CON.1

信息系统的安全建设立项要符合信息系统安全建设的总体规划, 经公司安全主管部门科学论证后方可进行设计和组织实施。

2.2.1.2.2 安全需求分析 OEN_REQ.1

安全需求分析阶段通常至少包括系统定义、威胁评估、脆弱性评估、影响评估、风险评估、确定安全要求等六个步骤。可以根据 ORA_THR.1、ORA_VUL.1、ORA_ANA.1、ORA_CTR.1 的要求进行安全需求分析。

2.2.1.2.3 安全功能规范 OEN_FSP.1

应该说明信息系统的安全属性和它的外部接口。

2.2.1.2.4 高层安全设计 OEN_HLD.1

应进行完整的高层安全设计，高层安全设计应该标识信息系统所要求的任何基础性硬件、固件、软件、和/或通信，和在这些硬件、固件、软件、和/或通信中实现的支持性保护机制所提供的功能表示。

2.2.1.2.5 安全产品选型 OEN_PRO.1

a） 安全产品具有在国内生产、经营和销售的许可证。

b） 密码产品符合国家密码主管部门的要求，来源于国家主管部门批准的密码研制单位。

2.2.1.2.6 外包软件安全控制.1

在软件的开发被外包时应当考虑许可安排、代码的所有权和知识产权以及质量合格证和所进行的工作的精确度。要减少软件中出现缺陷的可能性可以（但不限于）考虑如下方面：

a) 需要软件购买系统选择有良好声誉、可靠的记录而且有足够的资源和保险来负担因其软件导致的损失的供应商。

b) 要求所有软件都经过测试和验证。

c) 代码一旦被安装，就控制对代码的访问和修改；

2.2.1.2.7交付和运行 OEN_ADO.1

交付过程需要系统控制以及交付设备和程序来提供保证，以确保接收方所接受的信息系统的版本正是发送者发送的，而没有任何修改。

2.2.1.2.8系统安全检测和验收 OEN_TES.1

由验收组进行安全检测和验收。验收前，应编制验收大纲；验收大纲由验收组提出。

2.2.1.3OPM 类：物理环境管理

2.2.1.3.1机房管理 OPM_ROM.1

计算机机房是信息系统硬件资源的集中地，机房管理主要以加强机房物理访问控制和维护机房良好的运行环境为主。本安全级应按以下要求进行机房人员管理：

1) 机房出入应有人负责执守，未经允许的人员不准进入机房；
2) 获准进入机房的来访人员，其活动范围应受到限制，并有接待人员陪同；
3) 机房钥匙由专人管理，未经批准，不准任何人私自复制机房钥匙或服务器开机钥匙。
4) 没有指定管理人员的明确准许，任何记录介质、文件材料及各种被保护品均不准带出机房，与工作无关的物品（如：食品、香烟等）均不准带入机房。
5) 未经批准，禁止任何人移动计算机相关设备及其相关的系统或带离机房；
6) 机房内严禁吸烟及带入火种和水源。
7) 所有来访人员登记记录应妥善保存以备查；
8) 禁止测试物理访问控制；
9) 应经常打扫机房防止灰尘以及进行灭鼠工作。

2.2.1.3.2 办公环境管理 OPM_OFM.1

设置有网络终端的办公环境，是信息系统环境的组成部分，办公环境管理主要以加强信息保密性为主，防止利用终端系统窃取敏感信息或非法访问。本安全级应按以下要求进行终端办公环境的管理：

1) 工作人员下班后，终端计算机应关闭；
2) 存放敏感文件或信息载体的文件柜应上锁或设置密码；
3) 禁止使用调制解调器拨号上网。
4) 工作人员调离部门或更换办公室时，应立即交还办公室钥匙。

2.2.1.3.3 环境设备维护 OPM_MAI.1

机房内（包括电源间）的所有环境设备（如空调、电源等），由确定的部门负责管理，并随时受理和处理这些设备的突发事故。

2.2.1.4OHO 类：主机维护

2.2.1.4.1 主机设备维护 OHO_EQI.1

主机设备应当由指定的专人（主机设备管理人员）定期维护。

2.2.1.4.2 账户管理 OHO_ACC.1

1) 在系统初始化时，删除或者禁用不使用的系统缺省账户；
2) 对帐户进行分组或分级管理，并分别设置相应的权限；

2.2.1.4.3 远程登陆管理 OHO_TEL.1

a） 应当制定远程系统管理制度，记录和分配系统账户远程系统管理的操作权限分配；
b） 对系统进行远程管理和维护时应当：
   1) 不允许系统管理人员直接以具备系统管理权限的账户远程访问

登录系统，必须通过中转的方式，即先以普通权限用户身份登录系统，然后通过系统用户身份切换功能变换为系统管理员；

2) 对远程系统管理应当限定登录访问的地址范围，绝对不允许没有来源控制的远程系统管理；

c） 采用具有加密功能的远程终端和通信信道进行远程系统管理；

2.2.1.4.4 漏洞控制 OHO_VER.1

定期安装系统的最新补丁程序，并根据厂家提供的可能危害计算机的漏洞进行及时修补，并在安装系统补丁前对现有的重要文件进行备份。

2.2.1.4.5 防病毒管理 OHO_VIR.1

本级的病毒防护管理，根据所使用的病毒防护产品，提出了检查、记录、定期升级、汇报等的基本要求。

a） 应有指定人员检查网络内防病毒网关和主机的病毒检测情况，并保存染毒和杀毒记录。

b） 使用软盘、U 盘、光盘等外部移动存储设备之前应进行病毒检查；

c） 从不信任网络上所接收的文件，在使用前应首先检查是否有病毒；

d） 防病毒网关上安装的防病毒软件应每周定时升级。

2.2.1.5 ONE 类：网络维护

2.2.1.5.1 网络拓扑设计和规划 ONE_TOP.1

网络拓扑满足网络系统和业务需求，具有详细和完整的拓扑设计需求说明、设计文档、网络拓扑、实施过程文档以及网络拓扑变更文档，网络拓扑符合设计要求，网络拓扑图必须和当前实际运行情况保持一致，并保证和维护这些文档的机密性，使其只在允许的范围内被访问和获取。网络的设计必须考虑到网络容量、功能和结构。

2.2.1.5.2 IP 地址管理 ONE_IPM.1

具有 IP 地址管理规定，应当具有统一的 IP 地址管理机构/人员，由该机构/人员负责对外部和内部各个部门人员的 IP 地址进行登记、维护和分配。确保在网络中不发生地址冲突和盗用现象，应当采用一定的技术和管理制度保证不发生该类事件。并对违反 IP 地址管理规定的人员/部分依据相关管理制度进行处理。

2.2.1.5.3 网络可靠性管理 ONE_REL.1

应当制定网络可靠性保障需求，制定相关的 SLA，并指定专门的内部部门或者外部部门维护和保证。

针对各个内部/外部部门的不同需求，制定相应的 SLA，并与这些部门签署这些 SLA。并对这些 SLA 的执行情况进行跟踪监控，对出现违反 SLA 的情况进行相关处理。

建立网络可靠性监控系统，及时发现并处理可靠性中断/降低故障，对故障处理结果进行教训总结。

对 SLA 的执行情况进行定期的审计和计划，应当重点考虑以下问题：

a）SLA 的执行效率

b）SLA 维护情况

c）内部/外包商执行情况和问题

d）SLA 的违反情况

e）SLA 的改进建议

f） 可靠性的改进建议

2.2.1.5.4 路由管理 ONE_ROU.1

应当具有路由设计和规划，明确在网络的各个部分的选择和使用恰当的路由协议，具备基本的路由 SLA，保证网络的互联互通。

对网络中使用的路由协议运行情况进行监控：

a）静态路由管理

b）防止动态路由出现振荡、不收敛情况

c）防止路由出现异常的不可达现象

d）在边界对路由信息进行依据内部和外部规则进行必要的过滤。

对于动态路由，应当在满足互联互通的前提条件下实现可靠安全的认证交换制度，实现有效的防止路由欺骗功能。

对路由协议的变更进行管理和审批。

对路由中断情况进行实时发现和处理、经验教训总结。

应当强化以下内容：

a）路由协议管理和审计

b）路由使用情况审计

c）违反 SLA 的情况审计

d）路由中断处理审计

e）路由使用效能情况统计分析和改进建议

2.2.1.5.5 安全域规划 ONE_SED.1

针对不同的业务部门需求对其进行安全域规划，确定各个部门的安全功能需求，并按照这些安全功能需求设计和实现相应的安全隔离保护措施。

2.2.1.5.6 网络设备管理授权 ONE_ADV.1

采用网络设备自身提供的普通/特权两级授权管理机制管理设备。

2.2.1.6 OCO 类：配置和变更管理

配置和变更管理通过在细化和修改信息系统的过程中进行规范和控制，确保网络系统的完整性。配置和变更管理阻止对信息系统进行非授权的修改、添加或删除。

2.2.1.6.1 配置管理计划 OCO_PLA.1

应制定配置管理计划，并且每年进行审查和升级，以保证配置管理计划的可行性以及组织具有完成配置管理计划的能力。

2.2.1.6.2配置管理自动化 OCO_AUT.1

应该有措施来控制信息处理设备和系统的改变。对信息处理设备和系统变化的控制不够是系统或安全故障的通常原因。应在关键的设备上采用半自动的配置管理工具，并使用半自动的方法对计算机进行升级，并对相关人员进行配置管理的培训。

2.2.1.6.3配置管理能力 OCO_CAP.1

配置管理能力的设计应满足以下要求：

a）版本号，要求开发者所使用的版本号与所应表示的网络系统样本应完全对应，没有歧义。

b）配置项，要求配置项应有唯一的标识，从而对网络系统的组成有更清楚的描述。

2.2.1.6.4变更控制 OCO_CHA.1

系统的变更应有相关责任人对其控制。

2.2.1.6.5密钥管理 OCO_KEY.1

a) 存储密钥的介质必须严加保护，应以加密形式存储密钥；
b) 有关密钥存储方式和地方的信息不应被非授权人员获得；
c) 密钥必须由纯随机源产生。

2.2.1.7OBA 类：备份与恢复

2.2.1.7.1数据备份和恢复 OBA_DAT.1

为了保证在发生事故或灾难时，确保系统能够有效地恢复，应该通过数据备份和设备、系统冗余等方式，为可能发生的事故和灾难做出准备。数据备份和恢

复的主要目的是为了避免数据丢失风险和由此引起的业务中断风险。引起数据丢失的威胁有物理环境威胁和软硬件故障。除此之外，无作为和误操作也是经常引发数据丢失。数据存储和备份并非用于抵抗上述威胁，但可以有效降低上述威胁引发后果的严重性。数据备份的需求程度主要取决于数据的价值或业务中断造成后果的严重性。

本级数据备份和恢复的保护目标是在系统发生局部事故或灾难后，利用备份数据，至少能够恢复到一周前的状态，相关业务中断时间不超过 12 小时。

1） 数据应从运行的系统中备份到光盘、海量磁盘、磁带或磁带库等介质中，保存数据的介质必须由专人保管。

2） 机构应当制订备份和恢复相关的策略，相关的策略应覆盖（但不限于）如下一些内容：

- ✓ 应明确说明介质的分类、标记、查找方法。
- ✓ 应明确说明介质的使用、维护、保养、销毁方法。
- ✓ 应明确说明需定期备份重要业务信息、系统数据及软件等。
- ✓ 应确定重要业务信息的保存期以及其它需要永久保存的归档拷贝的保存期。
- ✓ 应明确说明可手工或软件产品进行备份和恢复。
- ✓ 应明确说明恢复审批和操作流程。

3) 数据恢复时，数据库管理员应填写数据恢复申请表，制订数据恢复计划报请主管批准。而后按恢复计划操作，登记数据恢复登记表。

4) 每周做一次包括数据和应用环境的全备份

2.2.1.7.2 设备和系统冗余 OBA_EQI.1

为了保证在发生事故或灾难时，确保系统能够有效地恢复，应该通过数据备份和设备、系统冗余等方式，为可能发生的事故和灾难做出准备。本级设备和系统冗余的保护目标是在系统发生局部事故或灾难后，利用冗余系统和冗余设备，保证至少能够恢复到一天前的状态，单次业务中断时间为小时级。

1) 系统内重要服务器，如重要的应用服务器和数据库服务器，应采用冷备、温备或热备的方式进行冗余设置。

2) 支持重要应用的网络设备应有冗余设置。

2.2.1.8ORM 类：存储介质管理

2.2.1.8.1 存储介质的保护 ORM_PRO.1

对存放重要数据和软件的各类记录介质（如纸介质、磁介质、半导体介质和光介质等）应受到控制和物理保护，其存储室必须符合防火、防水、防震、防腐烂、防鼠害、防蛀虫、防静电、防磁场、防盗以及符合制造商的储存规格的安全要求，确保其不受损、不丢失和不被非法访问。

2.2.1.8.2 存储介质的访问控制 ORM_ACO.1

1) 对借阅和复制的存储介质，要进行使用登记。

2) 对逾期未还的技术资料，应由技术资料存储室管理人员负责收回。

3) 一旦发现技术资料丢失或损坏，要立即报告有关部门，并采取补救措施。

2.2.1.8.3 存储介质的传输管理 ORM_TRA.1

1) 存储介质在物理运输时，例如通过邮递服务或者速递公司，会受到非法访问、滥用或被破坏，所以要对存储介质在机构之间的传递实施控制保障。

2) 管理层应该授权使用可靠的运输和速递公司，并按生产商的规格使用可靠的包装保护运输时不会物理破坏技术资料的内容。

2.2.1.8.4 存储环境管理 ORM_CIR.1

1) 介质存储室必须符合防火、防水、防震、防腐烂、防鼠害、防蛀虫、防静电、防磁场及防盗的安全要求。

2) 技术资料存储室管理员，负责技术资料存储室管理工作，并核查技术资料使用人员身份与权限。

2.2.1.8.5存储介质的备份 ORM_BAC.1

纸介质和电子介质之间实行交叉备份。

2.2.1.8.6存储介质的分类和归档 ORM_CLA.1

1) 技术资料按纸介质和电子介质分别集中分类管理、编制目录、造册登记。对同一内容以不同介质存储的技术资料要建立对应关系，以便于管理和使用。

2) 技术文档在保管和传递过程中必须采取保密和安全措施，并接受安全管理员的监督。

2.2.1.8.7存储介质的销毁 ORM_DES.1

1) 不再需要的的存储介质，应该安全地予以清除，因为如果处理不当，就会泄露敏信息。以下是一列可能需要安全清除的东西：

- ✓ 纸文件；
- ✓ 录音；
- ✓ 复写纸；
- ✓ 输出报表；
- ✓ 一次性打印色带；
- ✓ 磁带；
- ✓ 可换的磁盘或盒式磁带；
- ✓ 光盘（所有形式，包括所有生产商的软件光盘）；
- ✓ 程序列表；
- ✓ 测试数据；
- ✓ 系统说明文档；
- ✓ ……

2) 如果不再需要，可重用介质中的以前内容应该完全清除。

3) 所有机构要清除的技术资料应有授权。

2.2.1.9OBC 类：应急响应

2.2.1.9.1 应急响应计划的制定 OBC_EST.1

在业务连续性管理方面，除了要求机构能够制订备份和恢复策略来指导备份和恢复活动，对安全事件进行分类、分级来建立安全事件的报告制度，建立安全弱点和可疑事件的报告制度之外应制定应急计划的框架标准，规范机构各部门制定应急计划的行为，针对业务应用建立全面的应急计划，并对应急计划进行测试、维护和培训，并将应急计划文件化。

1) 本级应制定网络系统的简单的应急响应计划，其中至少应该包括以下几个方面的内容：

- ✓ 应急响应工作组织架构。
- ✓ 应急响应程序。
- ✓ 参与人员的职责。

2.2.1.9.2 应急响应计划的测试和演练 OBC_TES.1

1) 本级应对应急响应计划进行纸面模拟测试。
2) 纸面模拟测试应该涉及到（但不限于）以下领域：

- ✓ 考虑在备用平台上使用备份介质进行系统恢复；
- ✓ 考虑在恢复团队之间进行协调；
- ✓ 考虑内部和外部的连接性；
- ✓ 考虑备用设备的系统性能；
- ✓ 考虑正常操作的恢复；
- ✓ 考虑通知规程。

2.2.2 安全组织

2.2.2.1 OOR 类：安全组织和职责

2.2.2.1.1 安全管理组织 OOR_MNG.1

要求设立专职或兼职的信息安全人员，负责信息安全的管理和技术工作。

2.2.2.1.2 安全管理人员能力 OOR_CAP.1

应配备一定数量的计算机安全管理人员支持信息安全管理工作。安全管理人员可以由其他岗位的人员兼任。安全管理人员应该具有（但不限于）以下能力：

1) 基本的专业技术水平

2) 接受过安全意识教育和培训

3) 掌握安全管理基本知识等

2.2.2.1.3 岗位安全职责 OOR_STA.1

1) 根据最小特权原则，确定工作岗位、岗位职责和敏感程度。

2) 建立信息安全职责的考评制度。

2.2.2.1.4 关键岗位安全管理 OOR_KST.1

与计算机信息系统直接相关的系统管理员、网络管理员、重要业务开发人员、系统维护员、业务操作员等关键岗位应制定相应的管理制度进行特别管理。核实检查和安全处理的内容可能包括（但不限于）以下内容：

1) 人员上岗前必须经单位人事部门进行政治审查，技能考核等，合格者方可上岗。

2) 要害岗位人员应定期接受安全培训，加强自身安全意识和风险防范意识。

2.2.2.1.5 合作与沟通 OOR_COM.1

加强组织内部的合作与沟通，包括组织内各部门之间的合作与沟通、分部与总部的合作与沟通，共同协助处理信息安全问题。

2.2.2.2 OPE 类：人员管理

2.2.2.2.1 人员录用 OPE_EMP.1

对应聘者的道德行为和人品进行检查和确认，核实检查的内容可能包括（但不限于）以下内容：

1) 新招聘员工时，必须对应聘者的个人简历进行检查（针对完整性和准确性），对其毕业证、学位证以及声称的专业资格进行确认，审查应聘者的道德行为和人品。

2) 独立的身份检查（身份证或类似证件）。

2.2.2.2.2 人员离岗 OPE_DIM.1

对准备离岗人员应该在离岗前进行核实检查。核实检查的内容可能包括（但不限于）以下内容：

1）立即中止解雇的、退休的、辞职的或其他原因离开的员工的访问。

2）取回所有的身份证件、徽章。

3）收回机构提供的设备等等。

2.2.2.2.3 安全培训 OPE_TRA.1

要给予普通职员有关信息安全责任方面的指导，为安全管理人员提供安全技术、安全技能和安全操作培训，即对安全管理人员、安全技术人员、网络管理员、系统管理员、数据库管理员、软件开发人员等科技人员，进行安全技术和安全技能的培训。

2.2.2.2.4 第三方访问 OPE_OTT.1

第三方人员访问安全区域（例如机房、办公区域）时需要进行审批，由相关负责人审批通过后才能进入。

2.2.3 安全策略文档

2.2.3.1 PIN 类：安全策略制定与执行

2.2.3.1.1 安全策略范围 PIN_SCO.1

应当拥有信息安全管理所必须的管理制度、管理规定和操作规程等信息安全管理规章制度。安全规章制度应该能够满足安全管理的基本需要，至少包括下面内容的策略文档：机房管理、防病毒管理、网络管理、安全操作规程、组织结构和岗位职责、数据备份等。

2.2.3.1.2 安全策略执行 PIN_EXE.1

应当有明确的规定，要求所有人员必须遵守安全策略文档。

大部分员工知道与其相关的安全策略文档，并能够遵守安全策略文档。

2.2.3.2 PCO 类：安全策略发布与更新

2.2.3.2.1 策略发布 PCO_PUB.1

安全策略文档应该通过某种方式进行发布，使安全策略文档能够及时发布到所有相关人员手上。例如通过电子邮件把策略发送给相关人员、通过会议方式发布、把安全策略文档存放在服务器上、通过分发安全策略文档介质等方式进行发布。

2.2.3.2.2 策略更新 PCO_UPD.1

当发现安全策略文档有不适用或不合理的条款，进行更新。

3 二级系统基线安全要求（Baseline）

3.1 安全技术要求

3.1.1 TPR 类：物理环境安全

3.1.1.1供电 TPR_SUP

a) 应该保护设备以防电力中断和其他与电力供应有关的异态。应该根据设备制造商的说明提供合适的电力；
b) 紧急电源开关应位于设备室的紧急出口附近，以便在紧急情况下迅速切断电源。在主电源发生故障时，应该提供应急照明；
c) 供电系统应将动力、照明用电与网络系统供电线路分开，并配备应急照明装置；
d) 应使用双回路或多回路供电；
e) 提供紧急情况供电，配置 UPS 设备，以备常用供电系统停电时启用。
f) 采用线路稳压器，防止电压波动对网络系统的影响；
g) 采用有效措施，减少机房中电器噪声干扰，保证网络系统正常运行；
h) 防止电源线干扰，包括中断供电、异常状态供电（指连续电压过载或过低）、电压瞬变、噪声（电磁干扰）以及由于核爆炸或雷击等引起的设备突然失效事件；
i) 设置电源保护装置，如金属氧化物可变电阻、硅雪崩二极管、气体放电管、滤波器、电压调整变压器、避雷针和浪涌滤波器等。
j) 应配备双机 UPS 机组，防范 UPS 失效所带来的风险。
k) 配备发电机组，以便在发生长时间断电事故时进行供电。

3.1.1.2防雷击 TPR_THU

1) 重要的主机系统和网络系统，以及办公场所应当有防雷击措施。
2) XXX 所在的大厦要有避雷针等避雷设备，大厦应当具有符合要求的接地条件。
3) 应采用地桩、水平栅网、金属板、建筑物基础钢筋等构建接地系统，确保接地体良好的接地；
4) 设置信号地与直流电源地，应注意不造成额外耦合，保障去耦、滤波等的良好效果；
5) 设置避雷地，应以深埋地下、与大地良好相通的金属板作为接地点，至避雷针的引线则应采用粗大的紫铜条，或者使整个建筑的钢筋自地基以下焊连成钢筋网作为“大地”与避雷针相连。
6) 接地电阻〈4Ω，电源的地线与计算机设备的地线必须分别设置。
7) 设置安全防护地与屏蔽地，
8) 应采用阻抗尽可能小的良导体的粗线，以减小各种地之间的电位差；
9) 应采用焊接方法，并经常检查接地的良好，检测接地电阻，确保人身、设备和运行的安全。

3.1.1.3防火 TPR_FIR

1) 建筑材料防火：要求机房和记录介质存放间，其建筑材料的耐火等级，应符合 GBJ45-1987 中规定的二级耐火等级；机房相关的其余基本工作房间和辅助房，其建筑材料的耐火等级应不低于 TJ16-1987 中规定的三级耐火等级。
2) 报警和灭火系统：要求设置火灾报警系统，由人来操作灭火设备，并对灭火设备的效率、毒性、用量和损害性有一定的要求。
3) 必须按面积和设备数量配备适合计算机设备使用的灭火器（不得使用干粉、泡沫灭火器），有条件的可以安装配备感温、感烟探测器的固定灭火系统。
4) 建筑材料防火：机房相关的其余基本工作房间和辅助房，其建筑材料的

耐火等级应不低于 TJ16-1987 中规定的二级耐火等级。

5) 报警和灭火系统：要求设置火灾自动报警系统，包括火灾自动探测器、区域报警器、集中报警器和控制器等，能对火灾发生的部位以声、光或电的形式发出报警信号，并启动自动灭火设备，切断电源、关闭空调设备等。

3.1.1.4防潮 TPR_WAT

1) 防止空调冷凝水、暖气漏水等事故引发水患造成网络系统、文档和介质的损坏。
2) 水管安装，不得穿过屋顶和活动地板下。穿过墙壁和楼板的水管应使用套管，并采取可靠的密封措施；
3) 计算机设备应放在工作台上，并备有防水罩；
4) 对工作人员进行防水害教育，并使其了解机房进水管关闭阀的准确位置，做到人人会用；
5) 采取一定措施，防止雨水通过屋顶和墙壁渗透、室内水蒸气结露和地下积水的转移与渗透。
6) 安装对水敏感的检测仪表或元件，对机房进行防水检测、报警。

3.1.1.5空调 TPR_CON

a) 应有必要的空调设备，使机房温度/湿度达到所需的基本要求。
b) 应有较完备的中央空调系统，保证机房温度/湿度的变化在计算机运行所允许的范围。

3.1.1.6电磁防护 TPR_TEM

1) 应采用接地的方法防止外界电磁干扰和设备寄生耦合干扰；
2) 应采用屏蔽方法，对信号线、电源线进行电屏蔽，减少外部电器设备对

计算机的瞬间干扰；

3) 应采用距离防护的方法，将计算机机房的位置选在外界电磁干扰小的地方和远离可能接收辐射信号的地方。
4) 应采用低辐射材料和设备，防止电磁发射泄露；
5) 应采用屏蔽方法，对重要设备进行电磁屏蔽，削弱外部电磁场对计算机设备的干扰，防止电磁信号的泄露；
6) 对磁带、磁盘等磁记录介质的保管存放，应注意电磁感应的影响，如使用铁制柜存放。

3.1.1.7门禁 TPR_JAN

1) 规模较大的物理区域，应向所有的工作人员（包括来自外单位的长期工作人员）发放带有照片的身份证件，并定期进行检查或更换。
2) 短期工作人员或维修人员的证件，应注明有效日期，届时收回。
3) 参观人员必须由主管部门办理参观手续，参观时必须有专人陪同。
4) 因系统维修或其他原因需外国籍人进入办公区时，必须始终有人陪同。
5) 在无警卫的场合，必须保证室内无人时，关锁所有出入口。
6) 应该通过门禁系统对于出入进行控制。这种控制可能不仅仅限于进入，还可能包括离开，控制措施可以具体增加出示有效证件、登记姓名等。
7) 物理环境/机房的出入口应有专人负责，未经允许的人员不准进入机房；
8) 未经许可，不得在场所内拍照或摄影。
9) 机房应只设一个出入口，另设若干紧急疏散出口，标明疏散线路和方向；
10) 没有指定管理人员的明确准许，磁铁、私人电子计算机或电子设备、食品及饮料、香烟、吸烟用具等与上机工作无关的物品均不准带入机房；任何记录介质、文件材料及各种被保护品均不准带出机房。对于允许带进和带出的物品，如有疑问，应进行查验。
11) 获准进入机房的来访人员，其活动范围应受到限制；
12) 安全等级较高的计算机机房，除采取身份证件进行识别以外，还要考虑其他出入管理措施，如：安装自动识别登记系统，采用磁卡或 IC 卡等

机器可识别的介质。

13) 在机房中设有网络系统安全管理中心的，更应加强其安全防护，如进入不同区域时佩带有不同标记的证章、重要部位的出、入口设置电子锁、指纹锁等。
14) 进出口的钥匙应保存在约定的场所，由专人管理，并明确其责任。记录最初入室者及最后离室者和钥匙交换时间。
15) 相关安全制度应打印或制作成标牌，放置于醒目的位置

3.1.1.8位置选择 TPR_LOC

1) 按一般建筑物的要求进行机房场地选择。
2) 避开易发生火灾和危险程度高的地区，如油库、和其它易燃物附近的区域；
3) 避开尘埃、有毒气体、腐蚀性气体、盐雾腐蚀等环境污染的区域；
4) 避开低洼、潮湿及落雷区域；
5) 避开强震动源和强噪声源区域；
6) 避开强电场和强磁场区域；
7) 避开有地震、水灾危害的区域；
8) 避免在建筑物的高层以及用水设备的下层或隔壁。

3.1.1.9防静电 TPR_STA

1) 采用接地与屏蔽措施，使网络系统有一套合理的接地与屏蔽系统；
2) 人员服装应采用不易产生静电的衣料，工作鞋选用低阻值材料制作；
3) 控制机房温湿度，使其保持在不易产生静电的范围内。
4) 机房地板从地板表面到接地系统的阻值应保证防人身触电和产生静电；
5) 机房中使用的各种家具，工作台、柜等，应选择产生静电小的材料。

3.1.1.10 设备安全 TPR_EQI

a) 网络系统的设备和部件应有明显的无法除去的标记，以防更换和方便查找赃物；
b) 物理区域中应安装防盗报警装置，防止夜间从门窗进入的盗窃行为以及对系统的非法访问。
c) 应利用光、电、无源红外等技术设置机房报警系统，并有专人值守，防止夜间从门窗进入的盗窃行为；
d) 机房外部的网络设备，应采取加固防护等措施，以防止盗窃和破坏。
e) 通过保安监控系统进行 24 小时进行监控。

3.1.1.11 防干扰和窃听 TPR _TAP

a) 如有可能，接入信息处理设备的电源和通信线路应该铺设在地下，或者采取足够的可替代的保护。
b) 应该保护网络电缆以防未经授权的窃听或损坏，并保护电力电缆不受损坏。例如，通过使用电缆管道和避免通过公共区域，并有防鼠害的措施。
c) 电力电缆应该与通信电缆隔离，以防干扰。
d) 应采取一定措施，预防线路截获，使线路截获设备难以工作；应有探测线路截获装置，及时发现线路截获事件并报警。
e) 应采取有效措施，预防线路截获，使线路截获设备无法工作；
f) 应有探测线路截获装置，及时发现线路截获的事件并报警；
g) 应有定位线路截获装置，能发现线路截获窃取设备的准确位置。

3.1.2 TNI 类：网络与通信安全

3.1.2.1 主干网可用性保护 TNI_AVI.2

为保证骨干网的可用性，应满足以下原则：

1） 对骨干网的核心设备应采用冗余设计，包括设备模块冗余、设备热备等。

2） 对骨干网的链路采用冗余设计，采用如以太通道等技术，达到提高链路带宽、负载均衡、链路备份的目的。

3） 对冗余的方案/设备/线路等的测试方案，并定期（至少三个月一次）进行验证测试，以判别是否满足冗余要求，并对发生的问题进行及时处理和备案。

4） 启用动态路由协议的认证功能，并设置具有一定强度的密钥,相互之间交换路由信息的路由器必须具有相同的密钥。默认的认证密码是明文传输的，建议启用加密认证，如 MD5。

5） 启用访问列表过滤一些垃圾和恶意路由信息。

6） 启用访问控制列表过滤一些垃圾和恶意的流量。

7） 具备详尽的应急响应流程和措施，对应急响应的过程和处理方法进行详尽的记录。

8） 对骨干网出口，应采用多出口设计，并采用链路负载均衡设备对骨干网的出口链路提供负载均衡。

9） 制定网络可靠性保障需求，制定相关的 SLA，并指定专门的内部部门或者外部部门维护和保证。建立网络可靠性监控系统，及时发现并处理可靠性中断/降低故障，对故障处理结果进行教训总结。对 SLA 的执行情况进行定期的审计和计划，应当重点考虑以下问题：

- ✓ SLA 的执行效率
- ✓ SLA 维护情况
- ✓ 内部/外包商执行情况和问题
- ✓ SLA 的违反情况
- ✓ SLA 的改进建议
- ✓ 可靠性的改进建议

3.1.2.2 内部网络防护 TNI_INT.2

在网段划分上，提出了“同一子网支持单一业务”的原则，以形成清晰的边界。同时，对保密性要求高的网络，在其传输上提出了更高的结构安全要求：

1) 根据各组的工作职能、重要性、所涉及信息等级等因素，划分不同的子

网或网段。不同的区域在交换机上划分不同 VLAN，不同 VLAN 之间的路由设置访问控制。

2) 按照方便管理和控制的原则为各子网、网段分配 IP 地址段。例如，地址规划应便于路由汇总以方便路由管理、提高路由广播效率以及简化访问控制列表的配置。

3) 网络结构需要根据应用系统、业务流程和数据流向的特点进行设计。采用子网的概念进行网络逻辑和物理划分，同一子网应尽可能地只支持单一的业务、服务或流程，形成清晰的网络边界。

3.1.2.3 网络设备登录控制 TNI_TEL.2

对设备的所有管理端口进行访问控制，对登录的记录包括通过设备自身记录以及人工记录。要求至少采取下列措施中的一种或者多种，以达到所需的安全需求：

1）采用带外管理方式，使得管理链路和数据交换链路隔离，通过专用内部管理网络访问管理设备，防止威胁主体通过对数据交换链路的监听获取密码和管理信息。

2) 对设备的登录控制措施效能评估和审计，对审计和评估的结果进行相关处理。

3) 限制管理网络设备的网管机的 IP 地址，防止来自非授权 IP 的主机登录管理网络设备。

3.1.2.4 网络设备用户身份鉴别 TNI_IDT.2

1) 采用用户集中管理方式进行用户身份鉴别，如 Radius 或者 TACACS+等，对用户的分配和管理集中在认证服务器端。

2) 维护对用户的权限分配记录和注销记录，并定期审查这些用户和记录，确保权限分配记录和实际配置的一致性。对发现的不符合情况进行必要的调查和报告。

3) 记录并审计用户的身份鉴别记录。

3.1.2.5 密码技术 TIN_ENC.2

1) 对称加密算法的密钥位数必须等同于 128 位 DES 算法。

2) 非对称加密算法的密钥位数必须等同于 1024 位 RSA 算法；

3) 对于任何密钥，都必须设定其生命期，并提供相应的版本更替方案；

4) 系统的密码管理必须由相应硬件装置来完成。

5) 通信过程中，应对整个报文或会话过程进行加密，如采用 SSH、HTTPS 等连接形式。

3.1.3 TEB 类：边界保护

3.1.3.1 网络边界访问控制 TEB_NAC.2

网络边界的访问控制机制主要是限制用户可以建立什么样的连接以及通过网络传输什么样的数据。网络访问控制的目的就是在各网络连接之间建立一个安全控制点，通过允许、拒绝经过网络访问控制设备的数据流，实现对进、出内部网络的服务和访问的审计和控制。

有数据交换的不同网络之间的边界处都需要网络访问控制。一般来说，采用防火墙，路由器访问控制列表等方式对边界进行保护，保护对象为任何向外部系统提供信息发布的设备/系统，至少包括：

- 路由交换信息
- 主机
- 网络设备
- 应用服务

在本级要求在 OSI 模型的 3 到 7 层上检查数据包，并具有对应用层协议中的命令、格式、内容进行过滤的功能，具体的技术功能要求包括：

访问控制中的一个重要的步骤是对参与通信的一个或多个团体或个人进行授权，即定义其访问权限。授权将一组权限赋予一个实体。实体的访问权限通常与其真实身份相关，身份不同，工作的内容、性质、所在的部门就不同，因此所应关注的系统操作也不同，授予的权限也就不同。如系统管理员与普通用户的访

问权限就有很大的差别。

访问权限的定义内容包括定义哪些用户能登录到系统并获取网络资源;哪些用户对网络有什么样的操作权限;哪些用户对目录、文件或设备有什么样的操作权限（如读权限、写权限、创建权限、删除权限、修改权限、查找权限等）等。总之，凡是需要进行网络访问控制的地方都应该先定义访问权限。

定义访问权限可以通过访问控制列表、为应用系统数据流建立的调查表、设备接入检查等技术来实现。

1) 访问授权与拒绝：

✓ 此类产品应能根据数据包的源地址、目的地址、源端口号、目的端口号、协议、出入的接口等，提供明确的访问保障能力和拒绝访问能力，并支持地址通配符的使用。

✓ 过滤表的大小应能满足用户的实际需求。

✓ 具有抵御常见的端口扫描的能力。

✓ 具有会话流控制功能。此类产品应能根据会话状态信息（包括数据包的源地址、目的地址、源端口号、目的端口号、协议、出入的接口、会话序列号、发出信息的主机名等信息，并应支持地址通配符的使用），为数据流提供明确的访问保障能力和拒绝访问能力。这里所控制的对象，不再是数据包，而是数据流。

✓ 支持 IP 地址与 MAC 地址绑定功能。

✓ 能限制流出内部网络的地址必须是属于内部网络的。

✓ 具有抵御常见的端口扫描和攻击的能力：包括 IP 地址欺骗、DoS 攻击（如 TCP SYN Flood 等）、中间人攻击、碎片攻击等。

✓ 支持动态地址、网络地址转换（NAT）、访问控制列表（ACL）、Vlan 等多种技术以限制对客户端的主动连接访问。

✓ 从外部接入专用网络必须经过鉴别（包括回叫设备，动态口令，智能卡等）、认证、授权，对号码进行身份识别。

2) 支持属性修改，此类产品自身的安全功能应(仅向授权管理员)提供修改下述（包含但不仅限于）参数的能力：源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性）；增加、修改或删除管理员帐号；(仅向授权管理员)提供修改下述（包含但不仅限于）参数的能力：配置的安全参数。例如：最大鉴别失败次数、最大审计存储容量等数据。

3）支持属性查询：此类产品自身的安全功能应(仅向授权管理员)提供以下查询：源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性)。

4）具有建立三个以上网络区域的能力：外网、内网、一个或多个 DMZ 区

5）支持详细的通信/管理审计，审计存储和查阅保护功能。

6）硬件 MTBF（平均无故障运行时间）不低于 8760 小时（1 年）

3.1.3.2 远程访问 TEB_TEL.2

应监控远程访问接入对于内部系统的访问，必须采取适当的监控记录手段，记录接入时间，地址，电话，人员，访问对象等。

1）对远程访问进行监控的主要技术功能要求

✓ 在网络中部署网络监控设备，包括数据中心网管工作站、系统性能监视、系统资源监视、会话连接监视、应用错误监视等几部分，由操作员负责监视以采集网络中的流量，设备运行情况等信息。

✓ 能对所有监控工作都应进行记录。

✓ 能通过分析监控信息发掘异常事件，并根据异常事件的类型和严重程度进入相关事件处理流程。

✓ 异常事件及其处理应当进入审计系统。

✓ 实现对监控事件的实时性响应和多种方式的报警功能。

2）对远程访问中身份鉴别的具体技术功能要求

✓ 所有的远程访问必须具备身份鉴别和访问授权控制，只有通过适当的身份鉴别和访问授权，才能允许远程访问。

✓ 存储口令的加密方式应当是不可逆的。

✓ 用户每次登录系统时应当进行身份鉴别，并对此过程进行记录。

✓ 应定义鉴别尝试允许次数，并通过延长鉴别失败超出允许次数后再次允许鉴别的时间间隔来限制重复尝试，并对此过程进行记录。

✓ 用于身份鉴别的用户名/口令对应当在信道中加密传输。

✓ 应当对用户的来源进行控制和监控；

✓ 不允许系统管理人员直接以具备系统管理权限的账户远程访问登录系

统，必须通过中转的方式，即先以普通权限用户身份登录系统，然后通过系统用户身份切换功能变换为系统管理员。

✓ 对远程系统管理应当限定登录访问的地址范围，绝对不允许没有来源控制的远程系统管理。

✓ 必须对远程访问的用户进行统一集中管理，具备相关的申请登记流程和审批流程，其中应当至少包括人员背景调查等方面。

✓ 必须对用户的操作过程进行记录，至少保证前 1000 条操作被正确纪录，供审计分析。

3）其他技术功能要求

✓ 远程访问必须只允许来自可信信道的连接，对与其他信道则不允许。

✓ 采用具有加密功能的远程终端和通信信道进行远程访问。

✓ 应当保证系统管理权限的等级化划分。

✓ 不允许同一账户（用户 ID）同时登录访问系统。

✓ 不显示系统或应用信息，直到登录流程成功的完成之后。

✓ 显示警告信息，描述未授权的访问可能导致的后果。

✓ 在登录过程中，不提供任何可能帮助未授权用户的信息。

✓ 在完成所有的输入数据时，才确认登录信息。当发生错误时，系统不应提示数据的错误范围。

✓ 在成功的登录流程完成之后，显示从上一次成功登录以来的不成功的登录尝试的详细情况。

✓ 通过自动化的记录功能或者工具记录，并对管理员的登录行为和操作行为进行完整记录、审计和分析，发现异常及时报告和处理。

电话拨号等（包括模拟电话/公共交换电话网 PSTN 和综合服务数字网 ISDN）经接入服务器联入用户网，当拨号用户通过认证后，接入服务器将为之分配用户网范围内的地址，远程用户在逻辑上就成为网络内部用户。

1）拨入方式远程访问的技术功能要求（接入服务器的功能要求）

✓ 按用户需求支持模拟 modem/公共交换电话网 PSTN 拨号接入。

✓ 按用户需求支持 ISDN 拨号接入。

✓ 具有对拨号接入用户的严格认证功能。

✓ 具有对拨号接入用户的网络访问授权功能。

- ✓ 具有回拨功能。
- ✓ 支持挑战响应、动态口令，智能卡等高级认证方式。

3.1.3.3 防病毒网关 TEB_TVI.2

防病毒网关是网络安全的重要组成部分，其主要功能是对从外部网络进入用户内部网络的病毒进行过滤，一般主要针对 HTTP、HTTPS、FTP 和 SMTP 等协议进行过滤，保护用户内部网络不受病毒感染。

对防病毒网关的主要技术功能要求有：

1）具有集中分发软件、进行病毒特征码升级的控制台——病毒集中监控中心。

2）病毒集中监控中心应支持安全管理中心的集中管理。

3）能根据单位内部的不同部门需要设置不同的防病毒策略。

4）防止病毒进出内部网络。

5）支持对常见格式压缩文件的病毒检测。

6）至少对基于 http、ftp、socks/mms、telnet、gopher、smtp、imap、pop3 等主要网络协议的事件进行检测，剥离 ActiveX 和 Java Script、Java Applet 等恶意代码。

7）支持对宏病毒和可疑宏的高效检查功能。

8）代理内容过滤。基于网页标题和内容，设置过滤规则和规则库，实现对浏览网页的过滤。过滤垃圾和违规邮件侵扰，至少可对标题、文本、html、附件（文本、html、常见压缩包）等进行内容过滤、病毒过滤及恶意代码过滤，允许管理员定制过滤规则，以符合企业或各机关单位内部网络的需要。

9）支持自动定时升级。

10） 网络病毒集中监控，支持病毒监控中心的统一管理。防病毒网关发现病毒后在病毒监控中心报警，病毒监控中心可以进行远程管理操作（例如杀毒等）。

11） 防病毒网关不能影响原有的网关系统。

12） 硬件 MTBF（平均无故障运行时间）不低于 25000 小时（3 年）。

3.1.3.4 网络入侵防范 TEB_IDS.2

基于网络的入侵检测产品通过对计算机网络中的若干关键点收集信息并对其进行分析，以发现网络中是否有违反安全策略的行为和被攻击的迹象。

在一个网络环境中，有很多配置点可以考虑设置网络 IDS。IDS 设置在防火墙之外，可以观察到未被防火墙过滤的原始的外部网络通信；设置在防火墙的内部，提供了对目的地是内部网络的外部流量或目的地是外部网络的内部流量的监测，而并不监测仅在内部网络中流动的通信。在内部网络环境中，网络 IDS 通常被设置在客户机与服务器、通信路径的中间，可以监测所有通信层次上的数据。本节主要介绍在边界处的入侵防范。

在确定 IDS 配置点和数目的时候，需要考虑的因素包括：操作员对每一个 IDS 发出的报警进行分析和划分的工作负担；对多个监测器监测到同一事件的报警进行关联分析的复杂性以及不同配置点的选择所带来的系统采购、安装、运行和维护的成本。

具体技术功能要求为：

1)数据检测功能要求

✓ 数据收集：应具有实时获取受保护网段内的数据包的能力。获取的数据包应足以进行检测分析。

✓ 协议分析：至少应监视基于以下协议的事件：HTTP、FTP、TFTP、TCP、UDP、IP、ICMP、IMAP、SNMP、TELNET、DNS、SMTP、POP3、NETBIOS、NFS、NNTP、ARP、RIP、RPC 等。

✓ 行为监测：至少应监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫攻击等。

2)入侵分析功能要求

✓ 数据分析：应对收集的数据包进行分析，发现攻击事件。

✓ 攻击事件的过滤规则调整：可以对网络中检测到的事件实施灵活的过滤规则，如根据监控网卡、事件类型等，减少对系统资源的占用。

✓ 事件合并：应具有对高频度发生的相同安全事件进行合并告警，避免出现告警风暴的能力。

3)入侵响应功能要求

✓ 安全报警：当产品检测到入侵时，应自动采取相应动作以发出安全警告。

✓ 响应方式：可对检测到的攻击行为采取告警、记录日志、会话阻断等响应方式。告警可以采取屏幕实时提示、E-mail 告警、声音告警等几种方式。

✓ 排除响应：应允许用户定义对被检测网段中指定的主机或特定的事件不予告警，降低误报。

4)管理控制功能要求

✓ 图形界面：产品应提供友好的用户界面用于管理、配置网络安全监控报警产品。管理配置界面应包含配置和管理产品所需的所有功能。

✓ 事件数据库：产品的事件数据库应包括事件定义和分析、详细的漏洞修补方案、可采取的对策等。

✓ 事件分级：产品应按照事件的严重程度将事件分级，以使授权管理员能从大量的信息中捕捉到危险的事件。

✓ 策略配置：应提供方便、快捷的网络安全监控报警策略配置方法和手段。

✓ 升级能力：产品应具有及时更新、升级产品和事件库的能力。

✓ 统一升级：产品应提供由管理控制中心对各探测器的事件库进行统一升级的功能。

5)检测结果处理要求

✓ 事件记录：产品应记录并保存检测到的入侵事件。入侵事件信息应至少包含事件发生时间、源地址、目的地址、危害等级、事件详细描述以及解决方案建议等内容。

✓ 事件查看：用户应能通过管理界面实时清晰地查看入侵事件。

✓ 事件可视化：产品应提供具有统计、查询等功能的工具，供用户阅读入侵事件数据。

✓ 事件导出：产品应具有导出入侵事件数据的功能。

✓ 报告生成：产品应能生成详尽的检测结果报告。

✓ 报告查阅：产品应具有全面、灵活地浏览检测结果报告的功能。

✓ 报告输出：检测结果报告可输出成标准格式（如 HTML、文本文件等）。

6)产品灵活性要求

✓ 窗口定义：产品可提供有效的手段支持用户自定义窗口显示的内容和显示方式。

✓ 报告定制：产品应支持授权管理员按照自己的要求修改和定制报告内容。

✓ 事件定义：产品应允许授权管理员自定义事件，或者对开发商提供的事件作修改，并应提供方便、快捷的定义方法。

✓ 协议定义：产品除支持默认的网络协议集外，还应允许授权管理员定义新的协议，或对协议的端口进行重新定位。

✓ 支持集中管理模式，能向安全管理中心提供必要的信息。

7)性能指标要求

✓ 稳定性：在产品设计适应的带宽下，入侵检测产品应能长期稳定工作。

✓ 网络影响：产品不应对原网络的正常运行产生明显影响。

✓ 平均响应时间：当背景数据流达到网络的有效带宽时，入侵检测产品应保证有足够快的响应时间。

✓ 漏报率：产品应在满足自己声明的运行条件的情况下，提供漏报率的分析数据。

✓ 误报率：产品应在满足自己声明的运行条件的情况下，提供误报率的分析数据。产品应将误报率控制在应用许可的范围，不得对正常应用产品产生较大影响。

3.1.4 TCE 类：保护计算环境

3.1.4.1应用系统测试 TCE_APT

a) 通过监控系统辅助人工实现对系统运行状态、性能、资源和容量进行监控，并可设定报警阀值。
b) 提供多种报警方式；
c) 明确响应流程。

3.1.4.2病毒和恶意代码防范 TCE_VIR

1) 在其运行网络环境的边界系统（如网关、电子邮件服务器）部署病毒防范系统；

2) 部署计算机防病毒软件，开启病毒实时防护功能，并定期进行病毒码升级；
3) 及时安装系统的最新补丁程序。

3.1.4.3计算环境访问控制 TCE_TAC

1) 采用自主访问控制策略，可以用访问控制表及其相应的访问规则所组成的访问控制策略，确定相应的访问权限。
2) 无论采用何种访问控制策略所实现的自主访问控制功能，都要求能够：
    1) 了解掌握当前资源的访问控制能力。
    2) 允许命名用户以用户和/或用户组的身份规定并控制共享方式，并阻止非授权用户获取或者篡改敏感信息。
    3) 对访问是跨网络的情况，如果在物理上分隔（如内存与磁盘）间传递用户数据时，应严格执行访问控制策略，以防止信息的泄漏、篡改和丢失。也可以根据数据属性，按照密码支持第一级的要求保证数据在通过网络传输时的保密性和完整性。
    4) 对访问是非注册用户，如通用匿名访问的情况，应重点考虑对其获取信息的控制、写访问的严格控制以及相关必须的审计策略。
3) 有更细粒度的自主访问控制，即基于角色的访问控制，能够实现系统管理员采用指定方式或默认方式确定用户的访问权限，并将访问控制的粒度控制在单个用户，同时实现只有系统管理员才能进行授权，而阻止那些非授权的用户进行任何访问，也阻止授权用户以非授权的操作形式进行访问。
4) 要求自主访问控制能与身份鉴别和审计功能相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。
5) 对访问是跨网络的情况，如果在物理上分隔（如内存与磁盘）间传递用户数据时，应严格执行访问控制策略，以防止信息的泄漏、篡改和丢失。也可以根据数据属性，按照密码支持第二级的要求保证数据在通过网络

传输时的保密性和完整性。

3.1.4.4身份鉴别 TCE_IDT

a) 必须采用用户名/口令对的方式进行身份鉴别；
b) 应当保证在身份鉴别过程中口令不可见；
c) 采用加密方式存储口令；
d) 应当保证身份鉴别的时效性，在登录或者注销时，应当对相关的身份鉴别状态进行标记，以便指示新的过程；
e) 用户每次登录系统时应当进行身份鉴别，并对此过程进行记录；
f) 应定义鉴别尝试允许次数，并通过延长鉴别失败超出允许次数后再次允许鉴别的时间间隔来限制重复尝试，并对此过程进行记录；
g) 存储口令的加密方式应当是不可逆的；
h) 用于身份鉴别的用户名/口令对应当在信道中加密传输；
i) 应当对用户的来源进行控制和监控；

3.1.4.5安全审计 TCE_SAU

1) 要求产生完整的审计数据；
2) 提供审计数据的查阅；
3) 对审计数据和分析结果进行保存，确保审计数据的可用性
4) 可自定义审计数据查阅的方式和视图；
5) 对审计数据进行分析，包括分类、排序和趋势分析等；
6) 对特定异常事件进行审计分析，并提高实时报警功能；
7) 以风险分析为依据进行审计事件选择；

3.1.4.6数据库设计安全 TCE_DBS

a) 系统在设计时不应留有“后门”，即不应以维护、支持或操作需要为借口，设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口。

b) 安全结构应是一个独立的、严格定义的软件系统子集，并应防止外部干扰和破坏，如修改其代码或数据结构；

c) 数据库管理系统应进行分层设计，并将数据库管理系统进程与和用户进程进行隔离；

d) 应提供设置和升级配置参数的安装机制，在初始化和对与安全有关的数据结构进行保护之前，应对用户和管理员的安全策略属性应进行定义；

e) 应区分普通操作模式和系统维护模式，全系统操作恢复的启动、配置系统内部的数据库和表等动作应在维护模式中执行。

f) 应防止普通用户从未经允许的系统进入维护模式，并防止普通用户与系统内维护模式交互,从而保证在普通用户访问系统之前，系统能以一个安全的方式进行安装和配置。

g) 当数据库管理系统安装完成后，在普通用户访问之前，系统应配置好初始用户和管理员职责、审计参数、系统审计跟踪设置以及对客体的合适的访问控制。

h) 执行系统所提供的实用程序，应限定于对系统的有效使用，只允许系统管理员修改或替换系统提供的实用程序。

i) 系统应能识别由通信渠道接收的信息的来源者，所有待确认的数据应能从进入点被安全地传送到确认系统，如口令不应由公共的或共享的网络以明文发送，可使用数据加密设备或通过加密信道用加密方式传送。

3.2 安全管理要求

3.2.1 安全运作

3.2.1.1ORA 类：风险管理

3.2.1.1.1 资产鉴别 ORA_ASE.2

应该清晰识别每项资产、其拥有权、责任人以及资产现在的位置等，对于支持信息系统运行的网络设备、主机设备及安全设备等，进行分类、标识和登记。用定性的方法对系统的重要资产进行赋值。

重要资产可能包括（但不限于）以下内容：

a) 信息资产：数据文件、数据库文件、系统文件、用户手册、培训资料、操作和支持程序、持续性计划、存档信息等；
b) 软件资产：应用软件、系统软件、开发工具和实用程序等；
c) 有形资产：计算机设备，通信设备、磁媒体、其他技术装备等；

3.2.1.1.2 威胁分析 ORA_THR.2

在国内外标准和相关参考文档的基础上，结合业务应用、系统结构特点以及访问流程等因素，建立并维护一个较全面的威胁列表。

通常情况下，不同业务系统面临的威胁是不同的，在没有明确系统资产前，难以找到适用于系统的威胁列表。因此，维护的威胁列表可能不是一个，而是每个或者每类资产有一个威胁列表。威胁列表应当随时适应业务的变化、系统的变化、环境的变化、技术的更新等。

3.2.1.1.3 脆弱性分析 ORA_VUL.2

应用人工评估、工具扫描、安全访谈等方法或工具对系统的脆弱性进行分析和评估，形成脆弱性列表。

脆弱性的工具扫描可以（但不限于）从以下几方面考虑：

a) 网关设备的脆弱性扫描；

b) 网络设备的脆弱性扫描；

c) 主机设备的脆弱性扫描；

d) 安全设备的脆弱性扫描；

脆弱性的人工分析可以（但不限于）从以下几方面考虑：

a) 系统配置检查；

b) 用户管理检查；

c) 系统日志和审计检查。

每个资产都要自己的脆弱性。为了减小管理的复杂度，可以针对资产组合、资产类编制脆弱性列表和脆弱性检查表。脆弱性列表将成为系统加固、改进和安全项目建设的依据。

3.2.1.1.4 风险分析 ORA_ANA.2

应采用多层面、多角度的系统分析方法，由安全管理人员和外部安全专家对资产、威胁和脆弱性等方面进行定性综合评价，最终形成风险评估报告。

3.2.1.1.5 选择安全控制措施 ORA_CTR.2

根据风险评估的结果，并结合公司对于信息安全的需求对相关的各种控制措施进行综合评价，来选择合适的控制措施对抗安全风险。

3.2.1.1.6 安全措施的实施与确认 ORA_VAD.2

根据选择的安全控制措施，编写安全解决方案从管理手段和技术手段来实现安全控制措施，通过安全管理、部署安全产品和安全技术进行风险控制措施的实施。进行残余风险评估，确认残余风险在可接受范围内，并由高层管理人员来做出风险接受的决定。

3.2.1.2OEN 类：工程建设安全管理

3.2.1.2.1 安全项目的立项管理 OEN_CON.2

信息系统的安全建设立项要符合信息系统安全建设的总体规划, 经公司安全主管部门组织内部相关专家科学论证后方可进行设计和组织实施。

3.2.1.2.2 安全需求分析 OEN_REQ.2

安全需求分析阶段通常至少包括系统定义、威胁评估、脆弱性评估、影响评估、风险评估、确定安全要求等六个步骤。可以根据 ORA_THR.2、ORA_VUL.2、ORA_ANA.2、ORA_CTR.2 的要求进行安全需求分析。

3.2.1.2.3 安全功能规范 OEN_FSP.2

应编写正式的安全功能规范。功能安全规范是用户可见接口和信息系统的安全功能行为的一个高层描述。它是信息系统安全功能要求的一个实例化，应该描述信息系统的安全属性和它的外部接口。

3.2.1.2.4 高层安全设计 OEN_HLD.2

应进行完整的高层安全设计，高层安全设计应该标识信息系统所要求的任何基础性硬件、固件、软件、和/或通信，和在这些硬件、固件、软件、和/或通信中实现的支持性保护机制所提供的功能表示。

还应将功能安全规范细化到子系统。对于信息系统的每一个子系统，高层安全设计描述并标识出包含在子系统中的安全功能。高层安全设计也定义所有子系统之间的相互关系。这些相互关系将适当地被表示成数据流、控制流等的外部接口。

高层设计应该标识信息系统的安全相关子系统的所有接口，标识哪些接口是外部可见的。高层设计应该包括信息系统深度防御的描述、标识技术的和非技术的对策的组合是如何降低残余风险的级别到一个可接受的级别的。

3.2.1.2.5 安全产品选型 OEN_PRO.2

c） 安全产品具有在国内生产、经营和销售的许可证。

d） 密码产品符合国家密码主管部门的要求，来源于国家主管部门批准的密码研制单位。

e） 关键安全产品或信息技术产品的安全模块应获得国家相关安全认证，在选型中根据实际需要制定安全产品选型的标准。

3.2.1.2.6 外包软件安全控制.2

在软件的开发被外包时应当考虑许可安排、代码的所有权和知识产权以及质量合格证和所进行的工作的精确度。还应进行质量审核、在安装之前进行测试以检测特洛伊代码，并要求已方提供源代码以及相关设计、实施文档。要减少软件中出现缺陷的可能性可以（但不限于）考虑如下方面：

a) 需要软件购买系统选择有良好声誉、可靠的记录而且有足够的资源和保险来负担因其软件导致的损失的供应商。

b) 要求所有软件都经过测试和验证。

c) 代码一旦被安装，就控制对代码的访问和修改；

对外包软件的开发应制定控制程序进行控制。在控制程序中应当考虑（但不限于）如下内容：

a) 代码的所有权和知识产权；

b) 软件开发过程的质量控制要求；

c) 代码质量检测要求；

3.2.1.2.7 交付和运行 OEN_ADO.2

交付过程需要系统控制以及交付设备和程序来提供保证，以确保接收方所接受的信息系统的版本正是发送者发送的，而没有任何修改。

还需要编写安装、生成和启动程序，以确保信息系统在开发者所期望的安全方式下进行安装、生成和启动是有用的。

3.2.1.2.8 系统安全检测和验收 OEN_TES.2

应进行安全测试论证信息系统是否满足安全功能规范。应该论证功能规范中所描述信息系统安全功能和测试文档所标识的测试之间的对应性是完备的。并论证测试文档中所标识的测试足以论证信息系统安全功能运行和它的高层设计是一致的。

3.2.1.3OPM 类：物理环境管理

3.2.1.3.1 机房管理 OPM_ROM.2

计算机机房是信息系统硬件资源的集中地，机房管理主要以加强机房物理访问控制和维护机房良好的运行环境为主。本安全级应按以下要求进行机房人员管理：

1) 机房出入应有保安人员负责执守，未经允许的人员不准进入机房；
2) 获准进入机房的来访人员，应出示有效证件并履行严格的登记手续。其活动范围应受到限制，并有接待人员陪同；
3) 机房钥匙由专人管理，未经批准，不准任何人私自复制机房钥匙或服务器开机钥匙。
4) 没有指定管理人员的明确准许，任何记录介质、文件材料及各种被保护品均不准带出机房，与工作无关的物品（如：食品、香烟等）均不准带入机房。
5) 未经批准，禁止任何人移动计算机相关设备及其相关的系统或带离机房；
6) 应禁止携带磁铁、个人计算机等电子设备进入机房；
7) 机房内严禁吸烟及带入火种和水源。
8) 所有来访人员登记记录以及门禁系统的电子记录应妥善保存以备查；
9) 禁止测试物理访问控制；
10) 应经常打扫机房防止灰尘以及进行灭鼠工作。

3.2.1.3.2 办公环境管理 OPM_OFM.2

设置有网络终端的办公环境，是信息系统环境的组成部分，办公环境管理主要以加强信息保密性为主，防止利用终端系统窃取敏感信息或非法访问。本安全级应按以下要求进行终端办公环境的管理：

1) 工作人员下班后，终端计算机应关闭；
2) 存放敏感文件或信息载体的文件柜应上锁或设置密码；
3) 禁止使用调制解调器拨号上网。
4) 工作人员调离部门或更换办公室时，应立即交还办公室钥匙。
5) 工作人员离开座位超过 30 分钟以上，应将桌面上含有敏感信息的纸件文档在抽屉或文件柜内；
6) 工作人员离开座位超过 30 分钟以上，计算机应退出登录状态，采用屏幕保护口令加以保护或关机；

3.2.1.3.3 环境设备维护 OPM_MAI.2

机房内（包括电源间）的所有环境设备（如空调、电源等），由确定的部门负责管理，并随时受理和处理这些设备的突发事故。机房值班员要每天到机房巡视至少一次。

a) 机房值班员要对各种设备的运转情况（包括电源、空调）进行必要的检查，记录有错误代码的设备，供有关人员检修使用。
b) 机房空调必须定期例行检修：
    1) 空调系统出现故障报警，有关人员要及时处理解决，不得拖延；
    2) 每月清洁一次过滤网、排水管和加湿器，定期更换加湿罐（随各地水质而定）；
    3) 每季清扫一次室外冷凝机组，保证通风良好。
c) 电源系统必须定期例行检修：
    1) 每季度要分析一次机器运行记录，查找隐患，并采取相应的对策；
    2) 每半年要对蓄电池做一次充放电测试。清洁或更换机器过滤网，检查机器易损件的运行情况；

3) 在确保不影响正常生产的情况下，每年要对 UPS 设备进行一次双机切换演练。并对电源配电柜检修；
4) 在确保不影响正常生产的情况下，每年要做一次 UPS 设备、备用发电机、总配电柜切换模拟实验。

d) 机房环境管理员每月定时对各种设备例行检查，每年进行一次检修，检修要彻底清扫各种设备的空气过滤器，运行测试程序、作规定的设备测试，检查各设备的记录信息码，查找隐患。
e) 机房场地监控系统、门禁保安系统信息记录资料每月收集整理一次，消防设施每年定期检查是否在有效期内，及时更换过期设备。

3.2.1.4OHO 类：主机维护

3.2.1.4.1 主机设备维护 OHO_EQI.2

a) 主机设备应当由指定的专人（主机设备管理人员）定期维护，制定明确的维护目标和要求、维护流程和操作规范，测试规范，制定相关的维护制度，维护对主机设备的维护纪录。
b) 应当与主机设备厂商保持畅通的沟通联系，以便能及时从厂商处获取必要的技术支持。
c) 主机设备维护人员应当具备相应的专业技能，并取得相应的资质。
d) 主机设备维护人员应当根据主机设备维护情况向上级管理机构报告主机设备运行状态。

3.2.1.4.2 账户管理 OHO_ACC.2

1) 在系统初始化时，删除或者禁用不使用的系统缺省账户；
2) 对帐户进行分组或分级管理，并分别设置相应的权限；
3) 定期检查系统中是否存在未使用的或过期的帐户；
4) 对系统中的账户情况进行定期审计，对发现的异常账户应当及时报告并进入相关处理流程；
5) 建立账户管理制度，负责系统账号的登记造册、用户名分配、初始口

令分配、用户权限分配、系统资源分配、注销等。

6) 为不同用户分配不同的用户名或用户标识符，确保用户名或用户标识符具有唯一性；

7) 用户名或用户标识符在系统内部全局唯一，在用户名或用户标识符被删除后，同名用户名或用户标识符不可再被创建；

3.2.1.4.3 远程登陆管理 OHO_TEL.2

a） 应当制定远程系统管理制度，记录和分配系统账户远程系统管理的操作权限分配；

b） 对系统进行远程管理和维护时应当：

1) 不允许系统管理人员直接以具备系统管理权限的账户远程访问登录系统，必须通过中转的方式，即先以普通权限用户身份登录系统，然后通过系统用户身份切换功能变换为系统管理员；

2) 对远程系统管理应当限定登录访问的地址范围，绝对不允许没有来源控制的远程系统管理；

c） 必须对远程系统管理进行记录和分析，对发现的异常行为进行报告和相应处理。

d） 采用具有加密功能的远程终端和通信信道进行远程系统管理；

e） 应当保证系统管理权限的等级化划分；

f） 不允许同一账户（用户 ID）同时登录访问系统；

g） 设置详细的登录策略，具体设计如下：

1) 不显示系统或应用信息，直到登录流程成功的完成之后；

2) 显示警告信息，描述未授权的访问可能导致的后果；

3) 在登录过程中，不提供任何可能帮助未授权用户的信息；

4) 在完成所有的输入数据时，才确认登录信息。当发生错误时，系统不应提示数据的错误范围；

5) 在成功的登录流程完成之后，显示从上一次成功登录以来的不成功的登录尝试的详细情况；

3.2.1.4.4 漏洞控制 OHO_VER.2

定期安装系统的最新补丁程序，并根据厂家提供的可能危害计算机的漏洞进行及时修补，并在安装系统补丁前对现有的重要文件进行备份，并对补丁程序进行初步测试，以防止对现有软件的不兼容性。

3.2.1.4.5 防病毒管理 OHO_VIR.2

本级的病毒防护管理，根据所使用的病毒防护产品，提出了检查、记录、定期升级、汇报等的基本要求。

a） 应有指定人员检查网络内防病毒网关和主机的病毒检测情况，并保存染毒和杀毒记录。

b） 使用软盘、U 盘、光盘等外部移动存储设备之前应进行病毒检查；

c） 从不信任网络上所接收的文件，在使用前应首先检查是否有病毒；

d） 定期进行总结汇报，使主管领导和相关人员及时了解病毒安全状况。

e） 所有网络内的计算机、防病毒网关上安装的防病毒软件应每周定时升级，紧急情况下应增加升级次数。

3.2.1.5ONE 类：网络维护

3.2.1.5.1 网络拓扑设计和规划 ONE_TOP.2

网络拓扑满足网络系统和业务需求，具有详细和完整的拓扑设计需求说明、设计文档、网络拓扑、实施过程文档以及网络拓扑变更文档，网络拓扑符合设计要求，网络拓扑图必须和当前实际运行情况保持一致，并保证和维护这些文档的机密性，使其只在允许的范围内被访问和获取。网络的设计必须考虑到网络容量、功能和结构。

还需要强化网络拓扑/结构的变更过程和审批过程，使得任何的网络拓扑结构的变更都在知晓和可控制的状态下进行。

在网络设计图（拓扑图）中必需体现出实际的物理位置和物理连接情况。

网络的设计必须考虑到网络容量、功能和结构的拓展需求

a）必须对网络容量、可承受能力、功能制定相应的测试和验证方案供实施参考。

b）必须预留网络的容量、功能和结构的拓展性设计。

c）必须考虑安全性问题。

3.2.1.5.2 IP 地址管理 ONE_IPM.2

具有 IP 地址管理规定，应当具有统一的 IP 地址管理机构/人员，由该机构/人员负责对外部和内部各个部门人员的 IP 地址进行登记、维护和分配。确保在网络中不发生地址冲突和盗用现象，应当采用一定的技术和管理制度保证不发生该类事件。并对违反 IP 地址管理规定的人员/部分依据相关管理制度进行处理。

实现对地址使用情况的实时动态监控，维护记录地址的使用情况，及时关闭被废止的地址，具有对 IP 地址的容量规划设计，确保各个部门有一定的地址容量冗余供扩展使用。

防止地址的伪造和欺骗。及时发现违反使用 IP 事件，并进行相关处理。

应当实现对 IP 地址使用情况的审计功能，审计内容至少包括以下内容：

a) IP 地址登记和使用情况

b) IP 地址废止和使用情况

c) 当前 IP 地址容量和使用情况

d) 违反 IP 地址管理规定的情况及其处理结果

审计周期至少保证半年一次，审计结果应当上报相关职能部门。

3.2.1.5.3 网络可靠性管理 ONE_REL.2

应当制定网络可靠性保障需求，制定相关的 SLA，并指定专门的内部部门或者外部部门维护和保证。

针对各个内部/外部部门的不同需求，制定相应的 SLA，并与这些部门签署这些 SLA。并对这些 SLA 的执行情况进行跟踪监控，对出现违反 SLA 的情况进行相关处理。

建立网络可靠性监控系统，及时发现并处理可靠性中断/降低故障，对故障处理结果进行教训总结。

3.2.1.5.4 路由管理 ONE_ROU.2

应当具有路由设计和规划，明确在网络的各个部分的选择和使用恰当的路由协议，具备基本的路由 SLA，保证网络的互联互通。

对网络中使用的路由协议运行情况进行监控：

a）静态路由管理

b）防止动态路由出现振荡、不收敛情况

c）防止路由出现异常的不可达现象

d）在边界对路由信息进行依据内部和外部规则进行必要的过滤。

对于动态路由，应当在满足互联互通的前提条件下实现可靠安全的认证交换制度，实现有效的防止路由欺骗功能。

3.2.1.5.5 安全域规划 ONE_SED.2

针对不同的业务部门需求对其进行安全域规划，确定各个部门的安全功能需求，并按照这些安全功能需求设计和实现相应的安全隔离保护措施。

需要对安全域的保护功能进行详细的安全功能设计，并对设计进行必要的验证和审批。构建安全域时必须考虑对业务连续性的影响。

还需要对安全域的使用和划分情况进行管理、审计和维护，至少包括以下内容：

a）安全域的使用情况和改进

b）安全域内部系统和外部系统的变更

c）安全域级别和位置的变更

d）变更的执行和审批过程

e）安全域保护功能的验证

f）违反安全域的使用情况及其处理

3.2.1.5.6 网络设备管理授权 ONE_ADV.2

采用设备提供的多级用户管理授权，对每一个不同的用户授予不同的设备管理权限，需要维护一个数据记录，该纪录包含设备用户及其管理权限，并定期管

理和审计这些记录，并针对发现的异常进行处理和报告。

3.2.1.6OCO 类：配置和变更管理

配置和变更管理通过在细化和修改信息系统的过程中进行规范和控制，确保网络系统的完整性。配置和变更管理阻止对信息系统进行非授权的修改、添加或删除。

3.2.1.6.1配置管理计划 OCO_PLA.2

应制定配置管理计划，并且每半年进行审查和升级，以保证配置管理计划的可行性以及组织具有完成配置管理计划的能力。

3.2.1.6.2配置管理自动化 OCO_AUT.2

应该有措施来控制信息处理设备和系统的改变。对信息处理设备和系统变化的控制不够是系统或安全故障的通常原因。应在关键的设备上采用半自动的配置管理工具，并使用半自动的方法对计算机进行升级，并对相关人员进行配置管理的培训。

应确保网络系统的实现表示是通过自动方式控制的，从而解决复杂实现或众多合作者合作开发，以及在开发过程中多种变化情况所出现的人工难以解决的问题，并确保这些变化是已授权的行为所产生的。配置管理计划应描述所使用的自动工具，并说明如何使用这些工具。

3.2.1.6.3配置管理能力 OCO_CAP.2

配置管理能力的设计应满足以下要求：

a） 版本号，要求开发者所使用的版本号与所应表示的网络系统样本应完全对应，没有歧义。

b） 配置项，要求配置项应有唯一的标识，从而对网络系统的组成有更清楚的描述。

c） 配置管理计划应描述系统是如何使用的，并说明运行中的配置管理

系统与配置管理计划的一致性；

d） 配置管理文档应足以说明已经有效地维护了所有的配置项；

e） 配置管理系统应确保对配置项只进行授权修改。

3.2.1.6.4 变更控制 OCO_CHA.2

系统的变更应有相关责任人对其控制。应该制订正式的管理责任和程序以确保满足对设备、软件或程序的所有改变的控制。可行的情况下，应把操作和应用的变更控制程序整合起来。

3.2.1.6.5 密钥管理 OCO_KEY.2

a) 存储密钥的介质必须严加保护，应以加密形式存储密钥；

b) 有关密钥存储方式和地方的信息不应被非授权人员获得；

c) 应根据密钥的种类、系统的要求确定密钥更换周期；会话密钥应在每次会话后更换；主密钥更换时间间隔可视具体情况而定；

d) 密钥必须由纯随机源产生，并应经过随机性检验，生成密钥时不能降低密码算法设计中所规定的密钥空间；

3.2.1.7 OBA 类：备份与恢复

3.2.1.7.1 数据备份和恢复 OBA_DAT.2

为了保证在发生事故或灾难时，确保系统能够有效地恢复，应该通过数据备份和设备、系统冗余等方式，为可能发生的事故和灾难做出准备。数据备份和恢复的主要目的是为了避免数据丢失风险和由此引起的业务中断风险。引起数据丢失的威胁有物理环境威胁和软硬件故障。除此之外，无作为和误操作也是经常引发数据丢失。数据存储和备份并非用于抵抗上述威胁，但可以有效降低上述威胁引发后果的严重性。数据备份的需求程度主要取决于数据的价值或业务中断造成后果的严重性。

本级数据备份和恢复的保护目标是在系统发生局部事故或灾难后，利用备份数据，至少能够恢复到一周前的状态，相关业务中断时间不超过 12 小时。

1） 数据应从运行的系统中备份到光盘、海量磁盘、磁带或磁带库等介质中，保存数据的介质必须由专人保管。

2） 机构应当制订备份和恢复相关的策略，相关的策略应覆盖（但不限于）如下一些内容：

✓ 应明确说明介质的分类、标记、查找方法。

✓ 应明确说明介质的使用、维护、保养、销毁方法。

✓ 应明确说明需定期备份重要业务信息、系统数据及软件等。

✓ 应确定重要业务信息的保存期以及其它需要永久保存的归档拷贝的保存期。

✓ 应明确说明可手工或软件产品进行备份和恢复。

✓ 应明确说明恢复审批和操作流程。

3) 采用磁盘或磁带进行离线备份或在线备份方案，每日进行增量备份，每周做一次包括数据和应用环境的全备份。

4) 本地直接存储(DAS)方式，数据可直接通过存储系统进行自动备份。

5) 数据恢复时，数据库管理员应填写数据恢复申请表，制订数据恢复计划报请主管批准。而后按恢复计划操作，登记数据恢复登记表。

6) 备份介质应定期接受检查，如实际许可，保证在紧急情况时可以使用；

7) 恢复程序应定期接受检查及测试，以确保在恢复操作程序所预定的时间内完成。

8) 恢复策略应该根据数据的重要程度和引入新信息的频率设定备份的频率（如每日或每周、增量或整体）。

9) 数据备份策略应指明已备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法。

3.2.1.7.2 设备和系统冗余 OBA_EQI.2

为了保证在发生事故或灾难时，确保系统能够有效地恢复，应该通过数据备份和设备、系统冗余等方式，为可能发生的事故和灾难做出准备。本级设备和系统冗余的保护目标是在系统发生局部事故或灾难后，利用冗余系统和冗余设备，保证至少能够恢复到一天前的状态，单次业务中断时间为小时级。

1） 系统内重要服务器，如重要的应用服务器和数据库服务器，应采用冷备、温备或热备的方式进行冗余设置。

2） 支持重要应用的网络设备应有冗余设置。

3） 采用技术措施保证服务器出现故障经更换或修复后，能够自动安装操作系统、应用软件，并恢复数据。

4） 采用支持数据快照，文件系统检查点等技术，提供高速的数据恢复手段。

3.2.1.8ORM 类：存储介质管理

3.2.1.8.1 存储介质的保护 ORM_PRO.2

1） 对存放重要数据和软件的各类记录介质（如纸介质、磁介质、半导体介质和光介质等）应受到控制和物理保护，其存储室必须符合防火、防水、防震、防腐烂、防鼠害、防蛀虫、防静电、防磁场、防盗以及符合制造商的储存规格的安全要求，确保其不受损、不丢失和不被非法访问。

2） 根据所承载的数据和软件的重要程度对介质加贴标识并进行分类，存储在由专人管理的介质库或档案室中，防止被盗、被毁以及信息的非法泄漏

3） 必须制定介质存放存储室、管理员、入库、转储、使用、销毁等管理制度和办法，明确执行各项制度和办法的责任人。

4） 应设立存储介质入库、转储、使用、销毁登记记录。对各类技术资料入库、使用、转储、销毁应有审批手续和传递记录。

5） 对保密性影响级较高的信息介质，其借阅、拷贝、传输须经一定级别的领导同意后方可执行，各种处理过程应登记在册。

6） 存储介质的销毁必须经批准并按指定方式进行，不得自行销毁。

3.2.1.8.2 存储介质的访问控制 ORM_ACO.2

1） 对借阅和复制的存储介质，要进行使用登记，并应严格执行技术资料借阅制度，不得随意扩大技术资料借阅范围。

2） 对逾期未还的技术资料，应由技术资料存储室管理人员负责收回。

3） 一旦发现技术资料丢失或损坏，要立即报告有关部门，并采取补救措施。

4） 存储介质使用管理中，应该有冗余保护措施，达到存储介质备份规定的要求

5） 定期对存储介质进行检查、清理、统计、核对。对失效的存储介质要严格执行销毁登记、审批、销毁、监销制度。

6） 对存储介质应实施密期管理，包括密期的注册、修改及撤消。

3.2.1.8.3 存储介质的传输管理 ORM_TRA.2

1） 存储介质在物理运输时，例如通过邮递服务或者速递公司，会受到非法访问、滥用或被破坏，所以要对存储介质在机构之间的传递实施控制保障。

2） 管理层应该授权使用可靠的运输和速递公司，并按生产商的规格使用可靠的包装保护运输时不会物理破坏技术资料的内容。

3） 定期检查确实是使用统一安排的速递公司。

- **存储环境管理 ORM_CIR.2**

1） 介质存储室必须符合防火、防水、防震、防腐烂、防鼠害、防蛀虫、防静电、防磁场及防盗的安全要求。

2） 技术资料存储室管理员，负责技术资料存储室管理工作，并核查技术资料使用人员身份与权限。

3） 技术资料存储室管理必须制定存储室、管理员、入库、转储、使用、销毁等管理制度和办法，明确执行各项制度和办法的责任人。

3.2.1.8.4 存储介质的备份 ORM_BAC.2

1） 纸介质和电子介质之间实行交叉备份。

2） 经常需要使用的存储介质，应有双份备份。

3.2.1.8.5 存储介质的分类和归档 ORM_CLA.2

1） 技术资料按纸介质和电子介质分别集中分类管理、编制目录、造册登记。对同一内容以不同介质存储的技术资料要建立对应关系，以便于管理和使用。

2） 技术文档在保管和传递过程中必须采取保密和安全措施，并接受安全管

理员的监督。

3） 系统一旦投入运行，应由项目负责人把完整的技术资料归档入库。归档入库的技术资料应完整、协调、准确，可行性研究报告、项目开发计划、配置管理计划、需求书、数据要求、概要设计、详细设计、数据库设计说明书、用户手册、操作手册、模块开发卷宗、测试计划、测试分析报告、开发进度表、源程序、执行代码等之间保持一致。

4） 由于业务发展和安全管理需要，对系统的变更如机房改造、网络改造、网络重新配置、系统软件的升级、应用系统的维护等而编制的技术资料也必须归档入库并登记。入库登记必须保证同一系统的完整性和持续性。

5） 归档入库的技术资料未经批准任何人不得增加、删除和修改。

3.2.1.8.6 存储介质的销毁 ORM_DES.2

1) 不再需要的的存储介质，应该安全地予以清除，因为如果处理不当，就会泄露敏信息。以下是一列可能需要安全清除的东西：

- ✓ 纸文件
- ✓ 录音
- ✓ 复写纸
- ✓ 输出报表
- ✓ 一次性打印色带
- ✓ 磁带
- ✓ 可换的磁盘或盒式磁带
- ✓ 光盘（所有形式，包括所有生产商的软件光盘）
- ✓ 程序列表
- ✓ 测试数据
- ✓ 系统说明文档
- ✓ ……

2) 如果不再需要，可重用介质中的以前内容应该完全清除。

3) 所有机构要清除的技术资料应有授权。

4) 应制订正式的清除程序，把风险减到最低。

5) 有敏感信息的存储介质应安全地予以保存及清除，例如烧掉或撕碎，或使用另一个机构内应用系统把内容清除。很多机构提供收集及清除的服务，清除纸、设备及介质，要小心选择一个管理完善、经验丰富的服务商。

3.2.1.9OBC 类：应急响应

3.2.1.9.1 应急响应计划的制定 OBC_EST.2

在业务连续性管理方面，除了要求机构能够制订备份和恢复策略来指导备份和恢复活动，对安全事件进行分类、分级来建立安全事件的报告制度，建立安全弱点和可疑事件的报告制度之外应制定应急计划的框架标准，规范机构各部门制定应急计划的行为，针对业务应用建立全面的应急计划，并对应急计划进行测试、维护和培训，并将应急计划文件化。

本级制定的网络系统应急响应计划除包括应急响应工作组织架构、应急响应程序和参与人员的职责内容外，以下几个方面具体要达到以下要求：

1） 启动计划的条件，说明启动前要进行那些处理（如何评估情况，谁负责什么等等）。

2） 应急响应程序，说明发生严重干扰业务操作或关系生死存亡的事故后要进行哪些行动，包括事故报告制度和流程、事故处理流程、公关管理的安排，及与有关公用事务机构迅速联系，例如警察、消防局及当地政府。

3） 后备程序，说明转移业务活动或支持服务到某个暂时地点的行动，以及在限定时间内把业务进程恢复；并且明确每项业务的恢复时间。

4） 恢复程序，说明回到正常业务操作的行动。

5） 维护时间表，说明将如何、在什么时候测试及维护该计划的过程。

6） 意识及教育培训，目的是让员工更好地了解业务连续性管理，并使计划持之有效。

7） 每个人的职责，说明谁负责执行计划的哪部分，可以考虑指定候补人员。

8） 每个计划应指定某个人负责。应急响应程序、手工后备计划及恢复程序，都应该是各业务资源或处理的所有者的责任。后备技术服务的安排，例如信息处理及通讯设备，应是服务供应商的责任。

3.2.1.9.2 应急响应计划的测试和演练 OBC_TES.2

1） 对应急响应计划进行桌面测试，包括的方面有：

✓ 在桌面上对业务不同阶段中断时进行测试

✓ 模拟（特别是为了培训事件或危机之后的管理的角色）

2） 应该对所涉及到的人员进行应急响应计划培训，应该对系统相关的人员进行培训使他们知道如何以及何时使用应急计划中的控制手段及恢复策略。对应急计划的培训至少每年举办一次；拥有计划规定职责的新雇员应该在被雇用后接受短期培训。和应急计划相关的人员所接受的培训最终应该使得他们能够无需实际文档的协助就能够执行相应的恢复规程。

3） 应急计划相关人员培训应包含（但不限于）以下内容：

✓ 计划的目的

✓ 团队之间的协调与沟通

✓ 汇报规程

✓ 个人职责

3.2.2 安全组织

3.2.2.1 OOR 类：安全组织和职责

3.2.2.1.1 安全管理组织 OOR_MNG.2

1） 要求设立专职或兼职的信息安全人员，负责信息安全的管理和技术工作。

2) 成立信息安全管理部门，负责信息安全工作的具体执行。

3) 设立专职的信息安全人员，负责信息安全的管理和技术工作。

3.2.2.1.2 安全管理人员能力 OOR_CAP.2

应配备一定数量的计算机安全管理人员支持信息安全管理工作。安全管理人员可以由其他岗位的人员兼任。安全管理人员应该具有（但不限于）以下能力：

1) 基本的专业技术水平

2) 接受过安全意识教育和培训

3) 掌握安全管理基本知识等

4) 能够进行基本的系统安全风险分析

应配备专职的计算机安全管理人员支持信息安全管理工作。安全管理人员不可兼任。专职的安全管理人员应该具有（但不限于）以下能力：

1）业务素质高、遵纪守法、恪尽职守。

2）计算机安全管理工作多年以上经历，具备安全管理的知识和经验。

3）安全管理工作的组织能力等等。

3.2.2.1.3 岗位安全职责 OOR_STA.2

1) 根据最小特权原则，确定工作岗位、岗位职责和敏感程度。

2) 信息安全人员要求通过相关认证，计算机操作人员要持证上岗。

3) 建立信息安全职责的考评制度。

3.2.2.1.4 关键岗位安全管理 OOR_KST.2

与计算机信息系统直接相关的系统管理员、网络管理员、重要业务开发人员、系统维护员、业务操作员等关键岗位应制定相应的管理制度进行特别管理。核实检查和安全处理的内容可能包括（但不限于）以下内容：

1) 关键安全事务应当双人临岗，互相监督：例如一人负责操作，另外一人负责监督和确认。

2) 人员上岗前必须经单位人事部门进行政治审查，技能考核等，合格者方可上岗；

3) 关键岗位人员有责任保护系统的秘密，并以签署保密协议的方式作出安全承诺。

4) 要害岗位人员应定期接受安全培训，加强自身安全意识和风险防范意识；

5) 关键岗位人员调离岗位，必须严格办理调离手续，承诺其调离后的保密

义务 。

3.2.2.1.5 合作与沟通 OOR_COM.2

1) 加强组织内部的合作与沟通，包括组织内各部门之间的合作与沟通、分部与总部的合作与沟通，共同协助处理信息安全问题。

2) 加强与兄弟单位、公安机关、电信公司的合作与沟通，以便在发生安全事件时能够得到及时的支持。

3) 加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通，获取信息安全的最新发展动态，当发生紧急事件的时候能够及时得到支持和帮助。

4) 安全信息的交流应该加以限制，以确保企业的秘密信息不会泄漏到未经授权的人员手中。

3.2.2.2 OPE 类：人员管理

3.2.2.2.1 人员录用 OPE_EMP.2

对应聘者的道德行为和人品进行检查和确认，雇佣条款和条件应该阐明雇员对信息安全的责任。对准备录用人员应该在招聘时进行核实检查。核实检查的内容可能包括（但不限于）以下内容：

1) 新招聘员工时，必须对应聘者的个人简历进行检查（针对完整性和准确性），对其毕业证、学位证以及声称的专业资格进行确认，审查应聘者的道德行为和人品。

2) 独立的身份检查（身份证或类似证件）。

3) 新招聘的员工，需要签署保密协议，作为其聘用的必要条件。

3.2.2.2.2 人员离岗 OPE_DIM.2

对准备离岗人员应该在离岗前进行核实检查和安全处理。

核实检查和安全处理的内容可能包括（但不限于）以下内容：

1）立即中止解雇的、退休的、辞职的或其他原因离开的员工的所有访问。

2）取回所有的身份证件、徽章、密钥、访问控制记号和其他有关安全的项目。

3）收回机构提供的设备等等。

3.2.2.2.3 安全培训 OPE_TRA.2

应当对各类人员进行安全意识教育和培训，制定详细的安全教育和培训计划并分批进行培训。包含以下工作：

1) 安全技术、安全技能和安全操作培训：

✓ 对安全管理人员、安全技术人员、网络管理员、系统管理员、数据库管理员、软件开发人员等科技人员，进行安全技术和安全技能的培训。

✓ 对于运行维护人员、计算机操作人员，进行安全操作培训。

2) 从事计算机应用的人员，均需通过有关部门组织的上岗培训，持证上岗。

3) 安全管理、技术人员需要具备权威机构颁发的资质认证。

3.2.2.2.4 第三方访问 OPE_OTT.2

1) 第三方人员访问安全区域（例如机房、办公区域）时需要进行审批，由相关负责人审批通过后才能进入。

2) 对重要安全区域的访问，需要由接待人或指定专人陪同。

3) 制定第三方人员安全管理制度，严格按照制度对第三方人员进行管理，至少包括以下内容：

✓ 根据第三方人员的可信任程度、访问对象的安全级别、访问方式等等因素对第三方人员进行分类，针对不同类别的第三方人员采取相应的控制管理措施。

✓ 评估第三方人员的安全风险。

✓ 第三方人员的进出管理。

✓ 第三方人员的网络接入安全管理。

✓ 第三方人员的安全保密管理。

✓ 第三方人员的安全操作管理。

✓ 对第三方的访问的安全风险评估应该是定期进行，每年至少一次，及时发现潜在的第三方安全威胁。

3.2.3 安全策略文档

3.2.3.1 PIN 类：安全策略制定与执行

3.2.3.1.1 安全策略范围 PIN_SCO.2

1) 应当拥有信息安全管理所必须的管理制度、管理规定和操作规程等信息安全管理规章制度。安全规章制度应该能够满足安全管理的基本需要，至少包括下面内容的策略文档：机房管理、防病毒管理、网络管理、安全操作规程、组织结构和岗位职责、数据备份等。

2) 拥有信息安全方针层面的规章制度，给出信息安全的定义、整体目标、指导原则、重要性、适用范围和安全工作的重点，为信息安全工作提供方向和指引。

3) 建立全面、严谨、科学的安全策略文档体系，能够完全满足信息安全管理的需求：

✓ 安全策略文档体系的内容涉及信息安全管理相关的各个方面：信息安全方针、安全组织、资产管理、人员安全、物理和环境安全、网络安全、主机安全、应用安全、数据安全、业务连续和应急响应、项目安全管理、运行维护、风险管理等。

✓ 安全策略文档体系的体系结构应包括信息安全标准、安全规范、安全指南、安全管理办法/规定/制度、安全操作规程、组织结构和岗位职责等。

3.2.3.1.2 安全策略执行 PIN_EXE.2

1) 应当有明确的规定，要求所有人员必须遵守安全策略文档。
2) 大部分员工知道与其相关的安全策略文档，并能够遵守安全策略文档。
3) 安全策略文档能够被有效执行。
4) 定期检查安全策略文档的执行情况。

3.2.3.2 PCO 类：安全策略发布与更新

3.2.3.2.1 策略发布 PCO_PUB.2

安全策略文档应该通过正式的有效的发布渠道进行发布，确认相关人员能够及时获取到安全策略文档。通过正式发布可以保证安全策略文档的权威性。正式发布根据企业的不同习惯，可采取正式发文、领导签署、策略文档盖公章等方式。

3.2.3.2.2 策略更新 PCO_UPD.2

定期对安全策略文档进行评审，检查安全策略是否适用和合理，回顾安全策略文档的执行效果，对不适用或不合理或欠缺的条款进行更新和补充。

4 三级系统基线安全要求（Baseline）

4.1 安全技术要求

4.1.1 TPR 类：物理环境安全

4.1.1.1供电 TPR_SUP

a) 应该保护设备以防电力中断和其他与电力供应有关的异态。应该根据设备制造商的说明提供合适的电力；
b) 紧急电源开关应位于设备室的紧急出口附近，以便在紧急情况下迅速切断电源。在主电源发生故障时，应该提供应急照明；
c) 供电系统应将动力、照明用电与网络系统供电线路分开，并配备应急照明装置；
d) 应使用双回路或多回路供电；
e) 提供紧急情况供电，配置 UPS 设备，以备常用供电系统停电时启用。
f) 采用线路稳压器，防止电压波动对网络系统的影响；
g) 采用有效措施，减少机房中电器噪声干扰，保证网络系统正常运行；
h) 防止电源线干扰，包括中断供电、异常状态供电（指连续电压过载或过低）、电压瞬变、噪声（电磁干扰）以及由于核爆炸或雷击等引起的设备突然失效事件；
i) 设置电源保护装置，如金属氧化物可变电阻、硅雪崩二极管、气体放电管、滤波器、电压调整变压器、避雷针和浪涌滤波器等。
j) 应配备双机 UPS 机组，防范 UPS 失效所带来的风险。
k) 配备发电机组，以便在发生长时间断电事故时进行供电。
l) UPS 设备应该定期检查，并按照制造商的建议测试。
m) 对发电机组应进行定期检查和测试，使其处于良好状态。
n) 应制定与电力供应相关的应急计划，明确在电力供应中断时所采取的行动。并对应急计划进行演练。

4.1.1.2防雷击 TPR_THU

a) 重要的主机系统和网络系统，以及办公场所应当有防雷击措施。
b) XXX 所在的大厦要有避雷针等避雷设备，大厦应当具有符合要求的接地条件。

c) 应采用地桩、水平栅网、金属板、建筑物基础钢筋等构建接地系统，确保接地体良好的接地；
d) 设置信号地与直流电源地，应注意不造成额外耦合，保障去耦、滤波等的良好效果；
e) 设置避雷地，应以深埋地下、与大地良好相通的金属板作为接地点，至避雷针的引线则应采用粗大的紫铜条，或者使整个建筑的钢筋自地基以下焊连成钢筋网作为“大地”与避雷针相连。
f) 接地电阻〈4Ω，电源的地线与计算机设备的地线必须分别设置。
g) 设置安全防护地与屏蔽地，
h) 应采用阻抗尽可能小的良导体的粗线，以减小各种地之间的电位差；
i) 应采用焊接方法，并经常检查接地的良好，检测接地电阻，确保人身、设备和运行的安全。
j) 设置交流电源地线，交流供电线应有规范连接位置的三芯线，即相线、中线和地线，并将该“地线”连通机房的地线网，以确保其安全保护作用。

4.1.1.3防火 TPR_FIR

a) 建筑材料防火：要求机房和记录介质存放间，其建筑材料的耐火等级，应符合 GBJ45-1987 中规定的二级耐火等级;机房相关的其余基本工作房间和辅助房，其建筑材料的耐火等级应不低于 TJ16-1987 中规定的三级耐火等级。
b) 报警和灭火系统：要求设置火灾报警系统，由人来操作灭火设备，并对灭火设备的效率、毒性、用量和损害性有一定的要求。
c) 必须按面积和设备数量配备适合计算机设备使用的灭火器（不得使用干粉、泡沫灭火器），有条件的可以安装配备感温、感烟探测器的固定灭火系统。
d) 建筑材料防火：机房相关的其余基本工作房间和辅助房，其建筑材料的耐火等级应不低于 TJ16-1987 中规定的二级耐火等级。
e) 报警和灭火系统：要求设置火灾自动报警系统，包括火灾自动探测器、区域报警器、集中报警器和控制器等，能对火灾发生的部位以声、光或电的形式发出报警信号，并启动自动灭火设备，切断电源、关闭空调设备等。
f) 建筑材料防火，要求机房和重要的记录介质存放间，其建筑材料的耐火等级，应符合 GBJ45-1987 中规定的一级耐火等级；
g) 区域隔离防火，要求机房布局要将脆弱区（例如大机以及数据库存放区域）和危险区（例如配电室、UPS 室）用防火墙进行隔离，防止外部火灾进入脆弱区，特别是重要设备地区应采取安装防火门、使用阻燃材料装修等；

4.1.1.4防潮 TPR_WAT

a) 防止空调冷凝水、暖气漏水等事故引发水患造成网络系统、文档和介质

的损坏。

b) 水管安装，不得穿过屋顶和活动地板下。穿过墙壁和楼板的水管应使用套管，并采取可靠的密封措施；
c) 计算机设备应放在工作台上，并备有防水罩；
d) 对工作人员进行防水害教育，并使其了解机房进水管关闭阀的准确位置，做到人人会用；
e) 采取一定措施，防止雨水通过屋顶和墙壁渗透、室内水蒸气结露和地下积水的转移与渗透。
f) 安装对水敏感的检测仪表或元件，对机房进行防水检测、报警。
g) 机房应设有排水口，并购置水泵，以便迅速排出积水。

4.1.1.5空调 TPR_CON

a) 应有较完备的中央空调系统，保证机房温度/湿度的变化在计算机运行所允许的范围。
b) 应有完备的中央空调系统（有冗余），保证机房各个区域的温度/湿度变化能满足计算机运行、人员活动和其它辅助设备的要求。

4.1.1.6电磁防护 TPR_TEM

a) 应采用接地的方法防止外界电磁干扰和设备寄生耦合干扰；
b) 应采用屏蔽方法，对信号线、电源线进行电屏蔽，减少外部电器设备对计算机的瞬间干扰；
c) 应采用距离防护的方法，将计算机机房的位置选在外界电磁干扰小的地方和远离可能接收辐射信号的地方。
d) 应采用低辐射材料和设备，防止电磁发射泄露；
e) 应采用屏蔽方法，对重要设备进行电磁屏蔽，削弱外部电磁场对计算机设备的干扰，防止电磁信号的泄露；
f) 对磁带、磁盘等磁记录介质的保管存放，应注意电磁感应的影响，如使用铁制柜存放。
g) 应采用屏蔽方法，对整个物理区域进行电磁屏蔽，防止外部电磁场对计算机设备的干扰。

4.1.1.7门禁 TPR_JAN

a) 规模较大的物理区域，应向所有的工作人员（包括来自外单位的长期工作人员）发放带有照片的身份证件，并定期进行检查或更换。
b) 短期工作人员或维修人员的证件，应注明有效日期，届时收回。
c) 参观人员必须由主管部门办理参观手续，参观时必须有专人陪同。
d) 因系统维修或其他原因需外国籍人进入办公区时，必须始终有人陪同。
e) 在无警卫的场合，必须保证室内无人时，关锁所有出入口。
f) 应该通过门禁系统对于出入进行控制。这种控制可能不仅仅限于进入，

还可能包括离开，控制措施可以具体增加出示有效证件、登记姓名等。

g) 物理环境/机房的出入口应有专人负责，未经允许的人员不准进入机房；
h) 未经许可，不得在场所内拍照或摄影。
i) 机房应只设一个出入口，另设若干紧急疏散出口，标明疏散线路和方向；
j) 没有指定管理人员的明确准许，磁铁、私人电子计算机或电子设备、食品及饮料、香烟、吸烟用具等与上机工作无关的物品均不准带入机房；任何记录介质、文件材料及各种被保护品均不准带出机房。对于允许带进和带出的物品，如有疑问，应进行查验。
k) 获准进入机房的来访人员，其活动范围应受到限制；
l) 安全等级较高的计算机机房，除采取身份证件进行识别以外，还要考虑其他出入管理措施，如：安装自动识别登记系统，采用磁卡或 IC 卡等机器可识别的介质。
m) 在机房中设有网络系统安全管理中心的，更应加强其安全防护，如进入不同区域时佩带有不同标记的证章、重要部位的出、入口设置电子锁、指纹锁等。
n) 进出口的钥匙应保存在约定的场所，由专人管理，并明确其责任。记录最初入室者及最后离室者和钥匙交换时间。
o) 相关安全制度应打印或制作成标牌，放置于醒目的位置
p) 机房内部应分区管理，应根据每个工作人员的实际工作需要，确定其能进入的区域；
q) 在机房中设有网络系统安全管理中心的，除了二级中的要求之外，必要时可设置摄像监视系统。
r) 采用 IC 卡、指纹、虹膜自动识别设备，对人员进行识别、登记及出入管理。
s) 门禁系统的控制中心应当得到有效的保护。

4.1.1.8位置选择 TPR_LOC

1) 按一般建筑物的要求进行机房场地选择。
2) 避开易发生火灾和危险程度高的地区，如油库、和其它易燃物附近的区域；
3) 避开尘埃、有毒气体、腐蚀性气体、盐雾腐蚀等环境污染的区域；
4) 避开低洼、潮湿及落雷区域；
5) 避开强震动源和强噪声源区域；
6) 避开强电场和强磁场区域；
7) 避开有地震、水灾危害的区域；
8) 避免在建筑物的高层以及用水设备的下层或隔壁。
9) 应避免靠近公共区域，如运输邮件通道、停车场或餐厅等。

4.1.1.9防静电 TPR_STA

1) 采用接地与屏蔽措施，使网络系统有一套合理的接地与屏蔽系统；
2) 人员服装应采用不易产生静电的衣料，工作鞋选用低阻值材料制作；

3) 控制机房温湿度，使其保持在不易产生静电的范围内。
4) 机房地板从地板表面到接地系统的阻值应保证防人身触电和产生静电；
5) 机房中使用的各种家具，工作台、柜等，应选择产生静电小的材料。
6) 机房中使用的各种家具，工作台、柜等，应选择产生静电小的材料；
7) 在硬件维修时，应采用金属板台面的专用维修台；
8) 在机房中使用静电消除剂和静电消除器等，进一步减少静电的产生。

4.1.1.10 设备安全 TPR_EQI

1) 网络系统的设备和部件应有明显的无法除去的标记，以防更换和方便查找赃物；
2) 物理区域中应安装防盗报警装置，防止夜间从门窗进入的盗窃行为以及对系统的非法访问。
3) 应利用光、电、无源红外等技术设置机房报警系统，并有专人值守，防止夜间从门窗进入的盗窃行为；
4) 机房外部的网络设备，应采取加固防护等措施，以防止盗窃和破坏。
5) 通过保安监控系统进行 24 小时进行监控。
6) 安装部分透明玻璃及充足的照明设备，以便从室外可以确认室内情况；应安装应急灯等应急照明设备。
7) 安装电话、对讲机等通话设备，以便发生故障时可及时与安全管理机构保持联络。
8) 应利用闭路电视系统对机房的各重要部位进行监视，并有专人值守，防止夜间从门窗进入的盗窃行为；
9) 机房外部的网络设备，应采取加固防护等措施，必要时安排专人看管，以防止盗窃和破坏。
10) 保安监控系统应与报警系统相连，报警系统应当与当地公安机关和 XXX 内部的保卫部门相连。
11) 对保安监控系统及其控制中心进行有效的保护。

4.1.1.11 防干扰和窃听 TPR _TAP

a) 如有可能，接入信息处理设备的电源和通信线路应该铺设在地下，或者采取足够的可替代的保护。
b) 应该保护网络电缆以防未经授权的窃听或损坏，并保护电力电缆不受损坏。例如，通过使用电缆管道和避免通过公共区域，并有防鼠害的措施。
c) 电力电缆应该与通信电缆隔离，以防干扰。
d) 应采取一定措施，预防线路截获，使线路截获设备难以工作；应有探测线路截获装置，及时发现线路截获事件并报警。
e) 应采取有效措施，预防线路截获，使线路截获设备无法工作；
f) 应有探测线路截获装置，及时发现线路截获的事件并报警；
g) 应有定位线路截获装置，能发现线路截获窃取设备的准确位置。
h) 在监测点和端点处安装装甲管道以及上锁房间或盒子；

i) 使用可替换的路由选择或传输媒体；
j) 使用光纤电缆；
k) 启用对未经授权而联接在电缆上的设备的扫描；

4.1.2 TNI 类：网络与通信安全

4.1.2.1 主干网可用性保护 TNI_AVI.3

为保证骨干网的可用性，应满足以下原则：

1） 对骨干网的核心设备应采用冗余设计，包括设备模块冗余、设备热备等。

2) 对骨干网的链路采用冗余设计，采用如以太通道等技术，达到提高链路带宽、负载均衡、链路备份的目的。

3) 对冗余的方案/设备/线路等的测试方案，并定期（至少三个月一次）进行验证测试，以判别是否满足冗余要求，并对发生的问题进行及时处理和备案。

4) 启用动态路由协议的认证功能，并设置具有一定强度的密钥,相互之间交换路由信息的路由器必须具有相同的密钥。默认的认证密码是明文传输的，建议启用加密认证，如 MD5。

5) 启用访问列表过滤一些垃圾和恶意路由信息。

6) 启用访问控制列表过滤一些垃圾和恶意的流量。

7) 配置服务质量保证（QoS）。通过对不同服务类型数据流的带宽管理，保证正常服务有充足的带宽，有效抵御各种拒绝服务类型的攻击。

8) 具备详尽的应急响应流程和措施，对应急响应的过程和处理方法进行详尽的记录。

9) 对骨干网出口，应采用多出口设计，并采用链路负载均衡设备对骨干网的出口链路提供负载均衡。

10）制定网络可靠性保障需求，制定相关的 SLA，并指定专门的内部部门或者外部部门维护和保证。建立网络可靠性监控系统，及时发现并处理可靠性中断/降低故障，对故障处理结果进行教训总结。对 SLA 的执行情况进行定期的审计和计划，应当重点考虑以下问题：

- ✓ SLA 的执行效率

- ✓ SLA 维护情况
- ✓ 内部/外包商执行情况和问题
- ✓ SLA 的违反情况
- ✓ SLA 的改进建议
- ✓ 可靠性的改进建议

4.1.2.2 内部网络防护 TNI_INT.3

在网段划分上，提出了“同一子网支持单一业务”的原则，以形成清晰的边界。同时，对保密性要求高的网络，在其传输上提出了更高的结构安全要求：

1) 网络结构应具有清晰的层次，以便于进行网络逻辑隔离、访问控制、结构调整和应急处理。例如，大型网络应分为核心、汇接、接入三层，中小型网络可以选用其中的一到两层。

2) 根据各组的工作职能、重要性、所涉及信息等级等因素，划分不同的子网或网段。不同的区域在交换机上划分不同 VLAN，不同 VLAN 之间的路由设置访问控制。

3) 应防止 Vlan 穿越攻击。例如，所有连接用户终端的接口都应从 vlan1 中排除，将 trunk 接口划分到一个单独的 vlan 中。

4) 按照方便管理和控制的原则为各子网、网段分配 IP 地址段。例如，地址规划应便于路由汇总以方便路由管理、提高路由广播效率以及简化访问控制列表的配置。

5) 网络结构需要根据应用系统、业务流程和数据流向的特点进行设计。采用子网的概念进行网络逻辑和物理划分，同一子网应尽可能地只支持单一的业务、服务或流程，形成清晰的网络边界。

6) 同等安全水平的服务器应采用集中管理的方式，并与客户端工作站进行分离，以便进行有效的综合安全防护。

7) 对于同时与内部网络和外部网络有逻辑连接的服务器和工作站，应放置在 DMZ 区。

8) 任何用户终端设备不应当直接接入核心层网络设备。

4.1.2.3 网络设备登录控制 TNI_TEL.3

增强设备登录的安全控制和管理，要求至少采取下列措施中的一种或者多种，以达到所需的安全需求：

1） 采用带外管理方式，使得管理链路和数据交换链路隔离，通过专用内部管理网络访问管理设备，防止威胁主体通过对数据交换链路的监听获取密码和管理信息。

2） 采用数据加密信道方式，对登录信道进行数据保护，如采用 VPN 信道，SSH 隧道等技术，威胁主体通过监听获取的数据由于加密而无法从中获取有用信息，保证了登录安全。

3） 采用一次性口令技术，防止威胁主体通过信息重放的形式获取对设备的管理权。

4） 采用动态口令技术，防止威胁主体通过信息重放的形式获取对设备的管理权。

5) 对设备的登录控制措施效能评估和审计，对审计和评估的结果进行相关处理。

6) 限制管理网络设备的网管机的 IP 地址，防止来自非授权 IP 的主机登录管理网络设备。

7) 采用权限分级策略，为不同的管理员提供不同的权限，防止管理员滥用权利。

4.1.2.4 网络设备用户身份鉴别 TNI_IDT.3

1) 采用用户集中管理方式进行用户身份鉴别，如 Radius 或者 TACACS+等，对用户的分配和管理集中在认证服务器端。

2) 采用多因素身份鉴别技术，如采用 Token 技术，生物特征识别，IC 卡等。

3) 对身份鉴别过程的使用情况和效能进行审计，对发现的问题和情况进行分析、处理和改进、汇报。

4) 维护对用户的权限分配记录和注销记录，并定期审查这些用户和记录，确保权限分配记录和实际配置的一致性。对发现的不符合情况进行必要的调查和

报告。

5) 记录并审计用户的身份鉴别记录。

4.1.2.5 密码技术 TIN_ENC.3

1) 对称加密算法的密钥位数必须等同于 128 位 DES 算法。

2) 非对称加密算法的密钥位数必须等同于 1024 位 RSA 算法。

3) 对于任何密钥，都必须设定其生命期，并提供相应的版本更替方案；

4) 密码运算应由相应硬件装置完成。硬件密码装置必须具备防物理攻击的功能，达到 FIPS140-2 级。

5) 通信过程中，应对整个报文或会话过程（如采用 SSH、HTTPS 等）以及信（如 VPN）进行加密。

4.1.3 TEB 类：边界保护

4.1.3.1 网络边界访问控制 TEB_NAC.3

网络边界的访问控制机制主要是限制用户可以建立什么样的连接以及通过网络传输什么样的数据。网络访问控制的目的就是在各网络连接之间建立一个安全控制点，通过允许、拒绝经过网络访问控制设备的数据流，实现对进、出内部网络的服务和访问的审计和控制。

有数据交换的不同网络之间的边界处都需要网络访问控制。一般来说，采用防火墙，路由器访问控制列表等方式对边界进行保护，保护对象为任何向外部系统提供信息发布的设备/系统，至少包括：

- 路由交换信息
- 主机
- 网络设备
- 应用服务

在本级要求在 OSI 模型的 3 到 7 层上检查数据包，并具有对应用层协议中的命令、格式、内容进行过滤的功能，具体的技术功能要求包括：

1） 防火墙应该提供一个默认策略，保证所有经过防火墙的数据包都有相对

应的安全策略进行控制。这个默认策略可以是允许，也可以是拒绝。

2） 防火墙应该具有透明应用代理功能，能对信息流的内容按照一定方式进行过滤。支持 HTTP、FTP、TELNET、SMTP、POP3、NNTP、流媒体等各种常见应用协议；实现对 URL 的过滤；实现对 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制，实现对文件级的过滤。

3） 按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要业务数据主机进行通讯。

访问控制中的一个重要的步骤是对参与通信的一个或多个团体或个人进行授权，即定义其访问权限。授权将一组权限赋予一个实体。实体的访问权限通常与其真实身份相关，身份不同，工作的内容、性质、所在的部门就不同，因此所应关注的系统操作也不同，授予的权限也就不同。如系统管理员与普通用户的访问权限就有很大的差别。

访问权限的定义内容包括定义哪些用户能登录到系统并获取网络资源;哪些用户对网络有什么样的操作权限；哪些用户对目录、文件或设备有什么样的操作权限（如读权限、写权限、创建权限、删除权限、修改权限、查找权限等）等。总之，凡是需要进行网络访问控制的地方都应该先定义访问权限。

定义访问权限可以通过访问控制列表、为应用系统数据流建立的调查表、设备接入检查等技术来实现。

4） 支持动态地址、网络地址转换（NAT）、访问控制列表（ACL）、Vlan 等多种技术以限制对客户端的主动连接访问。

5） 从外部接入专用网络必须经过鉴别（包括回叫设备，动态口令，智能卡等）、认证、授权，对号码进行身份识别。

6） 能限制流出内部网络的地址必须是属于内部网络的。

7） 具有会话流控制功能。此类产品应能根据会话状态信息（包括数据包的源地址、目的地址、源端口号、目的端口号、协议、出入的接口、会话序列号、发出信息的主机名等信息，并应支持地址通配符的使用），为数据流提供明确的访问保障能力和拒绝访问能力。这里所控制的对象，不再是数据包，而是数据流。

8） 支持服务质量保证功能（QoS）。

9） 支持 IP 地址与 MAC 地址绑定功能。

10）支持双机热备。

11) 支持属性修改，此类产品自身的安全功能应(仅向授权管理员)提供修改下述（包含但不仅限于）参数的能力：源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性)；增加、修改或删除管理员帐号；(仅向授权管理员)提供修改下述（包含但不仅限于）参数的能力：配置的安全参数。例如：最大鉴别失败次数、最大审计存储容量等数据；允许/拒绝的应用层协议。

12) 支持属性查询：此类产品自身的安全功能应(仅向授权管理员)提供以下查询：源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性)；通过防火墙传送信息的用户名、主机名。

13) 具有建立三个以上网络区域的能力：外网、内网、一个或多个 DMZ 区

14) 支持详细的通信/管理审计，审计存储和查阅保护功能。网络中的审计体系至少包含网络设备、访问控制策略、远程访问、用户变更、地址变更、拓扑变更和路由变更等审计对象：

防火墙应该具有对以下事件进行安全审计的功能：

✓ 对于包过滤规则中涉及到的内部或外部网络上的主机，无论是允许还是拒绝其通过，都应该对事件进行审计，并把主机标识（主机名或者 IP 地址）记录下来。

✓ 对于安全属性（用户名、密码等）和安全规则（包过滤、审计的设定）的修改。

✓ 对于每一个审计记录，防火墙安全功能应至少记录以下信息：事件发生在哪一天、什么时候，是哪一类的事件（登录、策略修改或者包过滤等等)，用户或者源/目的地址，事件是成功或者失败了。

15) 具有抵御常见的端口扫描和攻击的能力：包括 IP 地址欺骗、DoS 攻击(如 TCP SYN Flood 等)、中间人攻击、碎片攻击等，能过滤异常分段、分段过小、源路由等异常包；能进行流量检测过滤等。

16) 支持多种告警方式，设置告警策略。

17) 具有清除遗留信息的能里，在为所有内部或外部网上的主机连接进行资源分配时，防火墙安全功能应保证不提供以前连接的任何信息内容。

18) 硬件 MTBF（平均无故障运行时间）不低于 25000 小时（3 年）

19) 支持集中管理模式，能向安全管理中心提供必要的信息。

20）抵御拒绝服务（DoS）攻击是网络边界防护中的一项重要要求。防火墙、路由器等边界防护设备一般都能提供一定的抵御拒绝服务攻击能力，但因为受技术体系、软硬件结构的限制，在抵御大流量拒绝服务攻击时性能往往不理想。在这种情况下，专门抵御拒绝服务攻击的设备就应运而生，它根据拒绝服务攻击与正常网络访问行为之间的差异，高效率地阻断拒绝服务攻击，保障正常的网络访问。

对该类产品的技术功能要求为：

✓ 应能够识别拒绝服务攻击报文，过滤拒绝服务攻击，降低拒绝服务攻击对网络/主机造成的影响。

✓ 应能够抵御 Connection Flood、SYN Flood、ACK Flood、UDP Flood、（M）Stream Flood、ICMP FloodPing of Death、Land、Tear Drop 和 WinNuke 等常见拒绝服务攻击。

✓ 应能够抵御 DNS Flood 等针对高层协议的拒绝服务攻击。

✓ 部署方式灵活，能够保护单个主机或者整个网络。

✓ 配置简单，做到“零配置”快速在网络中部署。

✓ 不应对原网络的正常运行产生明显影响。

✓ 能够实现双机热备。

✓ 能对拒绝服务攻击进行记录；日志记录中至少包含以下内容：拒绝服务攻击类型、源地址、目的地址、发生时间等可以查看详细的日志信息。

✓ 能对用户认证和用户行为进行审计；审计内容符合本级要求。

✓ 能提供多种方便灵活的软件升级方法。

✓ 系统与控制端间通过网络通信时使用加密协议。

✓ 要求不需要使用任何 IP 地址（管理端口除外）。

✓ 硬件产品必须符合国家相关电气标准。

4.1.3.2远程访问 TEB_TEL.3

应监控远程访问接入对于内部系统的访问，必须采取适当的监控记录手段，记录接入时间，地址，电话，人员，访问对象等。

1）对远程访问进行监控的主要技术功能要求

✓ 在网络中部署网络监控设备，包括数据中心网管工作站、系统性能监视、系统资源监视、会话连接监视、应用错误监视等几部分，由操作员负责监视以采集网络中的流量，设备运行情况等信息。

✓ 具有对业务交易按规定要求进行监控，并对异常交易及时报告的能力。

✓ 能对所有监控工作都应进行记录。

✓ 能通过分析监控信息发掘异常事件，并根据异常事件的类型和严重程度进入相关事件处理流程。

✓ 异常事件及其处理应当进入审计系统。

✓ 实现对监控事件的实时性响应和多种方式的报警功能。

✓ 实现对相关事件的关联处理、分析能力，实现对不良事件的应急处理能力，包括：

- 功能阻断
- 功能隔离
- 启动应急处理流程等

✓ 具有全面评估监控体系的效能，分析其中存在不足和问题，并不断修正和改进监控能力。

在远程访问中应当建立独立的身份认证、鉴别和授权服务器，强化身份认证和鉴别能力。

2）对远程访问中身份鉴别的具体技术功能要求

✓ 所有的远程访问必须具备身份鉴别和访问授权控制，只有通过适当的身份鉴别和访问授权，才能允许远程访问。

✓ 应当采用消息摘要和数字证书等方式进行身份鉴别，避免在网络中传递口令等重要信息。

✓ 存储口令的加密方式应当是不可逆的。

✓ 应采用双因素或多因素认证机制，除采用口令进行鉴别，应采用一种或以上更加严格的身份鉴别，如采用智能 IC 卡、人体生物特征（指纹、视网膜）等特殊信息进行身份鉴别。

✓ 用户每次登录系统时应当进行身份鉴别，并对此过程进行记录。

✓ 应定义鉴别尝试允许次数，并通过对鉴别失败超过允许次数即封锁账户或封锁场地的方法来限制重复尝试。

✓ 用于身份鉴别的用户名/口令对应当在信道中加密传输。

✓ 应当对用户的来源进行控制和监控；

✓ 不允许系统管理人员直接以具备系统管理权限的账户远程访问登录系统，必须通过中转的方式，即先以普通权限用户身份登录系统，然后通过系统用户身份切换功能变换为系统管理员。

✓ 对远程系统管理应当限定登录访问的地址范围，绝对不允许没有来源控制的远程系统管理。

✓ 必须对远程访问的用户进行统一集中管理，具备相关的申请登记流程和审批流程，其中应当至少包括人员背景调查等方面。

✓ 必须对用户的操作过程进行记录，至少保证前 1000 条操作被正确纪录，供审计分析。

3）其他技术功能要求

✓ 远程访问必须只允许来自可信信道的连接，对与其他信道则不允许。

✓ 采用具有加密功能的远程终端和通信信道进行远程访问。

✓ 应当保证系统管理权限的等级化划分。

✓ 不允许同一账户（用户 ID）同时登录访问系统。

✓ 不显示系统或应用信息，直到登录流程成功的完成之后。

✓ 显示警告信息，描述未授权的访问可能导致的后果。

✓ 在登录过程中，不提供任何可能帮助未授权用户的信息。

✓ 在完成所有的输入数据时，才确认登录信息。当发生错误时，系统不应提示数据的错误范围。

✓ 在成功的登录流程完成之后，显示从上一次成功登录以来的不成功的登录尝试的详细情况。

✓ 通过自动化的记录功能或者工具记录，并对管理员的登录行为和操作行为进行完整记录、审计和分析，发现异常及时报告和处理。

✓ 系统必须完整记录系统管理人员的操作越权行为，一旦发现必须以两种以上的方式报警：通知管理人员当前操作无效、记录系统日志、通告上级管理人员和系统审计人员。

✓ 强化对远程访问的审计功能，审计内容至少包括：

• 登记人员变更情况，开户/销户情况

- 远程访问情况
- 失败访问情况
- 访问范围情况
- 访问时间情况

✓ 在远程访问过程中当信息从主机输出时，应当进行安全属性控制（例如更改成只读属性、加密等）。当信息输入主机时，必须进行安全检测，以验证其合法性、有效性和可用性。

电话拨号等（包括模拟电话/公共交换电话网 PSTN 和综合服务数字网 ISDN）经接入服务器联入用户网，当拨号用户通过认证后，接入服务器将为之分配用户网范围内的地址，远程用户在逻辑上就成为网络内部用户。

4）拨入方式远程访问的技术功能要求（接入服务器的功能要求）

✓ 按用户需求支持模拟 modem/公共交换电话网 PSTN 拨号接入。

✓ 按用户需求支持 ISDN 拨号接入。

✓ 具有对拨号接入用户的严格认证功能。

✓ 具有对拨号接入用户的网络访问授权功能。

✓ 具有回拨功能。

✓ 支持挑战响应、动态口令，智能卡等高级认证方式。

✓ 支持集中式认证、授权、审计（AAA）。

4.1.3.3防病毒网关 TEB_TVI.3

防病毒网关是网络安全的重要组成部分，其主要功能是对从外部网络进入用户内部网络的病毒进行过滤，一般主要针对 HTTP、HTTPS、FTP 和 SMTP 等协议进行过滤，保护用户内部网络不受病毒感染。

对防病毒网关的主要技术功能要求有：

1） 具有集中分发软件、进行病毒特征码升级的控制台——病毒集中监控中心。

2） 病毒集中监控中心应支持安全管理中心的集中管理。

3） 能根据单位内部的不同部门需要设置不同的防病毒策略。

4） 对要求更高的网络或大型网络，病毒集中监控中心应考虑到管理容量问题，也就是每一个集中监控中心的控制台能够有效管理到的客户机的数目，所以

有必要要求各病毒监控中心可做到集联控制。

5） 防止病毒进出内部网络。

6） 限定内部网络指定的 IP 段通过代理服务器访问外部，禁止内部网络用户对外部某些网站或域名的访问。

7） 支持对常见格式压缩文件的病毒检测。

8） 至少对基于 http、ftp、socks/mms、telnet、gopher、smtp、imap、pop3 等主要网络协议的事件进行检测，剥离 ActiveX 和 Java Script、Java Applet 等恶意代码。

9） 支持对宏病毒和可疑宏的高效检查功能。

10）代理内容过滤。基于网页标题和内容，设置过滤规则和规则库，实现对浏览网页的过滤。过滤垃圾和违规邮件侵扰，至少可对标题、文本、html、附件（文本、html、常见压缩包）等进行内容过滤、病毒过滤及恶意代码过滤，允许管理员定制过滤规则，以符合企业或各机关单位内部网络的需要。

11）支持自动定时升级。

12）防病毒软件应在不停止杀毒任务的同时自动更新病毒代码库。

13）网络病毒集中监控，支持病毒监控中心的统一管理。防病毒网关发现病毒后在病毒监控中心报警，病毒监控中心可以进行远程管理操作（例如杀毒等）。

14）防病毒网关不能影响原有的网关系统。

15）应具有与防火墙联动的功能。

16）硬件 MTBF（平均无故障运行时间）不低于 25000 小时（3 年）。

4.1.3.4网络入侵防范 TEB_IDS.3

基于网络的入侵检测产品通过对计算机网络中的若干关键点收集信息并对其进行分析，以发现网络中是否有违反安全策略的行为和被攻击的迹象。

在一个网络环境中，有很多配置点可以考虑设置网络 IDS。IDS 设置在防火墙之外，可以观察到未被防火墙过滤的原始的外部网络通信；设置在防火墙的内部，提供了对目的地是内部网络的外部流量或目的地是外部网络的内部流量的监测，而并不监测仅在内部网络中流动的通信。在内部网络环境中，网络 IDS 通常被设置在客户机与服务器、通信路径的中间，可以监测所有通信层次上的数据。

本节主要介绍在边界处的入侵防范。

在确定 IDS 配置点和数目的时候，需要考虑的因素包括：操作员对每一个IDS 发出的报警进行分析和划分的工作负担；对多个监测器监测到同一事件的报警进行关联分析的复杂性以及不同配置点的选择所带来的系统采购、安装、运行和维护的成本。

具体技术功能要求为：

1）数据检测功能要求

✓ 数据收集：应具有实时获取受保护网段内的数据包的能力。获取的数据包应足以进行检测分析。

✓ 协议分析：至少应监视基于以下协议的事件：HTTP、FTP、TFTP、TCP、UDP、IP、ICMP、IMAP、SNMP、TELNET、DNS、SMTP、POP3、NETBIOS、NFS、NNTP、ARP、RIP、RPC 等。

✓ 行为监测：至少应监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫攻击等。

✓ 流量监测：应监视整个网络或者某一特定协议、地址、端口的报文流量和字节流量。

2）入侵分析功能要求

✓ 数据分析：应对收集的数据包进行分析，发现攻击事件。

✓ 攻击事件的过滤规则调整：可以对网络中检测到的事件实施灵活的过滤规则，如根据监控网卡、事件类型等，减少对系统资源的占用。

✓ 事件合并：应具有对高频度发生的相同安全事件进行合并告警，避免出现告警风暴的能力。

✓ 防躲避能力：应能发现躲避或欺骗检测的行为，如 IP 碎片重组，TCP 流重组，协议端口重定位，URL 字符串变形，shell 代码变形等。

✓ 事件关联：应具有把不同的事件关联起来，发现低危害事件中隐含的高危害攻击的能力。

3）入侵响应功能要求

✓ 安全报警：当产品检测到入侵时，应自动采取相应动作以发出安全警告。

✓ 响应方式：可对检测到的攻击行为采取告警、记录日志、会话阻断等响应方式。告警可以采取屏幕实时提示、E-mail 告警、声音告警等几种方式。

✓ 排除响应：应允许用户定义对被检测网段中指定的主机或特定的事件不予告警，降低误报。

✓ 定制响应：应允许用户对被检测网段中指定的主机或特定的事件定制不同的响应方式，以对特定的事件突出告警。

✓ 阻断能力：产品在监测到网络上的非法连接时，应具有阻断的功能；

✓ 设备联动：产品应具有与其它网络设备和网络安全部件进行联动的能力。

4）管理控制功能要求

✓ 图形界面：产品应提供友好的用户界面用于管理、配置网络安全监控报警产品。管理配置界面应包含配置和管理产品所需的所有功能。

✓ 事件数据库：产品的事件数据库应包括事件定义和分析、详细的漏洞修补方案、可采取的对策等。

✓ 事件分级：产品应按照事件的严重程度将事件分级，以使授权管理员能从大量的信息中捕捉到危险的事件。

✓ 策略配置：应提供方便、快捷的网络安全监控报警策略配置方法和手段。

✓ 升级能力：产品应具有及时更新、升级产品和事件库的能力。

✓ 统一升级：产品应提供由管理控制中心对各探测器的事件库进行统一升级的功能。

5）检测结果处理要求

✓ 事件记录：产品应记录并保存检测到的入侵事件。入侵事件信息应至少包含事件发生时间、源地址、目的地址、危害等级、事件详细描述以及解决方案建议等内容。

✓ 事件查看：用户应能通过管理界面实时清晰地查看入侵事件。

✓ 事件可视化：产品应提供具有统计、查询等功能的工具，供用户阅读入侵事件数据。

✓ 事件导出：产品应具有导出入侵事件数据的功能。

✓ 报告生成：产品应能生成详尽的检测结果报告。

✓ 报告查阅：产品应具有全面、灵活地浏览检测结果报告的功能。

✓ 报告输出：检测结果报告可输出成标准格式（如 HTML、文本文件等）。

6）产品灵活性要求

✓ 窗口定义：产品可提供有效的手段支持用户自定义窗口显示的内容和显

示方式。

✓ 报告定制：产品应支持授权管理员按照自己的要求修改和定制报告内容。

✓ 事件定义：产品应允许授权管理员自定义事件，或者对开发商提供的事件作修改，并应提供方便、快捷的定义方法。

✓ 协议定义：产品除支持默认的网络协议集外，还应允许授权管理员定义新的协议，或对协议的端口进行重新定位。

✓ 通用接口：产品应提供对外的通用接口，以便与其它安全设备（如网络管理软件、防火墙等）共享信息或规范化联动。

✓ 支持集中管理模式，能向安全管理中心提供必要的信息。

7）性能指标要求

✓ 稳定性：在产品设计适应的带宽下，入侵检测产品应能长期稳定工作。

✓ 网络影响：产品不应对原网络的正常运行产生明显影响。

✓ 平均响应时间：当背景数据流达到网络的有效带宽时，入侵检测产品应保证有足够快的响应时间。

✓ 数据截取率和还原率：在产品设计适应的带宽下，入侵检测产品应具有良好的数据包处理能力。当背景数据流低于网络有效带宽的 80%时，入侵检测产品应保证数据的截取和还原以线速进行。

✓ 漏报率：产品应在满足自己声明的运行条件的情况下，提供漏报率的分析数据。

✓ 误报率：产品应在满足自己声明的运行条件的情况下，提供误报率的分析数据。产品应将误报率控制在应用许可的范围，不得对正常应用产品产生较大影响。

4.1.4 TCE 类：保护计算环境

4.1.4.1应用系统测试 TCE_APT

a) 编制测试文档；

b) 对安全功能进行黑箱测试。

c) 对所有安全功能进行白箱测试；

d) 根据容量规划进行压力测试。

e) 要求测试能够提供具备每项安全功能的证据。

4.1.4.2病毒和恶意代码防范 TCE_VIR

1) 在其运行网络环境的边界系统（如网关、电子邮件服务器）部署病毒防范系统；

2) 部署计算机防病毒软件，开启病毒实时防护功能，并定期进行病毒码升级；

3) 及时安装系统的最新补丁程序。

4) 建立病毒防范的日常管理机制和审查机制。

4.1.4.3计算环境访问控制 TCE_TAC

a) 采用自主访问控制策略，可以用访问控制表及其相应的访问规则所组成的访问控制策略，确定相应的访问权限。

b) 无论采用何种访问控制策略所实现的自主访问控制功能，都要求能够：

1) 了解掌握当前资源的访问控制能力。

2) 允许命名用户以用户和/或用户组的身份规定并控制共享方式，并阻止非授权用户获取或者篡改敏感信息。

3) 对访问是跨网络的情况，如果在物理上分隔（如内存与磁盘）间传递用户数据时，应严格执行访问控制策略，以防止信息的泄漏、篡改和丢失。也可以根据数据属性，按照密码支持第一级的要求保证数据在通过网络传输时的保密性和完整性。

4) 对访问是非注册用户，如通用匿名访问的情况，应重点考虑对其获取信息的控制、写访问的严格控制以及相关必须的审计策略。

c) 有更细粒度的自主访问控制，即基于角色的访问控制，能够实现系统管理员采用指定方式或默认方式确定用户的访问权限，并将访问控制的粒度控制在单个用户，同时实现只有系统管理员才能进行授权，而阻止那些非授权的用户进行任何访问，也阻止授权用户以非授权的操作形式进

行访问。

d) 要求自主访问控制能与身份鉴别和审计功能相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。

e) 对访问是跨网络的情况，如果在物理上分隔（如内存与磁盘）间传递用户数据时，应严格执行访问控制策略，以防止信息的泄漏、篡改和丢失。也可以根据数据属性，按照密码支持第二级的要求保证数据在通过网络传输时的保密性和完整性。

f) 当信息从主机输出时，应当进行安全属性控制（例如更改成只读属性、加密等）。

g) 当信息输入主机时，必须进行安全检测，以验证其合法性、有效性和可用性。

h) 可采用强制访问控制策略和功能，具体内容如下：

1) 权职分离。应由专门设置的系统安全员统一管理计算机网络系统中与该访问控制有关的事件和信息。为了防止由于系统管理人员或特权用户的权限过于集中所带来的安全隐患，应将系统的常规管理、与安全有关的管理以及审计管理，分别由系统管理员、系统安全员和系统审计员来承担，并按最小授权原则分别授予它们各自为完成自己所承担任务所需的最小权限，还应在三者之间形成相互制约的关系。

2) 安全模型。强制访问控制当前常用的安全策略模型是多级安全模型。通过标记方式设置安全属性（等级和范畴），这些安全属性共同组成属性库，作为访问控制的基本数据。该模型并按由简单保密性原则确定的规则——从下读、向上写，根据不同的安全属性，实现每次访问的强制性控制。也可以设置某些补充规则以满足专门的需要。

3) 控制范围。强制访问控制应与用户身份鉴别、标记、审计等安全功能要素密切配合，使系统对用户的安全控制包含从用户进入系统到退出系统的全过程。

4.1.4.4身份鉴别 TCE_IDT

a) 必须采用用户名/口令对的方式进行身份鉴别；
b) 应当保证在身份鉴别过程中口令不可见；
c) 采用加密方式存储口令；
d) 应当保证身份鉴别的时效性，在登录或者注销时，应当对相关的身份鉴别状态进行标记，以便指示新的过程；
e) 用户每次登录系统时应当进行身份鉴别，并对此过程进行记录；
f) 应定义鉴别尝试允许次数，并通过延长鉴别失败超出允许次数后再次允许鉴别的时间间隔来限制重复尝试，并对此过程进行记录；
g) 存储口令的加密方式应当是不可逆的；
h) 用于身份鉴别的用户名/口令对应当在信道中加密传输；
i) 应当对用户的来源进行控制和监控；
j) 应当采用消息摘要和数字证书等方式进行身份鉴别，避免在网络中传递口令等重要信息；
k) 应采用双因素或多因素认证机制，除采用口令进行鉴别，应采用一种或以上更加严格的身份鉴别，如采用智能 IC 卡、人体生物特征（指纹、视网膜）等特殊信息进行身份鉴别；
l) 应定义鉴别尝试允许次数，并通过对鉴别失败超过允许次数即封锁账户或封锁场地的方法来限制重复尝试。
m) 定期审计身份鉴别，对发现的异常进行及时处理，对累积性事件进行必要的趋势分析。

4.1.4.5安全审计 TCE_SAU

1) 要求产生完整的审计数据；
2) 提供审计数据的查阅；
3) 对审计数据和分析结果进行保存，确保审计数据的可用性
4) 可自定义审计数据查阅的方式和视图；
5) 对审计数据进行分析，包括分类、排序和趋势分析等；

6) 对特定异常事件进行审计分析，并提高实时报警功能；
7) 以风险分析为依据进行审计事件选择；
8) 提供自动响应功能，例如进行实时报警，终止违例进程，取消异常服务等；
9) 建立并持续改进事件特征库，提高审计的进度和范围；
10) 支持集中审计和事件关联分析。

4.1.4.6数据库设计安全 TCE_DBS

a) 系统在设计时不应留有“后门”，即不应以维护、支持或操作需要为借口，设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口。
b) 安全结构应是一个独立的、严格定义的软件系统子集，并应防止外部干扰和破坏，如修改其代码或数据结构；
c) 数据库管理系统应进行分层设计，并将数据库管理系统进程与和用户进程进行隔离；
d) 应提供设置和升级配置参数的安装机制，在初始化和对与安全有关的数据结构进行保护之前，应对用户和管理员的安全策略属性应进行定义；
e) 应区分普通操作模式和系统维护模式，全系统操作恢复的启动、配置系统内部的数据库和表等动作应在维护模式中执行。
f) 应防止普通用户从未经允许的系统进入维护模式，并防止普通用户与系统内维护模式交互,从而保证在普通用户访问系统之前，系统能以一个安全的方式进行安装和配置。
g) 当数据库管理系统安装完成后，在普通用户访问之前，系统应配置好初始用户和管理员职责、审计参数、系统审计跟踪设置以及对客体的合适的访问控制。
h) 执行系统所提供的实用程序，应限定于对系统的有效使用，只允许系统管理员修改或替换系统提供的实用程序。
i) 系统应能识别由通信渠道接收的信息的来源者，所有待确认的数据应能从进入点被安全地传送到确认系统，如口令不应由公共的或共享的网络

以明文发送，可使用数据加密设备或通过加密信道用加密方式传送。

j) 数据库系统因故障或其它原因中断后，应有一种机制恢复系统。系统应提供在管理维护状态中运行的能力，管理维护状态只能被系统管理员使用，且各种安全功能全部失效。

k) 数据库系统应为系统管理员提供一种机制，来产生安全参数值的详细报告。

4.2 安全管理要求

4.2.1 安全运作

4.2.1.1ORA 类：风险管理

4.2.1.1.1 资产鉴别 ORA_ASE.3

采用业务应用为主线的方式，用体系架构的方法描述信息资产。信息资产的体系架构和机构业务体系架构一脉相承。信息资产体系架构已经不是简单的资产清单，而是通过对各个资产之间有机的联系和关系的描述，而形成的较复杂结构。

应该清晰识别每项资产、其拥有权、责任人以及资产现在的位置等，对于支持信息系统运行的网络设备、主机设备及安全设备等，进行标识和登记。用半定量的方法对系统的重要资产进行赋值。

重要资产可能包括（但不限于）以下内容：

a) 信息资产：数据文件、数据库文件、系统文件、用户手册、培训资料、操作和支持程序、持续性计划、存档信息等；

b) 软件资产：应用软件、系统软件、开发工具和实用程序等；

c) 有形资产：计算机设备，通信设备、磁媒体、其他技术装备等；

d) 无形资产：计算和通信服务；

4.2.1.1.2 威胁分析 ORA_THR.3

应采用一种系统化风险分析方法对威胁进行分析，对威胁的可能性（Likelihood）和影响（Impact）这两个属性通过赋值进行量化，从而得到威胁的量化取值。威胁评估可以通过对于可能性和强度的评价来综合获得。

对威胁的可能性和影响的分析可以（但不限于）从以下几方面考虑：

a) 通过国际权威机构数据；

b) 历史安全事件统计分析；

c) 用户账户安全事件统计分析；

d) 通过问题发生的后果来间接衡量等等。

4.2.1.1.3 脆弱性分析 ORA_VUL.3

应用人工评估、工具扫描、安全访谈、渗透测试等方法或工具对系统的脆弱性进行分析和评估，形成脆弱性列表。

脆弱性的工具扫描可以（但不限于）从以下几方面考虑：

a) 网关设备的脆弱性扫描；

b) 网络设备的脆弱性扫描；

c) 主机设备的脆弱性扫描；

d) 安全设备的脆弱性扫描；

脆弱性的人工分析可以（但不限于）从以下几方面考虑：

a) 系统配置检查；

b) 用户管理检查；

c) 系统日志和审计检查。

使用渗透测试应该考虑（但不限于）如下一些问题：

a) 渗透测试方使机构负责人了解测试可能带来的后果，并做好充分准备；

b) 机构不应单单依赖于渗透测试方的报告来监测其安全程序；

c) 机构应要求渗透测试方作出不得泄漏测试结果的书面承诺。

针对不同的资产和资产组合，采用不同的评估方法和工具进行综合分析和评估。对不同的方法和工具所得出来的评估结果，应当综合起来，并对综合指标进

行量化赋值，从而得到脆弱性的量化取值。

每个资产都要自己的脆弱性。为了减小管理的复杂度，可以针对资产组合、资产类编制脆弱性列表和脆弱性检查表。脆弱性列表将成为系统加固、改进和安全项目建设的依据。

将定期的脆弱性评估和报告形成一种制度，制定相关的制度文件。制度文件可以包括（但不限于）如下内容：

a) 定期进行脆弱性评估的时间；

b) 进行脆弱性评估的责任；

c) 脆弱性评估结果的报告程序；

d) 报告中包括新发现的漏洞、已修补的漏洞、漏洞趋势分析等。

4.2.1.1.4 风险分析 ORA_ANA.3

应采用多层面、多角度的系统分析方法，由安全管理人员和外部安全专家对资产、威胁和脆弱性等方面进行半定量综合评价，根据“风险值=威胁可能性 X 资产价值 X 弱点严重性”，计算出安全风险的值，最终形成风险评估报告。应将风险评估中的信息资产、威胁、脆弱性、防护措施等评估项综合到一个数据库中进行管理。

并配备必要的资源保证风险管理活动有一个良好的环境，并能顺利、有效进行。应制订文档化的安全风险分析和评估活动程序规范风险管理活动。

安全风险分析和评估活动程序可能包括（但不限于）以下内容：

a) 信息安全风险管理和机构业务风险管理密切相关的内容；

b) 信息安全风险管理的基本观念和方法；

c) 风险管理的组织和资源保证等。

4.2.1.1.5 选择安全控制措施 ORA_CTR.3

对评估的安全风险按照风险值排序，并对各条风险进行分析，选择安全风险的处理方式，例如降低安全风险、消除安全风险、接受安全风险等等。并结合公司对于信息安全的需求通过定性或者半定量的方法，对相关的各种控制措施进行综合评价，以便得出紧迫性、优先级、投资比重等，来选择合适的控制措施对抗

安全风险，并根据业务系统的整体重要程度来确定选择的控制措施的强度。

4.2.1.1.6 安全措施的实施与确认 ORA_VAD.3

根据选择的安全控制措施，编写安全解决方案从管理手段和技术手段来实现安全控制措施，通过安全管理、部署安全产品和安全技术进行风险控制措施的实施。在风险控制措施实施后，结合已采用的安全控制措施，进行残余风险评估，确认残余风险在可接受范围内，并由高层管理人员来做出风险接受的决定。而后采用系统化的方法实施二次风险评估，验证防护措施的有效性。

4.2.1.2OEN 类：工程建设安全管理

4.2.1.2.1 安全项目的立项管理 OEN_CON.3

信息系统的安全建设立项要符合信息系统安全建设的总体规划, 经公司安全主管部门组织内部和外部相关专家科学论证后方可进行设计和组织实施。

4.2.1.2.2 安全需求分析 OEN_REQ.3

安全需求分析阶段通常至少包括系统定义、威胁评估、脆弱性评估、影响评估、风险评估、确定安全要求等六个步骤。可以根据 ORA_THR.3、ORA_VUL.3、ORA_ANA.3、ORA_CTR.3 的要求进行安全需求分析。

4.2.1.2.3 安全功能规范 OEN_FSP.3

应编写正式的安全功能规范。功能安全规范是用户可见接口和信息系统的安全功能行为的一个高层描述。它是信息系统安全功能要求的一个实例化，应该描述信息系统的安全属性和它的外部接口。并且功能安全规范应该是内在一致的，应该完备地表示信息系统的安全属性。

4.2.1.2.4 高层安全设计 OEN_HLD.3

应进行较为完整的高层安全设计，高层安全设计应该标识信息系统所要求的

任何基础性硬件、固件、软件、和/或通信，和在这些硬件、固件、软件、和/或通信中实现的支持性保护机制所提供的功能表示。

还应将功能安全规范细化到子系统。对于信息系统的每一个子系统，高层安全设计描述并标识出包含在子系统中的安全功能。高层安全设计也定义所有子系统之间的相互关系。这些相互关系将适当地被表示成数据流、控制流等的外部接口。

高层设计应该标识信息系统的安全相关子系统的所有接口，标识哪些接口是外部可见的。高层设计应该包括信息系统深度防御的描述、标识技术的和非技术的对策的组合是如何降低残余风险的级别到一个可接受的级别的。

还要编写安全子系统功能规范。安全子系统/产品规范将保证与高层安全设计一致，保证研究并确定系统安全设计要素，以及论证安全保障要求是完备的、一致的、在技术上合理的、并适合作为信息系统开发的基础。

建设者应该提供与安全相关的指南，还应该为运行系统的用户和管理员提供与安全相关的指南。运行指南告诉用户和管理员在以安全模式进行安装、配置、运行和淘汰系统时必须做些什么。

安全子系统安全属性的描述还应该尽可能地描述由它所提供的安全和非安全服务，以及安全子系统的范围和边界，在通常意义下既要用物理方式又要用逻辑方式来表述。

4.2.1.2.5 安全产品选型 OEN_PRO.3

a） 安全产品具有在国内生产、经营和销售的许可证。

b） 密码产品符合国家密码主管部门的要求，来源于国家主管部门批准的密码研制单位。

c） 所有安全产品或信息技术产品的安全模块应获得国家相关安全认证，在选型中根据实际需要制定安全产品选型的标准。

d） 系统集成商的资质要求：国家权威部门认可的系统一级集成资质。

e） 工商要求：

1) 产品或系统提供单位的营业执照和税务登记在合法期限内；

2) 产品或系统提供商的产品或系统提供资格；

3) 连续赢利期限要求；

4) 连续无相关法律诉讼年限要求；

5) 没有发生重大管理、技术人员变化和流动的期限要求；

6) 没有发生主业变化期限要求。

f） 安全服务商资质：应具有国家一级安全服务资质。

g） 人员资质要求：系统集成人员以及相关管理人员获得国家权威部门颁发的信息安全人员资质认证。

h） 其它要求：系统符合国家相关法律、法规，按照相关主管部门的技术管理规定对非法信息和恶意代码进行有效控制，按照有关规定对设备进行控制，使之不被作为非法攻击的跳板。

4.2.1.2.6 外包软件安全控制.3

在软件的开发被外包时应当考虑许可安排、代码的所有权和知识产权以及质量合格证和所进行的工作的精确度。还应进行质量审核、在安装之前进行测试以检测特洛伊代码，并要求已方提供源代码以及相关设计、实施文档。还要对源代码进行安全审核。

要减少软件中出现缺陷的可能性可以（但不限于）考虑如下方面：

a) 需要软件购买系统选择有良好声誉、可靠的记录而且有足够的资源和保险来负担因其软件导致的损失的供应商。

b) 要求所有软件都经过测试和验证。

c) 代码一旦被安装，就控制对代码的访问和修改；

对外包软件的开发应制定控制程序进行控制。在控制程序中应当考虑（但不限于）如下内容：

a) 代码的所有权和知识产权；

b) 软件开发过程的质量控制要求；

c) 代码质量检测要求；

d) 在安装之前进行测试以检测特洛伊代码。

4.2.1.2.7交付和运行 OEN_ADO.3

交付过程需要系统控制以及交付设备和程序来提供保证，以确保接收方所接受的信息系统的版本正是发送者发送的，而没有任何修改。

还需要编写安装、生成和启动程序，以确保信息系统在开发者所期望的安全方式下进行安装、生成和启动是有用的。安装、生成和启动程序应准确描述信息系统安全地安装、生成和启动所必要的步骤。

4.2.1.2.8 系统安全检测和验收 OEN_TES.3

应进行安全测试论证信息系统是否满足安全功能规范。应该论证功能规范中所描述信息系统安全功能和测试文档所标识的测试之间的对应性是完备的。并论证测试文档中所标识的测试足以论证信息系统安全功能运行和它的高层设计是一致的。还应当严格地论证功能规范所标识的信息系统的所有外部接口已经被完备测试过了。

应制定有关安全项目建设的管理办法：《公司信息安全项目建设管理办法》

4.2.1.3OPM 类：物理环境管理

4.2.1.3.1 机房管理 OPM_ROM.3

计算机机房是信息系统硬件资源的集中地，机房管理主要以加强机房物理访问控制和维护机房良好的运行环境为主。本安全级应按以下要求进行机房人员管理：

1) 机房出入应有保安人员负责执守，未经允许的人员不准进入机房；
2) 获准进入机房的来访人员，应出示有效证件并履行严格的登记手续，佩戴临时出入证。其活动范围应受到限制，并有接待人员陪同；
3) 内部人员须在门禁处使用工卡（得到指示方可进入），不允许利用别人的工卡进入（包括别人刷卡，跟随进入）；
4) 机房钥匙由专人管理，未经批准，不准任何人私自复制机房钥匙或服务器开机钥匙。

5) 没有指定管理人员的明确准许，任何记录介质、文件材料及各种被保护品均不准带出机房，与工作无关的物品（如：食品、香烟等）均不准带入机房。
6) 未经批准，禁止任何人移动计算机相关设备及其相关的系统或带离机房；
7) 应禁止携带磁铁、个人计算机等电子设备进入机房；
8) 机房内严禁吸烟及带入火种和水源。
9) 所有来访人员登记记录以及门禁系统的电子记录应妥善保存以备查；
10) 禁止测试物理访问控制；
11) 应经常打扫机房防止灰尘以及进行灭鼠工作。

4.2.1.3.2 办公环境管理 OPM_OFM.3

设置有网络终端的办公环境，是信息系统环境的组成部分，办公环境管理主要以加强信息保密性为主，防止利用终端系统窃取敏感信息或非法访问。本安全级应按以下要求进行终端办公环境的管理：

1) 工作人员下班后，终端计算机应关闭；
2) 存放敏感文件或信息载体的文件柜应上锁或设置密码；
3) 禁止使用调制解调器拨号上网。
4) 工作人员调离部门或更换办公室时，应立即交还办公室钥匙。
5) 工作人员离开座位超过 30 分钟以上，应将桌面上含有敏感信息的纸件文档在抽屉或文件柜内；
6) 工作人员离开座位超过 30 分钟以上，计算机应退出登录状态，采用屏幕保护口令加以保护或关机；
7) 应尽可能使办公环境与机房的物理位置在一起，以便进行统一的物理保护。

4.2.1.3.3 环境设备维护 OPM_MAI.3

机房内（包括电源间）的所有环境设备（如空调、电源等），由确定的部门负责管理，并随时受理和处理这些设备的突发事故。机房值班员要每天到机房巡

视至少一次。

a) 机房值班员要对各种设备的运转情况（包括电源、空调）进行必要的检查，记录有错误代码的设备，供有关人员检修使用。

b) 机房空调必须定期例行检修：

1) 空调系统出现故障报警，有关人员要及时处理解决，不得拖延；

2) 每月清洁一次过滤网、排水管和加湿器，定期更换加湿罐（随各地水质而定）；

3) 每季清扫一次室外冷凝机组，保证通风良好。

c) 电源系统必须定期例行检修：

1) 每月要分析一次机器运行记录，查找隐患，并采取相应的对策；

2) 每季要对蓄电池做一次充放电测试。清洁或更换机器过滤网，检查机器易损件的运行情况；

3) 在确保不影响正常生产的情况下，每半年要对 UPS 设备进行一次双机切换演练。并对电源配电柜检修；

4) 在确保不影响正常生产的情况下，每年要做一次 UPS 设备、备用发电机、总配电柜切换模拟实验。

d) 机房环境管理员每周定时对各种设备例行检查，每半年进行一次检修，检修要彻底清扫各种设备的空气过滤器，运行测试程序、作规定的设备测试，检查各设备的记录信息码，查找隐患。

e) 机房场地监控系统、门禁保安系统信息记录资料每两周收集整理一次，消防设施每年定期检查是否在有效期内，及时更换过期设备。

4.2.1.4OHO 类：主机维护

4.2.1.4.1 主机设备维护 OHO_EQI.3

a) 主机设备应当由指定的专人（主机设备管理人员）定期维护，制定明确的维护目标和要求、维护流程和操作规范，测试规范，制定相关的维护制度，维护对主机设备的维护纪录。

b) 应当与主机设备厂商保持畅通的沟通联系，以便能及时从厂商处获取必

要的技术支持。

c) 主机设备维护人员应当具备相应的专业技能，并取得相应的资质。

d) 主机设备维护人员应当根据主机设备维护情况向上级管理机构报告主机设备运行状态。

制定主机设备维护指标考评体系。指标考评体系应当至少包括：

a) 主机设备的平均无故障运行时间；

b) 主机设备的故障修复时间；

c) 主机设备的故障恢复时间；

d) 主机设备的故障发生率（次数和频度）；

e) 对设备发生故障的类型统计；

f) 评估主机设备故障对业务连续性的影响；

g) 主机设备管理人员的技术保障能力；

h) 主机设备厂商的技术支持提供能力。

应当有相关职能部门负责监督和执行该考评体系。

考评的结果应当至少反映到对主机设备供应商的选择，管理维护人员的业务考评等方面。并将主机设备维护纳入业务连续性保障计划的一个重要组成部分。

4.2.1.4.2 账户管理 OHO_ACC.3

1) 在系统初始化时，删除或者禁用不使用的系统缺省账户；

2) 对帐户进行分组或分级管理，并分别设置相应的权限；

3) 定期检查系统中是否存在未使用的或过期的帐户；

4) 对系统中的账户情况进行定期审计，对发现的异常账户应当及时报告并进入相关处理流程；

5) 建立账户管理制度，负责系统账号的登记造册、用户名分配、初始口令分配、用户权限分配、系统资源分配、注销等，并定期检查系统中的帐户分配情况，以及帐户权限设置的正确性。

6) 为不同用户分配不同的用户名或用户标识符，确保用户名或用户标识符具有唯一性；

7) 记录用户的系统登录活动，定期审计和分析用户账户的使用情况，对

发现的问题和异常情况进行相应处理。

8) 用户名或用户标识符在系统内部全局唯一，在用户名或用户标识符被删除后，同名用户名或用户标识符不可再被创建；

9) 对于账号管理制度的执行情况进行检查和监督，对发现的问题和异常情况进行相关处理。

4.2.1.4.3 远程登陆管理 OHO_TEL.3

a） 应当制定远程系统管理制度，记录和分配系统账户远程系统管理的操作权限分配；

b） 对系统进行远程管理和维护时应当：

1) 不允许系统管理人员直接以具备系统管理权限的账户远程访问登录系统，必须通过中转的方式，即先以普通权限用户身份登录系统，然后通过系统用户身份切换功能变换为系统管理员；

2) 对远程系统管理应当限定登录访问的地址范围，绝对不允许没有来源控制的远程系统管理；

3) 必须对用户的操作过程进行记录，至少保证前 1000 条操作被正确纪录，供审计分析；

c） 必须对远程系统管理进行记录和分析，对发现的异常行为进行报告和相应处理。

d） 采用具有加密功能的远程终端和通信信道进行远程系统管理；

e） 应当保证系统管理权限的等级化划分；

f） 不允许同一账户（用户 ID）同时登录访问系统；

g） 设置详细的登录策略，具体设计如下：

1) 不显示系统或应用信息，直到登录流程成功的完成之后；

2) 显示警告信息，描述未授权的访问可能导致的后果；

3) 在登录过程中，不提供任何可能帮助未授权用户的信息；

4) 在完成所有的输入数据时，才确认登录信息。当发生错误时，系统不应提示数据的错误范围；

5) 在成功的登录流程完成之后，显示从上一次成功登录以来的不成

功的登录尝试的详细情况；

h） 通过自动化的记录功能或者工具记录，并对管理员的登录行为和操作行为进行完整记录、审计和分析，发现异常及时报告和处理。

i） 定期审计系统管理人员的远程系统管理情况，对审计中发现的异常和问题及时处理和报告；

j） 系统必须完整记录系统管理人员的操作越权行为，一旦发现必须以两种以上的方式报警：通知管理人员当前操作无效、记录系统日志、通告上级管理人员和系统审计人员；

4.2.1.4.4 漏洞控制 OHO_VER.3

定期安装系统的最新补丁程序，并根据厂家提供的可能危害计算机的漏洞进行及时修补，并在安装系统补丁前对现有的重要文件进行备份，并对补丁程序进行初步测试，以防止对现有软件的不兼容性。

a) 定期进行系统漏洞扫描：采用专业化的工具进行系统漏洞扫描，可以及时发现系统的现有安全控制措施是否足够，应当定期进行扫描。

b) 定期进行系统安全评估：通过专用评估工具定期进行系统评估，可以检查无法采用扫描工具的系统的安全性。

c) 根据业务需求最小化系统的服务：系统默认的服务存在一些与业务和现有操作无关的服务，同时这些服务中可能存在容易被利用的漏洞。因此应当最小化系统的服务，确保系统的安全性。

4.2.1.4.5 防病毒管理 OHO_VIR.3

本级的病毒防护管理，根据所使用的病毒防护产品，提出了检查、记录、定期升级、汇报等的基本要求。

a） 应有指定人员检查网络内防病毒网关和主机的病毒检测情况，并保存染毒和杀毒记录。

b） 使用软盘、U 盘、光盘等外部移动存储设备之前应进行病毒检查；

c） 从不信任网络上所接收的文件，在使用前应首先检查是否有病毒；

d） 定期进行总结汇报，使主管领导和相关人员及时了解病毒安全状况。

e） 安全管理员应检查网络内计算机病毒库的升级情况，并进行记录。

f） 每周定时整体网络统一策略、统一升级、统一控制，紧急情况下增加升级次数；

g） 安全管理员每周对计算机主机防病毒产品、防病毒网关和邮件防病毒网关上截获的各种高风险病毒进行及时分析处理，并提供相应的报表；

h） 分别进行月度、季度和年度总结汇报，使主管领导和相关人员及时了解病毒防护状况。

4.2.1.5ONE 类：网络维护

4.2.1.5.1 网络拓扑设计和规划 ONE_TOP.3

网络拓扑满足网络系统和业务需求，具有详细和完整的拓扑设计需求说明、设计文档、网络拓扑、实施过程文档以及网络拓扑变更文档，网络拓扑符合设计要求，网络拓扑图必须和当前实际运行情况保持一致，并保证和维护这些文档的机密性，使其只在允许的范围内被访问和获取。网络的设计必须考虑到网络容量、功能和结构。

还需要强化网络拓扑/结构的变更过程和审批过程，使得任何的网络拓扑结构的变更都在知晓和可控制的状态下进行。

在网络设计图（拓扑图）中必需体现出实际的物理位置和物理连接情况。

网络的设计必须考虑到网络容量、功能和结构的拓展需求

a）必须对网络容量、可承受能力、功能制定相应的测试和验证方案供实施参考。

b）必须预留网络的容量、功能和结构的拓展性设计。

c）必须考虑安全性问题。

需要对网络的设计、变更和审批进行定期的复核和审计，复核审计的手段至少至少包括以下内容：

a) 网络拓扑图与实际运行情况的核查及其相关处理

b) 网络设计与网络拓扑图的核查及其相关处理

c) 网络变更及其执行过程、结果的核查及其相关处理

d) 网络审批及其执行过程、结果的核查及其相关处理

e) 网络容量、功能的测试和结果核查及其相关处理

f) 网络可拓展性的验证、测试结果核查及其相关处理

g) 网络的安全性验证、测试结果核查及其相关处理

h) 复核审计周期（频度）应当至少保证半年一次。

i) 应当对复核审计结果进行适当的维护，确保其连续性、完整性和机密性。

对于在复核审计中发生/发现的问题，应当根据其情节严重程度，依据其他相关管理制度进行处理。

4.2.1.5.2 IP 地址管理 ONE_IPM.3

具有 IP 地址管理规定，应当具有统一的 IP 地址管理机构/人员，由该机构/人员负责对外部和内部各个部门人员的 IP 地址进行登记、维护和分配。确保在网络中不发生地址冲突和盗用现象，应当采用一定的技术和管理制度保证不发生该类事件。并对违反 IP 地址管理规定的人员/部分依据相关管理制度进行处理。

实现对地址使用情况的实时动态监控，维护记录地址的使用情况，及时关闭被废止的地址，具有对 IP 地址的容量规划设计，确保各个部门有一定的地址容量冗余供扩展使用。

防止地址的伪造和欺骗。及时发现违反使用 IP 事件，并进行相关处理。

应当实现对 IP 地址使用情况的审计功能，审计内容至少包括以下内容：

a) IP 地址登记和使用情况

b) IP 地址废止和使用情况

c) 当前 IP 地址容量和使用情况

d) 违反 IP 地址管理规定的情况及其处理结果

审计周期至少保证半年一次，审计结果应当上报相关职能部门。

4.2.1.5.3 网络可靠性管理 ONE_REL.3

应当制定网络可靠性保障需求，制定相关的 SLA，并指定专门的内部部门或者外部部门维护和保证。

针对各个内部/外部部门的不同需求，制定相应的 SLA，并与这些部门签署这些 SLA。并对这些 SLA 的执行情况进行跟踪监控，对出现违反 SLA 的情况进行相关处理。

建立网络可靠性监控系统，及时发现并处理可靠性中断/降低故障，对故障处理结果进行教训总结。

对 SLA 的执行情况进行定期的审计和计划，应当重点考虑以下问题：

a）SLA 的执行效率

b）SLA 维护情况

c）内部/外包商执行情况和问题

d）SLA 的违反情况

e）SLA 的改进建议

f） 可靠性的改进建议

4.2.1.5.4 路由管理 ONE_ROU.3

应当具有路由设计和规划，明确在网络的各个部分的选择和使用恰当的路由协议，具备基本的路由 SLA，保证网络的互联互通。

对网络中使用的路由协议运行情况进行监控：

a）静态路由管理

b）防止动态路由出现振荡、不收敛情况

c）防止路由出现异常的不可达现象

d）在边界对路由信息进行依据内部和外部规则进行必要的过滤。

对于动态路由，应当在满足互联互通的前提条件下实现可靠安全的认证交换制度，实现有效的防止路由欺骗功能。

对路由协议的变更进行管理和审批。

对路由中断情况进行实时发现和处理、经验教训总结。

应当强化以下内容：

a）路由协议管理和审计

b）路由使用情况审计

c）违反 SLA 的情况审计

d）路由中断处理审计

e）路由使用效能情况统计分析和改进建议

4.2.1.5.5 安全域规划 ONE_SED.3

针对不同的业务部门需求对其进行安全域规划，确定各个部门的安全功能需求，并按照这些安全功能需求设计和实现相应的安全隔离保护措施。

需要对安全域的保护功能进行详细的安全功能设计，并对设计进行必要的验证和审批。构建安全域时必须考虑对业务连续性的影响。

还需要对安全域的使用和划分情况进行管理、审计和维护，至少包括以下内容：

a）安全域的使用情况和改进

b）安全域内部系统和外部系统的变更

c）安全域级别和位置的变更

d）变更的执行和审批过程

e）安全域保护功能的验证

f）违反安全域的使用情况及其处理

4.2.1.5.6 网络设备管理授权 ONE_ADV.3

采用集中统一设备管理授权，并通过中心服务器实现对各个设备的用户管理，用户授权，使用情况记录和审计功能，并针对发现的异常进行处理和报告。

4.2.1.6 OCO 类：配置和变更管理

配置和变更管理通过在细化和修改信息系统的过程中进行规范和控制，确保网络系统的完整性。配置和变更管理阻止对信息系统进行非授权的修改、添加或删除。

4.2.1.6.1 配置管理计划 OCO_PLA.3

应制定配置管理计划，并且每季度进行审查和升级，以保证配置管理计划的

可行性以及组织具有完成配置管理计划的能力。

4.2.1.6.2 配置管理自动化 OCO_AUT.3

应该有措施来控制信息处理设备和系统的改变。对信息处理设备和系统变化的控制不够是系统或安全故障的通常原因。应在关键的设备上采用半自动的配置管理工具，并使用半自动的方法对计算机进行升级，并对相关人员进行配置管理的培训。

应确保网络系统的实现表示是通过自动方式控制的，从而解决复杂实现或众多合作者合作开发，以及在开发过程中多种变化情况所出现的人工难以解决的问题，并确保这些变化是已授权的行为所产生的。配置管理计划应描述所使用的自动工具，并说明如何使用这些工具。

并且先对所有的配置变更进行测试，方能正式执行。还能自动确定网络系统版本间的变化，并标识出哪个配置项会因其余配置项的修改而受到影响。

4.2.1.6.3 配置管理能力 OCO_CAP.3

配置管理能力的设计应满足以下要求：

a） 版本号，要求开发者所使用的版本号与所应表示的网络系统样本应完全对应，没有歧义。

b） 配置项，要求配置项应有唯一的标识，从而对网络系统的组成有更清楚的描述。

c） 配置管理计划应描述系统是如何使用的，并说明运行中的配置管理系统与配置管理计划的一致性；

d） 配置管理文档应足以说明已经有效地维护了所有的配置项；

e） 配置管理系统应确保对配置项只进行授权修改。

版本号、配置项、授权控制的基础上确认对配置项的任何生成和修改都是由授权者进行的。为此，配置管理系统应支持网络系统的建设，验收计划应描述用来验收修改过的或新建的配置项的过程，并作为网络系统的一部分。

4.2.1.6.4变更控制 OCO_CHA.3

系统的变更应有相关责任人对其控制。应该制订正式的管理责任和程序以确保满足对设备、软件或程序的所有改变的控制。可行的情况下，应把操作和应用的变更控制程序整合起来。在程序变更时，应该保留包括所有相关信息的审计日志。

4.2.1.6.5密钥管理 OCO_KEY.3

a) 存储密钥的介质必须严加保护，应以加密形式存储密钥；
b) 有关密钥存储方式和地方的信息不应被非授权人员获得；
c) 应根据密钥的种类、系统的要求确定密钥更换周期；会话密钥应在每次会话后更换；主密钥更换时间间隔可视具体情况而定；
d) 密钥必须由纯随机源产生，并应经过随机性检验，生成密钥时不能降低密码算法设计中所规定的密钥空间；
e) 密钥传送要有专门的密钥传送机制，密钥分发应专门设计密钥分发设备；
f) 用于现场加密信息的密钥，应注入加密算法或加密设备中，长期驻留的密钥及其变形必须加物理保护；
g) 系统密钥的保存应由专门设计的密钥管理协议完成，若采用密钥卡保存用户密钥，应加强密钥卡的保护措施并防止丢失；
h) 密钥副本的保存必须是物理安全的；
i) 应及时发现和废止已泄露和怀疑泄露的密钥，并及时作出更换处理；
j) 当密钥定期更换时，旧密钥必须安全归档，并在规定的时间内，在安全管理负责人的严密监督下，由管理责任人销毁；

4.2.1.7OBA 类：备份与恢复

4.2.1.7.1 数据备份和恢复 OBA_DAT.3

为了保证在发生事故或灾难时，确保系统能够有效地恢复，应该通过数据备份和设备、系统冗余等方式，为可能发生的事故和灾难做出准备。数据备份和恢复的主要目的是为了避免数据丢失风险和由此引起的业务中断风险。引起数据丢失的威胁有物理环境威胁和软硬件故障。除此之外，无作为和误操作也是经常引发数据丢失。数据存储和备份并非用于抵抗上述威胁，但可以有效降低上述威胁引发后果的严重性。数据备份的需求程度主要取决于数据的价值或业务中断造成后果的严重性。

本级数据备份和恢复的保护目标是在系统发生局部事故或灾难后，利用备份数据，至少能够恢复到一周前的状态，相关业务中断时间不超过 12 小时。

1） 数据应从运行的系统中备份到光盘、海量磁盘、磁带或磁带库等介质中，保存数据的介质必须由专人保管。

2） 机构应当制订备份和恢复相关的策略，相关的策略应覆盖（但不限于）如下一些内容：

- ✓ 应明确说明介质的分类、标记、查找方法。
- ✓ 应明确说明介质的使用、维护、保养、销毁方法。
- ✓ 应明确说明需定期备份重要业务信息、系统数据及软件等。
- ✓ 应确定重要业务信息的保存期以及其它需要永久保存的归档拷贝的保存期。
- ✓ 应明确说明可手工或软件产品进行备份和恢复。
- ✓ 应明确说明恢复审批和操作流程。

3） 采用磁盘或磁带进行离线备份或在线备份方案，进行小时级增量备份，每天做一次包括数据和应用环境的全备份。

4） 备份过程必须双人在场，全程监视并记录。

5） 本地直接存储(DAS)方式，数据可直接通过存储系统进行自动备份。

6） 数据恢复时，数据库管理员应填写数据恢复申请表，制订数据恢复计划报请主管批准。而后按恢复计划操作，登记数据恢复登记表。

7） 备份介质应定期接受检查，如实际许可，保证在紧急情况时可以使用；

8） 恢复程序应定期接受检查及测试，以确保在恢复操作程序所预定的时间内完成。

9） 恢复策略应该根据数据的重要程度和引入新信息的频率设定备份的频率（如每日或每周、增量或整体）。

10) 数据备份策略应指明已备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法。

11) 每日的备份数据应异地保存并由专人保管。

12) 可采用磁带、磁盘和在线数据远程复制的备份方案。

13) 应对数据恢复工具进行严格控制，在生产环境中，尽可能的清除数据恢复工具，防止误操作。并且数据的恢复工具应有详细的操作说明、操作步骤以及注意事项说明。

14) 实现存储区域网(SAN)方式，当本地系统和数据丢失或不可用时，异地数据自动启用，使得业务得到延续。

4.2.1.7.2 设备和系统冗余 OBA_EQI.3

为了保证在发生事故或灾难时，确保系统能够有效地恢复，应该通过数据备份和设备、系统冗余等方式，为可能发生的事故和灾难做出准备。本级设备和系统冗余的保护目标是在系统发生局部事故或灾难后，利用冗余系统和冗余设备，保证至少能够恢复到一天前的状态，单次业务中断时间为小时级。

1） 系统内重要服务器，如重要的应用服务器和数据库服务器，应采用冷备、温备或热备的方式进行冗余设置。

2） 支持重要应用的网络设备应有冗余设置。

3） 采用技术措施保证服务器出现故障经更换或修复后，能够自动安装操作系统、应用软件，并恢复数据。

4） 采用支持数据快照，文件系统检查点等技术，提供高速的数据恢复手段。

5） 采用高可用性软件，应提供二节点或更多节点的集群，支持高可用性和数据库并行应用。

4.2.1.8ORM 类：存储介质管理

4.2.1.8.1 存储介质的保护 ORM_PRO.3

1） 对存放重要数据和软件的各类记录介质（如纸介质、磁介质、半导体介质和光介质等）应受到控制和物理保护，其存储室必须符合防火、防水、防震、防腐烂、防鼠害、防蛀虫、防静电、防磁场、防盗以及符合制造商的储存规格的安全要求，确保其不受损、不丢失和不被非法访问。

2） 根据所承载的数据和软件的重要程度对介质加贴标识并进行分类，存储在由专人管理的介质库或档案室中，防止被盗、被毁以及信息的非法泄漏，必要时加密存储。

3） 必须制定介质存放存储室、管理员、入库、转储、使用、销毁等管理制度和办法，明确执行各项制度和办法的责任人。

4） 应设立存储介质入库、转储、使用、销毁登记记录。对各类技术资料入库、使用、转储、销毁应有审批手续和传递记录。

5） 对保密性影响级为二级的信息介质，其借阅、拷贝、传输须经一定级别的领导同意后方可执行，而对于保密级达到三级或三级以上信息介质，其借阅、拷贝、传输须经一定级别的领导的书面审批后方可执行，各种处理过程应登记在册。

6） 存储介质的销毁必须经批准并按指定方式进行，不得自行销毁。

7） 存储介质的携带出工作环境时，必须受到监控和内容加密。

8） 对于完整性、可用性要求达到三级或三级以上的信息介质，应每三个月进行一次完整性和可用性检查和验证，确认其中的数据或软件没有受到损坏或丢失。

4.2.1.8.2 存储介质的访问控制 ORM_ACO.3

1） 对借阅和复制的存储介质，要进行使用登记，并应严格执行技术资料借阅制度，不得随意扩大技术资料借阅范围。

2） 对逾期未还的技术资料，应由技术资料存储室管理人员负责收回。

3） 一旦发现技术资料丢失或损坏，要立即报告有关部门，并采取补救措施。

4） 存储介质使用管理中，应该有冗余保护措施，达到存储介质备份规定的要求

5） 定期对存储介质进行检查、清理、统计、核对。对失效的存储介质要严格执行销毁登记、审批、销毁、监销制度。

6） 对存储介质应实施密期管理，包括密期的注册、修改及撤消。

7） 对高安全等级的存储介质原则上不借阅和复制。

8） 对确实因工作需要，如系统改造和维护等，必须由项目负责人提出申请。借阅、复制存储介质要履行一定的手续，包括申请、审批、登记、归档等必要环节，并明确各环节当事人的责任与义务，确保技术资料的完整和安全，不得丢失和损坏。

4.2.1.8.3 存储介质的传输管理 ORM_TRA.3

1) 存储介质在物理运输时，例如通过邮递服务或者速递公司，会受到非法访问、滥用或被破坏，所以要对存储介质在机构之间的传递实施控制保障。

2) 管理层应该授权使用可靠的运输和速递公司，并按生产商的规格使用可靠的包装保护运输时不会物理破坏技术资料的内容。

3） 定期检查确实是使用统一安排的速递公司。

4） 应保证特别的控制保护敏感信息不被非法公开或更改，例如：

- ✓ 使用加锁的装运箱。
- ✓ 亲手递送。
- ✓ 防篡改的包装（可以显示有试图打开的迹象）。
- ✓ 在特别情况下，把托运物品分多次并按照多途径递送。

4.2.1.8.4 存储环境管理 ORM_CIR.3

1） 介质存储室必须符合防火、防水、防震、防腐烂、防鼠害、防蛀虫、防静电、防磁场及防盗的安全要求。

2） 技术资料存储室管理员，负责技术资料存储室管理工作，并核查技术资料使用人员身份与权限。

3） 技术资料存储室管理必须制定存储室、管理员、入库、转储、使用、销

毁等管理制度和办法，明确执行各项制度和办法的责任人。

4） 应设立入库、转储、使用、销毁登记记录。对各类技术资料入库、使用、转储、销毁应有审批手续和传递记录。

5） 技术资料存储室严禁其他人员擅自进入、逗留。

6） 严格、整齐、有序地管理好生产用各种数据和存储介质对要求补打报表的申请，一律要经主管的批准。

4.2.1.8.5存储介质的备份 ORM_BAC.3

1） 纸介质和电子介质之间实行交叉备份。

2） 经常需要使用的存储介质，应有双份备份。

3） 对设备系统功能至关重要的、不可替代的、毁坏后不能立即恢复的技术资料，或属于绝密、机密、秘密级的技术资料，必须双重和异地备份。

4） 可以等到与原资料等同的副本，但获取过程较困难或价格昂贵，或重要的技术资料，应有双重和异地备份。

4.2.1.8.6存储介质的分类和归档 ORM_CLA.3

1） 技术资料按纸介质和电子介质分别集中分类管理、编制目录、造册登记。对同一内容以不同介质存储的技术资料要建立对应关系，以便于管理和使用。

2） 技术文档在保管和传递过程中必须采取保密和安全措施，并接受安全管理员的监督。

3） 系统一旦投入运行，应由项目负责人把完整的技术资料归档入库。归档入库的技术资料应完整、协调、准确，可行性研究报告、项目开发计划、配置管理计划、需求书、数据要求、概要设计、详细设计、数据库设计说明书、用户手册、操作手册、模块开发卷宗、测试计划、测试分析报告、开发进度表、源程序、执行代码等之间保持一致。

4） 由于业务发展和安全管理需要，对系统的变更如机房改造、网络改造、网络重新配置、系统软件的升级、应用系统的维护等而编制的技术资料也必须归档入库并登记。入库登记必须保证同一系统的完整性和持续性。

5） 归档入库的技术资料未经批准任何人不得增加、删除和修改。

6） 对电子介质技术资料，要定期转储，并进行转储登记记录。

7） 在系统投入运行后，对系统开发过程中形成的技术资料副本由项目负责人收回，按失效介质销毁和监销。

4.2.1.8.7存储介质的销毁 ORM_DES.3

1) 不再需要的的存储介质，应该安全地予以清除，因为如果处理不当，就会泄露敏信息。以下是一列可能需要安全清除的东西：

- ✓ 纸文件；
- ✓ 录音；
- ✓ 复写纸；
- ✓ 输出报表；
- ✓ 一次性打印色带；
- ✓ 磁带；
- ✓ 可换的磁盘或盒式磁带；
- ✓ 光盘（所有形式，包括所有生产商的软件光盘）；
- ✓ 程序列表；
- ✓ 测试数据；
- ✓ 系统说明文档；
- ✓ ……

2）如果不再需要，可重用介质中的以前内容应该完全清除。

3）应制订正式的清除程序，把风险减到最低。

4）有敏感信息的存储介质应安全地予以保存及清除，例如烧掉或撕碎，或使用另一个机构内应用系统把内容清除。很多机构提供收集及清除的服务，清除纸、设备及介质，要小心选择一个管理完善、经验丰富的服务商。

5）所有机构要清除的技术资料应有授权，应把所有清除操作记录，当作日后审计跟踪之用

4.2.1.9OBC 类：应急响应

4.2.1.9.1 应急响应计划的制定 OBC_EST.3

在业务连续性管理方面，除了要求机构能够制订备份和恢复策略来指导备份和恢复活动，对安全事件进行分类、分级来建立安全事件的报告制度，建立安全弱点和可疑事件的报告制度之外应制定应急计划的框架标准，规范机构各部门制定应急计划的行为，针对业务应用建立全面的应急计划，并对应急计划进行测试、维护和培训，并将应急计划文件化。

本级制定的网络系统应急响应计划除包括应急响应工作组织架构、应急响应程序和参与人员的职责内容外，以下几个方面具体要达到以下要求：

1） 启动计划的条件，说明启动前要进行那些处理（如何评估情况，谁负责什么等等）。

2） 应急响应程序，说明发生严重干扰业务操作或关系生死存亡的事故后要进行哪些行动，包括事故报告制度和流程、事故处理流程、公关管理的安排，及与有关公用事务机构迅速联系，例如警察、消防局及当地政府。

3） 后备程序，说明转移业务活动或支持服务到某个暂时地点的行动，以及在限定时间内把业务进程恢复；并且明确每项业务的恢复时间。

4） 恢复程序，说明回到正常业务操作的行动。

5） 维护时间表，说明将如何、在什么时候测试及维护该计划的过程。

6） 意识及教育培训，目的是让员工更好地了解业务连续性管理，并使计划持之有效。

7） 每个人的职责，说明谁负责执行计划的哪部分，可以考虑指定候补人员。

8) 每个计划应指定某个人负责。应急响应程序、手工后备计划及恢复程序，都应该是各业务资源或处理的所有者的责任。后备技术服务的安排，例如信息处理及通讯设备，应是服务供应商的责任。

9） 应定期对应急响应内容的完备性进行检查。

4.2.1.9.2 应急响应计划的测试和演练 OBC_TES.3

1） 应该对所涉及到的人员进行应急响应计划培训，应该对系统相关的人员

进行培训使他们知道如何以及何时使用应急计划中的控制手段及恢复策略。对应急计划的培训至少每年举办一次；拥有计划规定职责的新雇员应该在被雇用后接受短期培训。和应急计划相关的人员所接受的培训最终应该使得他们能够无需实际文档的协助就能够执行相应的恢复规程。

2） 应急计划相关人员培训应包含（但不限于）以下内容：

- ✓ 计划的目的
- ✓ 团队之间的协调与沟通
- ✓ 汇报规程
- ✓ 个人职责

3） 应当对应急响应计划进行完全排练以确保它们是最新的和有效的。这样的测试也应当确保恢复小组的所有成员以及其他有关的职员都知道该计划。应急计划应得到测试以确保各个恢复规程的正确性和计划整体的有效性。总之从测试机构、人员、设备及处理多方面进行测试使应急计划可以应付业务停顿的情况。

4） 应急计划测试应该涉及到（但不限于）以下领域：

- ✓ 在备用平台上使用备份介质进行系统恢复
- ✓ 在恢复团队之间进行协调
- ✓ 内部和外部的连接性
- ✓ 使用备用设备的系统性能
- ✓ 正常操作的恢复
- ✓ 通知规程

4.2.2 安全组织

4.2.2.1 OOR 类：安全组织和职责

4.2.2.1.1 安全管理组织 OOR_MNG.3

1） 要求设立专职或兼职的信息安全人员，负责信息安全的管理和技术工作。

2） 成立信息安全管理部门，负责信息安全工作的具体执行。

3） 设立专职的信息安全人员，负责信息安全的管理和技术工作。

4) 成立信息安全领导小组或者安全管理委员会，由领导层和各部门的主要负责人构成，对信息安全工作进行领导、决策、协调和监督。

5) 成立专项的安全小组，例如安全技术小组、安全专家小组、安全检查小组和安全应急小组等等，为信息安全工作的开展提供支持和组织保障。

4.2.2.1.2 安全管理人员能力 OOR_CAP.3

应配备专职的计算机安全管理人员支持信息安全管理工作。安全管理人员不可兼任。专职的安全管理人员应该具有（但不限于）以下能力：

1）业务素质高、遵纪守法、恪尽职守。

2）计算机安全管理工作多年以上经历，具备安全管理的知识和经验。

3）安全管理工作的组织能力等等。

4.2.2.1.3 岗位安全职责 OOR_STA.3

应该清晰划分岗位，详细定义岗位职责，明确岗位的信息安全责任，明确各岗位的敏感程度和人员配置，选拔合格的人员任职各工作岗位。

1) 根据最小特权原则，确定工作岗位、岗位职责和敏感程度。

2) 信息安全人员要求通过相关认证，计算机操作人员要持证上岗。

3) 建立信息安全职责的考评制度。

4) 依据“权限分散，不得交叉覆盖”的原则设置，严格规定要害岗位的职责和权限，避免混岗现象。

5) 各岗位人员必须按规定行事，不得从事超越自己职责以外的任何作业。

6) 关键的工作岗位应该有人员储备计划。

4.2.2.1.4 关键岗位安全管理 OOR_KST.3

与计算机信息系统直接相关的系统管理员、网络管理员、重要业务开发人员、系统维护员、业务操作员等关键岗位应制定相应的管理制度进行特别管理。核实检查和安全处理的内容可能包括（但不限于）以下内容：

1) 关键安全事务应当双人临岗，互相监督：例如一人负责操作，另外一人负责监督和确认。

2) 关键的工作岗位应该有人员储备计划。

3) 关键的工作岗位人员根据实际情况实行强制休假制度和人员轮岗制度。

4) 人员上岗前必须经单位人事部门进行政治审查，技能考核等，合格者方可上岗；

5) 关键岗位人员有责任保护系统的秘密，并以签署保密协议的方式作出安全承诺。

6) 关键岗位人员上岗必须实行“权限分散、不得交叉覆盖”的原则；

7) 要害岗位人员应定期接受安全培训，加强自身安全意识和风险防范意识；

8) 关键岗位人员调离岗位，必须严格办理调离手续，承诺其调离后的保密义务 。涉及机构保密信息的要害岗位人员调离单位，必须进行离岗审计，在规定的脱密期后，方可调离。

4.2.2.1.5 合作与沟通 OOR_COM.3

1) 加强组织内部的合作与沟通，包括组织内各部门之间的合作与沟通、分部与总部的合作与沟通，共同协助处理信息安全问题。

2) 加强与兄弟单位、公安机关、电信公司的合作与沟通，以便在发生安全事件时能够得到及时的支持。

3) 加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通，获取信息安全的最新发展动态，当发生紧急事件的时候能够及时得到支持和帮助。

4) 安全信息的交流应该加以限制，以确保企业的秘密信息不会泄漏到未经授权的人员手中。

5) 聘请信息安全专家，作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等等。

4.2.2.2 OPE 类：人员管理

4.2.2.2.1 人员录用 OPE_EMP.3

对应聘者的道德行为和人品进行检查和确认，雇佣条款和条件应该阐明雇员对信息安全的责任，人员上岗前必须经单位人事部门进行政治审查。

对准备录用人员应该在招聘时进行核实检查。

核实检查的内容可能包括（但不限于）以下内容：

1) 新招聘员工时，必须对应聘者的个人简历进行检查（针对完整性和准确性），对其毕业证、学位证以及声称的专业资格进行确认，审查应聘者的道德行为和人品。

2) 独立的身份检查（身份证或类似证件）。

3) 新招聘的员工，需要签署保密协议，作为其聘用的必要条件。

4) 人员上岗前必须经单位人事部门进行政治审查

4.2.2.2.2 人员离岗 OPE_DIM.3

对准备离岗人员应该在离岗前进行核实检查和安全处理。

核实检查和安全处理的内容可能包括（但不限于）以下内容：

1) 立即中止解雇的、退休的、辞职的或其他原因离开的员工的所有访问。

2) 取回所有的身份证件、徽章、密钥、访问控制记号和其他有关安全的项目。

3) 收回机构提供的设备等等。

4) 当员工离职或换岗之前，需要对保密协议进行审查，必要时重新签署保密协议；需要进行安全审查，更换相关口令，删除相关帐号及权限。

4.2.2.2.3 安全培训 OPE_TRA.3

应当对各类人员进行安全意识教育和培训，制定详细的安全教育和培训计划并分批进行培训。包含以下工作：

1）安全技术、安全技能和安全操作培训：

✓ 对安全管理人员、安全技术人员、网络管理员、系统管理员、数据库管理员、软件开发人员等科技人员，进行安全技术和安全技能的培训。

✓ 对于运行维护人员、计算机操作人员，进行安全操作培训。

2）从事计算机应用的人员，均需通过有关部门组织的上岗培训，持证上岗。

3）安全管理、技术人员需要具备权威机构颁发的资质认证。

4）安全培训应该成为安全规划的一部分。

4.2.2.2.4 第三方访问 OPE_OTT.3

1) 第三方人员访问安全区域（例如机房、办公区域）时需要进行审批，由相关负责人审批通过后才能进入。

2) 对重要安全区域的访问，需要由接待人或指定专人陪同。

3) 制定第三方人员安全管理制度，严格按照制度对第三方人员进行管理，至少包括以下内容：

✓ 根据第三方人员的可信任程度、访问对象的安全级别、访问方式等等因素对第三方人员进行分类，针对不同类别的第三方人员采取相应的控制管理措施。

✓ 评估第三方人员的安全风险。

✓ 第三方人员的进出管理。

✓ 第三方人员的网络接入安全管理。

✓ 第三方人员的安全保密管理。

✓ 第三方人员的安全操作管理。

4) 与第三方人员签署保密协议，禁止第三方人员泄漏保密信息。

5) 除非必要，禁止第三方人员访问网络、操作重要的主机和设备。

6) 对第三方的访问的安全风险评估应该是定期进行，每年至少一次，及时

发现潜在的第三方安全威胁。

4.2.3 安全策略文档

4.2.3.1 PIN 类：安全策略制定与执行

4.2.3.1.1 安全策略范围 PIN_SCO.3

1) 应当拥有信息安全管理所必须的管理制度、管理规定和操作规程等信息安全管理规章制度。安全规章制度应该能够满足安全管理的基本需要，至少包括下面内容的策略文档：机房管理、防病毒管理、网络管理、安全操作规程、组织结构和岗位职责、数据备份等。

2) 拥有信息安全方针层面的规章制度，给出信息安全的定义、整体目标、指导原则、重要性、适用范围和安全工作的重点，为信息安全工作提供方向和指引。

3) 建立全面、严谨、科学的安全策略文档体系，能够完全满足信息安全管理的需求：

✓ 安全策略文档体系的内容涉及信息安全管理相关的各个方面：信息安全方针、安全组织、资产管理、人员安全、物理和环境安全、网络安全、主机安全、应用安全、数据安全、业务连续和应急响应、项目安全管理、运行维护、风险管理等。

✓ 安全策略文档体系的体系结构应包括信息安全标准、安全规范、安全指南、安全管理办法/规定/制度、安全操作规程、组织结构和岗位职责等。

4) 安全文档策略应该有良好的格式控制：要求风格基本统一，需要有良好的版本控制，需要有密级标识，需要有分发控制，需要注明批准人等。

5) 需要进行信息安全规划，信息安全规划包括长期（三年或更长）的安全规划和近期（一年）的安全规划，对安全工作、安全项目建设和信息安全投资进行规划，使安全工作和安全建设按计划推进。

4.2.3.1.2 安全策略执行 PIN_EXE.3

1) 应当有明确的规定，要求所有人员必须遵守安全策略文档。

2) 大部分员工知道与其相关的安全策略文档，并能够遵守安全策略文档。

3) 安全策略文档能够被有效执行。

4) 定期检查安全策略文档的执行情况。

5) 制定奖惩措施，明确违反安全策略文档的处罚措施，维护安全策略文档的有效执行。

6) 公布信息安全检查的结果，对发现的违反安全策略文档的情况进行通报和处罚。

7) 安全策略文档的执行情况与员工的绩效考核结合。

4.2.3.2PCO 类：安全策略发布与更新

4.2.3.2.1 策略发布 PCO_PUB.23

安全策略文档应该通过正式的有效的发布渠道进行发布，确认相关人员能够及时获取到安全策略文档。通过正式发布可以保证安全策略文档的权威性。正式发布根据企业的不同习惯，可采取正式发文、领导签署、策略文档盖公章等方式。

4.2.3.2.2 策略更新 PCO_UPD.3

定期对安全策略文档进行评审，检查安全策略是否适用和合理，回顾安全策略文档的执行效果，对不适用或不合理或欠缺的条款进行更新和补充。

附录 1：安全威胁详述

1 TFORCE 不可抗力

1.1 TFORCE.PEOP 关键人员损失

系统的关键维护人员损失（例如突然离职、生病等）可能导致系统恢复、升级等工作出现问题。

当损失的人员在 IT 领域中处于关键位置，并且无法被其他人员所代替时将导致技术专家的缺乏，甚至更为严重的后果。人员资源的损失可能也意味着专门知识和/或秘密信息的丢失。

对策：

- 关键岗位安全管理 OOR_KST
- 安全培训 OPE_TRA

1.2 TFORCE.FAIL IT 系统故障

IT 系统中单个组件的操作失败将导致整个 IT 操作的失败。当集成 IT 系统的组件存在开发瑕疵时，特别容易导致故障。例如，空气调节装置、电源、LAN 服务器或数据传输设备。

当 IT 系统出现故障时，不一定都是技术原因（如电源破坏），人员的错误（如因疏忽破坏设备或数据）或故意行为（如偷窃）也常是故障产生的原因。不可抗力也可能带来丢失会毁坏（如火灾、闪电、化学品事故），这时破坏的范围可能更大。

如果 IT 系统上运行的 IT 应用实时性要求较高，没有可用的替代系统时 IT 系统故障所带来的危害可能会十分严重。

对策：

- ✧ 主干网可用性保护TNI_AVI
- ✧ 主机设备维护OHO_EQI
- ✧ 网络可靠性管理ONE_REL
- ✧ 供电TPR_SUP
- ✧ 安全培训OPE_TRA
- ✧ OBC类：应急响应
- ✧ OOR类：安全组织和职责

1.3 TFORCE.THU 雷击和闪电

在雷阵雨的天气中，闪电是建筑物和安置在该建筑物中的 IT 设施的主要威胁。闪电所产生的成百上千伏电压和高达 200,000 安培的电流在 50~100μs 的时间中被释放。

如果建筑物直接被闪电击中，闪电的动态能量将会直接造成毁坏，包括建筑的物理毁坏（例如建筑物的屋顶和外表）；闪电所带来的火灾也会引起毁坏；超高电压会毁坏电子设备。

对策：

- ✧ 防雷击TPR_THU

1.4 TFORCE.FIR 火灾

将火灾所引起的危害和和其对建筑物和设备产生的危害分开，火灾带来的是系列危害，对 IT 系统而言这种危害是多维的。聚氯乙烯的燃烧产生氯气，这些气体和空气中的潮气以及灭火用水共同形成盐酸。出现火灾事故时这样的氯气通过空调系统扩散，导致那些 远离火灾现场敏感电子设备的损害。

火灾不仅仅是由易燃材料的处理不当引起的（如蜡烛等），也包括电子设备的使用不当。

以下的提到的内容和其他一些在此没有提出的事件都可能使火灾蔓延：

- 防火门被卡住

- 易燃材料存放不当
- 缺乏火灾检测设备
- 薄弱的火灾防范能力（如电缆缺乏防火绝缘层）

对策：

✧ 防火 TPR_FIR

1.5 TFORCE.WAT 水灾

指进入建筑物或房间的不可预知水流，这些威胁因素主要来源于：

- 雨、洪水
- 供水和排水系统的损坏
- 供热系统的损坏
- 连接到供水系统的空调系统损坏
- 洒水装置的问题
- 灭火系统所用的水

无论水是如何进入建筑物或房间的，存在的危险都是可能对供应设备或 IT 组件造成危害或导致其不可操作（如短路、设备毁坏或生锈等）。当中心供应设备在没有排水系统的建筑物的地下室时，进入的水将造成不可预测的危害。

对策：

✧ 防潮TPR_WAT

1.6 TFORCE.CON 温度和湿度超范围

每个设备都有它正常工作的温度范围。如果房间的温度在任何一个方向上超出这个范围，都将会导致服务的中断或设备的故障。

例如，安置在服务器房间中的设备消耗电能并加热了房间。如果通风不好，设备的操作温度可能升高。

服务器房间的窗子不该一直开着，例如在春天或秋天，这可能引起较大温度变化，导致温度下降。

对策：

✧ 空调TPR_CON

1.7 TFORCE.DUST 灰尘的积累

尽管电子器件在 IT 中扮演着越来越多的角色，它还要依赖于机械组件，包括磁盘（diskettes）、硬盘、可移动硬盘、磁盘驱动器、打印机、扫描器等，并且要为处理器和电源单元加上风扇。

对策：

- ✧ 机房管理OPM_ROM

1.8 TFORCE.MAG 强磁场导致数据丢失

运用磁存储介质的数据载体包括软磁盘、可移动硬盘和磁带。信息通过读写磁头写入这些介质。磁介质对磁场很敏感，因此这种存储介质不该被带到强磁场中，以防数据丢失。

对策：

- ✧ 电磁防护 TPR_TEM

2 TLIMIT 组织和管理缺陷

2.1 TLIMIT.DIS 安全管理规则和制度缺乏或不足

用于IT安全目的的组织规章和需求的重要性随着信息处理和信息处理过程中的保护需求的提高而提高。

规章涉及的范围很广，从职责分派到控制功能的分配。这些规则/规章的缺乏或不足将影响安全管理。

对策：

- ✧ 安全管理组织OOR_MNG
- ✧ 安全管理人员能力OOR_CAP
- ✧ 岗位安全职责OOR_STA
- ✧ 合作与沟通OOR_COM
- ✧ 安全策略范围PIN_SCO

- ✧ 安全策略执行PIN_EXE
- ✧ 策略发布PCO_PUB
- ✧ 策略更新PCO_UPD

2.2 TLIMIT.REQ 需求文档不明

单独一人所确定的需求文档不能确保IT操作的稳定性。需求文档必须为其适用对象知晓。当相关人员不能完全了解现存的需求文档时，不该以“我不知道这也是我负责的”或“我不知道该如何去做”作为推卸责任的借口。如：因处理软盘的职员经验不足可能造成计算机病毒的扩散。

对策：

- ✧ 岗位安全职责OOR_STA
- ✧ 人员录用OPE_DIM
- ✧ 安全培训OPE_TRA

2.3 TLIMIT.COMP 资源缺乏兼容性和适用性

资源提供不足会破坏IT相关操作。所需资源数量不足或没能按时提供可能导致服务中断。另外存在的问题也可能是所获取的是不合适或完全不是所需的资源。如：新采购的软硬件不兼容问题；新的数据传输线安装失败导致使用相关联接的IT操作失败；将不合适的连接线接到打印机上；计算机上的硬盘空间或主存不足导致新的数据库软件不能使用。

对策：

- ✧ 安全产品选型OEN_PRO
- ✧ 应用系统测试TCE_APT

2.4 TLIMIT.SUP 对 IT 安全措施监控不足

不对IT安全措施进行监控或者监控力度不足将无法确定这些措施是在被滥用还是在有效实施。对IT安全措施进行适当控制时才能使之更加有效，这些控制包括审计等。

对策：

- ✧ 存储介质的保护ORM_PRO
- ✧ 帐户管理OHO_ACC
- ✧ 存储介质的销毁ORM_DES
- ✧ 变更控制OCO_CHA
- ✧ 策略发布PCO_PUB

2.5 TLIMIT.MAI 缺乏维护或维护不足

系统的可操作性一定是基于定期维护的，缺乏维护或维护不足会导致无法估量的危害和后续影响。如：缺乏维护的 USP系统在电源出现故障时不能有效的发挥作用；缺乏维护的消防器材在出现火灾时失效；因通风维护不利导致激光打印机故障等。

对策：

- ✧ 安全策略范围PIN_SCO
- ✧ 账户管理OHO_ACC
- ✧ 安全策略执行PIN_EXE
- ✧ 安全产品选型OEN_PRO
- ✧ 变更控制OCO_CHA

2.6 TLIMIT.ROOM 未经允许进入需要保护的房间

如果未被授权的人员进入被保护的房间，所产生的危险不仅可能来自其故意的行为，也可能来自其不经意的行为。

对策：

- ✧ 门禁TPR_JAN
- ✧ 机房管理OPM_ROM
- ✧ 办公环境管理OPM_OFM

2.7 TLIMIT.PUR 未经许可使用权限

进入和访问硬件和软件的权限作为确保安全和IT系统正常使用的措施。如果这些权限被赋给不合适的人员或该权限被滥用，将削弱数据的机密性和完整性，也可能危及到计算机系统的可用性。

对策：

- ✧ 存储介质的保护ORM_PRO
- ✧ 环境设备维护OPM_MAI
- ✧ 账户管理OHO_ACC
- ✧ 岗位安全职责OOR_STA
- ✧ 配置管理计划OCO_PLA
- ✧ 配置管理能力OCO_CAP
- ✧ 网络设备管理授权ONE_ADV
- ✧ 脆弱性分析 ORA_VUL
- ✧ 网络边界访问控制TEB_NAC

2.8 TLIMIT.ERR IT 系统的变更错误

为IT系统和应用环境所创立的规则要遵从不断变化的需求，包括人员变化、职员搬到不同的房间、新软件或硬件的使用或补给链的变化。如果这些变更没能得到合适的调整将带来一定的风险。

对策：

- ✧ 账户管理OHO_ACC
- ✧ 岗位安全职责OOR_STA
- ✧ 安全策略范围PIN_SCO
- ✧ 配置管理计划OCO_PLA
- ✧ 变更控制OCO_CHA
- ✧ 存储介质的分类和归档ORM_CLA
- ✧ 配置管理自动化OCO_AUT
- ✧ 病毒和恶意代码防范TCE_VIR

- ✧ 系统安全检测和验收OEN_TES
- ✧ 存储介质的保护ORM_PRO
- ✧ 数据备份和恢复OBA_DAT

2.9 TLIMIT.AVI 数据存储介质在需要时不可用

数据媒体的正确使用对于IT应用处理特别重要。即使是最小的错误，如标识不足，存放地点不合适，缺乏数据媒体的输入或输出归档确认，这些使得不能在需要时及时定位获取数据媒体，这种结果的所产生的延迟会导致重大的危害。

比如：错误的将备份磁带归类为外部数据备份，因此，会因为无法及时获取磁带而延迟所需的数据恢复；错误的将存储不同内容的备份磁带分别标注，而不是按照时间进行标识导致新近的数据备份丢失。

对策：

- ✧ 存储介质的传输管理ORM_TRA
- ✧ 存储介质的访问控制ORM_ACO
- ✧ 存储介质的分类和归档ORM_CLA
- ✧ 存储介质的备份ORM_BAC
- ✧ 存储介质的销毁ORM_DES
- ✧ 变更控制OCO_CHA
- ✧ 病毒和恶意代码防范TCE_VIR
- ✧ 办公环境管理OPM_OFM

2.10 TLIMIT.BW 带宽规划不足

基于当前需求对网络带宽进行规划常会出现错误，其原因是：网络永远存在扩展需求；为满足数据传输需求必须增大网络带宽；鉴于网络的新需求，须安装其他类型电缆。

对策：

- ✧ 安全项目的立项管理OEN_CON
- ✧ 安全需求分析OEN_REQ

2.11 TLIMIT.CABL 布线文档不足

由于布线文档缺乏，无法确定电缆的精确位置，这可能导致建筑物内或外的电缆的毁坏，也可能拖延维修时间甚至是威胁生命，如发生电击。当管辖区域中添加新的终端设备时，文档不足使测试、电缆和跳线的维护和修理更难。

对策：

- ✧ 交付和运行OEN_ADO
- ✧ 电磁防护TPR_TEM

2.12 TLIMIT.COND 由于工作条件不佳有损 IT 使用

由于工作场所不能依据人体功效学或可操作环境（如灰尘和噪音等）进行组织，可能使IT设施无法使用或不适宜使用。

这部分指出的危害不会直接影响到IT设施的使用，而是使工作人员受到某种方式的影响，使其不能集中精力来完成任务，这些包括噪音、未组织的客人来访、房间灯光不合适或空调坏了，这些干扰降低了工作效率并且增加了许多小错误，这些不仅仅会影响工作而且也会使存储数据出现错误并且降低数据的完整性。

对策：

- ✧ 位置选择TPR_LOC
- ✧ 门禁TPR_JAN
- ✧ 机房管理OPM_ROM

2.13 TLIMIT.UNIX UNIX 系统敏感数据失去机密性

通过多种UNIX程序可能会读取/抽取与IT使用相关的数据，这些数据可能涉及许多用户执行任务的信息，因此必须关注秘密信息的保护。

对策：

- ✧ 远程访问TEB_TEL
- ✧ 计算环境访问控制TCE_TAC
- ✧ 身份鉴别TCE_IDT

- ✧ 安全审计TCE_SAU
- ✧ 主机入侵防范TCE_IDS
- ✧ 账户管理OHO_ACC
- ✧ 漏洞控制OHO_VER

2.14 TLIMIT.CHA 对便携电脑用户的变更不进行控制

便携式PC机用户的变更常常会被计算机的交接处理影响，用户无法检查计算机是否仍携带有敏感数据或计算机病毒。过了一段时间后无法确定谁在哪一段时间里在使用该计算机，甚至无法确定目前计算机是谁在使用。不对计算机的存储内容进行检查，不建立相关文档，对用户变化不进行控制使计算机的可用性降低并且会导致硬盘上残留的机密数据丢失。

对策：

- ✧ 办公环境管理OPM_OFM
- ✧ 账户管理OHO_ACC
- ✧ 漏洞控制OHO_VER
- ✧ 防病毒管理OHO_VIR
- ✧ 设备和系统冗余OBA_EQI
- ✧ 安全培训OPE_TRA

2.15 TLIMIT.MARK 数据存储介质标识不足

如果数据媒体进行交换时，媒体不能进行合适标识，接收者常常不能区分发送者所存储的信息或存储信息的目的。如果同一发送者规定几个数据媒体，标识不足可能导致数据乱序。

对策：

- ✧ 存储介质的分类和归档ORM_CLA
- ✧ 存储介质的访问控制ORM_ACO

2.16 TLIMIT.HAND 数据存储介质移交方式不当

如果数据存储媒体移交方式选择不当，存放在这些数据媒体中的机密数据可能落入非授权的人员手中或者不能及时到达目的地。

比如：错误的地址导致数据介质被传递给未经授权的人员；包装不善导致数据介质损坏或被未经授权人员获取；职责不明导致数据介质的处理被拖延；传递方式不当或说明不清导致数据介质延期到达；发送端职责不明导致数据介质传递被延迟。

对策：

- ✧ 存储介质的传输管理ORM_TRA
- ✧ 存储介质的访问控制ORM_ACO
- ✧ 存储介质的分类和归档ORM_CLA
- ✧ 存储介质的传输管理ORM_TRA
- ✧ 密钥管理OCO_KEY
- ✧ 存储介质的备份ORM_BAC

2.17 TLIMIT.KEY 密钥管理不当

如果加密系统被用于保护数据传输过程中的机密性，密钥管理不当将会给被保护内容带来损害。比如：密钥在不受保护的环境中产生或保存；密钥不合适或容易被猜到；加密或解密密钥没能通过安全途径发送给使用者。

对策：

- ✧ 密钥管理OCO_KEY
- ✧ 安全培训OPE_TRA
- ✧ 人员录用OPE_EMP
- ✧ 岗位安全职责OOR_STA

2.18 TLIMIT.REX 调换用户管理不当

如果有多个用户在不同时间工作在一个 IT 系统上，用户的调换是不可避免

的。如果组织和管理不充分就可能会不满足安全需求，造成这些问题的原因可能包括：

- 当前应用不能正确关闭
- 当前数据没存储
- 数据被保存在主存或临时文件中
- 前一个用户没有退出登录
- 新用户不能正确登录到 IT 系统

对策：

✧ 计算环境访问控制TCE_TAC

✧ 岗位安全职责OOR_STA

2.19 TLIMIT.AUD 缺乏对审计数据的评估

审计数据提供了检测已经发生的危害或危害企图的行为方式。审计的更深一步功能在于其威慑功能。如果审计数据能被定期评估攻击企图就能尽早被检测到，相反，如果不对审计数据进行评估或评估力度不够将丧失其威慑功能。

还有许多 IT 系统或应用缺乏足够的审计能力。

对策：

✧ 安全审计TCE_SAU

✧ 安全产品选型OEN_PRO

2.20 TLIMIT.CONF 被保护网络的敏感数据丧失机密性

如果防火墙保护的网络被连接到外部网络（如 Internet），各种来自内部网络的数据包括邮件地址、IP 地址、计算机名和用户名能在外网获取。从这些数据可以推导出内部网络结构和用户。入侵者获取更多的信息将会给网路带来更大的风险。例如可以通过用户名可以对口令进行强力破解。

对策：

✧ 网络边界访问控制TEB_NAC

✧ 网络入侵防范TEB_IDS

2.21 TLIMIT.DOC 文档缺乏或不足

各种文档都应被考虑，产品描述、管理员和用户手册等。如果 IT 系统相关的文档缺乏或不足在危害发生时会影响处理决定。

如果在硬件故障和程序问题出现时文档不足会延迟错误纠正的时间或导致修复行为错误。

对策：

- ✧ 配置管理能力OCO_CAP
- ✧ 变更控制OCO_CHA

2.22 TLIMIT.DOMAIN 域规划不足

网络中的域和它们之间关系的规划不足，会导致域中的信任关系不再可信。

对策：

- ✧ 安全域规划ONE_SED

2.23 TLIMIT.CTRL 通讯线路的使用失控

在 IT 系统（传真、调制解调器或 ISDN 卡）里通讯卡的使用中，无法明确的显示是否有更多的数据被传递给其他用户。一旦被激活，通讯卡就可能无需用户激活和用户不期望的终端之间建立连接。另外，第三方也可能访问用户所不知道的远程功能。如：传真卡安装时会向厂家发送用户的初始信息；大量的调制解调器支持远程访问 IT 系统的功能，因此 IT 系统可能会被从外部通过调制解调器所操纵。

对策：

- ✧ 办公环境管理OPM_OFM

2.24 TLIMIT.DATA 数据库安全机制实现不够

数据库软件通常包括大量安全机制以保护数据不被非授权访问和入侵。然而，大多数安全机制不是自动启用的，如果这些机制不能使用，数据的机密性和

安全性都不能保证。

对策：

- ✧ 数据库设计安全TCE_DBS
- ✧ 主机设备维护OHO_EQI

2.25 TLIMIT.COM 网络组件不兼容

运用未完全标准化通讯协议的网络组件可能会因为不兼容存在问题。这时，厂商需要对组件所缺失的部分进行补充，或者使用部分可用的标准。主动网络组件来自于不同的厂商则可能会引起类型的不兼容。

处于同一网络上对同一协议进行不同实现的主动组件会削弱整个网络、某些网络片断或某些服务的的可用性。两种典型的不兼容情况为：通讯协议彼此不能通讯，导致相关组件不能通讯；即使组件之间能够通讯，但某些服务的实现方式不同，导致这些服务不可用。

对策：

- ✧ 安全需求分析OEN_REQ
- ✧ 安全功能规范OEN_FSP
- ✧ 系统安全检测和验收OEN_TES
- ✧ 应用系统测试TCE_APT

2.26 TLIMIT.BUG 网络设计缺陷

能否正确规划网络安装和扩展确定了所有网络操作的成功与否，IT 日益缩短的创新周期给那些由于设计原因不能满足新需求的网络带来了挑战，因此极易出现瓶颈，如：

- 网络设计必须和网络用户的需求一致，否则会给网络或其中的网络片断的完整性带来威胁；
- 新应用需要的带宽高于网络规划阶段，这将降低网络的可用性。

对策：

- ✧ 安全需求分析OEN_REQ

- ✧ 安全功能规范OEN_FSP
- ✧ 安全项目的立项管理OEN_CON
- ✧ 网络拓扑设计和规划ONE_TOP
- ✧ 安全域规划ONE_SED
- ✧ 网络可靠性管理ONE_REL
- ✧ 主干网可用性保护TNI_AVI

2.27 TLIMIT.DIM 超过线缆/总线长度或环的尺寸

为了确保应用标准决定的网络功能，网络中线缆的最大长度以及最大环尺寸需要确保和线缆的类型、拓扑和所涉及的协议一致。超长线缆、总线或环延长了信号传输时间，超过了传输协议类型规定的限制，降低了这部分网络的可用性或通讯带宽。

对策：

- ✧ 网络拓扑设计和规划ONE_TOP
- ✧ 安全需求分析OEN_REQ
- ✧ 安全功能规范OEN_FSP
- ✧ 主干网可用性保护TNI_AVI

2.28 TLIMIT.TRANS 文件和数据存储介质的不安全传递

文件、数据存储介质和文件在办公机构和其他地方（如家里的工作站）之间运输传递时，可能存在这些危险：

- 丢失
- 偷窃
- 被查看或操纵
- 交给未经授权的接收者

那些不存在拷贝的条目的毁坏、机密性丢失或被操纵会带来严重的危害。

对策：

- ✧ 存储介质的传输管理ORM_TRA

- ✧ 存储介质的备份ORM_BAC
- ✧ 数据备份和恢复OBA_DAT

2.29 TLIMIT.HOM 数据存储介质和文档在家里的办公环境中放置不当

在家办公时想安全地放置数据存储介质和文档是困难的，第三方可能从文档和数据载体中全部或部分的获取数据，所造成的结果依赖于被偷窃的信息的价值

对策：

- ✧ 应急响应计划的制定OBC_EST
- ✧ 存储环境管理ORM_CIR
- ✧ 办公环境管理OPM_OFM
- ✧ 数据备份和恢复OBA_DAT

2.30 TLIMIT.TRA 远程工作人员培训不足

在家工作的远程工作人员主要依赖自己来解决问题，这就意味着他们必须比那些在办公场所工作的员工更熟悉 IT 系统。如果远程工作人员不能充分熟悉 IT 系统，就可能在出现问题时导致系统长时间无法恢复。

对策：

- ✧ 人员录用OPE_EMP
- ✧ 安全培训OPE_TRA
- ✧ 安全策略执行PIN_EXE
- ✧ 安全管理组织OOR_MNG
- ✧ 应急响应计划的制定OBC_EST

2.31 TLIMIT.DEL 临时远程工作人员引发的延迟

通常远程工作人员在家工作时不能遵守固定的工作时间。当一个工作被分为两部分，一部分由远程工作人员在家完成，另一部分由其他员工在办公室完成，

如果远程工作人员工作中需要获取或提供信息，将会在操作上带来延迟。即使通过电子邮件及时进行信息传输也不会缩短响应时间，这是因为远程工作人员无法确保定期阅读邮件。

对策：

- ✧ 人员录用OPE_EMP
- ✧ 安全培训OPE_TRA
- ✧ 安全策略执行PIN_EXE
- ✧ 安全管理组织OOR_MNG
- ✧ 合作与沟通OOR_COM

2.32 TLIMIT.TEL 远程工作人员被较差地集成到工作流中

远程工作人员主要在家中工作不会每天出现在办公室中，因此他们很少有机会参与和上司与同事之间地信息交流，这导致他们与整个机构间从属关系的意识淡薄。

信息不足导致远程工作人员所获取的安全信息不足或相对滞后，典型的例子就是关于计算机病毒的报警信息。

对策：

- ✧ 人员录用OPE_EMP
- ✧ 安全培训OPE_TRA
- ✧ 安全策略执行PIN_EXE
- ✧ 安全管理组织OOR_MNG
- ✧ 合作与沟通OOR_COM

2.33 TLIMIT.RES 当 IT 系统崩溃时响应时间比较长

当远程工作人员不能自行修好家里崩溃的 IT 系统时，不得不由 IT 系统工作专家到远程人员家中对系统进行修复，或者将崩溃的系统送到修理部门，这一过程将花费一定的时间，在系统维护或新组件/软件安装时也会出现相同的情况。

对策：

- ✧ 应急响应计划的制定OBC_EST
- ✧ 应急响应计划的测试和演练OBC_TES
- ✧ 安全策略执行PIN_EXE
- ✧ 安全策略范围PIN_SCO

2.34 TLIMIT.SUB 远程工作人员更替制度不当

通常远程工作人员都认为自己能长时间独立工作，但存在的问题是当远程工作人员病倒时很难找到替代者。如果在远程工作人员家和办公机构之间没有一条快速安全有效的途径，那么将病倒的远程工作人员家中的文件和数据传输到办公机构是困难的。

对策：

- ✧ 安全策略范围PIN_SCO
- ✧ 安全策略执行PIN_EXE
- ✧ 应急响应计划的制定OBC_EST

2.35 TLIMIT.CON 部分隐藏数据导致机密性丧失

在电子数据传输或通过数据存储介质传输过程中，那些不该被传输的信息频频被传递。导致信息无意中被传输的原因主要有：

- 文件可能包括某些隐藏不可见的文本片断，而这些文本片断可能包括那些不该被接收者看到的信息。
- 标准软件创建的文件包括文本处理或电子制表的程序，这些程序包括了目录结构、版本号、创建者、修改时间、最后一次打印时间、文件名字和文件描述符等额外信息。
- 如果文件被拷贝到软盘中，全部的物理存储块将被填满。如果原始文件不要求完整的内存块，IT 系统用隐藏数据填满了未用的块。

对策：

- ✧ 存储介质的传输管理ORM_TRA
- ✧ 存储介质的访问控制ORM_ACO

- ✧ 存储介质的销毁ORM_DES

2.36 TLIMIT.MED 用于应急的介质存储量不足

当 IT 系统毁坏时，必须将需要恢复的数据拷贝到分离的存储介质中，在数据库这种复杂数据结构中更应如此。数据恢复不一定总是顺利和无错误的，如果存储空间不足，应急过程中草率的举动可能造成额外的数据丢失。

对策：

- ✧ 应急响应计划的制定OBC_EST
- ✧ 应急响应计划的测试和演练OBC_TES
- ✧ 设备和系统冗余OBA_EQI
- ✧ 存储介质的备份ORM_BAC

2.37 TLIMIT.REG 未注册组件操作

系统管理员应该知道所有的网络组件。系统新组件在组织一层应该由系统管理员进行注册并发布，未被注册的组件存在安全风险。

对策：

- ✧ 安全管理人员能力OOR_CAP
- ✧ 安全策略执行PIN_EXE
- ✧ 岗位安全职责OOR_STA
- ✧ 安全培训OPE_TRA

2.38 TLIMIT.POL 网络和管理系统的策略不足或没落实

如果网络管理和系统管理没有全面的管理策略，会由于个人误解所进行的错误配置造成严重的问题，甚至可能引起系统在网络层面上完全崩溃。这种情况在具有多个域的大网络上尤为明显。

比如：管理策略出台前不能有效的分析需求；购买不可管理的组件；相关部分管理不协调；没有集成管理软件。

对策：

- ✧ 安全需求分析OEN_REQ
- ✧ 安全项目的立项管理OEN_CON
- ✧ 安全功能规范OEN_FSP
- ✧ 安全策略范围PIN_SCO
- ✧ 策略发布PCO_PUB
- ✧ 策略更新PCO_UPD
- ✧ 安全管理组织OOR_MNG
- ✧ 安全策略执行PIN_EXE

2.39 TLIMIT.PRI 未经授权收集私人信息

使用管理系统时，通常会产生大量的审计数据，这些数据应自动生成并进行评估。对网络和系统监控而言更该如此，比如不保存详细的系统行为信息，也就不可能检查出安全问题。监控系统需要确定哪些信息可以被访问，哪些用户可以访问这些信息。出于对安全因素的考虑需要对用户行为进行监控，监控者需要通知监控所涉及的用户。

在网络修订框架中，必须检查落实管理策略所涉及的需求，当管理系统执行某一常见功能时，可能会将临时日志存放在保护性很差的地方，导致包含了用户信息的日志文件存在被访问的可能性。

对策：

- ✧ 安全策略范围PIN_SCO
- ✧ 策略发布PCO_PUB
- ✧ 策略更新PCO_UPD
- ✧ 安全审计TCE_SAU
- ✧ 账户管理OHO_ACC
- ✧ 身份鉴别TCE_IDT
- ✧ 网络设备用户身份鉴别TNI_IDT
- ✧ 安全需求分析OEN_REQ
- ✧ 高层安全设计OEN_HLD

2.40 TLIMIT.EME 安全事件处理不当

在实践中采用再多的安全措施也不能消除那些危害极大的潜在安全事件出现的几率，如果不能在安全问题出现时采取恰当的措施，将会出现巨大的危害或信息丢失以至于发展为灾难。

对策：

- ✧ 应急响应计划的制定OBC_EST
- ✧ 选择安全控制措施ORA_CTR
- ✧ 安全策略执行PIN_EXE
- ✧ 安全策略范围PIN_SCO
- ✧ 策略发布PCO_PUB
- ✧ 策略更新PCO_UPD
- ✧ 安全管理组织OOR_MNG

2.41 TLIMIT.SAMBA SAMBA 配置复杂

SAMBA是一个用于UNIX操作系统的免费软件包，它在SMB（Server Message Block）和CIFS（Common Internet File System）协议之上提供了文件、打印和认证服务。其配置中可能会忽略某些方面，目录和文件的访问权限设置问题等

对策：

- ✧ 配置管理计划OCO_PLA
- ✧ 变更控制OCO_CHA
- ✧ 选择安全控制措施ORA_CTR
- ✧ 安全管理人员能力OOR_CAP

2.42 TLIMIT.SEC IT 安全缺乏或不足

现今许多企业内的 IT 系统很复杂，系统的组织化趋势使得对 IT 系统有组织的规划、实现和监控势在必行。实践证明仅仅布置安全措施是不够的，或缺乏时间来贯彻这些措施，安全措施的布置常常和个人（特别是 IT 用户）相关。因此

安全措施的实施往往不合要求，以至于无法达到满意的安全级别。即使能满足所需的安全级别也要不停的进行调整。

安全管理不足常常是整体管理水平差的表现，如：缺乏个人责任感；管理支持不足；策略和概念上的需求不足；投资不足或方向错误；安全概念无法实施；安全处理更新失败等。

对策：

- ✧ 安全需求分析OEN_REQ
- ✧ 安全项目的立项管理OEN_CON
- ✧ 安全功能规范OEN_FSP
- ✧ 安全管理组织OOR_MNG
- ✧ 安全策略执行PIN_EXE
- ✧ 选择安全控制措施ORA_CTR
- ✧ 人员录用OPE_EMP
- ✧ 安全培训OPE_TRA
- ✧ 岗位安全职责OOR_STA
- ✧ 安全管理人员能力OOR_CAP
- ✧ 安全策略范围PIN_SCO
- ✧ 策略发布PCO_PUB
- ✧ 策略更新PCO_UPD

3 THUMAN 人为疏忽

3.1 THUMAN.MIST IT 用户错误导致数据机密性/完整性丢失

IT用户的不当行为可能引起数据机密性/完整性丢失，危害的范围依赖于所涉及数据的灵敏性。这些行为包括：与人员相关数据的打印内容被留在打印机上；没有将先前的数据删除就将软盘发出；因错误授权导致某职员能够修改数据而无法评估这种行为对完整性的影响；新软件用非匿名数据进行测试，导致雇员访问

非授权信息。

对策：

- ✧ 应急响应计划的制定OBC_EST
- ✧ 选择安全控制措施ORA_CTR
- ✧ 安全培训OPE_TRA
- ✧ 岗位安全职责OOR_STA
- ✧ 安全策略执行PIN_EXE
- ✧ 安全管理组织OOR_MNG
- ✧ 存储介质的访问控制ORM_ACO
- ✧ 存储介质的销毁ORM_DES

3.2 THUMAN.NEG 因疏忽大意破坏设备或数据

疏忽以及未受训练的操作可能给设备或数据带来损坏，这将严重的损害IT系统的进一步操作。对于IT应用的不适当使用也能导致这样的危害，以至于产生错误的结果、无意中修改或删除数据。一个删除命令的无意使用可能删除整个文件结构。

对策：

- ✧ 安全培训OPE_TRA
- ✧ 安全策略执行PIN_EXE
- ✧ 岗位安全职责OOR_STA
- ✧ 安全管理组织OOR_MNG
- ✧ 安全管理人员能力OOR_CAP
- ✧ 数据备份和恢复OBA_DAT
- ✧ 应急响应计划的制定OBC_EST

3.3 THUMAN.EXE 不执行 IT 安全措施

由于疏于检查或检查不充分，人员常常不能完全或完全不执行所推荐和规定的IT安全措施。那些原本可以预防或者本降低到最低点的危害发生。如果相应人

员在被漠视的措施中处于重要的位置时，严重的危害就会发生。

由于缺乏安全意识，IT安全措施频频被忽视。典型的现象就是漠视重复出现的错误信息。

对策：

- ✧ 人员录用OPE_EMP
- ✧ 安全培训OPE_TRA
- ✧ 岗位安全职责OOR_STA
- ✧ 安全管理组织OOR_MNG
- ✧ 安全管理人员能力OOR_CAP
- ✧ 安全策略执行PIN_EXE
- ✧ 应急响应计划的制定OBC_EST
- ✧ 选择安全控制措施ORA_CTR

3.4 THUMAN.PER 未经许可的电缆连接

除了技术故障之外，未被许可的连接产生错误连线，如当为跳线和接合分配器接设线缆时，文档错误和线缆标识不足常会导致无意错误或者错误检测变得复杂。由于存在非授权连接，数据可能被传输到错误的地址。

对策：

- ✧ 安全需求分析OEN_REQ
- ✧ 安全功能规范OEN_FSP
- ✧ 电磁防护TPR_TEM
- ✧ 位置选择TPR_LOC

3.5 THUMAN.CAB 因疏忽造成的电缆损害

若在电缆的铺设过程中缺乏保护则存在因疏忽而对电缆造成危害的风险。这样的危害不一定会立即导致连接的中断。这种情况可能会导致意外出现未被允许的连接。

这种危害比较典型的例子有：

- 建筑物内：
  - 设备电缆被强行拉出
  - 隐蔽电缆在钻或钉过程中被损坏
  - 窗沿或窗台电缆管道进水
  - 在建筑物清洁过程中地下管道或地板下管道进水
  - 搬运大物体时那些暴露在墙或地板上的线缆被毁坏
- 建筑物外：
  - 低成本建筑过程中线缆的损害
  - 地下线缆进水

对策：

- 位置选择TPR_LOC
- 防火TPR_FIR
- 防潮TPR_WAT
- 第三方访问OPE_OTT

3.6 THUMAN.CLE 清洁人员或外来人员带来的危害

清洁人员和外来人员所带来的危害程度不等：如技术设备的不适当处理；试图使用 IT 系统；偷窃 IT 组件。

对策：

- 选择安全控制措施ORA_CTR
- 第三方访问OPE_OTT
- 安全策略范围PIN_SCO
- 数据备份和恢复OBA_DAT
- 存储环境管理ORM_CIR
- 存储介质的备份ORM_BAC

3.7 THUMAN.ITU IT 系统使用不当

IT 系统的不当使用包括对 IT 安全措施的忽视或无知，这将危及系统安全。

如果用户能获取正确操作和 IT 系统的信息则这种情况可能被避免。如：权限过于宽松；口令简单易猜；无意删除；未经授权人员访问数据介质和备份等。

对策：

- ✧ 安全培训OPE_TRA
- ✧ 人员录用OPE_EMP
- ✧ 第三方访问OPE_OTT
- ✧ 安全策略执行PIN_EXE
- ✧ 安全管理组织OOR_MNG
- ✧ 安全管理人员能力OOR_CAP
- ✧ 账户管理OHO_ACC
- ✧ 身份鉴别TCE_IDT
- ✧ 网络设备用户身份鉴别TNI_IDT
- ✧ 应急响应计划的制定OBC_EST

3.8 THUMAN.ITS IT 系统管理不当

不当的 IT 系统管理将威胁系统的安全。如那些没有定期对 IT 系统进行必要操作，或建立了面临巨大威胁的网络站点而且没有防护措施。

对于安全配置和扩展访问权限的每一次修改都可能为整个安全带来威胁。

对策：

- ✧ 配置管理计划OCO_PLA
- ✧ 数据备份和恢复OBA_DAT
- ✧ 变更控制OCO_CHA
- ✧ 配置管理能力OCO_CAP
- ✧ 安全管理人员能力OOR_CAP
- ✧ 安全策略执行PIN_EXE
- ✧ 安全管理组织OOR_MNG
- ✧ 安全培训OPE_TRA
- ✧ 应急响应计划的制定OBC_EST
- ✧ 安全策略范围PIN_SCO

- ✧ 策略发布PCO_PUB
- ✧ 策略更新PCO_UPD

3.9 THUMAN.UNIX UNIX 文件系统的错误输出

UNIX 的标识在文件/etc/exports 或/etc/dfs/dfstab 中有说明。这样计算机的用户可以被设定为任何的 UID 和 GID。只有目录使用了选项 root=, UID 0(root)时没有输出，当访问NFS服务器时，通常被映射为不同的UID（对用户而言就是nobody或 anonymous）。因此，仅仅那些属于 root 的文件被保护着。

利用 NFS 协议来输出文件系统或用 NIS 来分发系统文件时没有足够的保护措施用来保护这样的环境。这样的应用将为系统完整性带来威胁。

对策：

- ✧ 账户管理OHO_ACC
- ✧ 身份鉴别TCE_IDT
- ✧ 安全审计TCE_SAU
- ✧ 安全策略执行PIN_EXE
- ✧ 应急响应计划的制定OBC_EST
- ✧ 数据备份和恢复OBA_DAT

3.10 THUMAN.MAIL 邮件发送系统配置不当

过去邮件发送系统配置中的错误不断导致被影响的IT系统的安全泄漏（比如Internet蠕虫）。

对策：

- ✧ 防病毒网关TEB_TVI
- ✧ 病毒和恶意代码防范TCE_VIR
- ✧ 应用系统测试TCE_APT
- ✧ 系统安全检测和验收OEN_TES
- ✧ 安全需求分析OEN_REQ
- ✧ 安全功能规范OEN_FSP

3.11 THUMAN.LOSE 传递过程中数据存储介质丢失

数据媒体递送过程中没有进行好的包装（邮件信封），则包装的毁坏可能导致数据媒体的丢失（特别是软盘的丢失）。在邮递过程中也可能由于部分邮递人员的数据发生数据媒体丢失。例如，将软盘和信件放入一个大信封进行邮递，可能会因为不注意信封内物品而丢失。

对策：

- ✧ 存储介质的访问控制ORM_ACO
- ✧ 存储介质的传输管理ORM_TRA
- ✧ 存储介质的备份ORM_BAC

3.12 THUMAN.TRANS 错误或非预期的数据传输

被传递的数据存储介质可能包括早先的不能传递给接收者的保密的事务数据。如果没有主动的删除这些数据，数据媒体的接收者可能会看到这些数据。

如果被传输的数据所在的目录中包含额外的需要保护的数据，就存在它在不经意之间被也被传送到数据媒体上，使非授权的接收者可以访问这些数据。

如果数据记录不得不通过数据网络而不是存储介质进行传输（例如通过Internet，调制解调器连接，E-mail），通讯程序可能提供使用描述复杂的地址和分发列表。如果这样的分发没能集中保管或没能定期进行更新，数据记录可能被发送到那些没能授权的人员。

对策：

- ✧ 存储介质的保护ORM_PRO
- ✧ 存储介质的访问控制ORM_ACO
- ✧ 存储介质的传输管理ORM_TRA
- ✧ 存储环境管理ORM_CIR
- ✧ 存储介质的销毁ORM_DES
- ✧ 密码技术TNI_ENC

3.13 THUMAN.PUR 站点和数据访问权限管理不当

IT系统、存储数据和IT应用的访问权限应该被授予来执行必需的任务。这些权限授予不当可能导致操作故障。

对策：

- ✧ 人员录用OPE_EMP
- ✧ 安全培训OPE_TRA
- ✧ 岗位安全职责OOR_STA
- ✧ 账户管理OHO_ACC
- ✧ 身份鉴别TCE_IDT
- ✧ 网络设备用户身份鉴别TNI_IDT
- ✧ 安全审计TCE_SAU
- ✧ 安全域规划ONE_SED
- ✧ 选择安全控制措施ORA_CTR
- ✧ 安全策略执行PIN_EXE

3.14 THUMAN.CHA PC 用户的错误变更

当多个用户在一个PC机上工作时，可能会发生前一个用户还没退出登录，新来的用户不能正常登录，导致系统出现故障，如审计信息不可靠。

对策：

- ✧ 账户管理OHO_ACC
- ✧ 身份鉴别TCE_IDT
- ✧ 安全审计TCE_SAU
- ✧ 网络设备管理授权ONE_ADV
- ✧ 远程登陆管理OHO_TEL
- ✧ 变更控制OCO_CHA
- ✧ 安全策略执行PIN_EXE
- ✧ 安全管理组织OOR_MNG
- ✧ 安全培训OPE_TRA

- ✧ 岗位安全职责OOR_STA

3.15 THUMAN.SHA 共享目录、打印机或剪贴版

在运行在域中的Windows操作系统的计算机上使用文件或打印机管理器，共享目录、打印机或剪贴板时可能出现操作错误，必要的口令保护使用不当或根本没有使用口令，这些会导致资源无意中共享。使用Windows系统时为了共享必须清楚的进行授权，因此每一个用户不得不决定谁的访问被允许。

由于共享资源对所有的参与者是可视的，其他的参与者可以探测或滥用这一情况。可能发生不经授权阅读、改变或删除机密数据的问题。

共享目录可能自动进行，如果选择“下次启动时共享”，系统就会在下一次启动后自动共享，这时需要手动修改。

对策：

- ✧ 账户管理OHO_ACC
- ✧ 身份鉴别TCE_IDT
- ✧ 安全审计TCE_SAU

3.16 THUMAN.REG 注册表修改不当

Windows允许在限定PC的用户环境。通常这些能通过系统的编辑器（POLEDIT.EXE）或注册表编辑器（REGENDIT.EXE）这些程序使用中必须小心。注册表的变化应该仅仅应该由训练过的人员来完成。由于系统能很快的被放置到一个状态和PC机共同工作不可能的。最糟的情况时操作系统不得不被重装或某个硬件组件不得不被重新初始化（安装合适的驱动）

对策：

- ✧ 变更控制OCO_CHA
- ✧ 配置管理能力OCO_CAP
- ✧ 安全培训OPE_TRA
- ✧ 安全管理人员能力OOR_CAP
- ✧ 安全策略执行PIN_EXE

- ✧ 应急响应计划的制定OBC_EST
- ✧ 选择安全控制措施ORA_CTR

3.17 THUMAN.DBMS DBMS 系统管理不当

数据库管理系统管理中的疏忽或不当可能引起下列危害：数据丢失；（有意或无意）的数据被操纵；可信数据的未授权访问；数据库完整性缺失；数据库崩溃；数据库毁坏。

对策：

- ✧ 数据备份和恢复OBA_DAT
- ✧ 安全功能规范OEN_FSP
- ✧ 数据库设计安全TCE_DBS
- ✧ 身份鉴别TCE_IDT
- ✧ 账户管理OHO_ACC
- ✧ 安全审计TCE_SAU

3.18 THUMAN.UNC 无意中对数据操作

某一用户访问数据库的权限越多，无意中对数据的操作的风险就越大。这无法通过应用程序来防止。无意中对数据的操作的基本原因包括：

- 缺乏技术知识，或技术知识太差；
- 缺乏应用相关知识，或这些知识太差；
- 权限授予过于广泛；
- 疏忽

对策：

- ✧ 安全培训OPE_TRA
- ✧ 安全管理人员能力OOR_CAP
- ✧ 安全审计TCE_SAU
- ✧ 账户管理OHO_ACC
- ✧ 身份鉴别TCE_IDT

✧ 数据备份和恢复OBA_DAT

3.19 THUMAN.CONF 网络组件的配置不当

由于网络组件的配置不当则导致整个网络或这部分网络的可用性或信息的机密性以及数据的完整性被削弱。下面给出几种典型的错误配置：

• 网络组件被用于构建VLAN以实现网络的逻辑划分；配置不正确会导致VLAN内部或VLAN之间的通讯崩溃；

• 网络通过路由器进行划分，路由配置需配置得当；

对策：

✧ 安全域规划ONE_SED

✧ 网络可靠性管理ONE_REL

✧ 网络拓扑设计和规划ONE_TOP

✧ IP地址管理ONE_IPM

✧ 路由管理ONE_ROU

3.20 THUMAN.VLAN 未进行网络划分或网络划分不当

本地网络可以进行物理划分，或通过合适的VLAN配置进行逻辑划分。这时，连接网络的IT系统被分为多个部分。这不仅提高了网络的负载共享能力，而且便于管理。然而，这种做法会带来相应的威胁：

• 丢失可用性；

• 机密性保护不足；

对策：

✧ 安全域规划ONE_SED

✧ 网络可靠性管理ONE_REL

✧ 网络拓扑设计和规划ONE_TOP

✧ 安全需求分析OEN_REQ

✧ 应急响应计划的制定OBC_EST

3.21 THUMAN.ACC 私人未经授权使用远程工作站

职员在家中使用远程工作站很容易，因为监控这样应用的能力有限。这可能导致安装的软件不能被检测，或感染了病毒的数据被存放到远程工作站上。远程工作者以及亲属非授权使用远程工作站是可能的。特别是孩子和青少年可能会试图使用专用的工作站来玩游戏，而远程工作者没有意识到这些行为存在潜在危害，如：硬盘擦掉导致数据完全丢失，使公司承担重新安装和数据重新录入的费用。

对策：

- ✧ 选择安全控制措施ORA_CTR
- ✧ 应急响应计划的制定OBC_EST
- ✧ 远程登陆管理OHO_TEL
- ✧ 安全审计TCE_SAU
- ✧ 防病毒网关TEB_TVI
- ✧ 病毒和恶意代码防范TCE_VIR
- ✧ 主机入侵防范TCE_IDS
- ✧ 网络入侵防范TEB_IDS
- ✧ 人员录用OPE_EMP
- ✧ 第三方访问OPE_OTT
- ✧ 数据备份和恢复OBA_DAT

3.22 THUMAN.FRA 数据库未结构化

不适当的指令和/或缺乏职员训练可以导致数据存储介质上数据库混乱，这能导致各种问题，例如：

- 多次存储相同的数据将会浪费磁盘空间
- 匆忙地删除或不删除数据
- 未经授权的访问
- IT系统和不同的目录的版本号不一致

经验有限的新IT人员不能明确数据库结构的重要性，由于职员将所有的数据

存放在根目录而不单独创建子目录，因此易发生问题。

对策：

- ✧ 安全培训OPE_TRA
- ✧ 存储介质的保护ORM_PRO
- ✧ 存储介质的备份ORM_BAC
- ✧ 存储介质的分类和归档ORM_CLA
- ✧ 存储介质的传输管理ORM_TRA

3.23 THUMAN.ENC 加密模块使用不当

实践中，在许多情况下加密模块使用不当会带来危害，不当使用会带来各种结果。

- 数据传输前不能编码；
- 加密代码输入时部分输入不正确导致发送者和接收者都无法解码编码后的数据；
- 编码过程中电源突然中断导致部分数据已经编码，部分数据尚未编码，这种情况下编码的数据不能解码；
- 一些解码参数输入不正确可能导致加密算法数位不足或使用不安全的加密编码；

对策：

- ✧ 密码技术TNI_ENC
- ✧ 密钥管理OCO_KEY

3.24 THUMAN.CON 管理系统配置不当

为使网络系统和/或系统管理系统能被安全使用，所有组件的配置必须一致。尽管单独组件常常被中心平台管理，系统管理却由大量分布在网络中的单个组件构成。这些系统的配置应该一致。如果配置的一致性被损坏无论是有意还是无意组件都无法协调工作。

对策：

- ✧ 应急响应计划的制定OBC_EST
- ✧ 配置管理计划OCO_PLA
- ✧ 配置管理自动化OCO_AUT
- ✧ 配置管理能力OCO_CAP

3.25 THUMAN.SER 操作过程中服务器失效

如果网络通过管理系统进行管理，存在执行特定任务的服务器。存放管理信息的数据库被保存在管理服务器上。如果这样的服务器在操作中失效，那些存放在计算机内存中的数据不能被写回文件系统，结果导致管理数据的不一致性。因此大的管理系统趋向于使用具有转回较旧状态的机制的数据库。这减少了风险但不能完全规避风险。

对策：

- ✧ 选择安全控制措施ORA_CTR
- ✧ 应急响应计划的制定OBC_EST
- ✧ 数据备份和恢复OBA_DAT
- ✧ 设备和系统冗余OBA_EQI

3.26 THUMAN.MIS 事件的误解

使用管理系统时，系统管理员负责分析和解释管理系统的信息以便能采取合适的措施。系统管理员必须能识别错误的警报和不正确的信息，如果系统管理员不能正确的解释系统信息用于系统的对策可能使系统更糟。

对策：

- ✧ 安全培训OPE_TRA
- ✧ 安全策略执行PIN_EXE
- ✧ 安全管理组织OOR_MNG
- ✧ 安全管理人员能力OOR_CAP

3.27 THUMAN.CONFIG 配置和操作中的错误

当程序的参数和选项设置不正确或不完整时出现配置错误，包括访问权限发放不当。操作错误不仅仅是个人设置的不当，也可能是因为 IT 系统或应用没有被正确操作。如在计算机上启动不必要的程序可能导致计算机系统被犯罪者控制。

对策：

- ✧ 安全管理组织OOR_MNG
- ✧ 安全管理人员能力OOR_CAP
- ✧ 安全策略执行PIN_EXE
- ✧ 安全培训OPE_TRA
- ✧ 身份鉴别TCE_IDT
- ✧ 网络设备用户身份鉴别TNI_IDT
- ✧ 账户管理OHO_ACC

3.28 THUMAN.PW 口令处理不当

如果用户对必要的访问许可很不注意，则即使对认证过程进行精心设计，访问授权方法使用口令、PIN或认证标识，实际使用中这些信息常常被偷漏给其他的用户或不能确保安全。

主要包括以下几种情况：

为了方便将口令传递给他人或在工作团队中共享口令；认证标识的丢失；口令太多，导致系统管理人员记不住口令，进而导致口令丢失。对于非常安全的IT系统而言口令或标识的丢失将导致所有用户的丢失，因此口令被写到键盘等其他显而易见的位置，另一种防止口令丢失的方法是口令十分简单。

对策：

- ✧ 账户管理OHO_ACC
- ✧ 身份鉴别TCE_IDT
- ✧ 网络设备用户身份鉴别TNI_IDT
- ✧ 选择安全控制措施ORA_CTR

- ✧ 安全策略执行PIN_EXE
- ✧ 安全培训OPE_TRA
- ✧ 安全管理组织OOR_MNG

3.29 THUMAN.INF 信息处理草率

常常发现这样的问题，尽管在组织或安全技术上采取了大量的措施，但技术上的处理疏忽（草率）将导致安全性被破坏，如显示器上给出了所有访问口令；在安全相关信息处理过程中粗心大意、疏于职守或者鲁莽。

对策：

- ✧ 安全培训OPE_TRA
- ✧ 岗位安全职责OOR_STA
- ✧ 安全策略执行PIN_EXE
- ✧ 安全管理组织OOR_MNG
- ✧ 安全管理人员能力OOR_CAP

3.30 THUMAN.VAL 对通讯对象验证不足

在私人会谈、电话或e-mail中许多人传递的信息比其准备的多，常常假设对通讯伙伴而言谈话或e-mail内容是可信的，导致内部信息的无意泄漏，比如记者冒充另一个重要人物给某一重要人物打电话以获取保密信息。

对策：

- ✧ 安全培训OPE_TRA
- ✧ 安全策略执行PIN_EXE

4 TFAIL 技术故障

4.1 TFAIL.BRE 电源中断

尽管通常能高度保证持续供应，供电有时也会中断。这样的问题大部分仅持

续一秒钟，人们不会注意到它。当电力供应出现多于 10ms 的问题时 IT 操作就会被中断。

对策：

- ✧ 供电TPR_SUP
- ✧ 数据备份和恢复OBA_DAT
- ✧ 应急响应计划的制定OBC_EST

4.2 TFAIL.SUP 内部补给网络故障

内部补给网络故障包括：

- 电
- 电话
- 空气调节装置/通风装置

以上这些问题能导致IT操作的立即中断。以下领域中的问题也将带来破坏：

- 加热
- 水
- 消防用水流
- 排水系统
- 煤气
- 报告和控制装备（非法入侵者、火灾、家务管理装置）
- 内部对讲系统

这些破坏也可能所带来的故障延迟发生。

对策：

- ✧ 供电TPR_SUP
- ✧ 防火TPR_FIR
- ✧ 空调TPR_CON
- ✧ 防潮TPR_WAT
- ✧ 防静电TPR_STA
- ✧ 防雷击TPR_THU
- ✧ 电磁防护TPR_TEM

- ✧ 位置选择TPR_LOC
- ✧ 数据备份和恢复OBA_DAT
- ✧ 应急响应计划的制定OBC_EST

4.3 TFAIL.UNAV 安全措施不可用

由于技术缺陷或其他因素的影响（如年久、操作错误、缺乏维护、电源故障等），安全设备不可用，导致其保护能力被降低或中和掉了。如：

- 门锁缺陷
- 灭火装置不足
- 火灾检测设备被污染
- 用户 ID 卡或钥匙被毁坏
- 阻塞火灾紧急出口

对策：

- ✧ 位置选择TPR_LOC
- ✧ 电磁防护TPR_TEM
- ✧ 安全培训OPE_TRA
- ✧ 岗位安全职责OOR_STA
- ✧ 数据备份和恢复OBA_DAT
- ✧ 应急响应计划的制定OBC_EST

4.4 TFAIL.COND 因环境因素损害线路

用电子信号进行数据传输的信道容量会被电子和磁场所影响。该影响能否导致信号传输的实质性损害源于三个基本因素：

- 所暴露的电场/磁场的频率范围、强度和暴露的时间；
- 线缆防护程度；
- 数据传输中是否设置安全装置（如冗余、错误纠正等）。

许多情况下，损害能实现能事先识别：

- 沿着拉紧的线和临近大的发动机会产生强更感应区域（如铁路、工作车

间、电梯等）；

- 安装在发射机、电磁场等（如广播、公安/消防局、无线网络等）附近；
- 手提（移动）电话的通讯强度超过了许多IT系统的承受敏感度；
- 线缆之间互相影响。

除了电磁因素，其他的环境因素也可能影响线缆。如高温度、刺激性气体和高机械压力。

对策：

✧ 电磁防护TPR_TEM

✧ 位置选择TPR_LOC

✧ 防火TPR_FIR

4.5 TFAIL.DIM 串话干扰

串话干扰是一种特殊形式的线路干扰。在这种情况下故障通常不是环境因素引起的，而是由于临近线路上传输的电流或电压信号造成的。该影响的强度依赖于线缆的结构（屏蔽、线缆容量、绝缘质量）以及信息传输的电子参数（电流、电压和频率）。

不是每一条线都被串话干扰影响，但它们彼此一定会互相影响。这种现象和电话网络相似。

对策：

✧ 防干扰和窃听TPR _TAP

✧ 电磁防护TPR_TEM

4.6 TFAIL.VOL 电压变化/过高/过低

供电电压的变化可能导致IT系统的故障和损坏。这种变化可以是不会给IT系统带来危害的极小的变化，也可以是产生完全破坏的超高电压。这可能在电力供应的所有部门被引发，范围从整个网络到单个设备连接的电路。

对策：

✧ 供电TPR_SUP

- ✧ 数据备份和恢复OBA_DAT
- ✧ 应急响应计划的制定OBC_EST

4.7 TFAIL.DEST 数据存储介质的毁坏

数据缺陷和错误单存依赖于技术缺乏或毁坏是十分常见的。这样的存储介质包括大量的存储设备如硬盘、磁带等。硬盘可以被读写头损坏，而磁带和盒式磁带会因为机械损坏而损坏，CD的表面会因为擦伤而不再能使用。

产生问题的原因可能有灰尘、笔记本电脑因为摔打而造成毁坏，在多媒体PC机备份的过程中，一些ZIP磁盘可能会出现问题。

对策：

- ✧ 存储介质的保护ORM_PRO
- ✧ 存储介质的访问控制ORM_ACO
- ✧ 存储介质的传输管理ORM_TRA
- ✧ 存储环境管理ORM_CIR
- ✧ 存储介质的备份ORM_BAC
- ✧ 存储介质的分类和归档ORM_CLA
- ✧ 数据备份和恢复OBA_DAT

4.8 TFAIL.LEAK 出现软件漏洞

已有软件中总是存在多种漏洞，另外新软件的使用也会带来许多新问题。比如：UNIX环境下的发邮件BUG；UNIX下的gets；TCP/IP协议栈的cgi scripts问题等。

对策：

- ✧ 漏洞控制OHO_VER
- ✧ 应用系统测试TCE_APT
- ✧ 系统安全检测和验收OEN_TES
- ✧ 数据备份和恢复OBA_DAT
- ✧ 应急响应计划的制定OBC_EST

4.9 TFAIL.POW 内部电源的毁坏

XXXIT系统所用的笔记本电脑等有独立于主机的电源，这样的单元常常使用的是可以再充电的电池，这些电池可以持续的保持工作几个小时。在一定的时期中，IT系统可能不会再连接到主电源上，在这样工作过程中大多数的XXX系统不断的检查电源的电压，一旦电源的电压不再满足系统的需求则系统会突然不能再操作，导致的结果就是存在主存中的数据会来不及保存而丢失。

对策：

- ✧ 供电TPR_SUP
- ✧ 数据备份和恢复OBA_DAT
- ✧ 应急响应计划的制定OBC_EST

4.10 TFAIL.NIS NIS 服务器和 NIS 客户端之间缺乏认证能力

如果NIS域名是已知的，任何其他的计算机都被标识为客户端，所有的NIS映像能被读，特别是口令映像能被读，如果系统管理员权限能在一个系统上获得，NIS服务器进程能在一个特定的端口上启动。客户端进程ypbind在目标系统上重起。如果服务器比原来的响应快，会出现很多其他的信息被传送到客户端。

对策：

- ✧ 身份鉴别TCE_IDT
- ✧ 账户管理OHO_ACC
- ✧ 安全审计TCE_SAU
- ✧ 计算环境访问控制TCE_TAC
- ✧ 远程登陆管理OHO_TEL

4.11 TFAIL.XAUT X 服务器和 X 客户端间缺乏认证能力

没有合适的安全策略，例如在X Windows系统中Cookies应该仅仅在可信环境中使用。没有安全功能要求任何使用者都有可能破坏X客户端和X服务器。负责

计算机上述如何输出的X服务器进程无法检测和它通讯的X客户端所有者的身份。在这种情况下X客户端能访问所有的X服务器输入的数据，而X服务器无法指出X客户端从哪里收到数据。

例如：可以使用xspy工具自动记录远端xterm客户端的键盘输入；

对策：

- ✧ 身份鉴别TCE_IDT
- ✧ 账户管理OHO_ACC
- ✧ 安全审计TCE_SAU
- ✧ 计算环境访问控制TCE_TAC
- ✧ 远程登陆管理OHO_TEL

4.12 TFAIL.LOSE 存储数据丢失

存储数据的丢失将会对IT系统产生很大的影响。应用数据或消费数据库的缺乏和伪造将影响私人企业的存在。在政府机关中，重要数据的丢失或伪造会延迟或妨碍系统管理员和专家的工作。

存储数据可能因为多种原因造成丢失：

如：因为年久（温度、空气湿度等）出现磁数据存储介质的退磁现象；将磁存储介质放到强大的磁场中；不可抗拒力造成的数据存储介质破坏（火或水）；无意中的数据删除和覆写；外存的技术问题；不完善的数据存储介质。存储介质变更的失控（完整性缺失）；计算机病毒造成的文件删除。

对策：

- ✧ 存储介质的保护ORM_PRO
- ✧ 存储介质的传输管理ORM_TRA
- ✧ 存储环境管理ORM_CIR
- ✧ 存储介质的备份ORM_BAC
- ✧ 数据备份和恢复OBA_DAT
- ✧ 防火TPR_FIR
- ✧ 防潮TPR_WAT
- ✧ 防静电TPR_STA

- ✧ 电磁防护TPR_TEM
- ✧ 存储介质的保护ORM_PRO
- ✧ 存储介质的传输管理ORM_TRA
- ✧ 存储环境管理ORM_CIR
- ✧ 存储介质的备份ORM_BAC
- ✧ 数据备份和恢复OBA_DAT
- ✧ 防潮TPR_WAT
- ✧ 防静电TPR_STA
- ✧ 电磁防护TPR_TEM
- ✧ 病毒和恶意代码防范TCE_VIR
- ✧ 防病毒网关TEB_TVI

4.13 TFAIL.EXH 因存储介质耗尽引起的信息丢失

每个存储介质都有其存储极限。当到达存储界限时，可能导致数据丢失和服务不再可用，如：用户不能再存储更多的数据；到达的邮件被拒绝；不能再保存那些尚未评估的审计记录或审计数据，进行数据覆写。存储介质可能会因为多种原因被耗尽，如应用程序的错误，提高用户的存储需求或恶意攻击可能减少存储空间，这将妨碍审计记录的保存。

对策：

- ✧ 设备和系统冗余OBA_EQI
- ✧ 存储介质的保护ORM_PRO
- ✧ 病毒和恶意代码防范TCE_VIR

4.14 TFAIL.ELE 屏蔽区域的瞬间电流

在屏蔽区域内可能会产生瞬间电流，这会给设备的使用带来危害。

对策：

- ✧ 电磁防护TPR_TEM
- ✧ 数据备份和恢复OBA_DAT

4.15 TFAIL.BUG 软件漏洞或错误

所有的标准软件和其他软件对面临这样的问题：软件越复杂错误出现越频繁。出现该问题的原因在于用户的期望很高和软件的开发周期很短导致软件厂商在查出软件的所有错误之前就发布了软件。如果软件错误不能及时被检测到，可能会导致严重的后果。

对策：

- ✧ 漏洞控制OHO_VER
- ✧ 数据备份和恢复OBA_DAT

4.16 TFAIL.DBFN 数据备份中文件名的转换

如果备份文件不支持Windows长文件名，所有的文件名都将在备份之前用LFNBK.EXE和选项/B来转化，而后调用备份程序，最后原来文件名字用LFNBK.EXE /R.存储。

这一程序应谨慎使用，因为转化过程中文件名字出现信息丢失，另外其他文件不再按照PC目录结构存放，这会导致数据丢失。

对策：

- ✧ 存储介质的保护ORM_PRO
- ✧ 数据备份和恢复OBA_DAT

4.17 TFAIL.DBF 数据库故障

如果因为硬件/软件或破坏行为导致数据库故障，所产生结果的影响范围在于数据库的功能和重要性。这时，所有依赖于受侵害数据库数据的应用都不能使用了。这可能导致以下结果：

- 财务损失
- 可能影响人员福利的安全缺陷（如药物数据库）
- 操作部分或全部中断

对策：

- ✧ 数据库设计安全TCE_DBS
- ✧ 资产鉴别ORA_ASE
- ✧ 应用系统测试TCE_APT
- ✧ 系统安全检测和验收OEN_TES

4.18 TFAIL.ODBC 通过 ODBC 进行访问控制欺骗

如果数据库通过ODBC进行访问，并且ODBC的驱动没有正确安装，则已有的对数据库的访问控制能被欺骗。这可能导致机密数据被泄漏。

对策：

- ✧ 数据库设计安全TCE_DBS
- ✧ 资产鉴别ORA_ASE
- ✧ 威胁分析ORA_THR
- ✧ 脆弱性分析ORA_VUL
- ✧ 应用系统测试TCE_APT
- ✧ 系统安全检测和验收OEN_TES
- ✧ 计算环境访问控制TCE_TAC
- ✧ 数据备份和恢复OBA_DAT
- ✧ 应急响应计划的制定OBC_EST

4.19 TFAIL.DATA 数据库中数据的丢失

多种原因会造成数据库中数据丢失，如无意中删除数据、数据库崩溃和故意入侵。结果是数据的完整性和可用性不再得到保证。

对策：

- ✧ 数据库设计安全TCE_DBS
- ✧ 资产鉴别ORA_ASE
- ✧ 威胁分析ORA_THR
- ✧ 脆弱性分析ORA_VUL
- ✧ 计算环境访问控制TCE_TAC

- ✧ 系统安全检测和验收OEN_TES
- ✧ 数据备份和恢复OBA_DAT
- ✧ 应急响应计划的制定OBC_EST

4.20 TFAIL.SROR 存储空间缺乏引起的数据库中数据丢失

每种存储介质存放数据的空间都是有限的。因此数据库采用合并物理存储介质的方法来长期存储数据。一旦存储介质耗尽，数据库崩溃并导致数据丢失。这些结果在TFAIL.DATA数据库中的数据丢失中被描述。

存储介质会因为各种原因突然被耗尽，如应用程序错误、存储需求提高以及为了使审计失效故意实施入侵行为来降低存储能力。

对策：

- ✧ 设备和系统冗余OBA_EQI
- ✧ 存储介质的保护ORM_PRO
- ✧ 存储介质的备份ORM_BAC
- ✧ 数据备份和恢复OBA_DAT

4.21 TFAIL.INTE 数据库完整性/一致性丢失

数据库完整性或一致性丢失意味着虽然数据仍然在数据库中，但数据已经部分毁坏或不能被理解。结果数据不能正确操作。数据库的完整性和机密性能通过各种方式被削弱，如：无意中对数据的修改；事务的同步检查不足；有意的入侵。

对策：

- ✧ 数据库设计安全TCE_DBS
- ✧ 应用系统测试TCE_APT
- ✧ 系统安全检测和验收OEN_TES
- ✧ 数据备份和恢复OBA_DAT

4.22 TFAIL.DEF 网络组件的失败或故障

网络组件的失败或故障削弱了整个网络或部分网络的可用性。分为三种不同情况：

- 整个网络组件的失败或故障；
- 那些没有直接连接到网络或网络部分中的活跃组件故障，但是这些组件可能位于这些系统的信号传输路径上；
- 那些存在于第二层或冗余信号路径上的组件；

对策：

✧ 网络可靠性管理ONE_REL

4.23 TFAIL.SEND 信息发送失败

通过电子邮件发送数据具有快速和保密的特点，但却无法保持可靠性。信息会因为IT系统的软、硬件错误或传输线路问题而丢失。这些问题出现有很多原因，如线缆损坏、组件损坏、或者通讯软件被不正确的配置。电子邮件也会因为接收者地址不正确而丢失。这种情况存在的最大的问题是用户很少不会因为电子邮件发送失败而被通知。自动通报电子邮件传输失败机制也不可靠。一些邮件系统会提供“发送确认”或“接收确认”的选项，但不能对这种确认估价过高，当邮件到达邮件服务器却没能到达接收者的工作站时，这种功能不会给出提示。

对策：

✧ 网络可靠性管理ONE_REL

4.24 TFAIL.AUTH 认证性能差或缺失

认证机制被用于认证用户或组件或确定数据的来源。如果没有认证机制或认证机制的性能比较差，存在这样的风险：

- 未授权的用户能获取IT或数据的访问权限
- 无法确认问题出现的原因
- 无法确定数据源

对策：

✧ 身份鉴别TCE_IDT

✧ 网络设备用户身份鉴别TNI_IDT

✧ 安全审计TCE_SAU

4.25 TFAIL.ENCM 加密模块的故障

如果使用加密模块保护那些需要保护数据的机密性，加密模块的功能有效性十分重要。加密模块故障可能由多种原因引起：

- 因技术原因造成加密模块的功能削弱
- 加密模块被存放在不稳定的存储介质中，被删除
- 因故意或非故意的认为因素造成的毁坏

加密模块故障导致多种类型的损害。

对策：

✧ 密码技术TNI_ENC

✧ 密钥管理OCO_KEY

4.26 TFAIL.ENCY 加密算法不可靠

运用加密提高安全性的程度主要依赖于加密算法和加密代码的机密性。

不安全的加密算法指的是潜在的犯罪者具有资源和能力来破解该算法。犯罪者可利用的所资源一般包括分析工具、相关知识、可用时间、弱点知识等。

为检查所用的加密算法是否安全需要根据以下几个标准进行考虑：

• 加密编码低于60位时能够被多台计算机进行暴力破解，随着计算机计算能力的提高，可能破解80位的加密编码；

• 非对称算法的编码低于768位可以认为不安全

• HASH值少于128位时，可能出现冲突项

• 没有经验的开发者开发出来的加密算法，并且该算法没有经过充分验证，这样的算法可以认为是不安全的

• 那些在软件中运行很快的未正式发行的加密算法也被认为是不安全的

• 加密算法中常常是用随机数，如果随机数产生的不好，会影响整体的安全性

对策：

✧ 密码技术TNI_ENC

4.27 TFAIL.ENC 加密数据的错误

编码形式改变的数据不能被正确解码。由于编码方式的变化，意味着可能仅仅使一部分字节解码不正确或者所有的数据的解码都不正确。如果没对数据进行备份将导致所有数据的丢失。

加密代码错误索引发的问题可能更加严重。即使一位加密代码被改变久无法进行解码。

对策：

- ✧ 密码技术TNI_ENC

4.28 TFAIL.MAIL E-mail 缺乏时间真实性

电子邮件可能包括各种时间信息，如信息发送时间或信息接收时间。这些时间都没有基准。如信息发送时间能通过调整发送该信息计算机的系统时间来进行伪造。当邮件从发送者到接收者的过程中，邮件头部特别是其中的时间项目、邮件服务器的日期和地址都很容易伪造。接着就会出现系统的破坏和转换SMTP数据包的攻击。

对策：

- ✧ 主机入侵防范TCE_IDS
- ✧ 选择安全控制措施ORA_CTR
- ✧ 病毒和恶意代码防范TCE_VIR
- ✧ 漏洞控制OHO_VER

4.29 TFAIL.TRB 网络管理系统或系统管理系统组件故障。

网络管理系统或系统管理系统中的多种组件都有可能出现故障。引发的部分原因如下：

- 管理组件失败
- 监控组件失败
- 中心管理工作站不可用

- 管理信息传输过程中网络交换部分出现故障

对策：

✧ 网络可靠性管理ONE_REL

✧ 应急响应计划的制定OBC_EST

5 TMALICE 恶意行为

5.1 TMALICE.BREK IT 设备或附件被操纵或被破坏

破坏者可能出于各种原因（如报复、怨恨或受挫）对IT设备、附件、文档或其他相关设施进行操纵和破坏。后来，这些操作被检测出来，破坏人获取的知识越高，对工作站的影响越大。影响的范围从未经授权查看敏感数据到破坏数据存储介质或IT系统。

对策：

✧ 设备安全TPR_EQI

✧ 门禁TPR_JAN

✧ 机房管理OPM_ROM

✧ 存储介质的保护ORM_PRO

✧ 第三方访问OPE_OTT

✧ 安全策略执行PIN_EXE

5.2 TMALICE.DBCT 数据或软件被操纵

可以通过许多方式操纵数据或软件，如不正确的数据获取、访问权限的变换、统计或通讯数据的修改、操作系统变化等。入侵者通常仅能访问其所能操纵的数据或软件。人员所拥有的访问权限越多则他可能操纵数据或软件就越多。如果这些操作不能及时被检测，IT 操作的稳定性就可能被极大削弱。

对策：

✧ 机房管理OPM_ROM

✧ 存储介质的访问控制ORM_ACO

- ✧ 账户管理OHO_ACC
- ✧ 网络设备管理授权ONE_ADV
- ✧ 计算环境访问控制TCE_TAC
- ✧ 身份鉴别TCE_IDT
- ✧ 网络设备用户身份鉴别TNI_IDT
- ✧ 安全审计TCE_SAU
- ✧ 变更控制OCO_CHA
- ✧ 人员离岗OPE_DIM

5.3 TMALICE.BUI 未经授权进入建筑

未经授权进入建筑会给该建筑内的IT系统带来多种危险，如偷窃或被操纵。因此，应该针对不同危害采取相应的对策。

未经授权进入建筑所带来的直接影响就是物质损害。窗和门被暴力打开而不得不修理或更换。

对策：

- ✧ 设备安全TPR_EQI
- ✧ 门禁TPR_JAN
- ✧ 机房管理OPM_ROM
- ✧ 环境设备维护OPM_MAI

5.4 TMALICE.STE 偷窃

IT设备、附件、软件或数据被偷窃不仅需重建费用，也会导致可用性的丢失。另外，也会因机密性的缺失而带来损害。

对策：

- ✧ 设备安全TPR_EQI
- ✧ 门禁TPR_JAN
- ✧ 机房管理OPM_ROM
- ✧ 存储介质的保护ORM_PRO

- ✧ 第三方访问OPE_OTT

5.5 TMALICE.DES 恶意破坏行为

恶意破坏行为和入侵攻击行为很相似，不同的是恶意破坏行为是无目的的。恶意破坏行为的实际危害比入侵攻击更难评估，这是因为恶意破坏行为通常没有有意识的动机。个人问题或组织风气都可能是出现恶意破坏行为的潜在原因。

对策：

- ✧ 设备安全TPR_EQI
- ✧ 机房管理OPM_ROM
- ✧ 存储介质的保护ORM_PRO
- ✧ 办公环境管理OPM_OFM
- ✧ 第三方访问OPE_OTT
- ✧ 安全培训OPE_TRA
- ✧ 岗位安全职责OOR_STA
- ✧ 安全策略执行PIN_EXE

5.6 TMALICE.ATT 攻击行为

存在多种导致攻击发生的可能性：丢砖头、使用爆炸物、纵火等。无论 IT 操作者是否暴露在攻击的风险之下，都将依赖于建筑物的环境，他从事的业务和政治/社会的关系。如果 IT 操作者工作在颇具争议的政治领域，他可能就面临着更大的风险。

对策：

- ✧ 门禁TPR_JAN
- ✧ 办公环境管理OPM_OFM
- ✧ 合作与沟通OOR_COM
- ✧ 机房管理OPM_ROM
- ✧ 安全策略执行PIN_EXE
- ✧ 第三方访问OPE_OTT

5.7 TMALICE.INTER 线路侦听

由于被检测到的几率很低，线路侦听对 IT 安全的威胁不容忽视。没有任何线缆能够完全抵御侦听。不同类型电缆需要不同的努力来实施侦听。

线缆是否被侦听决定于攻击者的能力和目的；攻击者可以通过机械的 HTTP 连接分析获得秘密信息；口令窃听程序可以获取系统口令，以保证攻击者在后来能够容易进入被侵害计算机系统。

对策：

- ✧ 设备安全TPR_EQI
- ✧ 防干扰和窃听TPR _TAP
- ✧ 远程登陆管理OHO_TEL

5.8 TMALICE.COMM 通讯线路被操纵

将此威胁从线路侦听中分离出来是因为线路可能会由于其他原因被操纵。

如：心存不满的员工未经允许从公司外建立到公司内部网络的连接以破坏公司的 IT 运作；为节约费用操纵线路以供私人使用；为操纵传输数据而操纵线路等。

对策：

- ✧ 设备安全TPR_EQI
- ✧ 防干扰和窃听TPR _TAP
- ✧ 主干网可用性保护TNI_AVI
- ✧ 内部网络防护TNI_INT
- ✧ 人员离岗OPE_DIM

5.9 TMALICE.AUIT 未经授权使用 IT 系统

如果不对用户进行识别和授权而对 IT 系统进行控制在实际应用中是不可能的，即使 IT 系统提供用户 ID 和口令形式的识别和授权，仍会因为口令和用户 ID 过于接近而存在风险。

对策：

- ✧ 身份鉴别TCE_IDT
- ✧ 网络设备用户身份鉴别TNI_IDT
- ✧ 账户管理OHO_ACC
- ✧ 网络设备管理授权ONE_ADV
- ✧ 计算环境访问控制TCE_TAC
- ✧ 安全审计TCE_SAU
- ✧ 网络边界访问控制TEB_NAC

5.10 TMALICE.TELM 滥用远程维护端口

滥用系统远程维护端口会带来安全风险。

对策：

- ✧ 远程登陆管理OHO_TEL
- ✧ 网络设备管理授权ONE_ADV
- ✧ 身份鉴别TCE_IDT
- ✧ 网络设备用户身份鉴别TNI_IDT
- ✧ 账户管理OHO_ACC
- ✧ 安全审计TCE_SAU

5.11 TMALICE.INS 内部员工在维护/系统管理工作中造成的威胁

为了自己的利益或所喜欢的同事，内部员工在系统维护或系统管理过程中试图修改权限或激活用户设备。这会因为维护或系统管理知识和经验缺乏导致系统崩溃，或是硬件处理不当导致系统损坏。另外，维护职员能够全部或部分的访问存储的数据。

对策：

- ✧ 人员录用OPE_EMP
- ✧ 安全培训OPE_TRA

- ✧ 安全策略执行PIN_EXE
- ✧ 岗位安全职责OOR_STA
- ✧ 关键岗位安全管理OOR_KST

5.12 TMALICE.EXT 外部人员在维护/系统管理工作中造成的威胁

维护过程中 IT 系统能以任何一种方式被操纵。由于 IT 系统不能理解或进行有效的修正而出现严重威胁问题，外部维护工程师和内部员工一样也能访问到存储在系统内部的数据。

对策：

- ✧ 机房管理OPM_ROM
- ✧ 第三方访问OPE_OTT

5.13 TMALICE.CRACK 系统地进行口令破解

过于简单的口令可以通过系统地破解方式获取。

对策：

- ✧ 身份鉴别TCE_IDT
- ✧ 网络设备用户身份鉴别TNI_IDT
- ✧ 账户管理OHO_ACC
- ✧ 网络设备管理授权ONE_ADV

5.14 TMALICE.USER 滥用用户权限

为了损害系统或其用户，当某人通过正常途径故意获取口令或通过某些工具非法获取口令，这时就会出现用户权限被滥用的现象。

对策：

- ✧ 网络设备管理授权ONE_ADV
- ✧ 远程登陆管理OHO_TEL

- ✧ 安全培训OPE_TRA
- ✧ 人员离岗OPE_DIM
- ✧ 安全策略执行PIN_EXE
- ✧ 岗位安全职责OOR_STA
- ✧ 关键岗位安全管理OOR_KST

5.15 TMALICE.ADM 滥用系统管理员权限

为了损害系统或其用户，当某人通过正常途径故意获取或通过某些工具非法获取超级用户权限，这时就会出现用户权限滥用的现象。滥用系统管理员权限原因：root 权限不受限制；超级用户文件的滥用；自动上载；对控制台进行访问；软件错误。

对策：

- ✧ 网络设备管理授权ONE_ADV
- ✧ 岗位安全职责OOR_STA
- ✧ 关键岗位安全管理OOR_KST

5.16 TMALICE.TROY 特洛伊木马

特洛伊木马是一种隐藏的程序，用户无法影响其功能的执行。特洛伊木马的功能和病毒相似。任何一种应用软件都可以作为特洛伊木马的载体，特洛伊木马也可以植入能被操作系统解读的脚本语言中（如批文件、ANSI和Postscript等）。

特洛伊木马可能会存在于以下情况中：存在于变更登录信息的程序中、存在于Back Orifice and NetBUS中、存在于被控制的库和程序中等

对策：

- ✧ 病毒和恶意代码防范TCE_VIR
- ✧ 主机入侵防范TCE_IDS
- ✧ 变更控制OCO_CHA

5.17 TMALICE.MOV 偷窃可移动 IT 系统

和那些放在有保安的办公场所中的台式计算机不同的是可移动计算机系统常常被带到汽车、火车和其他人的办公室等场所，因此，就存在易于丢失的问题。

当可移动 IT 系统被偷窃之后，访问保护不足会导致数据轻易被偷窃者获取；可移动设备对远程服务器的访问认证导致远程访问的潜在威胁。

对策：

- ✧ 设备安全TPR_EQI
- ✧ 资产鉴别ORA_ASE
- ✧ 威胁分析ORA_THR
- ✧ 存储介质的备份ORM_BAC
- ✧ 计算环境访问控制TCE_TAC
- ✧ 远程访问TEB_TEL
- ✧ 安全策略执行PIN_EXE

5.18 TMALICE.VIRUS 计算机病毒

计算机病毒是一种具有破坏功能的程序，主要的危害是导致数据或其他程序的丢失和破坏。病毒功能通常是由某一事件触发的。计算机病毒具有自我复制性，所有的操作系统都可能感染病毒。

对策：

- ✧ 防病毒网关TEB_TVI
- ✧ 病毒和恶意代码防范TCE_VIR
- ✧ 存储介质的备份ORM_BAC
- ✧ 数据备份和恢复OBA_DAT

5.19 TMALICE.REP 信息重放

入侵者记录通讯信息并在后来不做任何修改的重放这些信息。

对策：

- ✧ 防干扰和窃听TPR _TAP
- ✧ 设备安全TPR_EQI
- ✧ 主干网可用性保护TNI_AVI
- ✧ 安全域规划ONE_SED
- ✧ 网络可靠性管理ONE_REL
- ✧ 安全审计TCE_SAU

5.20 TMALICE.POSE 伪装

入侵者通过获取用户 ID 和口令或者通过操纵信息的原始域（或是 I/O 地址）来进行伪装。被欺骗的用户可能会泄漏机密信息。

入侵者通过侵入已存在的连接来逃避身份认证。

对策：

- ✧ 身份鉴别TCE_IDT
- ✧ 网络设备用户身份鉴别TNI_IDT
- ✧ 网络设备管理授权ONE_ADV
- ✧ 安全审计TCE_SAU
- ✧ 防干扰和窃听TPR _TAP

5.21 TMALICE.FLUX 信息流分析

通过流量分析，破坏分子可以分析出是在谁在何时以多大频繁发送什么数据给谁。即使偷听者不能了解传输的内容，它也可以对用户的行为进行判断，并且能分析出发送者的相关信息。公司的邮件地址分配规律也可以被发现并被提供给广告发行者。

对策：

- ✧ 密码技术TNI_ENC
- ✧ 防干扰和窃听TPR _TAP
- ✧ 主干网可用性保护TNI_AVI
- ✧ 安全域规划ONE_SED

✧ 网络可靠性管理ONE_REL

5.22 TMALICE.DOS 拒绝服务

这种攻击的目的是阻止用户使用那些通常对其可用的功能或设备。攻击常常发生在分布式资源相关的连接上。导致 CPU 时间、磁盘空间、节点和目录的缺乏。

攻击的方式有多种，比如：

- 同时启动大量程序
- 同时启动大量占用 CPU 时间的程序
- 占用了 UNIX 操作系统中的所有节点，因此不能创建新的文件
- 在 DOS PC 的目录中创建大量小文件，因此不能在这个目录中创建新的文件
- 使网络带宽超载
- 切断网络连接

对策：

✧ 主干网可用性TNI_AVI

✧ 网络设备登录控制TNI_TEL

✧ 网络边界访问控制TEB_NAC

✧ 计算环境访问控制TCE_TAC

✧ 防病毒网关TEB_TVI

✧ 病毒和恶意代码防范TCE_VIR

✧ 安全域规划ONE_SED

✧ 网络可靠性管理ONE_REL

✧ 设备和系统冗余OBA_EQI

5.23 TMALICE.COPY 未经授权进行数据拷贝

在数据传输过程中，数据存储介质上的信息可能从一个安全环境经过不安全路径到达接入端不安全的环境。在这样的情况下，未经授权的人员能更容易的获

取信息。

对策：

- ✧ 存储介质的访问控制ORM_ACO
- ✧ 存储介质的保护ORM_PRO
- ✧ 存储介质的传输管理ORM_TRA
- ✧ 存储环境管理ORM_CIR
- ✧ 存储介质的备份ORM_BAC
- ✧ 存储介质的分类和归档ORM_CLA

5.24 TMALICE.UUDP 滥用带有 UUDP 功能的 UNIX 系统

UUDP 软件（UNIX 到 UNIX 拷贝）包允许在 IT 系统和远程 IT 系统之间交换 ASCII 和二进制文件。UUDP 最早是在 UNIX 系统上实现的，现在已经在许多操作系统中实现。通过 UUDP 进行通讯，远程计算机的 IT 用户能获取本地计算机的权限，如果这些权限没能认真进行授权，则本地系统就存在滥用风险。

对策：

- ✧ 身份鉴别TCE_IDT
- ✧ 账户管理OHO_ACC
- ✧ 远程访问TEB_TEL
- ✧ 网络设备管理授权ONE_ADV
- ✧ 网络设备登录控制TNI_TEL

5.25 TMALICE.ARP IP 欺骗

IP 欺骗是一种渗透方法，通过这种方法采用虚伪的 IP 标识来攻击 IP 系统。如 ARP 欺骗等等。

对策：

- ✧ 计算环境访问控制TCE_TAC
- ✧ 网络边界访问控制TEB_NAC
- ✧ 主机入侵防范TCE_IDS

- ✧ 网络入侵防范TEB_IDS
- ✧ 网络可靠性管理ONE_REL
- ✧ IP地址管理ONE_IPM

5.26 TMALICE.FROU 源路由的滥用

滥用源路由机制和协议很容易带来基于协议的攻击。IP 数据包中可能通过数据包要到达的目的地的路由或应答数据包应走的路由来描述数据通讯的路由。这些路由描述可能被操纵，因此传输过程中路由入口处和（如防火墙等）其他未受控制的路由安全所提供路由没能被使用。

对策：

- ✧ 网络边界访问控制TEB_NAC
- ✧ 路由管理ONE_ROU

5.27 TMALICE.ICMP 滥用 ICMP 协议

作为传输层协议，ICMP（Internet Control Message Protocol）需要传输错误和诊断信息。该协议可通过多种方式被滥用。一方面计算机的路由表可以通过重定向数据包进行修改，另一方面，入侵者可能通过伪造目的不可达信息使可用的网络连接无法正常工作。

对策：

- ✧ 网络边界访问控制TEB_NAC
- ✧ 主机入侵防范TCE_IDS
- ✧ 网络入侵防范TEB_IDS

5.28 TMALICE.OSPF 滥用路由协议

RIP 或 OSPF 这样的路由协议适合在两个联网系统之间传递路由变化信息。因此，动态改变路由表是可能的，该功能极易生成错误的 RIP 数据包并使路由配置不当。

动态路由的使用使得将路由信息动态发送到计算机成为可能，这种消息的使

用可能导致未经检查的路由表项被建立。入侵者可能会利用这种方式来改变连接。

对策：

- ✧ 网络边界访问控制TEB_NAC
- ✧ 网络入侵防范TEB_IDS
- ✧ 路由管理ONE_ROU

5.29 TMALICE.ADMIN 滥用 Windows 系统管理员权限

当合法或非法获取的系统员管理权限被故意用于毁坏系统和用户时称为权限滥用。

对策：

- ✧ 身份鉴别TCE_IDT
- ✧ 安全审计TCE_SAU
- ✧ 账户管理OHO_ACC
- ✧ 计算环境访问控制TCE_TAC

5.30 TMALICE.SNIF 网络分析工具

如果网络上传输的信息没被加密，可以通过网络分析工具（或称为 Sniffer）的帮助读取通讯内容。Sniffer 不能被看作黑客软件，因为许多的网络管理产品也包含这种功能。

对策：

- ✧ 网络设备管理授权ONE_ADV
- ✧ 防干扰和窃听TPR _TAP
- ✧ 远程登陆管理OHO_TEL
- ✧ 主干网可用性保护TNI_AVI
- ✧ 内部网络防护TNI_INT

5.31 TMALICE.ROUT 滥用远程访问路由的管理功能

路由器通过用于管理功能的远程访问端口进行装备，所有的系统管理、维护和信号发射任务都是通过这些端口实现的，远程访问端口十分有用，有时是不可或缺的，特别是对那些拥有多个路由器的大型网络和通过长距离线连接的 LAN。

存在两种类型的远程访问：

- 通过专用端口采用调制解调器进行访问
- 通过预留带宽进行直接访问

对策：

- ✧ 网络边界访问控制TEB_NAC
- ✧ 路由管理ONE_ROU
- ✧ 远程访问TEB_TEL
- ✧ 远程登陆管理OHO_TEL

5.32 TMALICE.TEL 通过远程 IT 系统滥用资源

远程 IT 系统（如远程办公工作站）常常访问公司网络的大量资源。这常常会导致数据或程序被窃的威胁，另外还提高了滥用服务的风险。为达到私人目的骗取通讯服务的使用（如传真网关、Internet 连接等）会导致额外的费用耗费。

对策：

- ✧ 网络边界访问控制TEB_NAC
- ✧ 网络设备登录控制TNI_TEL
- ✧ 远程登陆管理OHO_TEL
- ✧ 远程访问TEB_TEL

5.33 TMALICE.MANI 操纵数据库系统中数据或软件

由于故意行为导致数据被破坏或变得无用。 故意删除/修改数据库中的文件或标准数据库软件中的文件导致整个数据库系统的毁坏。

原则上讲，不可能防止用户使用自己的权限对数据进行操作和对数据库进行

破坏，然而一旦访问权限被第三方获取，那么，未被授权者能获取数据库的访问权并对其中的数据进行操作处理。

对策：

- ✧ 数据库设计安全TCE_DBS
- ✧ 身份鉴别TCE_IDT
- ✧ 安全审计TCE_SAU
- ✧ 计算环境访问控制TCE_TAC
- ✧ 数据备份和恢复OBA_DAT

5.34 TMALICE.DBDOS 数据库系统的拒绝服务

这种类型的入侵就是使用户可用的数据库功能和服务失效。例如，选取大量数据导致整个系统瘫痪，或封闭对数据记录的访问。

对策：

- ✧ 数据库设计安全TCE_DBS
- ✧ 主机入侵防范TCE_IDS
- ✧ 网络入侵防范TEB_IDS
- ✧ 数据备份和恢复OBA_DAT
- ✧ 设备和系统冗余OBA_EQI

5.35 TMALICE.CONN 未经授权将 IT 系统连接到网络

未经授权将 IT 系统连接到网络上的现象无法排除。这种连接可以通过空闲线缆设计进行预防。

未经授权将计算机连接到网络中常常难于检测这种访问能监控所在网络部分的所有数据通讯。其威胁举例如下：

- 操纵数据和软件
- 监控网络通讯
- 信息重放
- 分析信息流

- 拒绝服务攻击
- 未经授权执行网络管理功能
- 未经授权访问活跃的网络组件

对策：

✧ 网络可靠性管理ONE_REL

✧ 远程登陆管理OHO_TEL

✧ 网络设备登录控制TNI_TEL

✧ 设备和系统冗余OBA_EQI

✧ 安全培训OPE_TRA

✧ 选择安全控制措施ORA_CTR

✧ 应急响应计划的制定OBC_EST

✧ 安全策略执行PIN_EXE

5.36 TMALICE.NETM 未经授权执行网络管理功能

未经授权执行网络管理功能可以实现对网络活跃组件的部分或全部控制。这种控制出现的可能性取决于所使用的网络管理协议（如 SNMP 或 CMIP/CMOT）。该威胁削弱整个网络或某一部分的完整性和可用性以及数据的机密性/完整性。

对策：

✧ 网络可靠性管理ONE_REL

✧ 远程登陆管理OHO_TEL

✧ 网络设备登录控制TNI_TEL

✧ 安全审计TCE_SAU

✧ 安全策略执行PIN_EXE

5.37 TMALICE.ACNET 未经授权访问网络组件

网络组件通常通过串口连接到外部终端或便携 PC 上，这使得网络组件的管理本地化。

接口保护不足会导致入侵者未经授权访问网络组件。因为通过了本地安全检

查，（如输入正确的口令），入侵者可能会执行所有的系统管理功能。

通过读取获取组件的配置信息，入侵者能访问拓扑、安全机制和网络使用状况等机密信息。

对策：

- ✧ 远程登陆管理OHO_TEL
- ✧ 网络设备登录控制TNI_TEL
- ✧ 安全审计TCE_SAU
- ✧ 安全策略执行PIN_EXE
- ✧ 账户管理OHO_ACC

5.38 TMALICE.CONFI 保密信息机密性丢失

保密信息（如口令、人员相关的信息、事务和办公相关信息、研究与发展数据）因为信息本身的机密性具有固有的危险，因此其安全性会被有意或无意的削弱。保密信息可以从以下几处获取：内部存储介质（硬盘）、外部存储介质（软盘和磁带）、打印纸和数据传输线。存在多种获取保密信息的方式：读数据、拷贝数据、读数据备份、为经济利益偷窃数据存储介质、监控数据传输线、从屏幕上获取数据。数据越机密，第三方想获取或滥用该数据的动机就越强。

对策：

- ✧ 人员录用OPE_EMP
- ✧ 安全培训OPE_TRA
- ✧ 安全策略执行PIN_EXE
- ✧ 岗位安全职责OOR_STA
- ✧ 设备安全TPR_EQI
- ✧ 门禁TPR_JAN
- ✧ 机房管理OPM_ROM
- ✧ 存储介质的保护ORM_PRO
- ✧ 存储介质的访问控制ORM_ACO
- ✧ 存储介质的传输管理ORM_TRA
- ✧ 存储环境管理ORM_CIR

- ✧ 存储介质的销毁ORM_DES
- ✧ 主机设备维护OHO_EQI

5.39 TMALICE.MAIL 滥用 E-mail 服务

邮件系统的滥用可以发生在多个阶段：邮件发送工作站、内部网络、邮件服务器、或接收工作站。

如果用户邮件系统或组织的邮件系统没被充分保护，未经授权的人员可能会操纵这些 IT 系统。这可能导致不必要的传输耗费，也可能伴随着未经授权用户伪装合法用户所带来的危害。

另外，未经授权的人员不能读取邮件的内容。

对策：

- ✧ 账户管理OHO_ACC
- ✧ 身份鉴别TCE_IDT
- ✧ 安全审计TCE_SAU
- ✧ 安全策略执行PIN_EXE
- ✧ 存储介质的访问控制ORM_ACO
- ✧ 网络可靠性管理ONE_REL
- ✧ 安全域规划ONE_SED

5.40 TMALICE.CAM 伪装发件人

发送邮件时，伪装发件人相对比较简单。如果收件人认为邮件内的信息或附件是可信的，则会导致危害。

对策：

- ✧ 账户管理OHO_ACC
- ✧ 身份鉴别TCE_IDT
- ✧ 安全审计TCE_SAU

5.41 TMALICE.DNS （DNS spoofing）DNS 欺骗

为了和 Internet 上的其他计算机进行通讯就需要知道它的 IP 地址。由于 IP 地址的数字难易记忆，为所有的 IP 地址安排对应的名字，这就是 DNS（Domain Name System）。计算机名字和 IP 地址以及 IP 地址和计算机名字对应的数据库都存放在名字服务器上。两个数据库分别被用于安排名字和 IP 地址。由于这些数据库不需要相互一致，这时入侵者就可以将名字安排给错误的地址（或相反）来成功的实现 DNS 欺骗。

对策：

- ✧ 主机入侵防范TCE_IDS
- ✧ 网络入侵防范TEB_IDS
- ✧ IP地址管理ONE_IPM

5.42 TMALICE.WIN 未经授权获取 Windows 系统管理员权限

每一个 Windows NT/2k 系统标准安装时，都会创建一个系统管理员帐号。和用户配置的帐号不同，这些预定义的帐号不能删除或被失效，这是为了防止出现系统管理员帐号被故意封锁或出错而设定的。这所带来的问题是对系统管理帐号的口令进行尝试不会导致帐号被封锁，因此会导致系统被暴力破解。

对策：

- ✧ 账户管理OHO_ACC
- ✧ 身份鉴别TCE_IDT

5.43 TMALICE.DUPE 愚弄信息

愚弄信息包括警告将要出现一种危害严重的病毒或其他 IT 系统问题，导致大面积的恐慌。这样的信息通常是通过电子邮件进行传播的。愚弄信息不同于病毒。愚弄信息也可以通过移动电话进行传播。

对策：

- ✧ 安全培训OPE_TRA
- ✧ 安全策略执行PIN_EXE
- ✧ 选择安全控制措施ORA_CTR

5.44 TMALICE.AUTH 未经授权使用加密模块

如第三方未经授权成功的使用加密模块，将导致多种危害，如：使入侵者能读取加密编码甚至操作关键的安全参数，导致加密过程不再有效；导致加密模块工作在不安全的状态；利用加密模块实现伪装。

对策：

- ✧ 应用系统测试TCE_APT
- ✧ 系统安全检测和验收OEN_TES
- ✧ 计算环境访问控制TCE_TAC
- ✧ 密码技术TIN_ENC
- ✧ 账户管理OHO_ACC
- ✧ 身份鉴别TCE_IDT
- ✧ 网络设备用户身份鉴别TNI_IDT
- ✧ 安全审计TCE_SAU

5.45 TMALICE.ENCM 加密模块被操纵

犯罪者为了能读取加密编码、修改加密编码或修改重要的安全参数操纵加密模块。可以通过多种方式实现对加密模块的操纵，比如：获取超级口令；未注册测试模式的敏感部分随时可以访问；特洛伊木马；获取某一命令的访问权限等。

对策：

- ✧ 应用系统测试TCE_APT
- ✧ 系统安全检测和验收OEN_TES
- ✧ 计算环境访问控制TCE_TAC
- ✧ 账户管理OHO_ACC
- ✧ 身份鉴别TCE_IDT

- ✧ 网络设备用户身份鉴别TNI_IDT
- ✧ 安全审计TCE_SAU

5.46 TMALICE.KEY 危及密钥安全

进行加密时，安全性依赖于保密加密代码的机密性高低。因此潜在的破坏者总是试图获取加密所用的编码。可能出现的攻击点为：编码的处理不合适；编码没有被存放在一个安全的介质上就被输出；编码备份被盗；编码被暴力破解；加密模块被破解；内部破坏者散发加密编码。

对策：

- ✧ 密钥管理OCO_KEY
- ✧ 安全培训OPE_TRA
- ✧ 岗位安全职责OOR_STA
- ✧ 安全策略执行PIN_EXE
- ✧ 存储介质的保护ORM_PRO
- ✧ 存储介质的访问控制ORM_ACO
- ✧ 密码技术TIN_ENC

5.47 TMALICE.INTE 应被保护的信息的完整性缺失

数据完整性丢失将会带来多种问题：

- 数据不可读；
- 数据被伪造；
- 数据无法解码或拆包；
- 数据无法进行解码验证真实性。

产生数据完整性缺失有多种方式：

- 数据传输过程中载波超负荷；
- 传输错误；
- 计算机病毒对数据的改变或毁坏；
- 数据被操纵。

对策：

- ✧ 网络拓扑设计和规划ONE_TOP
- ✧ 网络可靠性管理ONE_REL
- ✧ 防病毒管理OHO_VIR
- ✧ 防病毒网关TEB_TVI
- ✧ 病毒和恶意代码防范TCE_VIR
- ✧ 数据库设计安全TCE_DBS
- ✧ 主机入侵防范TCE_IDS
- ✧ 网络入侵防范TEB_IDS
- ✧ 存储介质的保护ORM_PRO
- ✧ 存储介质的访问控制ORM_ACO
- ✧ 存储介质的备份ORM_BAC

5.48 TMALICE.CTRL 管理参数被操纵

故意的错误配置可能会导致针对管理系统的攻击。如果网络组件通过管理系统被控制，所有配置参数都被管理系统所控制。

对策：

- ✧ 账户管理OHO_ACC
- ✧ 岗位安全职责OOR_STA
- ✧ 配置管理计划OCO_PLA
- ✧ 安全审计TCE_SAU
- ✧ 选择安全控制措施ORA_CTR
- ✧ 安全策略执行PIN_EXE

5.49 TMALICE.WEB　web 欺骗

Web 欺骗包括伪造 WWW 服务器和运用 DNS 欺骗进行。

对策：

- ✧ 主机入侵防范TCE_IDS

- ✧ 网络入侵防范TEB_IDS
- ✧ 身份鉴别TCE_IDT
- ✧ 系统安全检测和验收OEN_TES

5.50 TMALICE.SCR 滥用脚本内容

在Internet上冲浪时，WWW站点上的脚本内容将被加载到用户的计算机上（如ActiveX或Java Applets）。这些脚本能自动检查来自用户的机密数据，并通过Internet将这些信息返回给入侵者。

对策：

- ✧ 主机入侵防范TCE_IDS
- ✧ 计算环境访问控制TCE_TAC

5.51 TMALICE.HIJ 网络连接的被劫持（控制）

连接劫持比连接被窃听更为严重。数据包的注入网络导致客户端故障。服务器不能检测到客户端被替代。当用户完成认证后，入侵者就可以顶替已经认证人员的名字工作。如 TELENT 连接被劫持。

对策：

- ✧ 防干扰和窃听TPR _TAP
- ✧ 网络可靠性管理ONE_REL
- ✧ 安全审计TCE_SAU
- ✧ 安全策略执行PIN_EXE