终端安全风险管理

李小平　等编著

机械工业出版社
CHINA MACHINE PRESS

终端安全风险管理

李小平　倪静石

于海波　孙　鸿　　编著

王国强　袁　宏　李雪莹

机械工业出版社

尽管人们已经认识到终端是网络中大部分行为的源头和起点，是最终的端点，并且认识到终端安全是网络与信息安全管理的重要内容，因此采用了大量产品和技术解决所面临的终端安全问题，但终端仍旧屡屡发生“问题”。其原因在于现有产品的技术工具色彩浓厚，单一功能性强，整体性不足。本书作者在多年实践经验的基础上，提出终端安全管理的实质就是终端安全风险管理，并系统地阐述了管理的关键是“管理自动化”的观点。本书从实际出发，基于信息安全风险评估理论，介绍可识别和分析的终端安全风险，构建结构性的终端安全风险体系，基于管理自动化的原则，构建终端安全管理体系的方法。本书有助于读者摆脱终端安全管理工作中面向威胁被动防护的局面，构建更为有效的面向能力的终端安全主动防御体系。

本书特别适合用作信息安全、计算机、通信、电子工程等领域的科技人员的技术参考书，或作为相关专业的教材。

图书在版编目（CIP）数据

终端安全风险管理 / 李小平等编著．—北京：机械工业出版社，2012.6

ISBN 978-7-111-37390-2

Ⅰ．①终… Ⅱ．①李… Ⅲ．①计算机网络-安全技术 Ⅳ．①TP393.08

中国版本图书馆 CIP 数据核字（2012）第 139077 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

策划编辑：丁 诚 宋 丹

责任编辑：丁 诚

责任印制：乔 宇

三河市宏达印刷有限公司印刷

2012 年 7 月 • 第 1 版第 1 次印刷

184mm×260mm • 18.5 印张 • 456 千字

0001－6000 册

标准书号：ISBN 978-7-111-37390-2

定价：52.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务

社 服 务 中 心：（010）88361066

销 售 一 部：（010）68326294

销 售 二 部：（010）88379649

读者购书热线：（010）88379203

网络服务

门户网：http://www.cmpbook.com

教材网：http://www.cmpedu.com

封面无防伪标均为盗版

序

信息革命是当今世界发展的大趋势，我国信息化也正快速发展，极大地促进着国民经济和社会的发展。但与此同时，信息安全也成为全球关注的焦点。

信息安全保障是多层次的复杂系统，其中终端是网络安全行为的源头，是安全防范的重点。据 IDC 统计，对于企业来说，来自内部终端的安全威胁占整个安全威胁的 70%以上。由于企业内部终端数量多，人员素质不同、流动性大，而产生病毒泛滥、终端滥用资源、非授权访问、恶意终端破坏、信息泄密等安全事件不胜枚举；政府部门也出现了不少的终端安全事件。

终端设备的多样性和复杂性，以及安全产品和服务的频繁更新，都使终端安全问题变得十分复杂，而头痛医头、脚痛医脚的安全防范策略是无法解决终端安全问题的。

在本书中，作者根据多年安全管理实践经验，体会到终端安全管理的实质就是终端安全风险管理，终端安全管理工作应以风险管控为主线。

作者采用分级分类的方法构建了终端安全风险体系，阐述了终端安全风险内容，从全生命周期、全过程和重要对象保护三个方面出发建立终端安全风险管理体系，力争做到终端安全管理工作“可知、可控、可管”。

本书把“终端安全风险体系”和“终端安全风险管理”二者在“防管一体化”的思想指导下统一起来，构建终端安全平台，对信息安全工作者具有借鉴意义。

中国工程院院士 何德全

前　言

1946 年，在美国宾夕法尼亚大学的莫尔电气工程学院揭幕典礼上，一个占地面积达 170 多平方米、重约 30 吨的庞然大物，为来宾呈现了一场精彩的“表演”——在 1 秒钟内进行了 5000 次加法运算，这比当时最快的继电器计算机的运算速度要快 1000 多倍。这个庞然大物——ENIAC 的完美亮相，不仅使得来宾们喝彩不已，也开启了科学计算的大门，成为人类进入信息时代的重要标志。1969 年，互联网的到来，又将人类带入了以计算机网络为核心的信息时代。21 世纪的今天，计算机已经成为社会生产和生活中必不可少的工具。

随着互联网在全世界的迅猛发展和广泛应用，网络也成为了悬在人们头上的达摩克利斯之剑，危机和风险无处不在，信息安全问题越来越严重。一则来自网上的报道说：“去年夏天，在拉斯维加斯举行的 DefCon 黑客安全会议上，两名安全顾问在一屋子黑客和计算机安全专家面前，演示了如何用 6 美元和几行代码就攻击并占领了一家公司的网站两个小时”。这个案例在让我们震惊的同时，也让我们感到了潜在的危机。在数字化、网络化的今天，网络上早就难有秘密可言，网络已经将我们变得透明。不过，这并不可怕，世界上很多的事情都大抵如此，可怕的是我们对此毫无防备，却主动一头扎进了陷阱里，还茫然不知。其实，从电脑诞生的那天起，信息安全就已经和它形影不离，但是，从来没有像今天这样备受瞩目，这样被广泛重视。

“千里之行始于足下”，解决信息安全问题，就要从基础和源头入手，从每个人使用的计算机——终端开始。因为，终端不仅关系着个人和单位的信息安全，同时终端也是网络的边界，影响着单位整个网络的信息安全。因此，终端安全是信息安全的基石，关注终端安全，就是关注信息安全，从使用者开始着手，防患于未然；解决终端安全风险，也就是解决了“托管”于使用者的网络边界的潜在危机。

本书从终端安全管理及其发展、终端安全风险分析、终端安全风险管理体系及其实现和终端安全风险行业化管理及应用案例四个方面，对终端的安全管理做了详细阐述和分析，并探索性地提供了终端安全在实际应用和行业型单位中的解决方案。书中提出终端安全管理就是风险管理的新理念和以风险管控为主线的新方法，对以前终端安全管理工作中存在的问题和弊端进行了深入分析，力求全面系统地展现终端安全问题的来源和发展方向；对终端安全体系和分类的构建方法作了介绍；通过终端“全生命周期”的风险分析，围绕安全重要对象保护和风险全过程管理，建立风险管理体系，力争实现终端安全风险的“可知，可控，可管”。本书倡导以安全效益为导向，以国家相关信息安全法律法规为依据，以终端安全规范建立为基础，以终端安全管理工作自动化开展为目标，以信息化为手段，建立“防管一体化”的终端安全平台，实现终端安全从“三分技术，七分管理”转向“七分技术，三分管理”，强调了技术支撑的必要性，提出了技术支撑的着眼点和落脚点。书中还构建“终端安全风险体系”和“终端安全风险管理体系”，提出了建设“终端安全防护平台”，建立终端安

全管理基础，及时发现、评估和防护风险，通过“机人”自动交接，实现从安全防护到安全管理的过渡衔接；提出了建设“终端安全管理平台”，建立终端安全管理架构、管理策略、残余风险处理和安全日常运维监控等体系，形成终端安全管理工作规范，强调安全重点对象、重要风险的管控和分析，建立终端安全保护基线。通过“防管一体化”终端安全平台的建设，努力实现能规避的风险自动防护，不能规避的风险，在风险发生之前，降低风险级别，减少风险发生次数，在风险发生之后，降低风险损失，缩短风险影响时间，实现现有终端安全从被动式管理向主动式管理的转变，保障终端安全的有序和全面系统管理。

知己知彼，方能百战不殆。作者编写本书的目的是为了让读者从不同角度、不同层面去认识和了解终端安全，在信息安全风暴来临前，有一个充分的准备。期望本书能成为读者了解信息安全知识的一个窗口，开拓现代科技事业的一条纽带，让终端安全风险管理为人类享受科技生活保驾护航。

本书编撰过程中得到了各方面的大力支持，特别是江苏省地方税务局，江苏省盐城地方税务局和北京天融信公司等单位的倾力协助，鸣谢（不分先后）：赵连才、刘斯宇、孙艳、朱惠林、刘红霞、罗秀春、朱俊龙、徐小兵、倪习同、钱磊、黄春亮、叶杨、惠喜岷、张凌云、刘扬、张铁铮、熊毅、唐宁、杨燕森、刘勇、杨圣峰、汤泰鼎、高晶、周国华、康新强、章露、李小刚、毕向阳、李林、杨光、黄善宇、魏琪、卢喜、孙艳丽、杜蕊、秦荔刚、陈俊、江志峰、张祯、郭艳峰、杨木超、项文峰、吴青松、杨军、李颖、彭鹏、黄蒙蒙、王栋、吴之奇、朱启坤。

作 者

2012 年 7 月

目　　录

附录 终端安全风险分析报告

第 1 部分

终端安全管理及其发展

第 1 章　认识终端与终端安全

1.1　什么是终端

偶然一个机会听了一堂营销管理的讲座，讲师重点讲解的是“终端营销”的方法。其中“终端”是指与消费者直接发生买卖关系的经营场所，即销售给最终客户的卖场、商家，是流通环节的最后一环，是产品的投放地，如大型物流中的沃尔玛、家乐福、国美和苏宁都属于“终端”。在营销领域谁控制了销售终端，谁就找到了创造企业价值的通路。图 1-1 为营销终端示意图。

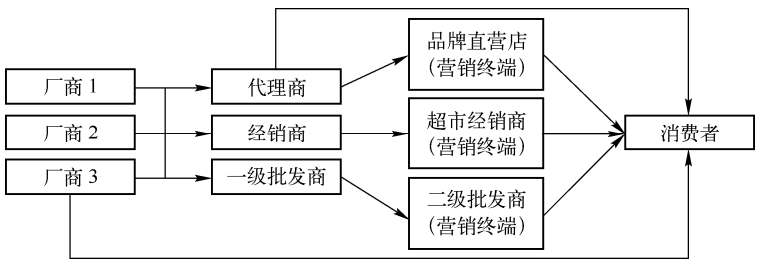

图 1-1　营销终端示意图

在通信行业，也会频繁听到“终端”这个词，在这里“终端”指的是“移动终端”，又叫做移动通信终端，如图 1-2 所示，这些终端通过通信网实现互联和信息交换。顾名思义，移动终端是指可以在移动中使用的计算机设备，广义上包括手机、笔记本、POS 机、车载电脑等。在通信行业中，大多数情况下终端指的是智能手机。就国内三大运营商争先恐后推出自己的智能终端的情况看，终端在运营商的心目中备受关注。

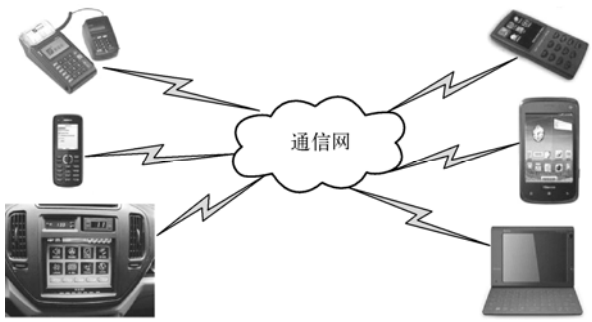

图 1-2　移动终端示意图

可见，“终端”一词在不同行业、不同领域有不同的定义，本书的内容紧紧围绕着“终

端”展开。那么“终端”概念最早出现在何时呢？本书中的“终端”具体指什么呢？

让我们回到40多年前。

1969年，为了军事研究的需要，在ARPA资助下，ARPA net于1969年投入使用，由此现代计算机网络产生，随之，计算机被分为主机（Host）和终端（Terminal）。当时的主机通常指大型机或功能较强的小型机，而终端则是指一种计算机外部设备，是一种字符型设备，包括多种类型。图 1-3 中展示了工作人员在早期的字符终端设备上工作的情景，其中工作人员面对的就是一台字符终端设备，主要作用是作为输入/输出信息的展示，实际操作的数据和相关的处理是在主机上进行的，就是旁边的“大设备”。

图 1-3　早期的字符终端设备

这个早期的字符设备就是最早的终端。终端的概念最早出现在计算机领域，当时的终端指的就是计算机终端。随着名字的宽泛化、关联化和象形化，终端一词逐步被其他领域引用并推广，其中就包括前面提到的营销领域和通信领域。

早期计算机主要是作为计算的工具被使用。主要应用于科学计算、工业过程自动化控制和军事应用（例如，雷达数据处理、武器控制、军事情报等）。其中的核心应用就是计算（表现在软件中计算指令使用率高）。20 世纪 80 年代中期，计算机网络和可视化技术的发展使计算机的应用迅速普及，其中心工作已经不是计算，而是逐步转为满足各种用户需要的业务任务的处理，主要是解决人类活动所产生的大量问题，计算机信息系统已经纳入人类活动的范围内，信息系统使用与人类活动与行为有直接关系，而且关系越来越密切。许多行业的业务活动已经离不开信息化系统支持。此时，计算机与计算机网络完全是人类活动的工具。㊀

随着业务信息化的推进，终端在业务专网中大量使用。本书重点讨论的终端，不是泛指计算机领域中的所有终端，而是指使用者在与互联网隔离的业务专网中直接使用的设备和网络安全的发生节点，包括 PC、工作站、服务器、笔记本等，这些终端共有的特征是接入网络，可以接收和发送信息与数据，可以在使用者的操作下，通过操作系统产生网络访问和数据交互，可以对网络环境产生影响。

1.2　终端的配件

终端在发展过程中，一开始是大型设备或者项目的附属工具，但是随着科技的发展，终端从设备的辅助和支持角色，逐渐转换成了工作中的主体角色，而在使用过程中，为了弥补和增强终端功能，使用了其他设备与之配合，这些设备通常称为终端的外部设备（简称外设）。终端外设现在已经成为了一个规模庞大的产业，拥有大量的行业规范和标准，甚至反过来约束和影响终端的发展。

终端外设种类繁多、功能多样，而且有的设备还是具有多种功能的组合型外设，从功能

㊀ 该段文字引自屈延文先生的《网络世界白皮书》。

的角度来分类，外设分为：输入设备、显示设备、打印设备、外部存储器和网络设备。

输入设备主要是指人机交互类设备，用于其他类型（文字、图像、声音等）数据的处理和转换，输入到终端设备中，使得终端设备可以继续处理。输入设备一般包括键盘（图 1-4）、鼠标（图 1-5）、扫描仪器、手柄、摄像设备等，这些设备的使用是数据采集的需要，其设备本身并不会产生安全风险，但是使用或者数据保存不当就容易产生安全问题，因此人机交互类设备往往以数据跟踪为监管重点，设备控制以支持和兼容为主。

图 1-4　键盘

图 1-5　鼠标

显示设备主要是指显示器（图 1-6）、投影仪等显示信息的设备，用于了解当前终端的操作过程和运行过程。现在终端设备往往需要复杂的操作和运行来实现功能，例如键盘输入、鼠标操作等，如果在没有显示设备支持的情况，基本上是不可使用的。同样的，操作之后终端的运行过程和运行结果也需要显示设备的支持，才能全面了解，由此可见显示设备对于终端的重要性。

打印设备主要是指打印机（图 1-7），打印机是最传统的外设，也是最常用的外设，因此也是安全管理过程中的重点。打印设备可以将终端的数据转化成纸质的信息，可以脱离终端使用和流通，不受终端的控制和监管，在方便工作和生活的使用过程中，也增加了信息的扩散和泄密的风险，对于打印设备的使用情况和打印内容的监管是终端安全的重要内容。

图 1-6　显示器

图 1-7　打印机

外部存储设备是终端使用过程中的有益补充和安全辅助，外部存储设备解决了数据长期保存、安全备份和快捷传递等问题。从经济角度来看，相对终端内部存储设备而言，使用低速、大容量和低成本的外部存储设备，可以有效提高设备的实用性。外部存储设备包括磁带

机、磁盘阵列和移动存储设备，其中移动存储设备由于使用灵活和携带便捷，已经成为现在工作和生活中不可或缺的一部分。移动存储设备的优点同样也是其发生安全问题的重大隐患，近年由于移动存储设备造成的泄密事件屡见不鲜，对于移动存储设备的监控也成为终端问题，甚至成为信息安全问题的重中之重。移动存储设备种类多样，根据设备基础类型分为U盘（图1-8）和移动硬盘（图1-9）两种类型，U盘的体积越来越小，容量越来越大，正是因为其经济实用的特性应用非常广泛。U盘的应用广泛也带来了管理上的问题，数据可以通过U盘进行传递，而U盘本身的管理存在困难，U盘的盗用和冒用现象非常多，通过U盘进行数据的非授权复制现象也很难有效控制。

图1-8 U盘

图1-9 移动硬盘

网络设备是指终端与终端之间连接在一起的硬件实体设备，包括调制解调器（Modem）、集线器（Hub）、交换机、路由器（图1-10）、防火墙等，网络设备除了可以完成网络连通的基础功能之外，还可以通过网络准入、网络过滤等方式解决网络安全问题。

图1-10 路由器

1.3 终端所处的环境

从单一终端出发分析终端的使用环境时，可分为其自身的运行环境和终端应用的网络环境。

终端自身运行环境包括Windows类操作系统、非Windows类操作系统，通常被称为Windows类终端和非Windows类终端。

Microsoft公司推出的Windows类操作系统以其友好易用的人机交互界面，在推动终端的普及过程中起到了决定性的作用，因此其在商务和家庭用户终端操作系统中占比最大。目前，国内主要的工作终端运行操作系统以Windows系列为主，常见的版本有XP、Vista、Win7等个人版本和NT、2003、2008等服务器版本。2005年4月25日，Microsoft公司在西雅图WinHEC 2005大会上正式推出64位操作系统后，业务网终端所使用的操作系统逐渐呈现从32位到64位的转变，目前很多企事业单位在用的终端操作系统的版本有32位和64位两种。

广大的用户群也使Windows类操作系统成为黑客、恶意软件最为青睐的攻击目标。尽

管 Windows 操作系统在漏洞修复、系统安全属性完善上做了大量的工作，但遭受病毒、木马入侵等的报道仍层出不穷。

非 Windows 类终端主要指不使用 Windows 类操作系统的终端，主要为 UNIX 类和非 UNIX 类，UNIX 类包括 BSD、Solaris、AIX、HP-UX、Linux，等等，非 UNIX 类包括 APPLE 公司的 MAC OS 等。非 Windows 类操作系统的终端普及范围远远低于 Windows 类终端，其遭受的攻击也远远少于 Windows 类系统。

网络的普及和业务信息化的趋势，使终端的使用从个体独立运行逐渐转变为集群协作，无论是工作协调还是信息传递，单一终端独立工作的情况越来越少，终端之间的影响也越来越大，终端在所处环境中与其他终端之间的联系也越来越紧密。网络有很多种，包括从网卡直连的对等互访，到网络设备连接的小型局域网，再到网络链路组成的专网和互联网。在这些网络中，专网的安全性问题最为引人关注。在实现业务的专网中，计算机终端是网络中大部分行为的源头和起点，也是安全问题（如病毒传播、从内部发起的恶意攻击、内部保密数据盗用或失窃等）发生的源头。对每个单位来说，终端安全管理都是非常重要的，良好的终端安全控制技术能够保证企业的安全策略真正得到实施，从而有效控制各种非法安全事件，遏制网络中屡禁不绝的恶意攻击和破坏。

终端的使用环境，可以从广义和狭义两个角度来看，狭义的终端环境，指单一终端自身的操作系统和所处的网络情况，即终端环境包括终端自身的运行环境和终端应用的网络环境；从广义上看，所有终端所处的网络环境也同样是终端环境，差别在于广义上终端不是独立的个体，而是所有环境中的一个影响因素，并且互相作用和影响。

1.4 终端的使用者

对于企事业单位而言，接入其业务网络的终端包括其自有终端和外来终端两种。终端的使用者就其与接入网络的企事业单位之间的关系可分为内部人员、临时人员和外来人员 3 大类。就这 3 类人员在实际工作中所承担的工作不同，对于终端的使用方式和操作内容也不同，可对这 3 类人员进行细分。

内部人员通常包括管理人员、业务人员、网络/系统管理员 3 类；临时人员主要指在一些辅助岗位工作的人员；外部人员包括单位所在系统内的外来人员、厂商运维人员等。

不同的人员涉及的终端类型不同，参见表 1-1。

表 1-1 终端使用者-管理规范对应表

终端使用者		使用终端设备	操 作 内 容
内部人员	管理人员	固定终端设备	业务系统 公文 个人信息
		移动终端设备	公文 个人信息
	业务人员	固定终端设备	业务系统 公文 外部信息 个人信息

（续）

终端使用者		使用终端设备	操 作 内 容
内部人员	业务人员	移动终端设备	公文 外部信息 个人信息
	网络/系统管理人员	固定终端设备	公文 资产信息 网络管理系统
临时人员	辅助岗位工作人员	固定终端设备	公文 外部信息 个人信息
外部人员	厂商运维人员	固定终端设备	外部信息 网络管理系统
		自带移动终端设备	外部信息 网络管理系统 专业工具软件 个人信息
	系统内外来人员	固定 PC 设备	业务系统 公文 外部信息 个人信息
		自带移动 PC 设备	公文 外部信息 个人信息

表中涉及的设备名称定义如下：

（1）“固定终端设备”指组织配备的固定办公用业务终端或者公共终端设备，包括 PC 和服务器。

（2）“移动终端设备”指组织配备的可移动办公的移动终端设备，如笔记本电脑。

（3）“自带移动终端设备”指非组织配备的可移动办公终端设备，如笔记本电脑。

1.5 聊聊终端的安全问题

计算机网络技术迅速发展，网络应用快速普及，使办公信息化成为一种趋势。得益于终端和网络的支撑的“无纸办公”，一方面带来了管理的规范化，提高了整体的工作效率；另一方面因为网络与生俱来的安全性问题带来诸多安全问题的困扰。

随着人们对计算机安全意识的加强，逐渐认识到在网络攻击面前最薄弱的环节和最容易出现问题的地方是终端，终端是人类世界与网络世界的接口，是真正的网络边界。终端作为网络行为的发起者和执行者，终端安全问题是信息安全领域的重要组成部分。终端安全已经成为制约信息安全的瓶颈，尽管在安全技术和培训中已经投入了大量人力和资金，但终端安全问题仍频频发生。

终端具体面临着哪些安全问题呢？

日常终端使用中常见到以下几种现象。

现象 1：终端使用中，基本配置工作，“去繁就简”。

“每次开机都要输密码，太麻烦了，设置为空，很方便的。”

“离开一会儿给电脑锁屏，回来还得重新登录，不方便，我离开从来不锁屏。屏保也不

设密码。”

“微软又出了好多补丁，打起来真慢，还有很多工作要做，稍晚几天再说吧。”

现象 2：运行使用中，我行我素。

“单位电脑上有炒股软件和游戏，不忙的时候，午休的时候可以玩会儿，或看一下，我这是工作生活两不误啊，哈哈！”

“明天要交的文件没写完，带笔记本回家写，写完了正好可以在家里上上网，下载点儿资料。”

现象 3：关注应用，忽视了数据。

“OA 系统账号忘了，要下载个文件，借用一下你的账号。”

终端所发生的安全问题可简单归结为 3 类。

（1）基础安全问题

终端自身软、硬件（图 1-11）使用时所出现的安全问题，这些问题的发生与是否接入网络无关。

基础类安全问题至少可包括：

- ✓ 操作系统安全性
- ✓ 操作系统的补丁和漏洞
- ✓ 操作系统账号密码修改周期
- ✓ 操作系统账号密码复杂度
- ✓ 操作系统账号密码长度
- ✓ 操作系统运行进程的安全性
- ✓ 操作系统支持的外设启/停
- ✓ CPU 占用
- ✓ 内存占用
- ✓ 硬盘占用
- ✓ 端口占用
- ✓ 多网卡使用安全性
- ✓ 共享文件
- ✓ 进程使用安全性
- ✓ 性能使用安全性
- ✓ 外设使用安全性
- ✓ 密码口令安全性
- ✓ 网络资源安全性
- ✓ IP 使用安全性
- ✓ MAC 使用安全性

（2）运行安全问题

终端接入网络（图 1-12）后，在使用中所出现的安全问题，这些问题是终端接入网络中时发生的。

终端在连接入网运行中，至少会遇到以下问题：

- ✓ 网络运行安全性

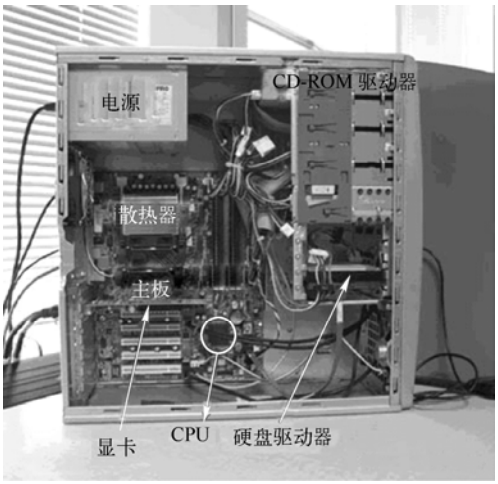

图 1-11　硬件

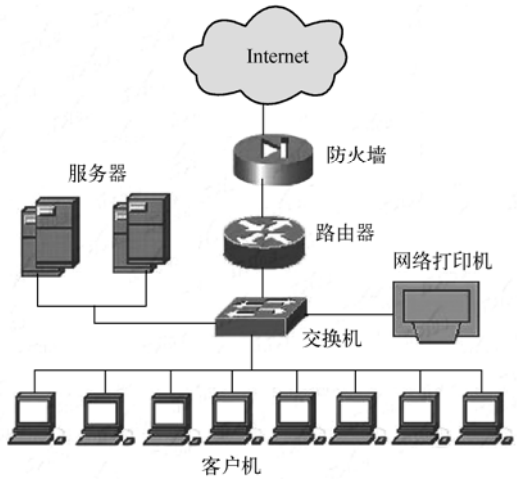

图 1-12　终端接入网络

- ✓ 终端产生的流量对网络的安全性
- ✓ 终端访问远程主机的方式对网络的安全性
- ✓ 网络信息安全性
- ✓ 网络内 IP 和 MAC 的安全使用
- ✓ 终端运行安全性
- ✓ 终端使用的进程安全性
- ✓ 终端使用的服务安全性
- ✓ 终端使用的操作系统性能安全性

（3）信息安全问题

与终端上所操作的信息的安全相关的问题，这些问题发生时将直接影响终端所操作或存储信息的机密性、可用性或完整性。

- ✓ 边界控制安全性
- ✓ 非法内联安全性
- ✓ 变更使用安全性
- ✓ 终端变更使用者安全性
- ✓ 终端变更使用范围安全性
- ✓ 终端转网安全性
- ✓ 信息的扩散和泄密
- ✓ 终端上重要文件的操作安全性
- ✓ 终端上重要文件的管理安全性
- ✓ 终端上移动存储设备使用安全性
- ✓ 管理类风险
- ✓ 管理人员操作安全性
- ✓ 管理工具安全性
- ✓ 监控信息安全性

第 2 章　怎样保障终端安全

2.1　终端安全管理到底是什么

自 1946 年 2 月，第一台电子计算机 ENIAC 在美国宾州问世以来，短短几十年时间，计算机在人类社会里经过了电子管时代（1946～1959 年）、晶体管时代（1960～1964 年）、集成电路时代（1965～1970 年）、大规模集成电路时代（1971 年至今）。4 个时代更迭，技术也在不断创新。

进入 20 世纪 70 年代以来，伴随着计算机技术的迅猛发展，一大批先驱为打破美国政府和军事工业集团对计算机技术的垄断，开始打造个人计算机（PC），其中就包括乔布斯和盖茨，使计算机的发展、人类的生活方式和通信的有效手段得到了跳跃式的进步。这些早期的计算机技术爱好者既推动了计算机技术的飞跃发展，也为计算机和信息安全埋下了一颗不小的定时炸弹。

1988 年，一个年轻有为的美国热血青年莫里斯，为发泄对美国经济和政府的不满，炫耀强大的才能，编写了“Morris 蠕虫”病毒，致使近 6000 台计算机瘫痪，涉及军队、政府、医疗和金融等多个行业，而他的父亲就是美国安全局（NAS）从事计算机研究的专家。

同年，美国还发生了入侵“星球大战”项目事件。

……

一系列安全事件后，在美国政府的资助下，卡内基·梅隆大学成立了全球第一个计算机应急安全响应组（CERT）。

随着计算机在人类生活各个领域所扮演的角色日趋重要，入侵、病毒爆发和木马对信息的窃取等计算机安全事件也日益严重，业界对于信息安全问题认识也不断深入，应对计算机安全事件的方式方法也不断更新和完善。

随着信息安全管理体系的不断实践、更新和完善，人们越来越发现，安全问题最终可归结为风险管理问题。信息安全管理体系的构建目的实际上就是解决安全风险的管理问题。

因此，终端安全管理的实质就是识别终端安全风险，构建终端风险体系并对终端风险进行安全管理，从而避免终端安全风险事件的发生。

2.2　时刻准备，及时防护

经过长时间的探索和分析，我们把计算机终端安全大致分为两方面，分别是计算机终端的物理安全和系统安全。

计算机终端的物理安全就是计算机所在物理环境的安全与计算机自身硬件的安全。物理环境安全就如同一个人的生存、生活和工作环境，环境适宜，心情和工作都会比较舒畅，环

境恶劣的时候人也会生病。同理，计算机也有比较适宜的工作环境（如周边环境的湿度、温度、电压和雷击等），当环境的某个或多个因素超过计算机的极限承受能力时，计算机也会像人一样“生病”。

计算机终端物理安全还包括计算机各个元器件的自身安全，如硬件的自身损耗、人为破坏和被盗丢失等。因此，计算机的使用过程中就要有对于硬件的保护和维护工作。

随着人类科技实力的不断提高，计算机各个零部件的寿命和强度都有了明显提高，但因为自身构造等特点，一些硬件使用不当极易遭到破坏，导致计算机无法正常使用。

目前，计算机已大规模步入人类文明生活的各个方面，对于人类生活的办公、娱乐和学习都有着重大影响。同时，木马和病毒在计算机世界横行（本书将对这些威胁进行详细介绍）。因为计算机存储了大量的个人、商业和军事信息，一些不法人员为非法牟取利益将黑手伸向了这些终端，盗取硬件、施放木马和恶意程序等，无不危害着计算机终端的正常使用和操作员的正常工作与生活。

以上就是对计算机终端安全中物理安全性的简单描述。计算机终端安全的另一方面则是系统安全，是本书重点介绍的部分。

计算机终端系统安全主要是操作系统相关技术和网络安全技术两个部分。

操作系统相关技术是针对目前终端使用的主要操作系统，如 Windows、UNIX 等，包括操作系统的驱动开发、信息获取和接口调用等。

网络安全技术包括网络设备的相关接口开发、网络信息的扫描和探测等。

与终端安全相关的事件统称为终端安全事件。有效地区分与终端安全相关的事件，是分析终端安全状况的首要工作和基础工作。

终端在使用过程中会产生众多事件，每一个事件都有可能与终端安全相关，但并不意味着这些内容都属于终端安全事件范畴，不对这些时间进行严格的区分、限定和归并，就极可能导致对于终端安全的分析工作陷入误区。因此记录终端和区分终端产生的事件是否属于安全事件就是终端安全工作需要完成的重要工作。终端自身产生的事件，取决于事件的产生源，不可能把所有的事件全部记录，所以，对于终端安全的相关事件，有相当大的一部分来自网络和第三方工具的分析。

终端安全防护主要是建立在计算机终端可能发生风险的各个方面的有效管控，通过制度与技术有效结合的方式，减少甚至杜绝各类风险事件的发生，针对终端使用过程中可能发生风险的操作行为进行详细记录，通过分析之后进行具有针对性的防护措施和相关功能的管控。管控措施如下：

1．基础类防护措施

（1）操作系统安全防护

对操作系统进行安全加固；关闭不必要的服务、端口和来宾组等；为不同用户开放不同的权限，防止安装过多应用软件及病毒和木马程序的自运行。

（2）进程运行监控

对运行以及试图运行的进程与进程树进行监视和控制；防止病毒和木马等恶意程序调用进程。及时了解操作系统开启服务与程序情况，防止恶意程序后台运行。

（3）操作系统性能监控

对操作系统内存和 CPU 利用率等基本性能的监控有助于了解对系统资源占用过大的程

序，从而鉴定其是否为正常运行或正常程序；有助于对计算机硬件利用率的掌握和硬件性能的维护。

（4）终端外设使用监控

对终端外设接口、外联设备使用的监视和控制能有效地控制计算机的资源利用率，规范计算机资源使用，防止因滥用计算机外接存储设备造成的木马、病毒的泛滥传播等。

（5）操作系统密码口令检查

定期改变具有一定复杂度的密码及密码策略可以有效地防止非授权人员进入计算机终端，防止非法人员窃取计算机终端信息，所以，对操作系统口令的检查能有效地督促计算机终端设置合规的用户口令，保证终端安全。

（6）网络配置信息监控

网络配置信息包含计算机网卡的 MAC、IP 地址和计算机路由器的接口信息等。对网络配置的有效监控可以及时发现非法接入信息系统的非法终端，防止非法终端接入可信网络窃取信息、传播病毒等。

2．运行类风险防护

（1）操作系统网络流量监控

对操作系统各用户、各时段的流量监控可以有效地判断计算机内是否存在程序、服务在上传或下载信息，及时判断计算机是否感染木马程序致使信息外发，或成为共享服务站造成信息泄漏。

（2）操作系统网络访问监控

对计算机终端进行的系统网络访问控制能有效地防止计算机进行违规互联，防止信息因共享等方式进行违规流转，防止木马、病毒在信息系统内大规模爆发。

（3）操作系统运行状态监控

对操作系统运行状态的监控可有效地了解到计算机终端长时间未登录、企图进入安全模式等绕过行为，监控主机调用的端口、服务等系统信息，保证计算机终端时刻处于被监控状态。

3．信息类风险防护

（1）安全准入控制

非法主机接入可信信息系统可能导致内网信息外泄、病毒、木马传播扩散和对内外服务器攻击等严重后果，因此对计算机终端的安全防护中，准入控制是极为重要的一项防护手段。

（2）终端使用者变更监控

计算机终端可能归属不同人员使用，不同用户及使用者对计算机终端有着不同的操作权限，对于变更使用者的计算机终端应及时改变资产所属人员以保证计算机使用权限正常，资产归属正常；防止计算机终端使用者非授权登录、使用计算机，保证计算机终端信息安全性。

（3）中心信息的防扩散和防泄密监控

按照国家保密标准及等级保护标准的明确规定，应有效控制信息的知悉范围，明确信息流向，对外泄信息进行安全回收，对外带便携式计算机及移动存储介质进行外泄后的信息清除，防止设备再次使用时信息被违规恢复。因此，做好信息的防扩散、防泄漏工作是非常必要的。

4．管理类风险

（1）管理人员操作监控

对管理人员的操作进行安全监控，一方面规范了管理员的操作行为，另一方面也使出现安全问题后的责任追查工作简单、明确、抗抵赖。

（2）管理工具运行状态监控

因管理工具为管理员所用，有着相同的用户权限，为防止管理工具内嵌木马、病毒等恶意程序，针对管理工具的状态监控，可有效防止管理员在不知情的状态下将木马、病毒等恶意程序感染传播至服务器等重要资源。

（3）监控信息实时分析

对于监控信息，应进行实时和准确的分析，在第一时间判断安全事件的发生所在，确定问题所在后进行快速响应与处理。

2.3 协调一致，全面管理

终端安全管理是将终端安全防护过程中发现的资产、脆弱性和威胁信息等，进行汇总、梳理和统计，实现对终端安全风险全生命周期的管理；通过对数据进行深度的关联分析，形成关联分析报告，为终端安全策略的制定提供依据；查看安全策略全局下发后的终端安全风险整体状况，为安全策略的调整提供决策支撑；为不同的用户提供不同的安全视图，保证不同层次的用户能够快速、方便地了解到所关心的安全信息。

其中，终端安全平台是终端安全管理体系的重要技术支撑平台，基于终端安全防护平台构建，终端安全管理平台在整个终端安全防护体系中起到的是“大脑”的作用，终端安全防护平台则起到“手”的作用。

由终端安全管理平台将防护策略下发到终端安全防护平台，终端安全防护平台在继承管理平台策略后，按照相应规则对计算机终端进行基于操作系统的进程、服务的监控、接口及外设的监控、终端资产及变更管理、管理员操作监控等行为监控。一旦终端安全防护平台监控到安全事件的发生，便将日志、报警信息等发送至终端安全管理平台，由终端安全管理平台对安全事件进行分析，确定终端安全事件根源所在，如非受控终端私自接入可信信息系统。将调整后的安全策略、相应信息发送到终端安全防护平台，由各个终端进行策略的集成和修改，对安全事件进行再次响应。

经过这样一个由头到手，手将信息反馈给头，再由头指挥手做出相关反应的过程，就完成了一个由安全管理平台、安全防护平台联合进行的终端安全事件的响应过程。

2.4 管理与技术并举

技术无论多成熟先进都是为人所用，为人服务的，技术的好与坏在非常大的层面上都取决于使用者，也就是说技术本身并无偏向性，但有了使用者的存在，技术就成了一把双刃剑。所以在注重技术管理的同时，人们也一直对计算机信息系统进行人为管理、人为干预，防止违法犯罪人员对计算机及信息系统进行破坏，从中牟利。

一直都说“三分技术，七分管理”，在计算机管理过程中的确曾出现过类似情况，技术

手段不够成熟，为防止计算机信息系统遭到破坏，为保护重要的数据资源，不得不耗费大量的人力对计算机进行安全保护，通过人为干预防止不法人员对计算机的破坏行为。

随着人类科技实力的不断提高，技术因素在计算机防护工作中所占比重日趋加大。以往的“三分技术，七分管理”逐渐演变为“五分技术，五分管理”，直至现阶段的“七分技术，三分管理”。虽然技术因素在计算机安全防护中所占比例越来越大，但是人的因素仍然在计算机安全防护中占有一定比重。

计算机技术发展至今，虽然能解决遇到的大部分问题，但是，诸如硬件被盗、摄影器材截屏、人为破坏等因素仍需要管理人结合管理制度进行安全管理，不能完全依赖于技术。如在进入涉密程度较高的区域时，必须将手机、照相机、PDA 等智能设备和图像处理设备上交且屏蔽管理；对于核心区域，应安排专职保安人员进行全天候值守，安放监控设备，防止不法人员侵入，造成计算机及数据流失；规范终端使用者的使用行为，防止因误操作将病毒和木马带入整个信息系统，防止终端资源被不合理利用。

作为一个完整的防护体系，在进行基于计算机的技术防护、人员管理之外，还应建立起一整套完整的管理制度用以辅助人员与技术管理。

一套完整的管理制度应至少包括：人员管理制度、计算机及信息使用制度、密码策略管理制度、资产使用管理制度、移动设备使用管理制度、人员奖惩制度和进入核心区域管理制度等。制度是由人来制定的，制定相关管理制度后更需要由管理人员进行实施和执行；对违规人员进行严肃处理；对于不再适应形势的制度应加以修改，使之被切实应用。

2.5 其他防护措施

随着人类社会的进步，科技文明的发展，计算机信息外泄的途径也变得多种多样。以上介绍了关于计算机操作系统和硬件的部分安全隐患和防范方式，下面对的计算机所面临的另一方面安全威胁进行详细分析，这个威胁就是电磁泄漏。

电磁信号广泛存在于生活的方方面面，电力传输、手机通信等诸多方面存在电磁信号，其中还包括日常应用的计算机及网络信号传输。

计算机在处理信息时，电磁信号会不可避免地夹带着信息数据通过导线、网线、空间等方式向外传播。实验表明，一千米内的计算机屏幕信号均可以被捕捉、还原，也就是说，在你处理信息时，一千米外就可能有人在看着你的显示器究竟出现了什么东西。网线在传输数据的同时也会夹杂着大量的数据信号向外扩散，甚至包括计算机所使用的电源都会将数据信号同电磁信息一起发出。这些数据信号一旦被非法还原将造成计算机大量的数据在处理信息的同时流失。

为保证电磁信号安全、不被还原，同时又能正常使用计算机，就必须对计算机进行电磁防泄漏处理，主要方式有 3 种：

1）基于显示器的电磁信号过滤。

2）基于导线传输的电磁信号过滤。

3）基于线路传导的电磁信号干扰。

对于显示器电磁泄漏现象，可使用电磁信号屏蔽仪对其进行电磁信号干扰，防止电磁信号被外部还原。电磁信号屏蔽仪主要分为两种：串接在机箱与显示器间进行视频信号的滤

波，通过对信号的过滤实现对电磁信号的保护；另一种则是安放在固定区域内，对固定直径范围内计算机电磁信号进行干扰，主要是以向外发送干扰信号的方式实现对固定范围内多台计算机电磁信号的干扰。两种干扰方式及干扰设备各有优劣。基于主机的方式较为安全稳定，但局限性高，对于笔记本无法实现防护；另一种则影响范围较大，但是根据实际测量情况反映，使用基于主机的电磁屏蔽设备较为安全。

对于线路电磁信号过滤，可采用线路传导干扰设备，串接在网线两端对流经网线的电磁信号进行滤波处理。线路传导干扰设备主要应用于远距离、不受控的信号传递间，对网线传输信息的质量、距离有一定影响。

对于计算机电源线的电磁泄漏，可通过使用红黑电源插座的方式实现。红黑电源插座的功能主要有两个：滤波、稳压。过滤流经插座的显示器、主机的数据信号，从而达到避免数据信息被还原的可能。

以上就是常见的几种电磁屏蔽设备，值得注意的是：任何设备都不是万能的，虽然可以避免绝大多数终端安全事件的发生，但是仍需使用者和管理者引起注意，防止因人为因素导致不必要的损失。再者，任何设备的增加都会不同程度地影响计算机的使用效率，但是，为保证终端安全，舍弃一部分资源作为终端及信息安全的代价也是值得的、应该的、必须的。

2.6 总结

到这里，几种终端常见的安全问题、解决办法和安全防护设备的介绍就告一段落了。须知，人作为终端的使用者和管理者才是事件的主导因素，计算机及信息技术只是作为一种工具存在，不能因为某些人、某些因素就以偏概全，否决计算机及信息技术给我们带来的利益及收获。随着技术的发展，将有层出不穷的信息技术应用于安全防护领域，对于可能发生的终端安全事件，应竭力避免，积极防御，引领计算机良性、健康地发展，营造良好的网络环境。

第 3 章 “终端安全管理”的现在和未来

3.1 国外终端安全管理是什么样的

国外信息安全工作往往呈现系统化和整体配套性，终端安全仅是整体信息安全的一个环节，是整个信息系统中的一个部分，与资产管理、人事管理、防病毒管理、网络管理、电子邮件、设施管理、Web 防护、数据管理、虚拟化和公众信息接口等整合在一起，系统化的解决来源于终端使用所带来的安全问题。

由于发达国家在信息领域的投入较早，重视较高，所以相对的，在集约化程度和管理制度方面明显优于国内，由于文化差异而造成的安全管理思路不同，所重视和发展的方向与国内也略有不同。以小见大，我们来分析一下一个跨国公司中的系统维护人员与终端相关的工作。

以下是一个系统运行维护工程师和终端相关工作的记录：

1）购置新的 PC 或者笔记本先到他们专门的 IT 服务部门。

2）事先根据他们的全球标准制定了相应的操作系统镜像（Image）文件。

3）利用 XX 网络引导，批量部署操作系统。整个过程完全自动完成，尽量减少因人为操作带来的配置更改和安全风险。

4）交付安装好的终端到最终用户。

5）用户使用 IT 部门分配的账号登录。

6）根据用户所在部门、业务需求，生成个性化桌面配置，应用系统安全策略，强制或者按需安装应用程序，包括各种业务客户端等（软件分发）。

7）后台实时更新操作系统补丁，并随时监控。

8）终端用户重要数据实时备份。包括个性化配置和数据文件。备份过程透明，无须用户干预。确保在操作系统崩溃或者硬件损坏时不致丢失重要数据。

9）记录软硬件资产，随时统计终端软硬件资产详情，记录变更情况并及时通知系统管理员（资产管理）。

10）终端出现使用问题时，远程接管用户终端，进行排错或者进行用户使用培训（远程维护）。

11）当操作系统损坏、操作系统升级时，直接利用平台的镜像部署机制，网络引导恢复用户操作系统，用户登录后所有的个性化配置和个人数据自动恢复。

12）硬件达到使用寿命报废，自动从系统里注销，并且在配置资产库和服务器平台注销/回收相关资源。

通过上述记录不难看出，运行维护工作覆盖了终端从购置到报废整个生命周期，整个维护工作有以下几个特点：

1）注重终端的资产管理　建立完善的终端设备的资产管理，以资产管理为中心，关注资产在全生命周期中的使用状态。

2）注重过程管理　在终端全生命周期中，对其进行严格的过程管理，有明晰的事务处理路线，以及过程控制指标。

3）注重策略标准化　根据终端使用环境特征，如部门、业务、人员、使用环境等特征，确定终端配置策略集。

4）终端安全防护自动化　对终端系统的安全维护工作自动化，如，软件分发、补丁管理、防病毒管理以及系统、数据的备份等。

5）注重策略的监控和审计　对终端的使用状况以及安全策略的执行情况，进行实施的监控和记录，便于终端安全风险的监控，以及对安全策略执行效果的审计，以便对策略进行考评，对现有策略标准进行调整和完善。

6）终端系统的维护管理　强调终端系统维护的集中性和专业性。

综合来看，国外的终端安全管理强调全生命周期管理，并利用各种技术支持管理流程的实现，以及对重要流程节点的控制，强调监控和审计的作用，做到安全策略持续改进。

3.2　国内终端安全管理在怎么做

目前国内终端安全关注较多，但是实际管理较少。终端安全管理工具较多，但是管理概念较少，管理制度较多，并且执行力度和执行手段较少。

总体来看，终端使用和管理中存在以下现象：

（1）重视基础硬件投入，忽视软件和制度投入

终端与办公效率直接相关，因此在终端采购上，往往预算和经费都十分充足，基于对终端发展速度的有效评估，现有终端的采购计划都会以短期高效、长期有效为指导方针。这也是因为硬件属于可见的可量化的资产。从 2011 年数据分析，国内 IT 领域硬件投入占总投入的 68%，软件投入仅占 21%，而安全相关的软件和制度投入更是远远小于这个比例。从发达国家的成熟经验来考虑，硬件、软件和安全的合理投入应该为 5∶3∶2，这说明现有的硬件投资中有相当一部分的设备没有配套的软件和安全，也就意味着这些没有配套软件和安全的设备，在运行过程中没有充分发挥应有的效能，大量的潜力被浪费，安全处于危险状态中，甚至相当一部分数量的设备处于无安全监控和防护的状态中，危害巨大。

（2）应用软件专业系统繁杂，安全管理软件单一

由于工作需要和市场推动，相关专业系统的开发处于蓬勃发展之中，应用软件也层出不穷，例如 MIS（Management Information System）中的办公自动化（Office Automation，OA）、工业控制系统（IPC）、辅助决策系统（DSS）、企业资源管理（ERP，Enterprise Resource Planning）等，部署方式也多种多样，有 B/S（Browser/Server）模式的，也有 C/S（Client/Server）模式的。由于缺少有效的信息安全指导和监控，部分软件和系统在设计之初就很少考虑安全问题，造成应用软件本身存在严重的安全漏洞，而已经加入的安全防护措施往往没有进行后期的升级和维护，不仅没有起到预期的安全防护作用，反而麻痹了信息安全管理人员，使之忽视了可能出现的安全问题，没能在第一时间发现和防范问题，造成了不必要的危害。目前，终端安全管理人员所用的安全管理软件主要是杀毒软件，导致终端安全的

发展严重失衡。

（3）终端应用范围和分布广泛，专业运维人员稀缺

由于终端设备发展的多样性和实用性，终端已经在社会各个领域广泛分布，各个角落都有部署，其中有部分终端处于无人值守的状态，如行政办公大厅、银行自动柜员机、税务办公大厅等都有这类公用终端。

有些已经指定的终端运维人员，本身并不具备足够的安全知识，且由于人手不足而无法及时出现在需要维护的终端上进行维护，再加上日常维护手段较少，日常维护工作量偏高。总得来讲，终端运维人员稀缺，终端的维护已经成为制约终端安全的重要因素。

（4）终端安全日常相关信息众多，总体态势分析和解决措施缺失

终端安全涉及的相关信息量非常大，日常需要处理和分析的内容非常多，由于这些信息的来源广泛，且格式和内容不一而同，导致缺乏总体态势分析。在没有整体分析结论的支持下，应对和解决措施往往不能对症下药，容易产生管理工作带来的安全隐患和风险。

（5）终端使用人员广泛，IT 技术和安全常识参差不齐

终端使用人员从专业技术人员到社会大众，每个人掌握的 IT 技术和安全常识参差不齐，且应用技术的出发点和目的也不同，导致终端在使用过程中，问题也层出不穷，如无意识的信息扩散和外泄，有目的的攻击和渗透。而管理技术手段和管理人员的有限，导致无力应对这些问题。

（6）资产种类和数量庞杂，管理流程缺乏统一和同步

终端资产在使用过程中也存在着变化。使用者会变更、使用范围会变化、使用地点会调整，这些内容原来都由不同的工作单位处理，但是信息却没有统一，资产的状态在不同的工作单位和范围内信息没有得到同步。在使用中，接入网络的设备除了业务终端外，还有其他设备。如智能手机、平板电脑等具备了同样的性能和功能的设备可以直接接入网络，也可以通过终端接入网络，由于传统的终端安全关注范围狭小，导致这些设备的违规使用泛滥，没有对应的管理流程和技术手段。

（7）终端应用发展迅速，安全管理技术和理念停滞不前

终端的发展迅猛，从 CPU 的更新换代，操作系统的推陈出新，终端的应用环境不断发展变化，网络速度的提升、应用的丰富，但与之相比，终端安全相关的管理技术和理念并没有同步更新，甚至远远落后于终端应用软件的发展。传统管理制度的要求和现有设备的使用环境格格不入。复杂的应用环境使终端设备的合法合规使用，在不同阶段和不同环境中是不一样的，管理程度也与使用人员的身份和处理信息的重要度息息相关，缺乏体系化的终端安全风险管理，缺少规范化的终端安全管理制度，最终造成终端信息安全只是空中楼阁，虚无缥缈，人人在谈，人人在用，但是无人在管，也无从下手。没有整体的分析和管理，盲目的管理和粗犷的约束，结果是制约终端的应用和降低工作的效率，与终端安全管理的初衷背道而驰。

3.3 终端安全管理产品有哪些

终端安全管理的根本在于管理的各项策略的落地实现，一个好的终端安全管理策略如果不能落地执行也是枉然，因此凡与终端管理各环节中安全相关的技术产品，即成为终端安全

产品范畴。终端安全产品是指安装和运行在终端上的安全保护，防止入侵、控制终端的安全模式和管理用户行为的安全软件。

大家常提到的终端安全软件包括：

（1）桌面防火墙（FW）

过滤来自互联网及其他公共信息网络对本地计算机终端的攻击，封堵木马、病毒等恶意软件经常调用的端口，监控异常端口流量，从而保护本地主机安全。

（2）桌面入侵防护（HIPS）

在某些文件、程序修改计算机其他文件、注册表信息等时进行防御性报警，提醒用户是否同意以上操作，如用户禁止此项修改，则此次修改行为不能继续进行。HIPS 还能极大地过滤木马向目地主机发送本地信息的行为。

（3）桌面反间谍

针对计算机内含有的或在浏览文件公共信息时激活的间谍软件进行报警和查杀，其功能区别于杀毒软件，对间谍软件、木马程序有较强的针对性。

（4）桌面反病毒

对本地计算机进行病毒查杀，从而达到对主机、网络、数据的防护效果。

（5）桌面合规性管理

对终端安装软件、补丁及版本等情况进行达标度检查，对终端维护提供可视化效果等。

（6）资产管理、客户端加密、补丁管理、漏洞管理等

这些软件是对计算机终端资产、计算机补丁及计算机所存在的漏洞进行更新管理的应用系统。

（7）终端安全准入

通过交换机、终端控制，对计算机的入网行为进行人为干预，防止非授权计算机接入可信信息系统。

（8）安全配置检查

主要针对计算机各项安全配置进行检查，如计算机用户名、密码设置，开启与禁用的服务、端口，目前计算机存在的进程信息等，降低人工手动检查的工作量。

（9）其他安全产品，漏洞扫描、文档加密等产品

目前市面上存在的安全产品较多，品牌也较为复杂，这里不做无意义赘述。但是由此可见，国内、外网络终端安全厂商较多，安全产品也很多，针对终端的各个领域都有不同的侧重。常见的安全软件可分类为桌面管理、网络接入、DLP、防病毒等，但是这些产品多是以工具的形式运用。

1）桌面管理类　主要以针对操作系统的各种状态收集、信息采集和运行监控为主，强调对于终端的个体管理和整体制度统一，可以对单一终端进行点对点的控制和管理，适用于小范围的网络安全管理。

2）网络接入类　主要是网络接入的合法和合规性管理，强调终端的使用者和使用范围必须遵循已有的网络安全定义，对于发现的风险可以通过网络隔离的方式，减小对于现有网络环境的影响，降低整体安全风险的威胁。

3）DLP　Data Leakage Prevention——数据泄漏防护，又称为 Data Loss Prevention——数据丢失防护。数据泄漏防护是通过一定的技术手段，防止企业的指定数据或信息资产以违

反安全策略规定的形式流出企业的一种策略。

目前，数据泄漏的途径可归类为 3 种：在使用状态下的泄密、在存储状态下的泄密和在传输状态下的泄密。一般企业可通过安装防火墙、杀毒软件等方法来阻挡外部的入侵，但是事实上 97%的信息泄密事件源于企业内部，所以就以上 3 种泄密途径分析，信息外泄的根源在于：

（a）使用泄漏

a）操作失误导致技术数据泄漏或损坏。

b）通过打印、剪切、复制、粘贴、另存为、重命名等操作泄漏数据。

（b）存储泄漏

a）数据中心、服务器、数据库的数据被随意下载、共享泄漏。

b）离职人员通过 U 盘、CD/DVD、移动硬盘随意复制机密资料。

c）移动笔记本被盗、丢失或维修造成数据泄漏。

（c）传输泄漏

a）通过 Email、QQ、MSN 等轻易传输机密资料。

b）通过网络监听、拦截等方式篡改、伪造传输数据。

4）防病毒　主要是防病毒软件和木马查杀工具，该领域受重视较早，关注也最多，因此发展相对稳定和成熟。

纵观以上分类，可以明显发觉工具色彩浓厚、单一性突出、整体性不足、体系性缺乏、没有从安全管理的角度来进行全局的掌控，缺少对于终端安全的全过程和全场景分析，因此会产生头痛医头、脚痛医脚的现象，经常出现安全管理员越多安全事件越多，工作内容越多监管工作越复杂，工具越多管理越少的局面。由此可见，系统性的安全管理平台在终端安全管理工作中的重要性日渐突出。

终端安全管理平台类产品国内外区分各有不同。

（1）国外终端安全管理平台产品

国外信息安全管理体系建设醒悟较早，终端产品基本从终端准入和桌面安全管理两方面入手，下面介绍 3 个典型产品的功能特点。

1）IBM Proventia 终端安全控制　结合了安全终端管理的多个关键领域，使得企业可以从众多供应商中自由选择最好的单点安全产品，并把它们当做一个整合的解决方案进行管理。涵盖的方面包括入侵防护系统（IPS）、防火墙与网络访问控制；数据保护（例如设备控制）、数据丢失防护与端点加密；安全配置与合规管理；以及 IT 安全操作（如安全补丁管理）和部署/删除安全工具。

2）CISCO NAC（网络准入控制）　为完全符合安全策略的终端设备提供网络接入，且有助于确保拒绝不符合策略的设备接入，将其放入隔离区以修复，或仅允许其有限地访问资源。

3）LANDesk 桌面管理套件　提供了从计算机资产管理、软件分发及应用以及远程帮助等方面的众多功能，包括服务器管理、补丁管理、软件分发、软件许可监控、远程维护、资产管理和 OS 映像迁移。

（2）国内终端安全管理平台产品

国内终端管理类产品起步较晚，开始于 2002 年左右，与国外产品相比，本土产品在稳定性和功能深入方面存在一定的差距，但是，各厂商产品也都具有一定的竞争优势。最大的

优势在于本土化优势，终端系统的使用特点具备很大的个性化成分，根据组织的业务、行政、文化和管理架构等的不同存在较大的差异，国内厂商在行业需求方面深入挖掘，根据组织终端使用特点以及国内信息安全相关标准规定，进行针对性的开发，因此，具备强大的适应能力和敏捷的反应能力。

下面就几款典型的终端安全管理产品进行简单的介绍。

1）TOPSEC 终端管理系统（TopDesk）：一款基于安全策略的终端管理产品，采用了开放式 B/S 体系结构和标准化数据通信方式，对局域网内部的网络安全行为进行全面监管，检测并保障桌面系统的安全。TopDesk 共分 3 大模块：桌面行为监管、桌面系统监管、系统资源管理，通过统一定制、下发安全策略并强制执行的机制，实现对局域网内部桌面系统的管理和维护，能有效保障桌面系统及重要数据的安全。

2）北信源终端安全管理系统（VRV SpecSEC）：VRV SpecSEC 体系覆盖桌面管理、安全准入、数据安全、行为管控、安全审计等多个方面，涉及管理计算机本身、计算机应用、计算机操作者、计算机使用单位管理规范等多个方面。

国内还有不少厂商都有终端安全管理系统产品，如启明星辰、圣博润、神州泰跃、中软华泰等安全公司。功能全面、符合国内安全标准也是这些本土产品所追求的共同目标。

3.4 终端还有安全问题么

在终端安全管理工作推行过程中存在主要困难有以下几个方面：

1）在终端风险处置过程中，缺少各项控制措施与信息安全风险的一一对应，所输出的众多信息安全管控措施难以统一规划。

在终端风险评估的过程中将会全面地、系统地对组织内的各项终端资产进行详细的风险分析，系统地分析出组织内终端系统所面临的各项风险，并对各项风险采取合理、有效的管控措施。基于风险评估得出的终端所面临多类实际信息安全风险，其风险个数很大。由于不同类别的信息安全风险所采取管控措施的优先级，通常也有很大的差别，如何针对数量庞大的风险及管控措施进行合理的规划，是一个很大的难题，因此对于规模比较庞大的组织，如何对风险评估后的管控措施进行统一、合理的规划至关重要。

2）难以在实践中对终端安全管理体系中的各级文件、模板及记录进行有条理的管理。

终端安全管理体系拥有很多文档化的方针、策略、规范和制度，并在体系运行的过程中将产生大量的记录。对于体系维护人员来讲如何对这些文件进行分门别类的管理，并且很好地对其中的逻辑性与一致性进行控制，是一个不大不小的难题。

3）终端安全管理体系实施及运作过程中，关键活动（如体系测量、组织内审、管理评审等）的策略、实施、记录很难系统化和程序化。

终端安全管理体系构建和实施运作过程中，规划、实施、内审和调整过程循环运行，由于这些活动关系到组织的多个部门，组织协调非常困难，因此将这些活动的组织策划自动化、实施过程的系统化，并在实施过程中记录完整化是体系推行人员的一个非常大的挑战。

为有效规避以上问题，需要在终端安全管理体系构建之前确定完善的终端安全管理体系构建方法论，通过结合终端安全风险管理体系明确终端安全管理流程，同步构建知识库，以便有效满足各级组织终端安全管理体系建设的需求。

传统信息安全体系建设系统包括安全体系规划、安全体系设计、安全体系实施以及安全体系保障 4 个主要模块。

1）安全体系规划　分析识别出终端安全风险体系，明确终端安全风险管理过程，分析识别出终端安全的终端信息安全改进措施，将需要增加或改进的措施分解成一项项任务或项目，明确每个任务或项目的目标、工作内容，分析任务或项目的实施优先级，根据实施优先级规划这些任务或项目的实施时间、实施范围及参与人员。

2）安全体系设计　建立体系相关部门、人员、职责及联系信息，系统管理各类方针、策略、程序及作业指导书的模板及具体文件的归档、版本控制。

3）安全体系实施　将各个任务实施的情况记录到系统中，对各项任务的实施的状态执行有效跟踪，并且评价各个任务实施的有效性。

4）安全体系保障　对体系内部审核、外部审核及管理评审等活动进行组织、策划、协调，并对内审、外审、管理评审的过程进行记录，对各不符合项及预防措施进行记录及状态跟踪。

3.5　终端安全管理的未来

从技术层面看，近年来国内外终端安全在技术领域的发展有以下几个趋势：

（1）集成趋势

最初的终端安全产品是以桌面防病毒、个人防火墙、主机防攻击、VPN 客户端等单独软件产品出现，随着人们开始将终端安全作为一个完整问题加以对待，终端安全正经历着一个从多个分立功能到多功能集成的过渡。功能从分立到集成并不是指将所有终端安全功能融合为一个厂家的一款产品，它的表现形式更多为以设置管理为纽带的多厂家产品的集成和互动，即由单一主机上多个代理组成的代理组来完成终端安全。

（2）硬件化趋势

运行在主机操作系统之上的终端安全产品完全由软件实现，依赖于操作系统，不仅增加了 CPU 的负担，也无法防止黑客利用其他应用软件和操作系统的漏洞获取主机控制权限，特别难以避免主机用户因安装含有恶意代码的软件而造成的问题。

有相应硬件支持，将很大程度上解决纯软件终端安全产品存在的问题。有 200 多家厂商参加的可信计算组织（Trusted Computing Group，TCG）已经制定了硬件和软件的标准来增强主机安全，其中非常重要的就是用来存放密钥、密码和数字证书的微控制器，即可信平台模块（Trusted Platform Module，TPM）。

与此同时，一些厂商也开始研制部署于网络接口的基于硬件的终端安全产品。这些产品以安全网卡形式出现，最终也可能集成到主板。在专用硬件网卡上内置的防火墙、VPN 以及入侵监测防护器（IDP）除了可以分担主机 CPU 的负担，而且可以独立运行，因而能够更好地支持中央管理，防止因主机被盗用引入的问题，在一定程度上可以阻断从被攻破的主机上发动攻击。例如可以使网卡内置的安全功能具有单独的安全认证，使得安全策略的设置和更改只能通过独立的配置手段进行；甚至可以使配置控制权不在主机而在管理中心，因而即使黑客侵入了某个主机并获得了它的管理员权限，也不能禁用或更改网卡内置的安全功能。又如，专用硬件网卡上内置的防火墙能够自动防止该主机伪造网包、IP 地址等。由于增加成

本的原因，这类产品的应用目前多见于服务器。

（3）综合趋势

终端安全产品要和网关及其他安全设施密切配合，分工协作，才有可能构架全面完整的安全防护保障体系。

终端安全的重要组成部分是设置管理或针对安全规范符合程度的检查、隔离和矫正。要做到这一点，终端安全已走出离散的、完全独立运行于单个主机的模式，而与中央管理产品综合在一起，逐步形成完善的全方位、多层次安全体系。中央管理产品本身可以是分层分布的，这样的布局使得安全解决方案更加严密，也具较好的灵活性。当网络的状况变化时，管理中心可以根据实际情况调整对于各个终端的安全要求和安全策略部署，并通过给各个终端分发任务和监督实施来保证整个网络系统的安全性。

综上所述，终端安全管理体系的构建实施过程需要依赖完善的方法论，对体系建设过程提供内部审核、管理评审、外部审核等管理活动支持，保障体系的有效实施。

第 4 章　终端安全管理的标准规范及要求

4.1　信息安全相关标准

（1）ISO/IEC27005《信息技术—安全技术—信息安全风险管理》

该标准给出了信息安全风险管理的指南，包括风险管理的原则，风险评估方法，风险处理和风险接受，风险的监视和评审等，以及给出了如何满足 ISMS 要求的更进一步的信息。明确了终端风险的管理原则等。

（2）ISO/IEC27001《信息安全管理体系—规范与使用指南》

该标准为建立、实施、运行、监视、评审、保持和改进信息安全管理体系（Information Security Management System，简称 ISMS）提供模型。

（3）ISO/IEC13335-2004《信息技术—安全技术—信息和通信技术安全的管理》

该标准是一个信息安全管理指南，这个标准的主要目的是给出如何有效地实施 IT 安全管理的建议和指南。

该标准目前分为 5 个部分。第 1 部分：IT 安全的概念和模型，这部分包括了对 IT 安全和安全管理的一些基本概念和模型的介绍；第 2 部分：IT 安全的管理和计划（Managing and Planning IT Security），建议性地描述了 IT 安全管理和计划的方式和要点；第 3 部分：IT 安全的技术管理（Techniques for the Management of IT Security），覆盖了风险管理技术、IT 安全计划的开发以及实施和测试，还包括一些后续的制度审查、事件分析、IT 安全教育程序等；第 4 部分：防护的选择（Selection of Safeguards），主要探讨如何针对一个组织的特定环境和安全需求来选择防护措施。这些措施不仅仅包括技术措施；第 5 部分：外部联接的防护（Safeguards for External Connections）。

（4）GB/T20984-2007《信息安全技术—信息安全风险评估规范》

标准提出了计算机风险评估的基本概念、要素关系、分析原理、实施流程和评估方法，以及风险评估在信息系统生命周期不同阶段的实施要点和工作形式。本标准适用于规范组织开展的风险评估工作。

（5）GB/T22239-2008《信息安全技术—信息系统安全等级保护基本要求》

本标准规定了不同安全保护等级信息系统的基本保护要求，包括基本技术要求和基本管理要求，适用于指导分等级的信息系统的安全建设和监督管理。

（6）《信息安全等级保护实施指南》

该标准详细介绍了计算机终端在进行分级保护时的实施流程，介绍了计算机运行维护、状态监控、安全检查等详细技术模型。

（7）GB/T 20270-2006《信息安全网络基础安全技术要求》

本标准用以指导设计者如何设计和实现所有以终端为基础的具有所需要求的安全等级的网络系统。实现了对等级保护技术要求中各个安全要求项目，网络系统应采取的安全技术措施，以及各级技术要求在不同安全等级保护中的具体差异。

（8）GB 20272-2006《信息安全技术操作系统安全技术要求》

本标准用于指导设计者如何设计和实现具有所需要求的安全保护等级的操作系统。主要说明技术要求中安全保护等级要求，操作系统应采取的安全技术措施，操作系统在不同安全保护等级中的具体差异。

（9）GB/T 20279-2006《信息安全技术网络和终端设备隔离部件安全技术要求》

本标准用于指导设计者如何设计和实现具有所需的安全等级的隔离部件，主要从对隔离部件的安全保护等级进行划分的角度来说明其技术要求。

4.2 行业化相关标准

（1）《税务系统网络与信息安全风险评估指南》

《税务系统网络与信息安全风险评估指南》就是为了对全国税务系统的信息安全风险评估工作提供实施的指导，从而统一全国税务系统风险评估工作的实施办法和工作流程，产生相同格式的工作成果，确保各地税务系统网络与信息安全风险评估工作结果的可比性。

（2）《电信系统安全规范——终端安全分册》

电信系统于2007年就出台了《安全规范——终端安全分册》，用于规范计算机终端的安全管理与规范应用。分册通过制定一整套的终端管理技术框架、提出详细的技术要求，为终端安全管理系统的建设提供指导，提高企业对于分散终端的安全管理能力，规范系统中终端用户的行为，降低来自终端的安全威胁，重点解决以下问题：

1）作为基本的业务处理平台和信息载体，终端自身安全防护的问题。

2）相对以往缺乏控制措施的现实，非授权终端网络接入控制的问题。

3）基于“防外和防内并重”的指导原则以及内控要求，内部用户行为监控的问题。

（3）《电信行业安全规范——用户管理分册》

本规范作为中国电信安全规范的重要组成部分，为中国电信进行用户管理统一建设提供依据。本规范的编制是在《CTG-MBOSS 安全分总规范》的总体框架体系指导下，参考了中国电信的现有的成果与经验，充分考虑了中国电信企业战略目标而形成的。

本规范是电信各系统建设时必须遵循的技术规范，阐述了终端用户生命周期管理在各个阶段需要遵循的具体内容，明确了终端密码管理办法。本规范适用于中国电信集团公司及下属省（市）电信公司用户集中管理系统规划和建设，为其提供指导和依据。

总而言之，各行业、集团为探索适宜的终端管理办法、保证内部终端安全，在各项国家标准、政策法规条件允许范围之内都会出台一些具有行业特色、针对性强、实用易用的行业标准，以达到对终端“因地制宜”的防护效果，在保证计算机终端安全的基础上，最大限度地发挥计算机的实用性能。

第 II 部分

终端安全风险分析

第 5 章　如何构建终端安全风险体系

第 6 章　对终端安全风险进行分类

第 5 章　如何构建终端安全风险体系

5.1　终端安全风险评估

终端安全风险评估是信息安全风险评估的重要组成部分，主要依据信息安全风险评估相关的技术和管理标准，对终端系统及其所存储、处理和传输的信息数据所面临的威胁，以及威胁利用脆弱性导致安全事件的可能性（即终端安全风险）进行识别分析，结合终端资产价值来判断终端安全事件一旦发生对组织所造成的影响。

依据信息安全风险评估理论，终端安全风险评估工作中主要遵循以下几个原则：

1）评估工作流程的可操作性原则。

2）评估工作质量的可控制性原则。

3）评估工作风险的可规避性原则。

4）评估工作内容的保密性原则。

5）评估工作最小化的影响原则。

终端安全风险评估过程中应综合运用定性与定量的方法，合理处理“主观与客观之间的关系，立足于“个性分析数据”，运用“共性分析数据”对终端安全风险进行识别。

终端安全风险评估常用的流程图 5-1 所示。

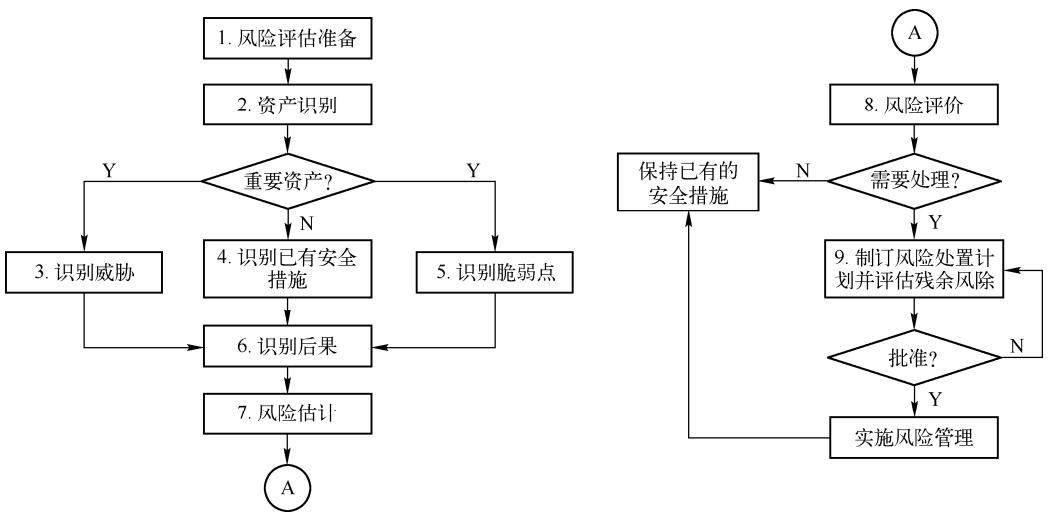

图 5-1　终端安全风险评估参考流程示意图

经过终端安全风险评估将获得一系列终端安全风险点，必须将这些识别出的风险点清晰的描述出来，避免在风险分析报告因缺少必要描述和格式化的描述方式，而使人“不知所

云”，进而在风险管控工作中“不知所措”。因此，本书对每一个风险点都从其发生的可能性和影响角度进行了详细阐述，并对每一类风险进行了更为细致的分析，针对每一威胁场景进行了阐述——即对每一类风险均拆解为风险点进行阐述。具体参见附录：终端安全风险分析报告。

基于详细的风险描述和格式化的展示方式，可以把每个风险点解释得比较清楚，但从总体上各个风险点还是孤立的，非层次化的，不利于整体把控风险，容易导致“只见树木，不见森林”的状况。因此，在通常所用的简单的列表的基础上，一定要以体系的方式展示风险，基于一定的分类、层次化构建方式来表明每个风险点在体系中所处的位置，便于组织从整体上监控风险。

5.2 识别终端资产

在信息安全领域，终端资产的价值不仅仅是以资产的经济价值来衡量，而是由资产的安全属性未达成时所造成的影响程度来确定。资产面临的威胁、存在的脆弱性、已采用的安全措施和是否存在应急预案都将影响到终端资产的安全。为此，需要对终端资产进行识别。

终端资产主要包括终端设备和终端所处理的信息。表 5-1 给出了基于表现形式的资产分类方式。

表 5-1 终端资产分类表

分类方式	具体分类
数据	保存在终端中的各种数据资料，包括可联网传递的数据信息和独立存储处理的数据信息
软件	系统软件：操作系统 应用软件：外部购买的应用软件和外包开发的应用软件等
硬件	计算机设备：大型机、小型机、服务器、工作站、台式计算机、移动计算机、智能手机和其他智能（移动）设备等 存储设备：光盘、移动硬盘、普通 U 盘、业务专用 U 盘、认证 Key 等

终端资产识别的内容包括物理资产、地点、设备厂商、型号、采购日期、上线日期、是否通过网络传输数据、行政所属等信息。重点在于了解相关资产如何让被各用户（如终端使用者、主机系统管理员、安全管理员等）所使用或管理。至于各个终端相关的具体信息资产，如操作系统类型、CPU、内存、当前已安装补丁的版本号等可以通过终端安全管理系统的客户端软件自动获取。具体参见第 9 章终端安全风险技术防护。

通常在实际资产综合评定方法中，被评估者可以根据自身的特点，选择对资产机密性、完整性和可用性中最为重要的一个属性的赋值等级，作为资产的最终价值结果；也可以根据资产机密性、完整性和可用性的不同等级，对其赋值进行加权计算得到资产的最终赋值结果。在本书附录中，结合终端资产的安全性特点，又引入了资产生命周期、人员和合规性要求 3 个要素，以便更突出地反映终端资产所面临风险的影响，便于终端安全管理者关注重要风险，在同样投入下，发挥更大的保障能力。

因资产识别中涉及物理位置、采购日期、设备型号等无法自动识别的信息，不存在自动完成资产识别的工具，但可借助带有资产识别和管理功能产品快速完成资产识别活动。终端

安全管理体系的技术支撑平台中终端安全防护平台的客户端、终端安全管理平台中的脆弱性管理子系统都可以完成对具有 IP 地址终端资产信息的自动收集（图 5-2）。商业扫描器也可实现 IP 地址终端资产部分信息的收集。

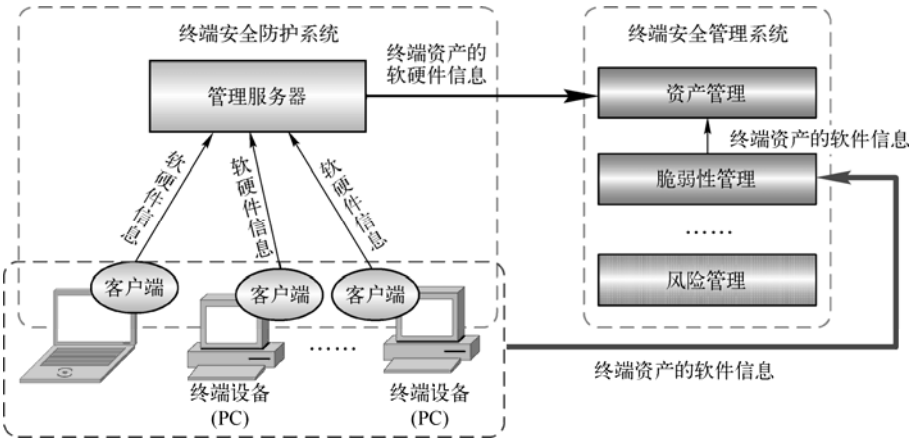

图 5-2　资产识别自动化工具工作示意图

资产识别通常采用人工识别加工具方法进行。资产的人工识别活动采用记录表格方式进行，表格中信息采用手工或自动方式导入到终端安全管理系统中，完成终端安全管理系统部署之初的资产预置工作。人工识别表格参见表 5-2。

表 5-2　人工识别表

资产识别记录单			
单位名称		部门名称	
用户信息			
姓名		性别	
职务		职称	
办公电话		移动电话	
家庭电话		传真	
邮箱			
资产信息			
所属业务		所属类别	
资产名称		资产编号	
IP 地址		物理位置	
生产厂商		设备型号	
机密性要求			
完整性要求			
可用性要求			
安全控制措施			
负责人			
备注			

终端安全管理体系中技术支撑平台的部署需基于现有网络进行，因此，在资产识别过程中应一并获取最新的、详细的网络拓扑图，以及行业终端资产使用的特殊性要求（如税务行业中的业务专用机和专用 U 盘等），这将有助于完备地进行资产识别和后续终端安全管理系统的部署实施。

5.3 识别终端威胁

终端安全威胁识别主要是识别对被评估组织终端资产直接或间接构成破坏可能性的因素。威胁是构成信息安全风险不可缺少的要素之一，当终端资产存在脆弱性且相应的安全控制措施缺失或薄弱的条件下，威胁因素通过某种途径作用在特定的终端资产上，破坏其一个或多个安全特定，产生安全事件。

识别终端安全威胁的主要目的是构建终端安全威胁场景，进行更为有效的风险分析。

威胁识别活动中需要识别实际威胁和潜在威胁。

实际威胁：指的是被评估组织近期内曾经实际发生过的威胁。

潜在威胁：指的是根据当前总体威胁态势可识别的被评估组织潜在的威胁。

威胁场景的实质是为每个关键资产或关键资产类别与其所面临的实际和潜在的威胁建立对应关系，这样做的好处是排除那些不可能存在的“关键资产–威胁”对，避免在风险识别过程中浪费时间和人力。

在威胁场景中不仅建立起了关键资产与其面临威胁之间的对应关系，还明确了威胁来源、途径和结果，有利于后续风险分析阶段中结合脆弱性和已有的安全控制措施进行影响和可能性分析。

为进行有效的风险分析，威胁场景构建过程中需遵循全场景、全过程和全方位原则，即：

1）全场景　从业务的视角，分别用关键资产，威胁，包括主体、途径、方位、行为、结果，来构建一个围绕关键资产或关键资产类的全面的威胁场景。

2）全过程　涉及终端资产使用全生命周期，包括入网阶段、运行阶段、维修阶段、报废阶段。

3）全方位　不仅考虑内部环境，还要考虑外部环境和移动计算环境；不仅考虑到技术因素，还要考虑到管理的因素。

终端资产可以分为终端资产、带有移动介质的终端资产和终端信息资产三大类，以下将分别为三大关键资产类构建威胁场景。

【场景 1】 针对带有移动介质的终端的威胁场景。

终端安全管理对象使用中存在关联关系，因此，在构建威胁场景时要全面考虑。本场景重点分析了带有移动介质使用过程的终端所面临的威胁（图 5–3）。

移动介质在终端使用过程中，需要面对以下的威胁，但不限于这些威胁。

（1）移动存储介质（注册）可以从文件保险箱中操作文件

1）注册过的移动存储介质是可以直接访问受保护的文件，该过程属于重要文件可能离网的合法方式之一。

2）移动存储介质不区分使用权限，可能存在信息扩散。

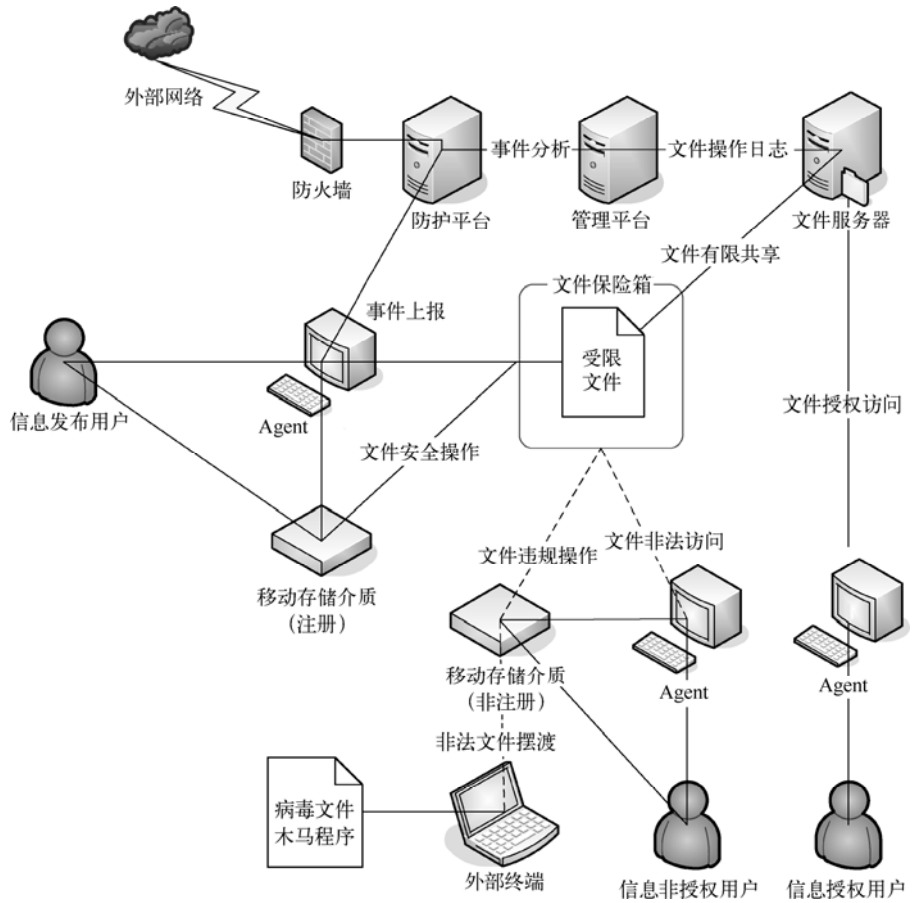

图 5-3　带有移动介质的终端的威胁场景

（2）文件保险箱限制非授权用户访问

✓ 文件保险箱中的文件一经放入就会受到严格限制，不可以自主公开，需要采用相关流程申请，经过审批之后才能提供给非授权用户

✓ 文件保险箱中的文件与用户身份相关，非信息拥有者不可以查看

✓ 重要文件没有放入文件保险箱可能存在非授权用户的操作和外泄

（3）授权用户从文件服务器获取共享的授权文件

✓ 授权用户通过服务器共享授权文件只能在文件保险箱中打开

（4）移动存储介质（非注册）在 Agent 上进行操作

✓ 非注册的移动存储介质在 Agent 操作可能带来信息外泄

✓ 非注册的移动存储介质在 Agent 操作可能带来病毒/木马

✓ 非注册的移动存储介质在 Agent 操作可能带来文件的非法摆渡

（5）信息非授权用户在 Agent 上的文件操作受到限制

✓ 信息非授权用户不可以查看文件保险箱中非授权的内容

✓ 信息非授权用户可能查看和操作终端上没有放入文件保险箱中的文件

✓ 信息非授权用户可能通过其他方式操作和传递终端本地文件

针对带有移动介质的终端的威胁场景分析见表 5-3。

表 5-3 针对带有移动介质的终端的威胁场景分析示意表

关键资产	威胁主体	威胁途径	方 位	意 图	威 胁	结 果
使用移动介质的PC 设备	人为威胁	网络	外部	故意行为	操作重要文件	信息外泄
				意外行为	内外网连通	信息外泄、感染病毒、遭受入侵
			内部	故意行为	重要文件不放入文件保险箱	信息外泄
				意外行为	查看文件保险箱中非授权的内容	信息扩散
		物理	外部	故意行为	非法拆卸硬盘	信息外泄
				意外行为	设备故障	信息丢失
			内部	故意行为	使用非注册移动介质	信息外泄、感染病毒木马
				意外行为	未使用文件保险箱	信息外泄
	非人为威胁	系统	外部	故意行为	远程操作	信息外泄
				意外行为	操作系统异常	信息损坏
			内部	故意行为	非 USB 外设	监控失效
				意外行为	USB 接口损坏	无法使用
		环境	外部	故意行为	掉电	文件损坏
				意外行为	网络异常	文件同步受影响
			内部	故意行为	文件共享	信息扩散
				意外行为	默认共享	信息扩散
移动介质	人为威胁	网络	外部	故意行为		
				意外行为		
			内部	故意行为	故意在非授权区域使用注册移动介质	信息外泄
				意外行为	无意中在非授权网络区域或终端上使用注册移动介质	信息外泄
		物理	外部	故意行为	非法使用注册移动介质	信息外泄、感染病毒木马
				意外行为	格式化注册移动介质	数据损坏
					无意中在业务网络中使用非注册移动介质	信息外泄、感染病毒木马
			内部	故意行为	口令泄密	信息外泄
				意外行为	移动介质丢失	信息外泄
	非人为威胁	系统	外部	故意行为	硬件接口变化	信息无法使用
				意外行为		
			内部	故意行为		
				意外行为	移动介质损坏	无法使用、信息丢失
		环境	外部	故意行为		
				意外行为		
			内部	故意行为		
				意外行为		

【场景 2】 业务专网中的终端安全威胁场景分析（重点从终端的使用环境角度进行分析）。

终端处在不同的应用环境中所面临的安全威胁有所不同，以下基于终端在业务专网中的使用进行威胁分析（图 5-4）。

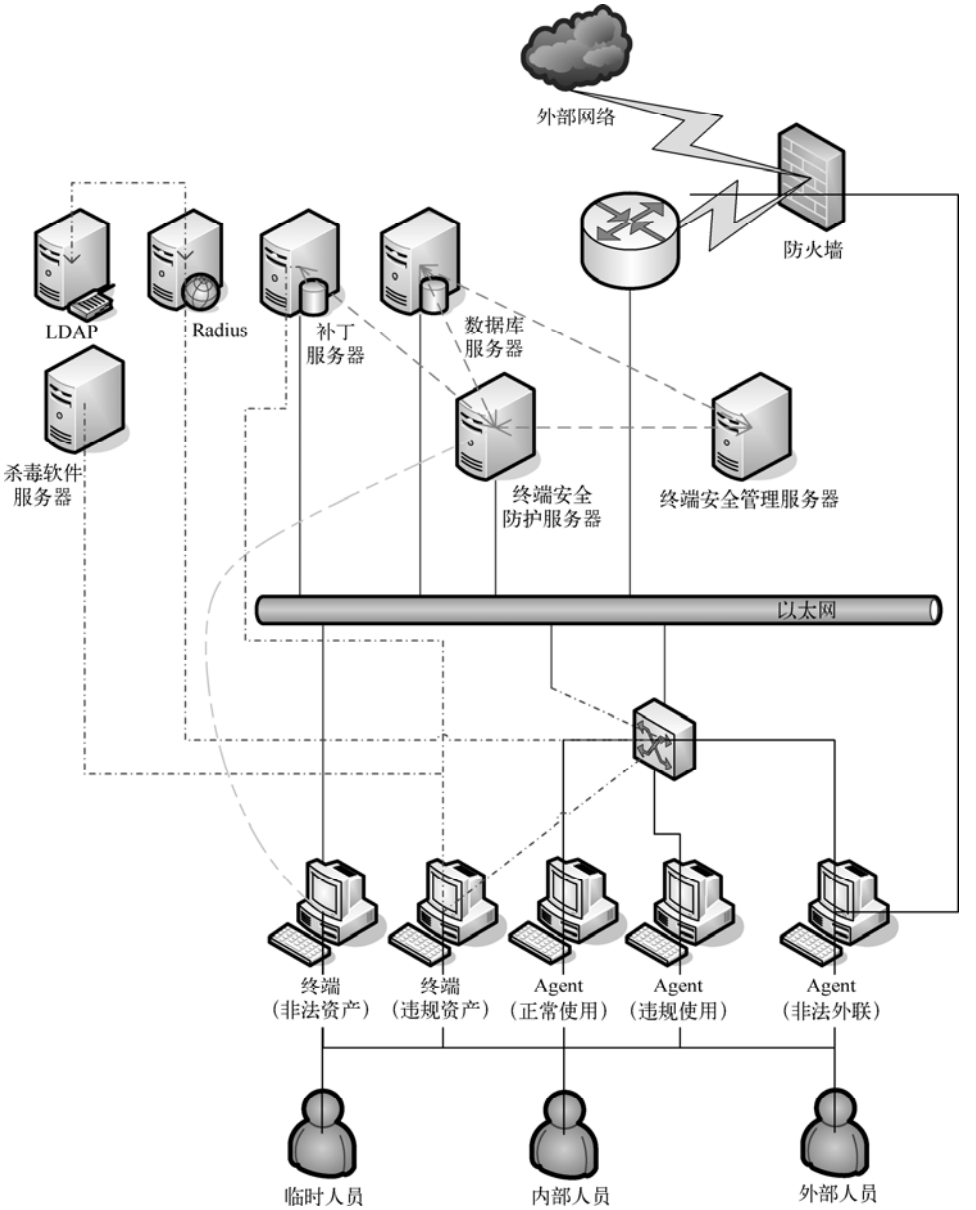

图 5-4　业务专网中终端的威胁场景

业务专网正常使用过程中，可能存在（但是不限于）以下内容的威胁：

（1）资产合法性威胁

✓ 资产是否符合登记信息的内容

✓ 资产是否配属登记信息关联的人员

（2）资产合规性威胁

✓ 资产是否安装了规定的软件
✓ 资产是否安装了规定的防病毒工具
✓ 资产是否满足网络安全对于操作系统的要求
✓ 资产是否升级了防病毒工具的病毒库

（3）终端行为违规

✓ 终端使用者是否操作了未经授权的文件
✓ 终端是否同时连通内外网
✓ 终端使用者是否运行了对终端或者网络有不良影响的进程
✓ 终端使用者是否开启了对终端或者网络有不良影响的端口
✓ 终端使用者是否访问了受限的网络
✓ 终端使用者是否连接了可能对终端或者网络有不良影响的外设
✓ 终端使用者是否设置了本地共享
✓ 终端使用者是否访问远程共享
✓ 终端使用者是否占用了过多的网络流量
✓ 终端使用者是否执行了拨号操作
✓ 终端使用者是否占用了过多的系统资源
✓ 终端使用者是否使用了非授权的网络资源

（4）操作系统漏洞威胁

✓ 操作系统面对补丁升级不完整威胁
✓ 操作系统面对漏洞不解决威胁
✓ 操作系统面对口令不及时修改威胁
✓ 操作系统面对口令复杂度不足威胁
✓ 操作系统面对用户账号变更威胁
✓ 操作系统面对用户权限变更威胁
✓ 操作系统面对使用者暂时离开他人使用的威胁

针对业务专网中的终端安全威胁场景分析见表5-4。

表5-4 针对业务专网中的终端安全威胁场景分析示意表

关键资产	威胁主体	威胁途径	方位	意图	威胁	结果
业务专网中终端资产	人为威胁	网络	外部	故意行为	终端同时连通内外网	
				意外行为		
			内部	故意行为		
				意外行为	资产是否满足网络安全对于操作系统的要求	
		物理	外部	故意行为	资产是否配属登记信息关联的人员	
				意外行为	资产是否符合登记信息的内容	
			内部	故意行为	资产是否安装了规定的软件 资产是否安装了规定的防病毒工具 资产是否升级了防病毒工具的病毒库 终端使用者是否操作了未经授权的文件	影响终端的正常运行

（续）

关键资产	威胁主体	威胁途径	方位	意图	威　胁	结　果
业务专网中终端资产	人为威胁	物理	内部	故意行为	终端使用者是否运行了对终端或者网络有不良影响的进程 终端使用者是否开启了对终端或者网络有不良影响的端口 终端使用者是否访问了受限的网络 终端使用者是否设置了本地共享 终端使用者是否访问远程共享 终端使用者是否占用了过多的网络流量 终端使用者是否执行了拨号操作 终端使用者是否占用了过多的系统资源 终端使用者是否使用了非授权的网络资源	影响终端的正常运行
				意外行为	终端使用者是否连接了可能对终端或者网络有不良影响的外设	
	非人为威胁	系统	外部	故意行为	操作系统面对使用者暂时离开他人使用的威胁	
				意外行为		
			内部	故意行为	操作系统面对口令不及时修改威胁 操作系统面对口令复杂度不足威胁 操作系统面对用户账号变更威胁 操作系统面对用户权限变更威胁	
				意外行为	操作系统面对补丁升级不完整威胁 操作系统面对漏洞不解决威胁	
		环境	外部	故意行为		
				意外行为		
			内部	故意行为		
				意外行为		

【场景 3】 信息扩散安全威胁场景分析。

信息扩散和泄密场景（图 5-5）中，包含（但是不限于）以下的威胁：

- ✓ 信息非授权用户非法访问重要信息
- ✓ 重要信息非法修改威胁
- ✓ 重要信息非法传递威胁
- ✓ 重要信息违规访问威胁
- ✓ 重要信息违规修改威胁
- ✓ 重要信息违规传递威胁
- ✓ 重要信息违规打印威胁
- ✓ 重要信息违规外网发布威胁

信息的来源包括终端自己产生的信息和外部进入的信息（如从主管机关复制带入的信息）。

信息分为涉密信息、工作秘密信息、内部非公开信息和内部公开信息 4 类。其中涉密信息属于国家及各级保密机构管理范围，内部非公开信息和内部公开信息不是管理重点，工作秘密信息是信息防扩散管理的重点。

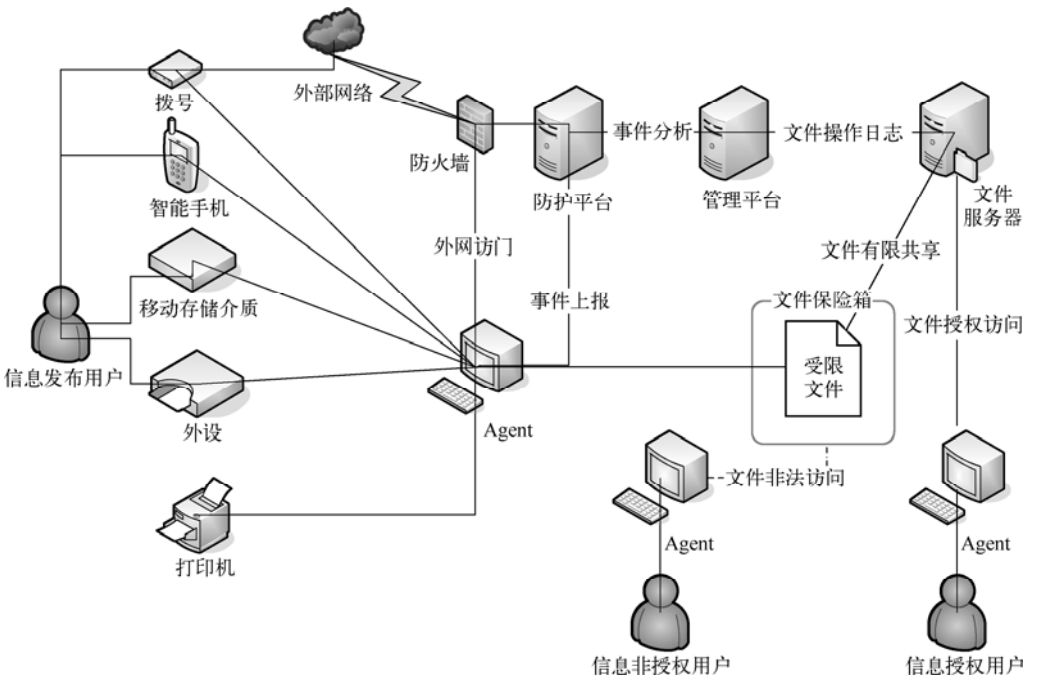

图 5-5　信息扩散的威胁场景

场景分析要覆盖信息自身生命周期。

信息扩散安全威胁场景分析见表 5-5。

表 5-5　信息扩散安全威胁场景分析示意表

关键资产	威胁主体	威胁途径	方位	意　图	威　胁	结　果
终端自己产生的信息	人为威胁	网络	外部	故意行为	重要信息违规外网发布	信息外泄
				意外行为	重要信息违规传递	信息外泄
			内部	故意行为	重要信息非法修改	信息损坏
				意外行为	重要信息违规修改	信息损坏
		物理	外部	故意行为	信息非授权用户非法访问重要信息	信息扩散
				意外行为	重要信息非法传递	信息扩散
			内部	故意行为	重要信息违规访问	信息扩散
				意外行为	重要信息违规打印	信息扩散
	非人为威胁	系统	外部	故意行为		
				意外行为		
			内部	故意行为		
				意外行为		
		环境	外部	故意行为		
				意外行为		
			内部	故意行为		

（续）

关键资产	威胁主体	威胁途径	方位	意　图	威　胁	结　果
				意外行为		
外来信息	人为威胁	网络	外部	故意行为	重要信息违规外网发布	信息外泄
				意外行为	重要信息违规传递	信息外泄
			内部	故意行为	重要信息非法修改	信息损坏
				意外行为	重要信息违规修改	信息损坏
		物理	外部	故意行为	信息非授权用户非法访问重要信息	信息扩散
				意外行为	重要信息非法传递	信息扩散
			内部	故意行为	重要信息违规访问	信息扩散
				意外行为	重要信息违规打印	信息扩散
	非人为威胁	系统	外部	故意行为		
				意外行为		
			内部	故意行为		
				意外行为		
		环境	外部	故意行为		
				意外行为		
			内部	故意行为		
				意外行为		

识别出终端威胁后，需要通过判断威胁出现的频率，对于威胁的影响程度进行评估，进而为相关风险定级提供参考。这个过程通常是根据经验和（或）有关的统计数据来进行判断。一般需要综合考虑以下 3 个方面，以形成在某种评估环境中各种威胁出现的频率：

1）以往安全事件报告中出现过的威胁及其频率的统计。

2）实际环境中通过检测工具以及各种日志发现的威胁及其频率的统计。

3）近一两年来国际组织发布的对于整个社会或特定行业的威胁及其频率统计，以及发布的威胁预警。

可以对威胁出现的频率进行等级化处理，不同等级分别代表威胁出现的频率的高低。等级数值越大，威胁出现的频率越高。

识别终端威胁所采用的工具和方法主要是人工访谈和工具这两种。人工访谈主要需要记录单，威胁识别工具通常采用安全审计工具、终端安全防护系统、漏洞扫描。

5.4　识别终端脆弱性

脆弱性是对一个或多个资产弱点的总称。脆弱性识别也称为弱点识别。弱点是资产本身存在的，如果没有相应的威胁发生，单纯的弱点本身不会对资产造成损害，而且如果系统足够强健，再严重的威胁也不会导致安全事件，并造成损失，即威胁总是要利用资产的弱点才可能造成危害。

资产的脆弱性具有隐蔽性，有些弱点只有在一定条件和环境下才能显现，这是脆弱性识别中最为困难的部分。需要注意的是，不正确的、起不到应有作用的或没有正确实施的安全措施本身就可能是一个弱点。

脆弱性通常包括技术脆弱性和管理脆弱性。其中各类技术脆弱性的存在，增加了终端安全事件发生的可能性，加大了终端的安全风险。因此在对终端安全风险进行管理时需要对终端中的脆弱性进行识别。

为了避免在脆弱性识别过程中发生遗漏，应围绕终端相关各对象指明需重点识别的脆弱性。脆弱性的识别可以以资产为核心，主要从技术和管理两个方面进行，技术脆弱性涉及物理层、网络层、系统层、应用层等各个层面的安全问题；管理脆弱性又可分为技术管理和组织管理两方面，前者与具体技术活动相关，后者与管理环境相关。

5.5 终端安全威胁与脆弱性

为便于进行进一步的风险分析工作，在识别脆弱性之后，需将其与能够利用它的威胁进行映射。表 5-6 为终端脆弱性和威胁映射表。

表 5-6 脆弱性与威胁对应关系

类型	识别对象	脆弱性子类	描　　述	威 胁 映 射
技术	物理环境	环境类	缺乏对建筑物门窗的保护	盗窃或故意破坏
			对机房或办公室的物理访问控制不足	盗窃或故意破坏
			电力供应不稳定	电压波动
	终端（含操作系统及系统服务）	硬件类	电压敏感性	电压波动
			温度敏感性	温度大幅度变化
			湿度、灰尘、尘土等敏感性	潮湿、灰尘、尘土等
			电磁辐射敏感性	电子干扰
			缺少配置更改控制	配置人员错误
		软件类	未停掉 Guest 账户	系统被非授权使用
			未删除不必要的用户账户（如测试用账户、共享账户等）	系统被非授权使用
			未将系统的 Administrator 账户改名	暴力破解
			多人共用一个账号	系统被非授权使用
			未启用密码复杂性策略	用户身份被冒名
			未启用密码长度策略	用户身份被冒名
			未启用账户锁定策略	系统被非授权使用
			未启用口令定期更改策略	系统被非授权使用
			离开电脑时没有退出登录	非授权方式使用系统
			未关闭不必要的服务	非授权方式使用系统
			未关闭不必要的端口	非授权方式使用系统
			未关闭默认共享	非授权方式使用系统
			未在关机时清除页面文件	信息泄漏

（续）

类型	识别对象	脆弱性子类	描　　述	威 胁 映 射
技术	终端（含操作系统及系统服务）	软件类	系统显示上次登录用户名	系统被非授权使用
			存在广为人知的系统漏洞	系统被非授权使用
			口令管理机制薄弱（如口令简单、没有口令定期更改策略等）	用户身份被冒名
			错误的访问权限分配	非授权的方式使用系统
			对软件下载和使用没有控制	恶意软件
			不必要的服务被启用	非授权方式使用系统
			未设置补丁更新策略	系统被非授权使用
			未安装病毒软件	病毒木马
			未设置病毒库升级策略	病毒木马
	网络结构	通信		
	数据库			
	应用系统	软件		
		业务应用		
管理	技术管理	文档		
		工作流程		
	组织管理	人员		
		工作流程		

5.6　终端安全风险分析模型

基于所识别的资产、所识别的威胁和所识别的脆弱性可对风险进行有效分析。

基于图 5-6 安全风险分析示意图，可见风险高低可通过以下方式获得。

1）风险=可能性后果。

2）信息安全风险值=安全事件的可能性&造成的损失。

3）安全事件的可能性=威胁&脆弱性。

4）造成的损失=资产价值&脆弱性。

上面的“&”符号表示关联。

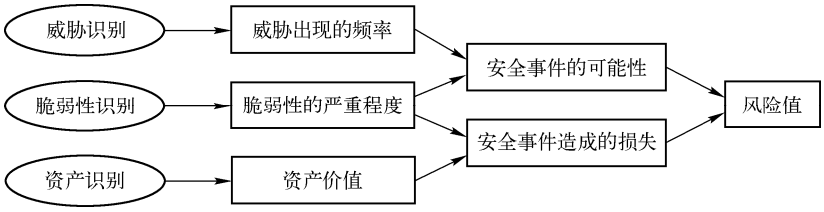

图 5-6　安全风险分析模型示意图

第 6 章　对终端安全风险进行分类

6.1　几种常见分类方式

终端应用的过程中操作分类复杂，风险点数量众多，这就导致对于终端安全风险的分析，很难进行简单的归类处理，往往对于一个风险点可能存在多种角度分析，不同的角度分析的方式和侧重是不同的，对于风险的估计也是不同的，因此对风险进行合理分类有利于风险的发现和管控。本章会基于不同维度对风险进行分解，把风险分解结构（RBS）用图解表示的形式进行说明。

常见的分解方式有：

1．基于风险来源

基于风险来源分解的第一层是按内部和外部分解，第二层是软件、硬件、移动介质等进行分解。

具体如图 6-1 所示。

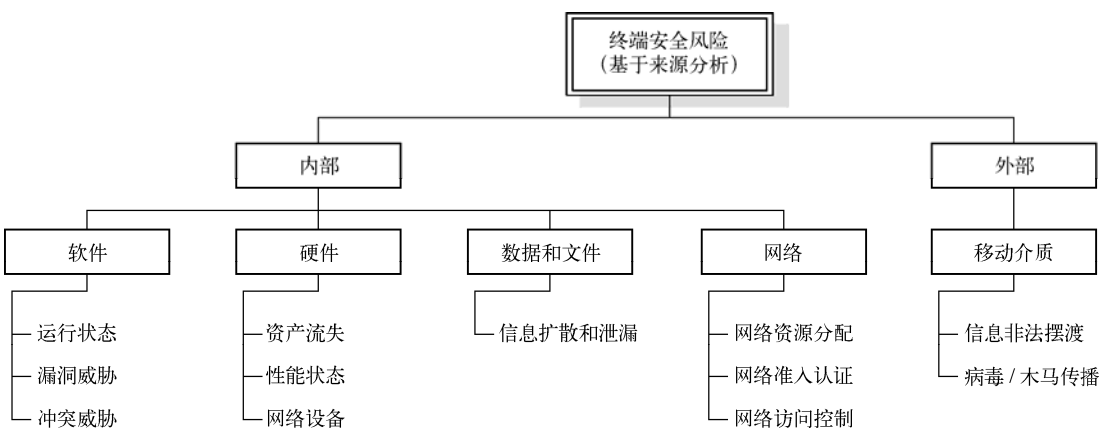

图 6-1　基于风险来源的终端安全风险分类示意图

基于来源的风险分类便于区分风险发生的原因，利于把握风险源头，有针对性实施管控手段。

内部是指在终端应用过程中，由于终端自身是风险的源头，此类风险的管控要以终端自身为主进行处理。内部区分为软件、硬件、数据和文件、网络。

1）软件的问题，比较容易定位和跟踪。如果有软件使用的安全规范，常用软件的问题通常都可以进行预防，但是如果没有规范，根据个人喜好选择软件，则对管理的要求很高，

出现问题的危险性也很高，如软件在运行过程中对系统资源的占用情况，对系统性能的影响情况，软件自身的安全漏洞问题，软件之间的冲突问题等。软件自身的安全漏洞问题和软件之间的冲突问题是终端安全管理过程中最大的风险点，安全漏洞会让所有的安全防护都成为纸老虎，被轻易地绕开。而软件之间的冲突问题是工作中最大的隐患和威胁，软件的冲突包含端口、系统资源、驱动程序等，其中驱动程序的冲突会导致终端操作系统异常，常见的现象就是蓝屏和黑屏，甚至导致操作系统不可修复的损坏。

2）硬件问题，属于物理设备问题，需要配合行政管理进行跟踪。终端最常遇到的硬件问题就是设备维修，终端维修也是安全管控过程中，最难以保障安全的一个环节，因为会涉及厂商和维修商等，人员和流程都很难掌控，只能在维修前进行登记和处理，维修后再进行验证和检查，不过由于部分设备比较特殊，例如硬盘等，可能会需要放弃维修，因为维修的风险明显高于直接报废更换新设备。硬件问题依赖行政管理，表现在设备的登记和状态的更新维护上，需要有配套的行政制度管理，更要有行政手段保证制度的执行，例如多网卡的使用、硬盘拆卸和更换等问题，在管理工具的配合下，是可以发现的，但是如果没有行政制度和规范，工具发现的种种威胁就会无法防范。

3）数据和文件，是信息安全风险问题。数据的处理是工作中必不可少的，但是数据的安全确认是工作中最容易疏忽的，数据的任意存放和传递会导致信息的扩散（如未经授权的内部人员查看了数据），甚至引起信息的泄密（如未经许可的外部人员查看了数据）。数据和文件的差别在于，数据是工作中的信息，文件是信息保存之后的形式，数据在终端上的存放方式一般是文件，可能数据在处理过程中是安全的，但是保存成文件之后，就不再受到业务系统的保护，而是操作系统可以直接进行操作和处理的，终端的任何使用者都可以操作，因此对于重要文件的操作也应该纳入监管。

4）网络是终端安全中比较特殊的一个部分，因为网络本身属于外部，但是网络参数和认证，甚至包括一部分控制，都还是在终端上来完成的。终端操作系统控制的网络参数，包括 IP、MAC、DNS 等，这些内容不仅对自身使用网络有影响，对同处在一个网络的其他终端也是有影响的。解决网络参数问题，要从终端和网络规划两个角度去处理，终端上规范网络参数使用，但是网络参数的合理性还是要从网络规划上进行处理，比较理想的方式是终端不能自行控制网络参数，而应统一集中由网络规划进行处理。网络准入认证是业务内网常用的限制接入手段，一般是配合网关类设备，这样才能保障实现效果，但是认证需要客户端，客户端就是属于终端的内部问题了。网络准入认证一般是网络访问控制配合在一起，因为仅仅使用网络准入，只能保障未经授权的终端和用户的接入限制，但是对于使用的限制就需要访问控制来实现了。

外部是指在终端使用过程中，问题来源不是在终端上的，主要是指外设，而外设中最容易出现问题的就是移动存储介质。

移动存储介质是现在终端使用中最常见的外设，便于文件传递，而且外形小巧，深受终端使用者的喜欢。但是移动存储介质的管理却是终端安全管理人员的麻烦。因为移动存储介质是很难区分用途的，公用和私用完全由使用者控制，使用范围也很难限制，如果统一下发专用的品牌，配合专用的工具，又会导致使用起来很麻烦，慢慢的闲置之后，只能取消。目前比较合理的使用方式是，对移动存储介质进行标签化管理，限定权限和类别，根据不同的用途和安全范围，进行规范管理。

2．基于风险属性的分类

基于风险属性分解的第一层是技术类和管理类，技术类在第二层又可分为基础安全、运行安全、信息安全和平台自身安全等，见图 6-2。

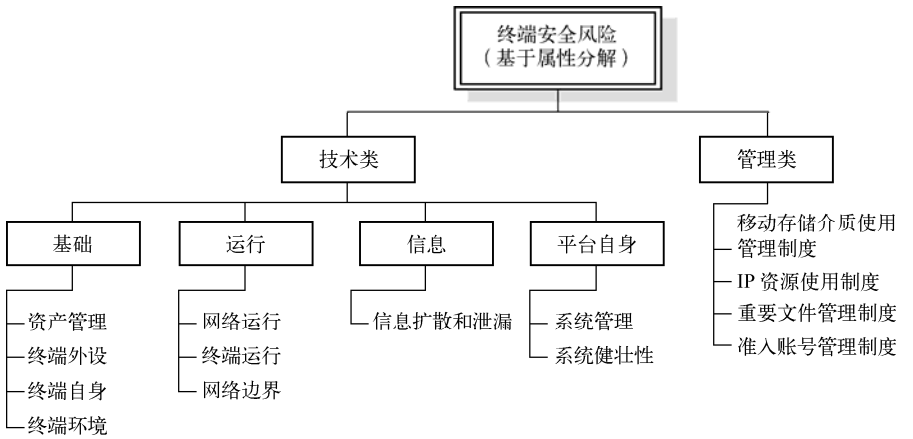

图 6-2　基于风险属性的终端安全风险分类示意图

基于风险属性的终端安全分类可有针对性的选择管控措施，如技术类风险重点基于技术手段自动解决问题，管理类风险重点在管理的制度、流程和人员上下功夫。

技术类是依赖工具实现的，工具包括客户端软件、网络管理工具、信息安全工具等，技术类比较典型的分类方式包括基础安全、运行安全、信息安全、平台自身安全。

1）基础安全，包括资产管理安全、终端外设安全、终端自身安全、终端环境安全等。基础安全是终端安全威胁的根源，是每个终端都不可以避免的。资产管理安全是终端在管理过程中进行定位的基础，对资产进行管理，是区分终端建立唯一性识别的基础，也是终端安全应对不同阶段的主要管理手段。终端首先是资产，只有对资产进行管理，才能确定终端的来源和用途，才能进行分类的安全管理和应对。终端外设安全是指红外、蓝牙、无线网卡、移动存储介质等，这些设备对于终端的信息安全是影响很大的，终端除了网络之外的通信就是靠外设实现的，外设可以跨越网络，实现信息的通信，在此过程中，安全就成为了问题，不止数据和信息可能扩散或者泄密，病毒和木马也有可能会被引进。终端自身安全是支持终端操作系统的安全，包括补丁、漏洞、系统性能、网络参数等等，终端自身安全是终端对于自身防护的重中之重，因为终端自身都不能保障安全的话，其他的安全就更不可能保障了。

2）运行安全，包括网络运行安全、终端运行安全、网络边界安全等。运行安全是终端的环境和终端的使用产生的安全问题。网络运行安全是终端在工作中需要使用网络而产生的威胁，网络运行过程中，包括接入安全、认证安全、访问安全等内容，由于现在的业务工作一般都离不开网络，网络运行安全越来越重要，已经成为终端安全工作的前提。终端运行安全是指终端运行过程中，为了保障终端正常运行而可能发生的威胁，终端的 CPU、内存、硬盘等都可能成为影响终端运行的要素，更不用说操作系统中运行的进程、端口、服务等。

3）信息安全，主要是信息的防扩散和防泄密。信息的防扩散主要是在信息上做权限区分，只有这样才能在使用时区分扩散的边界和范围，而信息上做权限又是一个比较麻烦的事情，从现在技术手段上来看，所有文件加密，按文件密级过滤是能够满足要求的最直接的办

法，但是这种方式对工作效率的影响很大。从信息安全的整体上来看，通过定义信息的特征，关注这些特征的信息传递的情况，可以追查信息的扩散途径，通过限制信息的边界，实现信息的安全，这是适用于信息安全要求级别没有达到机密级以上的情况。信息的防泄密，主要是针对信息的传递进行控制，信息一旦被带走，就有泄密的可能，控制信息的防泄密途径，就是对信息的安全传递进行控制。

4）平台自身安全，主要是终端安全管理工具的安全，这就包括系统自身的管理，系统健壮性等方面。系统自身的管理，又包括系统参数、系统性能、系统安全等等方面的内容，对于系统自身的管理重在设计，提前进行设计和应对，才是处理系统自身管理的基础。系统健壮性的方面，是要对系统的进行整体的测试，尤其是压力测试和破坏性测试，系统的健壮性对于系统的安全影响很大，系统不能稳定安全地运行，终端安全就没有足够的保障。系统的健壮性还体现在内部逻辑的关联影响上，如果某个模块或者环节出现了异常，那么系统是否还能正常运行？因为系统中部分操作是由使用者发起的，错误的操作也是应该考虑在内的，错误的操作是在什么时间，由什么人发起的？操作的内容和细节又是什么？这些操作是否能够还原？

管理类是对于技术类的补充，技术需要配合管理，才能让操作变得有意义，管理配合技术才能让管理的要求落到实处。

管理类主要指工作制度、工作规范、工作手册、应急流程等，这些内容是指导技术类的工具进行安全的引导和预防。

3．基于风险管控方式的分类

为了降低和规避终端系统的风险，需综合运用技术和管理手段来对风险进行管控。基于管控手段分析的第一层是风险发现方式分类，包括系统自动发现和结合人工发现；第二层是风险防护方式分类，包括自动防护和结合人工；第三层是具体的防护手段分类，包括禁止行为、修改配置等，见图 6-3。

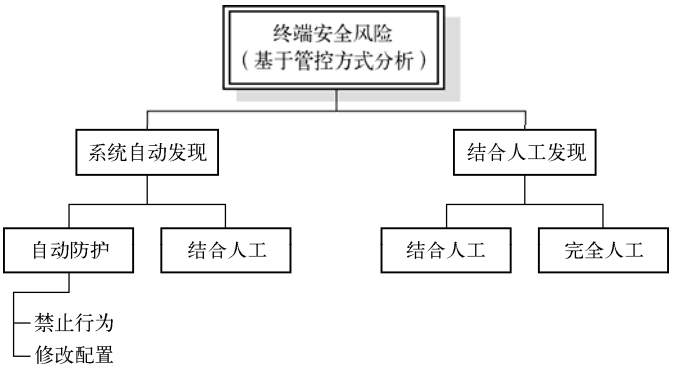

图 6-3　基于管控方式的终端安全风险分类

基于管控方式进行区分的目的，是对终端安全管理工作方式进行深入分析，区分和界定在终端安全管理工作中哪些工作是可以提前进行预防的，哪些工作是需要人工辅助处理，哪些是需要人工主动进行操作的，哪些是完全依赖人工完成的。

1）自动防护就是依靠工具可以提前进行预防和处理，一般是通过安全策略进行实现。

2）结合人工的自动防护，是通过工具或者客户端收集到的信息，人为判断其影响，再

调整安全策略或者进行直接处理。

3）人工处理就是在工具和技术不能处理的情况下，手动进行终端安全管理的操作，这些内容中包括空气湿度、电路的安全检查等等。

4）人工处理中也包括人工主动发起操作，再由工具配合进行终端安全管理的操作，包括通知、通报、消息、软件下发等方式。

4．基于风险管理对象的分类

终端包括 PC 设备、服务器、移动介质和相关设备所存储、处理的信息，见图 6-4。

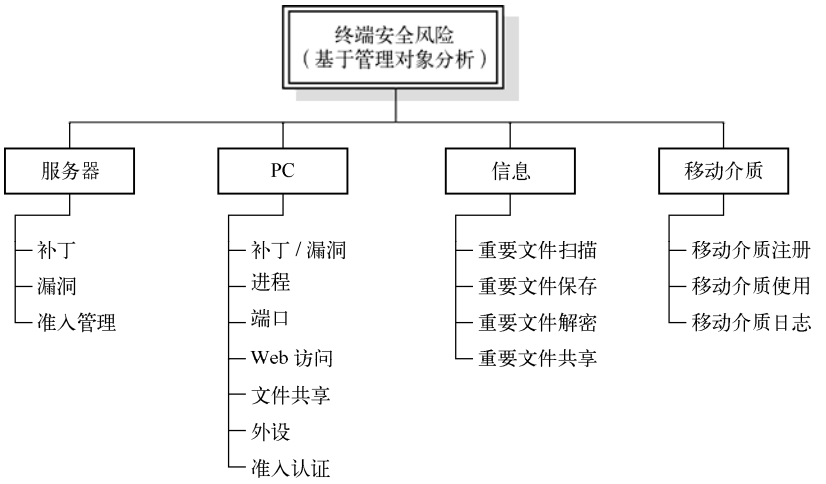

图 6-4　基于管理对象终端安全风险分类

基于风险管理对象的分类其目的是区分管理的主体，作用在不同主体上的风险在管理上是不一样的，尤其是在管理方式、管理手段、管理目标等方面都是不同的。明确风险管理对象，才能有效地进行风险的管控，不会出现明知道有风险，但是无从下手的情况。以下是这些管理对象分类的差别和意义：

1）服务器对象，主要包含服务器自身的补丁、漏洞以及自身安全的维护等内容。服务器是管理工作的前提，若不能保障服务器的稳定运行，就会严重影响业务工作，导致终端不能工作。

2）PC 对象，主要包含终端的各种威胁，包括补丁、进程、端口、Web 访问、文件共享、外设、准入认证等。终端的问题在狭义的范畴之内，就是 PC 的问题。

3）信息对象，主要包含重要文件的扫描、保存、解密、共享等。重要文件是安全的核心，终端工作的主要内容就是信息的处理，因此对于信息的处理一定是要全过程的监控。

4）移动介质对象，主要包含移动介质的注册、使用和日志管理。移动介质是终端管理工作中很容易被忽略的一个部分，也往往是安全问题最容易出现的地方，因此对移动介质进行分类管理，是对终端安全管理的完善和补充。

5．基于风险之间的关系划分

原生风险、次生风险和残余风险。

具体如图 6-5 所示。

1）原生风险　信息与资产本身客观存在的、与人员、使用状态等无关的风险。

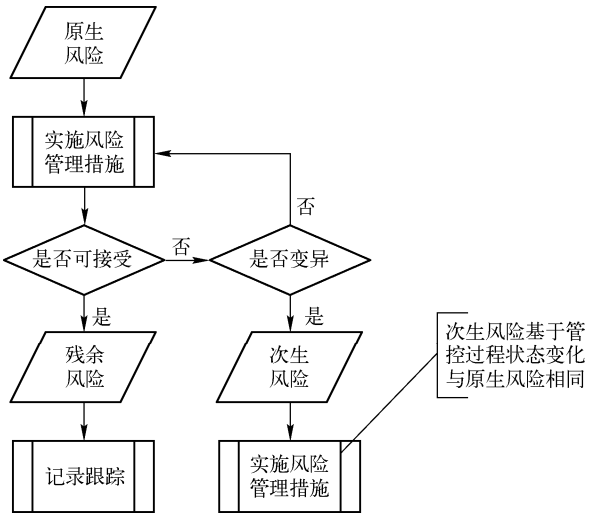

图 6-5　基于风险之间关系的终端安全风险分类

2）次生风险　实施某风险应对措施后出现的新风险称为次生风险。应当识别并规划应对措施。

3）残余风险　是采取应对措施后，风险无法全部消除，还剩余的那部分风险。也就是那些未能为项目团队所控制的战略风险和各经营流程的流程风险。残留风险通常是可接受的，如果剩余的风险超过组织的可接受风险水平，项目团队必须安排进一步的风险应对措施，将剩余风险降低到可接受的水平。

6.2　构建终端安全风险立体分类模型

综上所述，终端安全风险可以从多个维度进行划分。对于 PC、服务器、移动介质等不同的终端安全管理对象综合其风险各维度可构成其风险分类的立体分类模型。具体参见图 6-6。

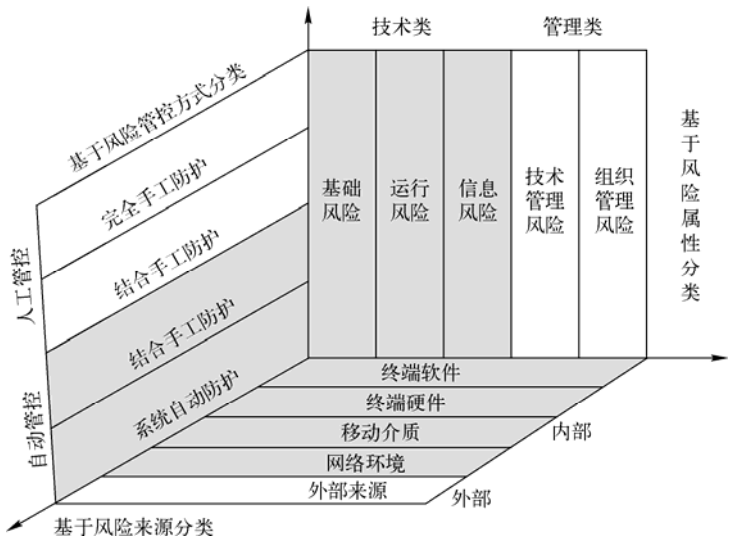

图 6-6　终端安全风险立体分类模式示意图

由图 6-6 可以看出，任何一个风险都是该立体模型中的一个点。通过不同的维度，可以分析风险的来源，风险的属性，风险管理的对象，对应风险的管控方式，这样就能在明确的对象上选择行之有效的管控方式，还可以预见到针对这种属性的处理，可以抑制住什么样来源的风险。

6.3 终端安全风险图谱

1. 基于风险来源

终端安全风险对应的威胁来源可分为内部和外部两类。针对不同的威胁来源的终端安全风险图谱见图 6-7。

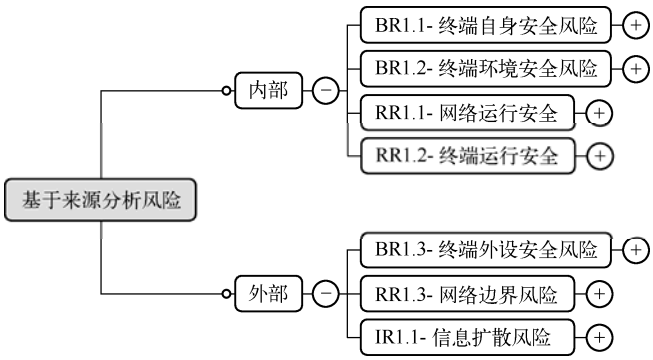

图 6-7 基于来源划分——终端安全风险图谱

2. 基于风险属性的分类

按照风险的属性，可把安全风险分为基础安全风险、运行安全风险和信息安全风险三大类。其中终端安全技术平台自身的风险，暂不列在内。

1）基础安全风险（Basic Risk，简写为 BR）指终端作为信息安全资产自身所存在的风险，与其是否运行、人、制度、流程等无关。

首先是终端自身存在风险，包括 BIOS 等硬件配置隐含的风险，也包含软件配置的风险，例如操作系统本身存在的漏洞和用户口令安全，杀毒软件和应用软件的安装使用风险，终端对于补丁和软件管理的风险；其次，是网络相关参数配置和网络防护措施的管理风险；另外还包括终端所带的外设、端口、注册表、驱动、操作系统驱动等相关的风险。

终端安全基础风险管理（防护）系统的所有安全基础管理功能类可以划分为自身安全风险、环境安全风险、外设安全风险，如图 6-8 所示。

终端安全基础风险管理是针对终端计算机的基础情况进行管理，此类管理不涉及各类具体安全风险事件，强调终端安全基础的安全性，侧重于自身安全的加固和风险的预防，是终端安全技术支撑平台的基础管理类。

2）终端安全运行风险（Running Risk，简写为 RR）指终端在运行过程产生的风险，包括操作系统运行过程相关的网络设备运行、流量、进程/服务等。与基础安全风险相比，终端安全运行风险更具动态性，随着时间和相关环境条件的变化。主要包括终端进行网络访问操作过程中所面临的风险、终端自身运行使用中软硬件的安全风险、终端作为网络中独立运

行的资产，在网络边界范围内所面临的风险，如图 6-9 所示。

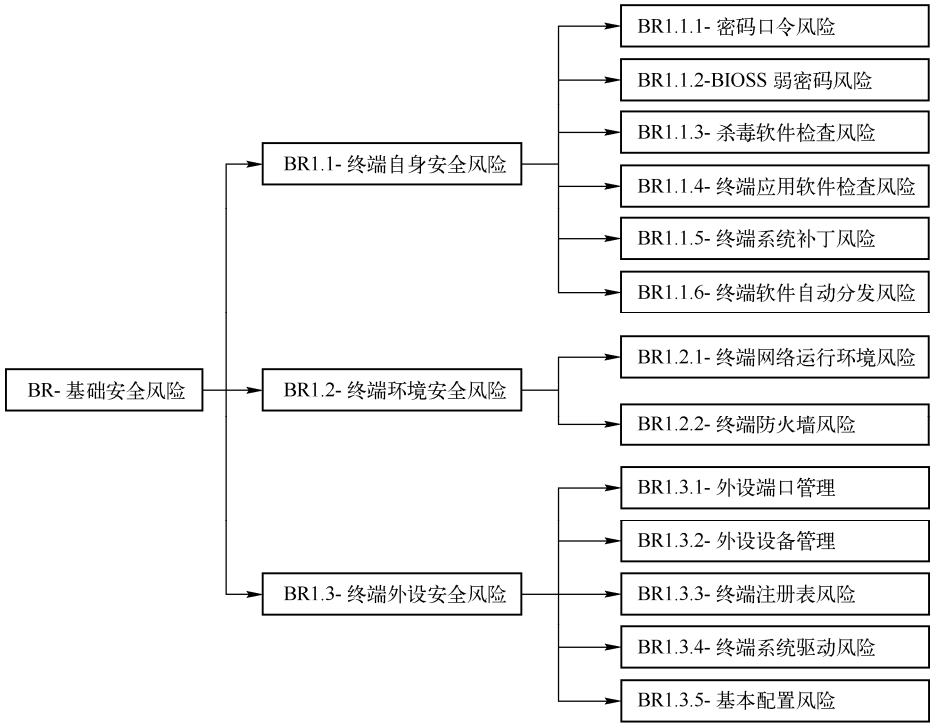

图 6-8　基于属性划分——终端基础安全风险图谱

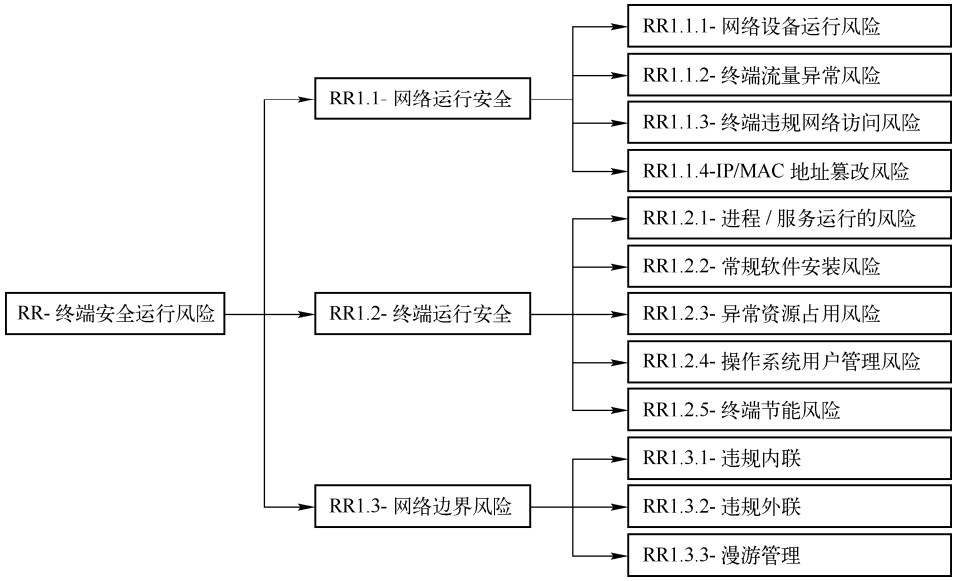

图 6-9　基于属性划分——终端安全运行风险图谱

终端安全运行风险管理主要就终端在运行期间的风险进行管理，这部分内容通常是终端安全管理技术支撑平台管理的重点内容。

3）信息安全风险（Information Risk，简称为 IR）指终端信息安全风险为终端中存储的信息，以及信息在传递过程中所面临的风险。该类风险包括传输过程风险、信息共享风险、介质存储风险以及加密使用风险，见图 6-10。

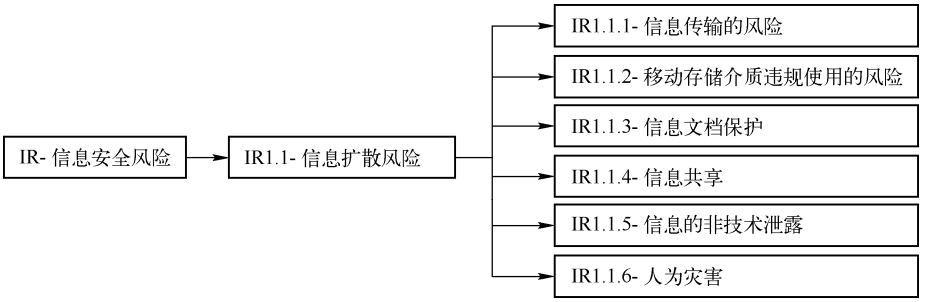

图 6-10　基于属性划分——终端信息安全风险图谱

3．基于风险管控方式的分类

终端安全风险的管控方式可分为基于技术平台全过程处理（即全自动）、基于技术平台人工协助处理（包括半自动、半人工）和全人工处理 3 类。

基于这些种方式可绘出以下终端安全风险图谱，见图 6-11。

风 险 分 类	基于技术平台人工协助处理		全人工处理	全过程处理	合计
	半人工	半自动	全人工	全自动	
基础安全风险（BR）	7	15	16	146	184
信息安全风险（IR）		4	9	28	41
终端安全运行风险（RR）	8	31	5	132	176
总　　计	15	50	30	306	401

图 6-11　基于管控方式——终端安全风险图谱

第 III 部分

终端安全风险管理体系及其实现

第 7 章　终端安全风险管理体系

第 8 章　终端安全风险管理策略

第 9 章　终端安全风险技术防护

第 10 章　终端安全风险日常运维管理

第 11 章　终端安全风险深度分析

第 7 章　终端安全风险管理体系

7.1　构建方法

终端安全风险是随着时间、环境、使用人、防范控制措施的变动而动态变化的。因此，不能把终端安全管理工作当作一个项目去看待。如果把终端安全管理工作仅仅当做一个项目来看待，就不可避免地会出现一些问题。

首先，任何项目都有一个起始和结束日期，项目结束后，人员就会被分配到其他项目中去，出现类似“拆东墙补西墙”的现象。其次，在开始终端安全管理计划时，确定了明确的目标，但是没有确立正确的结构和方法，不能确保终端安全管理成为一个持续不断的改进过程，导致后续工作中整个安全计划反复开始和结束，造成大量的重复工作，致使安全计划的成本增加，效率降低。

因此，最好的办法是对终端安全管理工作采用一种生命周期式的方法。

对于许多组织而言，在制定、实施和维护他们的安全管理计划时，都没有采用生命周期式的方法。有可能是因为他们并不知道如何使用这种方法，或者觉得这种方法过于麻烦，会浪费时间。不遵循生命周期方法，往往会出现以下问题。

- ✓ 书面的制度和管理要求无法与实际的终端安全管理活动相对应，或得不到安全管理活动的支持
- ✓ 组织内担负资产管理和保护工作的人员容易出现职责不清、任务不明而导致工作混乱
- ✓ 无法对终端安全管理工作进展情况进行评估，无法计算投资回报率
- ✓ 无法了解现行安全管理策略的缺陷，也不能用一种标准的方法来改善这些缺陷
- ✓ 无法保证合规性（符合国家、行业相关标准、规范要求）
- ✓ 完全依赖技术手段来解决所有的安全问题
- ✓ 拼凑独立的解决方案，没有整体的解决方案
- ✓ 对存在的安全风险采用一种“火警”式的方法，而不是一种平静、主动而探测性的方法
- ✓ 错误的安全意识，产生混乱的潜在倾向

7.2　构建过程

在具体工作中，要不断评估和改进终端安全管理工作。终端安全管理工作是一个永不终止的生命周期，了解这一点非常重要。任何流程的生命周期都可以通过不同的方式进行描述。我们将使用以下步骤：

1．计划和组织（Plan and Oragnize）
2．实施（Implement）
3．运作和维护（Operate and Maintain）
4．监控和评估（Monitor and Evaluate）

各个步骤要做的工作参见表 7-1。

表 7-1　各个步骤要做的工作

步　骤	工 作 内 容
计划和组织	确定管理承诺 成立监督指导委员会 评估业务推动力 了解组织威胁概况，构建威胁场景 进行风险分析，构建风险体系 在组织、应用软件、网络和组件层开发安全体系结构，构建风险管理体系 确定风险管理体系的解决方案 获得管理层的批准，以继续向前
实施	分配管理任务和责任 制定和实施安全策略 确定静态和动态敏感数据 实施以下终端安全管理工作任务的解决方案（管理的、技术的、物理的） 1）资产确定和管理 2）风险管理 3）隐患管理 4）法规遵从（合规性） 5）身份管理和访问控制 6）变更控制 7）软件开发生命周期 8）业务连贯性规划 9）意识和培训 10）物理安全 11）事件响应 开发每个终端安全管理工作任务的审计和监控解决方案 确定每个终端安全管理工作任务的目标、标准
运作和维护	遵循规程，确保安全管理要求在所实施的解决方案中得到满足 执行内部和外部审计 执行终端安全管理所列出的任务
监控和评估	核查终端安全管理技术支撑平台日志 审计终端安全管理工作结果 评估每个终端安全管理工作目标完成情况 定期与安全管理委员会举行会议 确定改进步骤，并将其整合到“计划和组织”阶段

总之，终端安全风险管理工作是个逐步改进完善的过程，基于 PIOM（Plan and Oragnize-Implement-Operate and Maintain-Monitor and Evaluate，简称 PIOM）过程模式构建和实施终端安全风险管理体系，是保证终端安全风险管理体系持续改进的有效方法。

PIOM 四个步骤成为一个闭环，通过这个环的不断运转，使终端安全管理体系得到持续改进，使信息安全绩效（Performance）螺旋上升，如图 7-1。

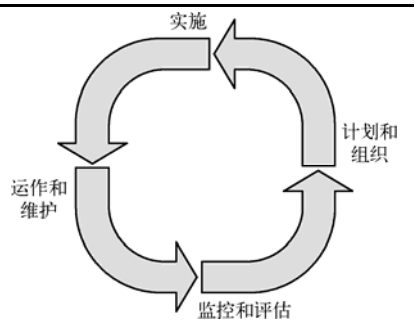

图 7-1　PIOM 过程模式图

采用有效的技术支撑手段是构建终端安全管理体系的关键之一。基于终端安全防护体系与终端安全管理体系两个大部分的技术支撑，从技术和管理角度对终端安全风险进行管理、防护和控制，降低风险的发生。终端安全防护的重点在于及时有效地识别终端安全风险，快速实施安全应对措施，终端安全管理重点在于风险的综合分析和控制，对于需复杂分析方法和控制手段的风险依据其发展的不同阶段，按照事前、事中、事后运用相应的应对措施，以规避、减少或控制风险，实现对于终端安全风险的全过程管理。基于终端安全风险运作管理过程中终端的各类情况进行监测和风险分析，根据监测和分析的结果不断改进和完善风险监控和防护的策略，持续提升终端安全风险管理各个部分的能力，逐步使所有终端风险都处于可承受的范围之内。

7.3 构建体系

终端安全管理体系由终端安全组织体系、安全策略管理、安全运维管理和安全技术管理4个部分构成。

（1）终端安全组织

终端安全组织管理体系主要包括安全组织和管理制度建设、安全管理人员的培训教育等。本文中主要阐述终端安全管理中的组织构成、人员角色和职责划分，具体参见 7.4 节“构建组织”。

（2）终端安全策略

安全策略体系主要通过建立完整的信息安全策略体系，提高员工的安全意识和技术水平，完善各种安全策略和安全机制；利用多种安全技术措施和信息安全管理实现对网络的多层保护，防范终端信息安全事件的发生，减少终端非法、违规使用的问题，防止终端信息的扩散。

（3）终端安全运作

终端安全运作管理是整个系统安全体系的驱动和执行环节。建立有效的信息安全保障体系需要在终端安全策略的指导下，依托终端安全防护和管理技术，强化安全组织管理，全面实现系统安全运作与保障。

1）安全运作管理是整个信息安全工作的日常体现和执行环节。应该在信息安全策略的指导下，制定并遵照安全维护的操作流程，实施信息安全运作。

2）应进行安全风险管理，以可以接受的成本或最小成本，确认、控制、排除可能影响信息系统的安全风险，并将其带来的危害最小化。

3）定期进行安全风险评估，通过对安全管理策略、信息系统结构、网络、系统、数据库、业务应用等方面进行安全风险评估，确定所存在的安全隐患和安全风险，了解安全现状以及如何解决这些问题的方法。

4）对于信息系统中重要业务系统、服务器和网络设备，制定安全配置标准和规定来规范安全配置管理工作，建立配置更改管理制度，并进行定期的审计和检查。

5）对于外包开发的业务系统软件，应制定业务软件安全标准来进行规范，要求有完善的鉴别和认证、访问控制、日志审计功能和数据验证功能，杜绝木马和后门，建立源代码控制和软件版本控制机制。

6）建立第三方安全管理的规范和制度，并要求其严格遵守。严格控制第三方对信息系统的访问，并在合同中规定其安全责任和安全控制要求，以维护第三方访问的安全性。

7）对于意外、灾难和入侵的处理，建立包含事件鉴别、事件恢复、犯罪取证、攻击者追踪的安全事件的紧急响应体系和机制，制定并遵照正确的安全事件处理流程，尽量减少安全事故和故障造成的损失，监督此类事件并从中吸取教训。

8）制定并实施安全培训和教育计划，进行安全意识、技能和安全制度培训。

9）对于员工违反安全策略和安全流程，制定相应的纪律处分规定进行处罚。

10）进行物理安全和环境安全的管理，建立机房管理制度。

（4）终端安全技术

终端安全技术框架主要由终端安全防护平台和安全管理平台构成。其中，终端安全管理平台完成管理层面的职能，终端安全防护平台完成技术层面的职能。终端安全平台有效地将安全组织管理、策略管理、运作管理和安全技术框架结合在一起，协调一致工作，完成终端安全管理任务。

具体参见图 7-2。

图 7-2　终端安全管理体系架构示意图

终端安全防护平台是整个安全体系的核心基础组件，负责终端信息的采集和维护、终端安全风险的管理和防护、终端安全事件的监测和控制，为管理平台提供所需要的各类数据的采集和传输。安全管理平台是整个安全体系的核心和枢纽，作为技术支撑平台，它向上为安全策略管理、安全组织管理、安全运作管理提供基于安全管理平台的自动化支持协助，向下贯彻整个技术层面，指导安全防护平台有效监控终端系统，并基于防护系统监控收集的信息，进行统一的自动化风险评估，评价这些系统是否符合安全管理的策略和基线，并报告给决策者，提供及时的响应。终端安全管理平台和终端安全防护平台无缝协作，保证了终端系

统符合终端安全管理的策略要求，符合安全管理运作流程，将安全风险降到最低。

7.4 构建组织

通过组建完整的信息网络安全组织机构，设置安全管理人员，规划安全策略确定安全组织机制，明确安全组织原则和完善安全组织措施；制定严格的安全组织制度，合理地协调法律、技术和组织 3 种因素，实现对系统安全组织的科学化、系统化、法制化和规范化，达到保障整体安全的目的。

7.4.1 组织结构

组织结构按照统一领导和分级组织的原则，安全组织必须设立专门的组织机构，配备相应的安全组织人员，并实行“一把手”责任制，明确主管领导，落实部门责任，各尽其职。其主要内容包括各级组织机构的建立；各级组织机构的职能、权限划分；人员岗位、数量、职责的确定。

信息安全管理组织架构是实施终端系统安全，进行终端安全管理的必要保证。图 7-3 是对应终端安全管理体系的组织架构图。

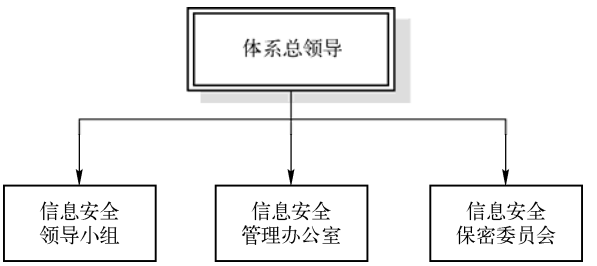

图 7-3　对应终端安全管理体系的组织架构图

（1）信息安全领导小组

信息安全是组织/企业工作人员必须共用承担的责任，因此，应建立信息安全领导小组。信息安全领导小组是单位网络与信息安全工作的最高领导决策机构，它不隶属于任何部门，直接对本单位最高领导负责，信息安全领导小组是一个常设机构，负责本单位信息安全工作的宏观管理。其主要职能如下。

- ✓ 负责领导落实系统安全建设的总体规划
- ✓ 制定规划并监督安全工作规划的制定与实施
- ✓ 负责组织制定信息系统安全策略并审批下级单位上报的信息系统安全策略调整建议
- ✓ 负责组织细化规章制度，制定相应程序指南，并监督落实规章制度
- ✓ 负责审阅信息安全工作报告
- ✓ 负责管辖范围内重大安全事故查处与向上级汇报工作

（2）信息安全管理办公室

信息安全管理办公室应该由本机构信息安全相关的若干管理部门共同完成，例如信息技术部门、业务应用部门、安全保卫部门、人事行政部门等。

- ✓ 信息技术部门对信息系统及信息系统安全保障提供技术决策和技术支持，在技术上对信息系统和信息系统安全保障承担管理责任
- ✓ 业务应用部门对信息系统的业务处理以及业务流程的安全承担管理责任
- ✓ 安全保卫部门对信息系统的场地以及系统资产的防灾、防盗、防破坏等承担管理责任
- ✓ 行政部门从行政上对信息安全保障执行管理工作

各个部门应与信息技术部门协作，共同对信息系统的建设和运行维护承担管理责任。

为明确安全职责，应在相关管理部门中指定对信息安全负责的主管，这些主管共同贯彻执行系统安全工作的方针政策、规章制度及有关的技术标准、规范和方案，并监督安全策略的落实。

（3）信息安全保密委员会

重要系统和文件的保密是一项重要的信息安全工作，根据国家保密局的相关规定，成立信息安全保密委，负责重要文件密码信息的管理。该委员会至少由负责领导和密钥管理员组成。

7.4.2 人员角色

对于信息系统建设和运行维护的具体执行，应该有相应的安全管理岗位，但考虑到具体情况有所差别，在本方案中定义了相应的安全角色和职责，对具体的安全岗位不做定义，各具体机构根据实际情况设置相应安全岗位，具体的安全角色和职责的描述如下。

终端相关人员分为使用人员和管理人员，其中，使用人员又分为内部人员和外部人员，终端使用人员的阐述参见 1.4 节描述。

终端管理人员包括终端使用者、主机系统管理员、资产管理员、认证管理员、安全管理员、安全审计员、安全保密管理员、安全主管。各种角色在终端安全风险管理工作的职责参见表 7-2。

表 7-2 终端安全管理人员角色-责任表

角　色	责　任
终端使用者	按照终端安全体系的相关制度操作终端
资产管理员	管理终端资产，维护资产的属性和状态，维护资产与责任人的关系
认证管理员	管理终端安全平台认证账号和账号安全策略，并且对于认证行为进行审计
主机系统管理员	负责主机操作系统的安全配置（包括及时修补系统漏洞）和日常审计，系统应用软件的安装，从系统层面实现对用户与资源的访问控制
	协助安全管理员制定主机操作系统的安全配置规则，并落实执行
	负责主机设备的日常管理与维护，保持系统处于良好的运行状态
	为安全审计员提供完整、准确的主机系统运行活动的日志记录
	在主机系统异常或故障发生时，详细记载发生异常时的现象、时间和处理方式，并及时上报
	编制主机设备的维修、报损、报废计划，报主管领导审核
安全管理员	执行组织制定和批准的终端安全风险管理策略
	负责组织审议相关各种安全方案、安全审计报告、应急计划以及整体安全管理制度
	负责对终端安全产品购置提供建议，负责组织制定各种终端安全产品策略与配置规则，负责跟踪终端安全产品投产后的使用情况

（续）

角　色	责　任
安全管理员	负责指导并监督系统管理员及普通用户与安全相关的工作
	负责组织终端系统的安全风险评估工作，并定期进行系统漏洞扫描，形成安全评估报告
	根据本机构的信息安全需求，定期提出本机构的信息安全改进意见，并上报信息安全管理部门主管
	定期查看信息安全站点的安全公告，跟踪和研究各种终端相关信息安全漏洞和攻击手段，在发现可能影响信息安全的安全漏洞和攻击手段时，及时做出相应的对策，通知并指导系统管理员进行安全防范
安全审计员	负责定期对主机系统、网络产品、应用系统的日志文件进行分析审计，发现问题及时上报
	负责对信息安全保障管理活动进行独立的监督，提供内部独立的审计和评估工作，并根据需要可以协同外部审计评估机构进行评估和认证，为决策领导提供信息系统和信息安全保障执行状况的客观评价
安全保密管理员	对保密终端按体系要求的保密规定进行保密工作的开展，包括对交易、传输、认证密钥的管理以及加密机的操作
安全主管	提出、制定并批准所管理范围的终端安全风险管理策略
	领导和组织所辖范围（部门）内的终端安全风险管理工作
	基于所辖范围中部署的终端安全防护和安全管理技术平台对终端安全风险的管理结果信息，判断终端系统是否出现次生风险，是否存在残余风险，次生和残余风险是否可接受，并判断终端系统是否在合法合规状态下运行
	检查终端安全管理系统中生成的终端安全状态报告
	定期或不定期地基于终端安全管理平台实现对于终端风险的评估

在多级组织中终端安全管理人员通常又可分为 3 级：全局安全管理人员、本地安全管理人员、组安全管理人员。

职责参见表 7-3。

表 7-3　多级组织中三级终端安全管理人员分类表

管理员类别	管 理 权 限	管 理 范 围	职　责
区域安全管理人员	高	区域终端	负责整个区域终端安全管理体系的安全管理； 能查看全部的终端的安全事件，并及时对下级反馈的安全问题提出整改的建议
本地安全管理人员	中	本地终端	负责本地的安全管理体系的安全管理； 有问题及时跟上级汇报并需求解决方案； 对安全问题及时记录以便于后续问题跟踪和定位
组安全管理人员	低	本组终端	负责本组的安全体系管理；及时向本地系统管理员汇报组内的安全问题； 只能对组内的终端进行安全管理操作； 对安全问题及时记录以便后续问题跟踪和定位

第 8 章　终端安全风险管理策略

8.1　基于资产全生命周期的管理

终端资产管理中，资产管理包括从资产申请、购置、验收、调拨、领用、使用、维修、盘点、清理和废弃整个生命周期的各个阶段，即该管理过程涉及资产的全生命周期各个阶段，称为资产全生命周期。

资产全生命周期包括可分配、已调拨、已领用、被借用、正常使用、维修中、待报废和已报废 8 个不同状态。就终端资产的使用而言，可将资产的全生命周期划分为入网阶段、运行阶段和废弃阶段三大阶段，鉴于资产维护工作的特殊性，将运行阶段中涉及变更和维修的工作抽离出来构成维护阶段。为了与传统的资产全生命周期的概念相区别，本书将入网、运行、维护和废弃 4 个阶段称为终端资产使用生命周期。终端资产全生命周期与终端资产使用生命周期对应关系参见图 8-1。

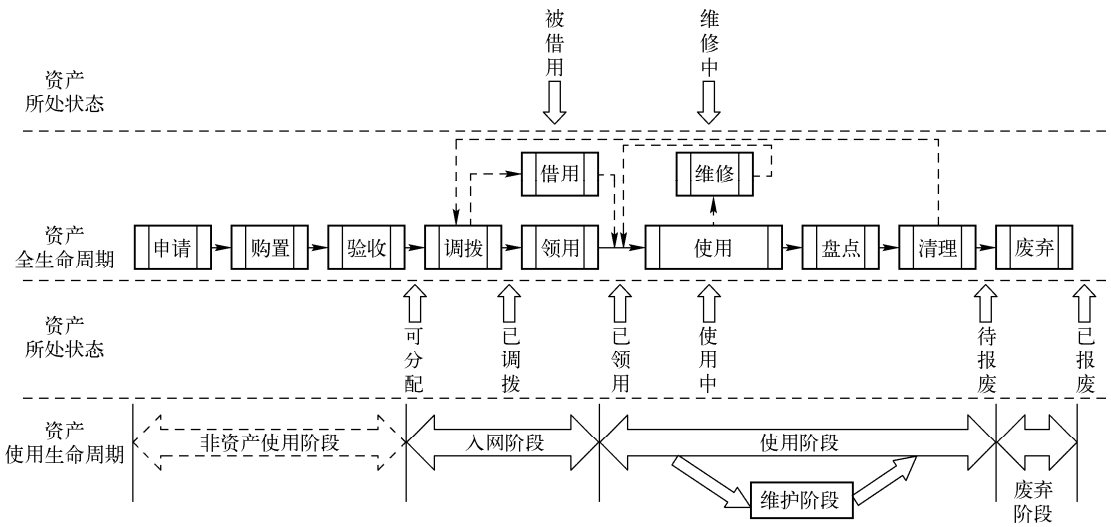

图 8-1　终端资产全生命周期与终端资产使用生命周期对应图

（1）入网阶段

入网阶段指终端设备从申请到入网期间的所有过程。其重点工作在于做好终端资产使用的准备，对于资产的定位在入网前确定下来，避免信息级别错位，导致信息安全存在隐患。

该阶段输入的是采购、验收入库的终端设备，对于采购信息的要求进行记录，核对验收入库时终端设备的相关信息，尤其是对终端设备的厂商进行标注，区分厂商的性质（国产、外资、合资等）。该阶段输出的应该是符合组织终端入网法规的终端资产，并且建立资产的

唯一性标识，全程建立资产在生命周期中的识别性保障。

（2）运行阶段

从使用周期上看，终端登记入网后到终端最终退库或废弃期间，终端资产都处于运行阶段。鉴于终端资产在使用过程中存在的硬件配件变更、资产自身更换使用人、资产所属部门单位变更、资产在行业内上下级调动、资产在不同网络之间的转换使用、资产因故障进行维修等多种情况，将终端入网后到废弃之间正常运行的过程称为运行阶段，将在期间软硬件变化、换人使用、转网使用、故障维修等工作过程统称为维护阶段。因维护阶段的存在，运行阶段可能是断续的时间段。运行阶段的重点工作是保证终端合法合规运行，并且对应资产的唯一性标识和人员的责任与使用建立直接关联，保障资产在该阶段中所有的风险都关联到具体的责任人和使用者，对于网络资源以及信息安全的的实际操作者进行全程的记录，杜绝资产管理、使用和操作的“盲区”。

该阶段的输入应是符合组织终端入网法规的终端资产。包括新申购的入网终端资产、软硬件变更后的终端资产、换人或转网使用的终端资产、维修后重新入网的终端资产等。该阶段的出口包括维护和废弃两个阶段，针对不同阶段的输出不同。

（3）维护阶段

维护阶段是运行阶段中的特殊阶段。从时间上看，该阶段处于运行阶段之中，维护阶段可能是断续的时间阶段。维护阶段的主要工作是对终端正常运行外出现的变更、维修等情况进行处理，以保证终端资产在出现软硬件、人员和使用环境变更或出现故障时进行有效的管理，保证终端资产再次合法合规的使用，重点在于维持终端在生命周期过程中的唯一性，避免因为维修操作的流程导致终端消失在管理和监控的范围内，出现信息安全级别混乱，资产流失等问题。

该阶段的输入为待维护资产及其变更或故障信息，输出为符合组织入网要求的变更或维修后的终端资产、资产管理信息更新。

（4）废弃阶段

当资产无法正常使用时，进入报废阶段。该阶段的主要工作是按照组织规定的流程和方法完成资产废弃前一系列的工作，包括做相关登记、信息处理等。该阶段工作的关键点是要准确识别并处理和废弃资产相关的组织其他资产，不能造成对废弃资产外组织其他资产损失或损坏，如必须将废弃终端设备中存储的工作信息进行处理即完成废弃工作，同时对资产的唯一性标识进行完结处理。

该阶段输入是待废弃资产（及相关资产），输出为废弃资产、资产管理信息变更、与待报废资产相关但并不进行报废的资产。

8.2 基于风险管控全过程的管理

终端安全风险全过程管理是指从风险的预防、事前、事中、事后和转移等的全生命周期中，进行分析、管理和处置着手，动态地从资产使用生命周期、风险生命周期、终端安全边界、人员和信息等多角度全面分析终端风险，跟踪风险、处理风险和审计风险，实现对风险的全生命周期管理。同时，将终端安全风险纳入到网络总体安全风险中，既可以作为单独的风险管理平台管控，又可以作为总体安全的一部分，从全局分析，并以此作为网络管理、风

险告警和辅助决策的依据。

每一个风险事件都可以分 3 个阶段：事前、事中和事后，需要针对每一个阶段制定相应的应对措施，控制风险。制定措施需要遵循以下原则。

1）事前　对于高风险必须进行有效防范，防止此类风险的发生。做到能够事前防范的风险决不留到后面的阶段进行处置。做好安全意识培训和预防工作。

2）事中　当出现意外导致高风险的事件发生的时候，需要立即通知管理人员进行处理。针对出现的违规行为，应该和当事人进行沟通，强化意识，减少违规行为的再度发生，并对违规行为及相应的处置措施进行详细记录。

3）事后　定期对终端运行和使用情况和人员各类操作行为情况进行汇总、分析、审计，发现和挖掘风险管理相关规律，改进管理措施。根据风险的类别和危害程度，对大部分能够技术控制的尽量自动化、技术化管理。对于有些高风险，技术达不到或者需要高科技人才处理的就转包给专业公司处理，通过转移风险，降低公司可能承担的风险。

在资产的使用周期的 4 个阶段中出现的任何一个风险，都可以按照事前、事中、事后进行分析，人和系统做到全程管理。从系统的角度看是闭环管理。

8.3　基于等保的合规性遵从管理

等级保护是我国重要的信息安全规范要求，在终端安全风险管理中应覆盖等级保护相关级别对于终端相关部分要求。在《终端安全风险分析报告》中对于每一类风险进行了等保合规性的详细分析。表 8-1，8-2 分别为等保 2、3 级系统相关要求与终端安全风险管控的对应表。

表 8-1　等保 2 级要求与终端安全风险管控的对应表

等保要求类	风 险 类 别	等级保护二级要求详细说明
6.1.3.1 身份鉴别（G2）	操作系统密码口令风险 （BR1.1.1）	a) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别 b) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换 c) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施 d) 当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听 e) 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性
6.1.3.5 恶意代码防范 （G2）	杀毒软件检查风险 （BR1.1.3）	a) 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库 b) 应支持防恶意代码的统一管理
6.2.5.8 恶意代码防范管理 （G2）	杀毒软件检查风险 （BR1.1.3）	a) 应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查 b) 应指定专人对网络和主机进行恶意代码检测并保存检测记录 c) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定
7.2.5.5 监控管理和安全管理中心 （G3）	终端应用软件检查风险 （BR1.1.4）	a) 应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存

（续）

等保要求类	风 险 类 别	等级保护二级要求详细说明
6.2.5.6 系统安全管理 （G2）	终端系统补丁风险 （BR1.1.5）	a) 应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补 b) 应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装
6.1.2.5 入侵防范（S2）	终端防火墙风险 （BR1.2.2）	应在网络边界处监视以下攻击行为：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 碎片攻击和网络蠕虫攻击等
6.2.5.3 介质管理 （G2）	外设端口管理 （BR1.3.1）	a) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理 b) 应对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点 c) 应对需要送出维修或销毁的介质，首先清除其中敏感数据，防止信息的非法泄漏 d) 应根据所承载数据和软件的重要程度对介质进行分类和标识管理
6.2.5.4 设备管理（G2）	外设设备管理 （BR1.3.2）	a) 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理 b) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作
6.2.5.6 系统安全管理 （G2）	基本配置风险 （BR1.3.4）	应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定
6.1.2.1 结构安全（G2）	网络设备运行风险 （RR1.1.1）	a) 应保证关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要 b) 应保证接入网络和核心网络带宽满足业务高峰期需要 c) 应绘制与当前运行情况相符的网络拓扑结构图 d) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段
6.1.2.3 安全审计（G2）	网络设备运行风险 （RR1.1.1）	a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录 b) 审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息
6.1.2.2 访问控制（G2）	终端流量异常风险 （RR1.1.2）	a) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为网段级 b) 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户 c) 应限制具有拨号访问权限的用户数量
6.1.2.3 安全审计（G3）	终端流量异常风险 （RR1.1.2）	应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录
6.1.2.2 访问控制（G2）	终端违规网络访问风险 （RR1.1.3） IP/MAC 地址篡改风险 （RR1.1.4）	应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户
6.1.2.3 安全审计（G2）	IP/MAC 地址篡改风险 （RR1.1.4）	a）应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录 b) 审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息
6.2.5.4 设备管理（G2）	终端节能风险 （RR1.2.5）	应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作
6.1.2.4 边界完整性检查 （S2）	违规外联 （RR1.3.2）	应能够对内部网络中出现的内部用户未通过私自联到外网的行为进行检查
6.2.5.3 介质管理（G2）	移动存储介质违规使用 （IR1.1.2）	a) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理 b) 应对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点 c) 应对需要送出维修或销毁的介质，首先清除其中敏感数据，防止信息的非法泄漏 d) 应根据所承载数据和软件的重要程度对介质进行分类和标识管理

（续）

等保要求类	风 险 类 别	等级保护二级要求详细说明
6.1.5.1 数据完整性 （S2）	信息文档保护 （IR1.1.3）	应能够检测到鉴别信息和重要业务数据在传输过程中完整性受到破坏
6.2.5.8 密码管理（G2）	信息共享 （IR1.1.4）	应使用符合国家密码管理规定的密码技术和产品
6.2.5.6 系统安全管理 （G2）	基本配置风险 （BR1.3.4）	应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定
6.2.3.1 人员录用（G2）	信息的非技术性泄漏 （IR1.1.5）	a) 应规范人员录用过程，对被录用人的身份、背景、专业资格等进行审查，对其所具有的技术技能进行考核 b) 应与从事关键岗位的人员签署保密协议
6.2.3.5 外部人员访问管理（G2）	信息的非技术性泄漏 （IR1.1.5）	应确保在外部人员访问受控区域前得到授权或审批，批准后由专人全程陪同或监督，并登记备案
6.2.5.1 环境管理（G2）	信息的非技术性泄漏 （IR1.1.5）	a) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定 b) 应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员等
6.1.1.10 电磁防护(S2)	信息的非技术性泄漏 （IR1.1.5）	电源线和通信线缆应隔离铺设，避免互相干扰
6.1.1.2 物理访问控制 (G2)	人为灾害 （IR1.1.6）	a) 机房出入口应安排专人值守，控制、鉴别和记录进入的人员 b) 需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围
6.1.5.2 数据保密性 （S2）	人为灾害 （IR1.1.6）	应采用加密或其他保护措施实现鉴别信息存储保密性
6.1.5.3 备份和恢复 （G2）	人为灾害 （IR1.1.6）	应能够对重要信息进行备份和恢复
等保范围外遵循的相关要求	BIOS 弱密码风险 （BR1.1.2）	对 BIOS 密码弱口令的要求，详细内容参考风险点描述
	终端软件自动分发风险 （BR1.1.6）	对终端软件自动分发的要求，详细内容参考风险点描述
	终端网络运行环境风险 （BR1.2.1）	对终端网络运行环境的要求，详细内容参考风险点描述
	终端注册表风险 （BR1.3.2）	对终端注册表管理的要求，详细内容参考风险点描述
	终端系统驱动风险 （BR1.3.3）	对终端系统驱动的要求，详细内容参考风险点描述
	进程/服务运行的风险 （RR1.2.1）	对终端进程/服务运行的要求，详细内容参考风险点描述
	违规软件安装风险 （RR1.2.2）	对终端软件安装的要求，详细内容参考风险点描述
	异常资源占用的风险 （RR1.2.3）	对终端异常资源占用的要求，详细内容参考风险点描述
	操作系统用户管理的风险（RR1.2.4）	对终端操作系统用户管理的要求，详细内容参考风险点描述
	漫游管理 （RR1.3.3）	对以漫游方式接入的终端的管理要求，详细内容参考风险点描述
	信息传输 （IR1.1.1）	对终端信息传输的管理要求，详细内容参考风险点描述
	违规内联 （RR1.3.1）	
	信息的非技术性泄漏 （IR1.1.5）	
	终端应用软件检查风险 （BR1.1.4）	

表 8-2　等保 3 级要求与终端安全风险管控的对应表

等保要求类	风 险 类 别	等级保护三级要求详细说明
7.1.3.1 身份鉴别（S3）	操作系统密码口令风险 (BR1.1.1)	a) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换 b) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施 c) 当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听 d) 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性 e) 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别
7.1.3.6 恶意代码防范（G3）	杀毒软件检查风险 (BR1.1.3)	a) 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库 b) 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库 c) 应支持防恶意代码的统一管理
7.2.5.8 恶意代码防范管理（G3）	杀毒软件检查风险 (BR1.1.3)	a) 应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查 b) 应指定专人对网络和主机进行恶意代码检测并保存检测记录 c) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定 d) 应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报
7.2.5.5 监控管理和安全管理中心（G3）	终端应用软件检查风险(BR1.1.4)	应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存
7.2.5.7 系统安全管理（G3）	终端系统补丁风险 (BR1.1.5)	应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装
7.1.2.5 入侵防范（G3）	终端防火墙风险 (BR1.2.2)	应在网络边界处监视以下攻击行为：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 碎片攻击和网络蠕虫攻击等
7.2.5.3 介质管理（G3）	外设端口管理 (BR1.3.1)	a) 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面做出规定 b) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理 c) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点
7.2.5.4 设备管理（G3）	外设设备管理 (BR1.3.2)	a) 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等 b) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作
7.2.5.7 系统安全管理（G3）	基本配置风险 (BR1.3.4)	应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面做出具体规定
7.1.2.1 结构安全（G3）	网络设备运行风险 (RR1.1.1)	a) 应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要 b) 应保证网络各个部分的带宽满足业务高峰期需要 c) 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径 d) 应绘制与当前运行情况相符的网络拓扑结构图 e) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段 f) 应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段 g) 应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主机
7.1.2.3 安全审计（G3）	网络设备运行风险 (RR1.1.1)	a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录 b) 审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息 c) 应能够根据记录数据进行分析，并生成审计报表 d) 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等

（续）

等保要求类	风 险 类 别	等级保护三级要求详细说明
7.1.2.2 访问控制（G3）	终端流量异常风险(RR1.1.2)	a) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级 b) 应限制网络最大流量数及网络连接数 c) 应限制具有拨号访问权限的用户数量
7.1.2.3 安全审计（G3）	终端流量异常风险(RR1.1.2)	应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录
7.1.2.2 访问控制（G3）	终端违规网络访问风险(RR1.1.3)	安全审计应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录
7.1.2.2 访问控制（G3）	IP/MAC 地址篡改风险(RR1.1.4)	重要网段应采取技术手段防止地址欺骗
7.1.2.3 安全审计（G3）	IP/MAC 地址篡改风险(RR1.1.4)	应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录
7.2.5.4 设备管理（G3）	终端节能风险(RR1.2.5)	应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作
7.1.2.4 边界完整性检查（S3）	违规内联(RR1.3.1)	应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断
7.1.2.4 边界完整性检查（S3）	违规外联(RR1.3.2)	应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断
7.2.5.3 介质管理（G3）	移动存储介质违规使用(IR1.1.2)	a) 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面做出规定 b) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理 c) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点 d) 应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁 e) 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同 f) 应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理
7.1.5.1 数据完整性（S3）	信息文档保护(IR1.1.3)	a) 应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施 b) 应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施
7.2.5.9 密码管理（G3）	信息共享(IR1.1.4)	应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品
7.2.5.7 系统安全管理（G3）		应根据业务需求和系统安全分析确定系统的访问控制策略
7.1.4.6 通信保密性	信息的非技术性泄漏(IR1.1.5)	a）在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证 b）在对通信过程中整个报文或会话过程进行加密
7.2.3.1 人员录用	信息的非技术性泄漏(IR1.1.5)	a）应签署保密协议 b）应对内部人员中选拔从事关键岗位的人员，并签署岗位安全协议
7.2.3.5 外部人员访问管理（G3）	信息的非技术性泄漏(IR1.1.5)	a）应确保在外部人员访问受控区域前提出书面申请，批准后由专人全程陪同或监督，并登记备案 b）对外部人员允许访问的区域、系统、设备、信息等内容应进行书面规定，并按照规定执行
7.2.5.1 环境管理（G3）	信息的非技术性泄漏(IR1.1.5)	a）应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定 b）应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室立即交还该办公钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸质文件等

（续）

等保要求类	风 险 类 别	等级保护三级要求详细说明
7.1.1.10 电磁防护	信息的非技术性泄漏(IR1.1.5)	应对关键设备和磁介质实施电磁屏蔽
7.1.1.2 物理访问控制	人为灾害(IR1.1.6)	a) 机房出入口应安排专人值守，控制、鉴别和记录进入的人员 b) 需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围 c) 应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域 d) 重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员
7.1.5.2 数据保密性（G3）	人为灾害(IR1.1.6)	应采用加密或其他保护措施实现系统管理数据、鉴别数据和重要业务数据存储保密性
7.1.5.3 备份和恢复（G3）	人为灾害(IR1.1.6)	应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份文件刻录光盘存放
等保范围外遵循的相关要求	BIOS 弱密码风险(BR1.1.2)	对 BIOS 密码弱口令的要求，详细内容参考风险点描述
	终端软件自动分发风险(BR1.1.6)	对终端软件自动分发的要求，详细内容参考风险点描述
	终端网络运行环境风险(BR1.2.1)	对终端网络运行环境的要求，详细内容参考风险点描述
	终端注册表风险(BR1.3.2)	对终端注册表管理的要求，详细内容参考风险点描述
	终端系统驱动风险(BR1.3.3)	对终端系统驱动的要求，详细内容参考风险点描述
	进程/服务运行的风险(RR1.2.1)	对终端进程/服务运行的要求，详细内容参考风险点描述
	违规软件安装风险(RR1.2.2)	对终端软件安装的要求，详细内容参考风险点描述
	异常资源占用的风险(RR1.2.3)	对终端异常资源占用的要求，详细内容参考风险点描述
	操作系统用户管理的风险(RR1.2.4)	对终端操作系统用户管理的要求，详细内容参考风险点描述
	漫游管理(RR1.3.3)	对以漫游方式接入的终端的管理要求，详细内容参考风险点描述
	信息传输(IR1.1.1)	对终端信息传输的管理要求，详细内容参考风险点描述

8.4 终端安全风险管理点

为及时发现终端安全风险，并进行有效管控，在资产使用生命周期中的各阶段的可能存在风险及隐患的时刻，对终端安全状态、风险状况和相关人的行为进行监测，在这些时间点上所作的监测称为终端安全风险管理点。具体参见表 8-3。

表 8-3 终端安全风险管理点

资产使用生命周期	风 险 管 控	风险管理点	监 测 内 容
入网阶段	事前	杀毒软件使用情况	隐患
	事前	补丁安装情况	隐患
	事前	软件安装情况	隐患
运行阶段	事中	软件安装/卸载行为	隐患和风险
	事中	应用软件分发	隐患和风险
	事中	补丁更新情况	隐患和风险

（续）

资产使用生命周期	风 险 管 控	风险管理点	监 测 内 容
运行阶段	事中	密码设置安全	隐患
	事中	网络流量监控	隐患和风险
	事前	网络资源使用监控	隐患
	事中	网络资源使用监控	隐患和风险
	事前	软件防火墙使用情况	隐患
	事中	软件防火墙运行情况	隐患和风险
	事前	终端外设控制	隐患
	事前	移动存储介质使用	隐患
	事中	移动存储介质应用	隐患和风险
	事后	移动存储介质应用	风险
	事前	光盘刻录机使用	隐患
	事中	光盘刻录机应用	隐患和风险
	事后	光盘刻录机应用	风险
	事中	操作系统驱动防护	隐患和风险
	事前	物理环境要求	隐患
	事中	物理环境监控	隐患和风险
	事中	设备使用寿命监控	隐患和风险
	事中	网络运行情况监控	隐患和风险
	事前	进程/服务运行要求	隐患
	事中	进程/服务运行监控	隐患和风险
	事前	系统性能要求	隐患
	事中	系统性能监控	隐患和风险
	事中	操作系统用户监控	隐患和风险
	事前	违规内联定义	隐患
	事中	违规内联监控	隐患和风险
	事后	违规内联审计	风险
	事前	违规外联定义	隐患
	事中	违规外联监控	隐患和风险
	事后	违规外联审计	风险
	事中	打印行为监控	隐患和风险
	事后	打印行为审计	风险
	事中	邮件外发监控	隐患和风险
	事后	邮件外发审计	隐患和风险
	事前	重要文件操作监控	隐患
	事后	重要文件操作审计	隐患和风险
维修阶段	事前	重要文件操作监控	隐患
	事后	重要文件操作监控	风险
	事前	密码设置安全	隐患
	事后	密码设置安全	隐患和风险

（续）

资产使用生命周期	风 险 管 控	风险管理点	监 测 内 容
维修阶段	事前	终端外设控制	隐患
	事后	终端外设控制	隐患和风险
	事前	操作系统用户监控	隐患
	事后	操作系统用户监控	风险
	事后	杀毒软件使用情况	风险
	事后	补丁安装情况	风险
	事后	软件安装情况	风险
废弃阶段	事前	重要文件操作监控	隐患
	事前	密码设置安全	隐患
	事前	终端外设控制	隐患
	事前	操作系统用户监控	隐患
	事后	操作系统用户监控	风险
	事后	杀毒软件使用情况	隐患和风险
	事后	补丁安装情况	隐患和风险
	事后	软件安装情况	隐患和风险

第 9 章　终端安全风险技术防护

9.1　终端安全风险处置

终端风险管理的内容包括以下几个方面。

终端信息的初始采集、辨别、发现客户系统中存在的威胁、脆弱性，现有的控制措施能否有效防护风险的发生，如果不能，则要采取相应的控制措施，以便消除风险、降低风险、规避风险。

审核和批准是指通过审查、测试、评审等手段，检验风险评估和风险处理手段是否满足信息系统的安全要求。

决策层依据审核的结果，做出是否认可风险控制结果的决定。

在终端环境发生变化或者引入、发现新的风险时，继续循环检查、处置。在此过程中，要不断和运维人员和终端用户沟通，从业务、不同角色人员等多角度评价风险。更贴切用户的安全风险需求，共同实现用户安全目标。同时也可以了解用户安全知识和技能，以提高用户的风险意识、知识和技能，最终实现企业安全目标。

9.2　主要技术管控措施

为了降低和规避终端系统的风险，需综合运用技术和管理手段来对风险进行管控。技术管控手段分为风险发现和风险防护两大部分；基于技术支撑平台的实现，这两部分又可以分为技术支撑平台自动执行和人为参与（或完全人为）执行两部分。具体参见“6.1 几种常见分类方式”中的第四种方式阐述。

9.3　终端安全风险管控列表

终端安全风险管控手段包括技术手段和管理手段，不同管控方式对终端安全风险管控的程度不同，可将风险管控方式分为以下 3 类。

基于技术平台全过程处理类（全自动）是指终端安全风险基于技术支撑平台自动发现、自动执行防护措施，可认为全过程处理类风险是完全依赖于技术平台达到风险管控的目的。

基于技术平台对这类风险防控后，将相关执行结果信息显示给系统管理人员或终端用户，系统自行记录以备日后审计分析。

基于技术平台全过程处理类的终端安全风险管控列表见表 9-1。

表 9-1　基于技术平台全过程处理类终端安全风险列表

风险大类	风　险　类	风 险 子 类	风　险　点
基础安全风险(BR)	终端自身安全风险(BR1.1)	密码口令风险(BR1.1.1)	BR1.1.1.1　密码复杂性不符合要求
			BR1.1.1.2　密码复杂性不符合要求的，没有提示终端用户修改
			BR1.1.1.3　密码复杂性不符合要求的，审计信息没有上报管理员
			BR1.1.1.4　用户并未按照密码复杂性不符合要求的提示信息进行修改
			BR1.1.1.5　密码最小长度不符合要求
			BR1.1.1.6　密码最小长度不符合要求的，没有提示终端用户修改
			BR1.1.1.7　密码最小长度不符合要求的，审计信息没有上报管理员
			BR1.1.1.8　用户并未按照密码最小长度不符合要求提示信息进行修改
			BR1.1.1.9　密码最长存留周期不符合要求
			BR1.1.1.10　密码最长存留周期不符合要求的，没有提示终端用户修改
			BR1.1.1.11　密码最长存留周期不符合要求的，审计信息没有上报管理员
			BR1.1.1.12　用户并未按照密码最长存留周期要求提示信息进行修改
			BR1.1.1.13　终端未设置屏保、屏保密码
			BR1.1.1.14　终端未设置屏保、屏保密码的信息未提示终端用户进行修改
			BR1.1.1.15　终端未设置屏保、屏保密码的审计信息未上报管理员
			BR1.1.1.16　用户并未按照提示对终端设置屏保和屏保密码
		BIOS 弱密码风险（BR1.1.2）	BR1.1.2.2　BIOS 密码强度不符合要求的，没有提示终端用户修改
			BR1.1.2.3　BIOS 密码强度不符合要求的，审计信息没有上报管理员
			BR1.1.2.4　BIOS 密码强度不符合要求，没有产生告警信息
			BR1.1.2.6　BIOS 密码设置为空
			BR1.1.2.7　BIOS 密码设置为空没有提示终端用户
			BR1.1.2.8　BIOS 密码设置为空没有产生告警信息
			BR1.1.2.9　BIOS 密码设置为空，审计信息没有上报管理员
			BR1.1.2.10　BIOS 密码设置为空，提示终端用户修改，用户修改后自己忘记 BIOS 密码
		杀毒软件检查风险(BR1.1.3)	BR1.1.3.1　终端没有安装防病毒软件
			BR1.1.3.2　终端未安装防病毒软件，没有告警信息
			BR1.1.3.3　终端安装防病毒软件后，防病毒软件的型号、版本、病毒库信息不能发现
		终端应用软件检查风险（BR1.1.4）	BR1.1.4.2　安装了非法软件
			BR1.1.4.3　安装非法软件不告警
			BR1.1.4.4　不能禁止安装非法软件
			BR1.1.4.5　安装非法软件后不能卸载
			BR1.1.4.6　卸载正常软件
			BR1.1.4.7　卸载正常软件不告警
			BR1.1.4.8　不能禁止卸载正常软件
		终端系统补丁风险(BR1.1.5)	BR1.1.5.1　不能识别终端已经安装的补丁的补丁号、补丁描述、补丁级别、补丁类型和安装时间等信息
			BR1.1.5.2　不能识别终端尚未安装的补丁信息，具体包括补丁号、补丁描述、补丁级别、补丁类型等信息的风险

（续）

风险大类	风 险 类	风 险 子 类	风 险 点
基础安全风险(BR)	终端自身安全风险(BR1.1)	终端系统补丁风险(BR1.1.5)	BR1.1.5.3 对没有安装补丁的终端不告警
			BR1.1.5.4 不能统一安装补丁
		终端软件自动分发风险(BR1.1.6)	BR1.1.6.1 应用软件不能自动分发
			BR1.1.6.2 应用软件不自动分发没有告警信息
			BR1.1.6.3 应用软件自动分发后没有分发成功
			BR1.1.6.4 应用软件自动分发后没分发成功无告警信息
			BR1.1.6.5 不能设定软件自动分发时间
			BR1.1.6.8 不能对分发的软件分发成功数、分发成功率、安装成功数、安装成功率等信息进行统计
	终端环境安全风险(BR1.2)	终端网络运行环境风险(BR1.2.1)	BR1.2.1.1 不能监控终端异常网络流量
			BR1.2.1.2 终端出现异常网络流量不告警
			BR1.2.1.3 不能监控终端使用多网卡
			BR1.2.1.4 发现终端使用多网卡不告警
			BR1.2.1.5 不能对终端 IP/MAC 地址进行绑定
			BR1.2.1.7 终端 IP/MAC 地址绑定后，不能发现终端克隆其他 IP、MAC 地址
		终端防火墙风险(BR1.2.2)	BR1.2.2.1 终端未安装防火墙软件
			BR1.2.2.2 终端未安装防火墙软件，没有告警信息
			BR1.2.2.3 终端安装防火墙软件后，防火墙软件的型号、版本、特征库信息不能发现
			BR1.2.2.5 终端防火墙软件程序和特征库不能升级到最新状态
			BR1.2.2.6 终端防火墙程序处于未运行状态
			BR1.2.2.8 防火墙程序处于未运行状态，没有告警信息
			BR1.2.2.9 终端防火墙不能进行 IP 地址控制
			BR1.2.2.10 终端防火墙软件采用了 IP 地址控制，但控制不生效
			BR1.2.2.11 终端防火墙不能进行端口控制
			BR1.2.2.12 终端防火墙软件采用了端口控制，但控制不生效
			BR1.2.2.13 终端防火墙不能协议控制
			BR1.2.2.14 终端防火墙软件采用了协议控制，但控制不生效
	终端外设安全风险(BR1.3)	外设端口管理(BR1.3.1)	BR1.3.1.1 光驱端口没有管控
			BR1.3.1.2 软驱端口没有管控
			BR1.3.1.3 USB 端口接入普通设备没有管控
			BR1.3.1.4 USB 端口接入存储介质没有管控
			BR1.3.1.5 打印机端口没有管控
			BR1.3.1.6 调制解调器端口没有管控
			BR1.3.1.7 串口没有管控
			BR1.3.1.8 并口没有管控
			BR1.3.1.9 1394 端口没有管控
			BR1.3.1.10 红外设备端口没有管控
			BR1.3.1.11 蓝牙设备端口没有管控

（续）

风险大类	风 险 类	风 险 子 类	风 险 点
基础安全风险(BR)	终端外设安全风险(BR1.3)	外设端口管理(BR1.3.1)	BR1.3.1.12 PCMCIA 设备端口没有管控
			BR1.3.1.13 磁带机设备端口没有管控
			BR1.3.1.14 无线网卡设备端口没有管控
			BR1.3.1.15 智能卡设备端口没有管控
			BR1.3.1.16 多媒体设备端口没有管控
			BR1.3.1.17 USB 端口接入普通设备禁用，导致人机交互类设备无法使用
			BR1.3.1.18 USB 端口接入普通设备禁用，导致认证 Key 类设备无法使用
			BR1.3.1.19 USB 端口接入存储设备禁用，导致照相机、MP3 等设备无法使用
		外设设备管理(BR1.3.2)	BR1.3.2.1 U 盘/移动存储卡使用，没有提示终端用户
			BR1.3.2.2 U 盘/移动存储卡使用，审计信息没有上报管理员
			BR1.3.2.3 U 盘/移动存储卡使用，没有产生告警
			BR1.3.2.4 移动硬盘使用，没有提示终端用户
			BR1.3.2.5 移动硬盘使用，审计信息没有上报管理员
			BR1.3.2.6 移动硬盘使用，没有产生告警
			BR1.3.2.7 软盘使用，没有提示终端用户
			BR1.3.2.8 软盘使用，审计信息没有上报管理员
			BR1.3.2.9 软盘使用，没有产生告警
			BR1.3.2.10 光盘驱动器使用，没有提示终端用户
			BR1.3.2.11 光盘驱动器使用，审计信息没有上报管理员
			BR1.3.2.12 光盘驱动器使用，没有产生告警
			BR1.3.2.15 光盘刻录机使用，没有提示终端用户
			BR1.3.2.16 光盘刻录机使用，审计信息没有上报管理员
			BR1.3.2.17 光盘刻录机使用，没有产生告警
			BR1.3.2.18 光盘刻录机刻录光盘内容没有上报管理员
			BR1.3.2.20 照相机/MP3/智能手机类设备使用，没有提示终端用户
			BR1.3.2.21 照相机/MP3/智能手机类设备使用，审计信息没有上报管理员
			BR1.3.2.22 照相机/MP3/智能手机类设备使用，没有产生告警
			BR1.3.2.25 3G 手机使用，没有提示终端用户
			BR1.3.2.26 3G 手机使用，审计信息没有上报管理员
			BR1.3.2.27 3G 手机使用，没有告警
			BR1.3.2.29 蓝牙使用，没有提示终端用户
			BR1.3.2.30 蓝牙使用，审计信息没有上报管理员
			BR1.3.2.31 蓝牙使用，没有告警
			BR1.3.2.33 红外使用，没有提示终端用户
			BR1.3.2.34 红外使用，审计信息没有上报管理员
			BR1.3.2.35 红外使用，没有告警
			BR1.3.2.37 便携式 WIFI 和无线网卡使用，没有提示终端用户
			BR1.3.2.38 便携式 WIFI 和无线网卡使用，审计信息没有上报管理员

（续）

风险大类	风 险 类	风险子类	风 险 点
基础安全风险(BR)	终端外设安全风险(BR1.3)	外设设备管理(BR1.3.2)	BR1.3.2.39 便携式 WIFI 和无线网卡使用，没有告警
			BR1.3.2.41 打印机使用，审计信息没有上报管理员
			BR1.3.2.42 打印机使用，没有告警
			BR1.3.2.45 传真机使用，审计信息没有上报管理员
			BR1.3.2.46 传真机使用，没有告警
			BR1.3.2.48 未经过准入控制的终端使用打印机
			BR1.3.2.49 投影仪/电视机/电子显示屏功能使用，审计信息没有上报管理员
			BR1.3.2.50 投影仪/电视机/电子显示屏功能使用，没有告警
			BR1.3.2.51 投影仪/电视机/电子显示屏功能使用，没有提示终端用户
		终端注册表风险(BR1.3.3)	BR1.3.3.1 没有对终端注册表系统关键项访问进行监控
			BR1.3.3.2 没有对终端注册表系统关键项增加进行监控
			BR1.3.3.3 没有对终端注册表系统关键项删除进行监控
			BR1.3.3.4 没有对终端注册表用户关键项访问进行监控
			BR1.3.3.5 没有对终端注册表用户关键项增加进行监控
			BR1.3.3.6 没有对终端注册表用户关键项删除进行监控
			BR1.3.3.7 对终端下发的注册表监控策略没有根据需要及时更新
			BR1.3.3.9 对终端下发的注册表策略被停止或被删除
		终端系统驱动风险(BR1.3.4)	BR1.3.4.1 没有监控终端系统的打印机驱动程序驱动文件加载、修改、删除操作
			BR1.3.4.2 没有监控终端系统的显卡/声卡驱动程序驱动文件加载、修改、删除操作
			BR1.3.4.3 没有监控终端系统的网卡驱动程序驱动文件加载、修改、删除操作
			BR1.3.4.4 没有监控终端系统的总线驱动程序驱动文件加载、修改、删除操作
			BR1.3.4.5 没有监控终端系统的硬盘驱动器驱动程序驱动文件加载、修改、删除操作
			BR1.3.4.6 没有监控终端系统的文件系统驱动程序驱动文件加载、修改、删除操作
			BR1.3.4.7 没有监控终端系统的扫描仪、数码相机驱动程序驱动文件加载、修改、删除操作
			BR1.3.4.8 没有对终端系统的打印机驱动程序做分析，建立白名单
			BR1.3.4.9 没有对终端系统的显卡/声卡驱动程序做分析，建立白名单
			BR1.3.4.10 没有对终端系统的网卡驱动程序驱动程序做分析，建立白名单
			BR1.3.4.11 没有对终端系统的总线驱动程序做分析，建立白名单
			BR1.3.4.12 没有对终端系统的硬盘驱动程序做分析，建立白名单
			BR1.3.4.13 没有对终端系统的文件系统驱动程序做分析，建立白名单
		基本配置风险(BR1.3.5)	BR1.3.5.1 通过安全配置中心给终端下发了基本配置策略，终端修改了基本配置
			BR1.3.5.2 终端修改了基本配置，没有提示终端用户
			BR1.3.5.3 终端修改了基本配置，审计信息没有上报管理员
			BR1.3.5.4 终端修改了基本配置，没有产生告警
			BR1.3.5.5 安全配置中心给终端下发的基本配置策略没有及时更新
			RR1.1.1.3 网络通信状态，拓扑不明
			RR1.1.1.4 缺乏基本的网络运行基线

（续）

风险大类	风 险 类	风 险 子 类	风 险 点
基础安全风险(BR)	终端外设安全风险(BR1.3)	基本配置风险(BR1.3.5)	RR1.1.1.8 没有及时获取网络设备的运行情况和联网信息
		终端流量异常风险(RR1.1.2)	RR1.1.2.1 没有监控终端发送和接收数据包的数量
			RR1.1.2.2 没有监控终端并发连接数的数量
			RR1.1.2.3 不能自动识别终端的 P2P 下载行为
			RR1.1.2.6 不能下发流量和连接数白名单策略
			RR1.1.2.7 不能及时发现流量和连接数白名单策略被停止或被删除
			RR1.1.2.8 发现白名单策略丢失后不能及时恢复
			RR1.1.2.10 发现终端连接数过大但不能控制
			RR1.1.2.11 发现终端流量过大但不能控制
		终端违规网络访问风险(RR1.1.3)	RR1.1.3.1 没有终端访问的 IP 范围
			RR1.1.3.2 没有终端访问的端口范围
			RR1.1.3.3 没有终端访问的业务服务器范围
			RR1.1.3.4 没有终端访问使用的协议范围
			RR1.1.3.5 策略本身没有及时更新完善导致终端访问的 IP 范围与限定的不一致
			RR1.1.3.6 策略本身没有及时更新完善导致终端访问的端口范围与限定的不一致
			RR1.1.3.7 策略本身没有及时更新完善导致终端访问的业务服务器与限定的不一致
			RR1.1.3.8 策略本身没有及时更新完善导致终端访问使用的协议与限定的不一致
			RR1.1.3.10 管理平台不能及时发现所有的上述违规的终端网络访问行为
			RR1.1.3.11 管理平台发现了上述违规的终端网络访问行为，但是不能对所有的违规及时告警或处理
		IP/MAC 地址篡改风险(RR1.1.4)	RR1.1.4.1 没有记录所有网卡的 MAC 地址和对应的 IP 地址
			RR1.1.4.2 终端的 IP/MAC 地址绑定可以随意修改
			RR1.1.4.3 不对终端的多网卡状态进行监控
			RR1.1.4.4 不能及时发现终端的多网卡状态
			RR1.1.4.5 不能及时发现终端的 IP/MAC 地址绑定随意修改状况
			RR1.1.4.6 不能发现终端的 IP/MAC 地址绑定模块被随意停止或删除
			RR1.1.4.7 发现终端的 IP/MAC 地址绑定模块随意修改后，不能采取技术手段及时恢复 IP 地址的初始状态
			RR1.1.4.8 发现终端的 IP/MAC 地址绑定模块随意修改后不能对终端进行采取提示违规行为记录并上报管理员，警告直至人工现场处理
	终端运行安全(RR1.2)	进程/服务运行的风险(RR1.2.1)	RR1.2.1.1 黑名单进程/服务运行
			RR1.2.1.2 黑名单进程/服务运行，没有提示终端用户
			RR1.2.1.3 黑名单进程/服务运行，审计信息没有上报管理员
			RR1.2.1.4 黑名单进程/服务运行，没有产生告警
			RR1.2.1.5 黑名单进程/服务运行，没有通过策略阻止
			RR1.2.1.6 黑名单进程/服务运行，提示用户禁止进程/服务，但用户又重启该进程/服务
			RR1.2.1.11 白名单进程/服务运行不完整，没有提示终端用户
			RR1.2.1.12 白名单进程/服务运行不完整，审计信息没有上报管理员

（续）

风险大类	风 险 类	风险子类	风 险 点
基础安全风险(BR)	终端运行安全(RR1.2)	进程/服务运行的风险(RR1.2.1)	RR1.2.1.13 白名单进程/服务运行不完整，没有产生告警
			RR1.2.1.15 白名单进程/服务运行不完整，提示用户启用进程/服务，但用户又禁止该进程/服务
			RR1.2.1.18 白名单进程/服务运行，不能用已有的白名单机制来检测，导致白名单进程/服务不能检测
			RR1.2.1.20 黑名单进程/服务运行，导致内存占用率持续高
		违规软件安装风险(RR1.2.2)	RR1.2.2.1 违规软件安装
			RR1.2.2.2 违规软件安装，没有提示终端用户
			RR1.2.2.3 违规软件安装，审计信息没有上报管理员
			RR1.2.2.4 违规软件安装，没有产生告警
			RR1.2.2.5 违规软件安装，没有通过策略卸载
			RR1.2.2.6 违规软件安装，提示用户卸载软件，但用户又重新安装了该软件
			RR1.2.2.9 违规软件安装，不能用已有的违规软件检查机制来检测，导致违规软件安装不能检测
			RR1.2.2.10 必须安装软件安装不完整
			RR1.2.2.11 必须安装软件安装不完整，没有提示终端用户
			RR1.2.2.12 必须安装软件安装不完整，审计信息没有上报管理员
			RR1.2.2.13 必须安装软件安装不完整，没有产生告警
			RR1.2.2.14 必须安装软件安装不完整，没有通过策略进行软件分发
			RR1.2.2.15 必须安装软件安装不完整，提示用户安装软件，但用户不安装软件
			RR1.2.2.18 必须安装软件的检测，不能用已有的必须安装软件列表来检测，导致必须安装的软件检测无法进行
			RR1.2.2.19 对终端软件安装信息变化不记录，不产生告警
			RR1.2.2.20 对终端软件安装信息变化不记录，不审计
		异常资源占用风险(RR7)(RR1.2.3)	RR1.2.3.1 终端 CPU 使用率持续高
			RR1.2.3.2 终端 CPU 使用率持续高，没有提示终端用户
			RR1.2.3.3 终端 CPU 使用率持续高，审计信息没有上报管理员
			RR1.2.3.4 终端 CPU 使用率持续高，没有按照设定的阈值，以产生告警
			RR1.2.3.5 终端内存使用率持续高
			RR1.2.3.6 终端内存使用率持续高，没有提示终端用户
			RR1.2.3.7 终端内存使用率持续高，审计信息没有上报管理员
			RR1.2.3.8 终端内存使用率持续高，没有按照设定的阈值，以产生告警
			RR1.2.3.9 终端磁盘剩余空间不足
			RR1.2.3.10 终端磁盘剩余空间不足，没有提示终端用户
			RR1.2.3.11 终端磁盘剩余空间不足，审计信息没有上报管理员
			RR1.2.3.12 终端磁盘剩余空间不足，没有按照设定的阈值，以产生告警
			RR1.2.3.14 当终端内存使用率过高时，将内存占用率高的进程信息上报管理员，管理员禁用了该进程，但该进程不应禁止
			RR1.2.3.15 当终端磁盘剩余空间不足时，将磁盘空间不足的信息上报了管理员，管理员对磁盘空间进行了清理，删除了一些不能删除的文件

（续）

风险大类	风 险 类	风 险 子 类	风 险 点
基础安全风险(BR)	终端运行安全(RR1.2)	异常资源占用风险(RR7)(RR1.2.3)	RR1.2.3.16 当终端磁盘剩余空间不足时，将磁盘空间不足的信息上报了管理员，管理员对磁盘空间进行了清理，改变一些文件的存放路径
		操作系统用户管理风险(RR1.2.4)	RR1.2.4.1 操作系统受限用户权限被变更为管理员用户
			RR1.2.4.2 操作系统受限用户权限被变更为管理员用户，审计信息不上报管理员
			RR1.2.4.3 操作系统受限用户权限被变更为管理员用户，不提示终端用户
			RR1.2.4.4 操作系统受限用户权限被变更为管理员用户，不产生告警
			RR1.2.4.5 操作系统受限用户权限被变更为管理员用户，用户使用变更后的权限登录终端，对终端进行操作
			RR1.2.4.6 操作系统管理员用户权限变更为受限用户
			RR1.2.4.7 操作系统管理员用户权限变更为受限用户，审计信息不上报
			RR1.2.4.8 操作系统管理员用户权限变更为受限用户，不提示终端用户
			RR1.2.4.9 操作系统管理员用户权限变更为受限用户，不产生告警
			RR1.2.4.10 操作系统管理员用户权限变更为受限用户，用户使用变更后的权限登录终端，对终端进行操作
			RR1.2.4.11 增加/删除系统管理员权限的操作系统用户
			RR1.2.4.12 增加/删除系统管理员权限的操作系统用户，审计信息不上报
			RR1.2.4.13 增加/删除受限用户权限的操作系统用户
			RR1.2.4.14 增加/删除受限用户权限的操作系统用户，审计信息不上报
			RR1.2.4.15 操作系统用户组权限修改
			RR1.2.4.16 操作系统用户组权限修改，不通知终端用户
			RR1.2.4.17 操作系统用户组权限更改，审计信息不上报管理员
			RR1.2.4.18 增加/删除操作系统用户组
			RR1.2.4.19 增加/删除操作系统用户组，审计信息不上报
		终端节能风险(RR1.2.5)	RR1.2.5.1 终端短时间不需要人机交互时，没有按规定设定待机
			RR1.2.5.2 终端较长时间不需要人机交互时，没有按规定设定休眠
			RR1.2.5.3 终端没有按照节能策略，在短时间不需要人机交互时，设定关闭显示器
			RR1.2.5.4 终端没有按照节能策略，在短时间不需要人机交互时，设定关闭硬盘
	网络边界风险(RR1.3)	违规内联(RR1.3.1)	RR1.3.1.1 终端资产没有在资产管理系统登记的违规内联
			RR1.3.1.2 终端资产与资产管理系统登记信息不符的违规内联
			RR1.3.1.6 终端病毒检查不合规的违规内联
			RR1.3.1.7 终端操作系统补丁检查不合规的违规内联
			RR1.3.1.8 终端应用软件检查不合规的违规内联
			RR1.3.1.9 终端木马检查不合规的违规内联
			RR1.3.1.10 终端外设控制检查不合规的违规内联
			RR1.3.1.13 不合规的违规内联终端，不被强制定位到隔离区
			RR1.3.1.14 隔离区的终端，不进行有效验证就被允许入网
			RR1.3.1.15 隔离区内的终端，用户未按流程进行合规化处理
			RR1.3.1.17 非内网终端连入内网，无流程化处理
			RR1.3.1.18 非内网终端连入内网，无应急处理

（续）

风险大类	风 险 类	风险子类	风 险 点
基础安全风险(BR)	网络边界风险(RR1.3)	违规内联(RR1.3.1)	RR1.3.1.19 非内网终端接入内网，无授权审批。
			RR1.3.1.20 非内网终端接入内网后，用户未按流程进行身份登记
			RR1.3.1.21 非内网终端授权接入内网，不进行安全检测
			RR1.3.1.22 非内网终端授权接入内网，不对其上传下载数据行为进行审计和记录
			RR1.3.1.23 授权接入内网的终端，使用未经系统管理员分配的 IP 或 IP 段
			RR1.3.1.24 对非授权使用 IP 的终端不进行提示
			RR1.3.1.25 对非授权使用 IP 的终端未进行审计上报
			RR1.3.1.26 非授权使用 IP 的终端，用户未按提示修改 IP
			RR1.3.1.28 对非授权开启服务器端服务的终端不进行提示
			RR1.3.1.29 对非授权开启服务器端服务的终端未进行审计上报
			RR1.3.1.30 非授权开启服务器端服务的终端，用户未按提示关闭服务
		违规外联(RR1.3.2)	RR1.3.2.1 终端在内网环境下的违规外联不能进行检测
			RR1.3.2.2 终端在内网环境下的违规外联不能进行阻断
			RR1.3.2.3 终端在内网环境下的违规外联进行阻断误报导致的正常使用终端断网
			RR1.3.2.4 不能检测终端在离网后的违规外联行为
			RR1.3.2.5 不能对终端离网后的违规外联行为进行审计记录和告警
			RR1.3.2.6 终端离网状态下不能进行阻断，产生信息外泄
		漫游管理(RR1.3.3)	RR1.3.3.1 终端在行业内部不同单位之间漫游时，目的地服务器不能发现，并自动接管漫游终端
			RR1.3.3.2 目的地服务器不能预定义漫游组，并自动将漫游终端归入漫游组中
			RR1.3.3.3 目的地服务器不能针对漫游组预定义各种安全策略
			RR1.3.3.4 源服务器对终端漫游数据下发错误导致漫游终端无法在目的地入网
			RR1.3.3.5 漫游目的地服务器下发的漫游组安全策略弱于漫游终端在源网络中的安全策略
			RR1.3.3.7 终端所属源服务器不能获取到终端漫游状态信息
			RR1.3.3.8 终端漫游时，不能自动将各种审计报警日志上报至目的地服务器
			RR1.3.3.9 回到注册源服务器后，不能及时上报终端的漫游期间的违规行为
信息安全风险(IR)	信息扩散风险(IR1.1)	信息传输的风险(IR1.1.1)	IR1.1.1.1 不能对发送邮件行为进行控制
			IR1.1.1.2 不能对发送邮件行为进行审计
			IR1.1.1.3 邮件发送行为的控制导致某些内容不违规邮件无法发送
			IR1.1.1.4 不能对打印管理
			IR1.1.1.6 不审计终端的打印行为（包括终端属性、打印时间、打印文件、份数、打印机等）
			IR1.1.1.7 终端通过传输文件带来的安全风险
			IR1.1.1.8 终端（包括移动存储设备）上存在国家秘密级或以上密级的文件的安全风险
		移动存储介质违规使用的风险(IR1.1.2)	IR1.1.2.1 移动存储介质没有进行资产登记管理对移动存储介质缺乏管理
			IR1.1.2.2 U 盘没有进行单独注册和授权
			IR1.1.2.3 移动存储介质没有进行安全等级划分
			IR1.1.2.4 光盘介质使用没有进行禁止、限制范围的管理

（续）

风险大类	风 险 类	风 险 子 类	风 险 点
信息安全风险(IR)	信息扩散风险(IR1.1)	移动存储介质违规使用的风险(IR1.1.2)	IR1.1.2.5 移动存储介质格式化，授权信息被更改
			IR1.1.2.6 移动存储介质被重新分区，授权信息被更改
			IR1.1.2.7 移动存储介质授权信息被更改，没有报警提示和禁止
			IR1.1.2.8 外部移动存储，传输外部信息进内网的风险
			IR1.1.2.9 外部信息使用内部移动介质，没有进行安全检查
			IR1.1.2.10 采用控制措施后，外部移动介质使用，没有报警、提示和禁止
			IR1.1.2.11 新增内网使用的移动存储介质，管理流程，无法确定其生命周期中的使用情况
			IR1.1.2.12 新增申请流程不明确，造成移动介质滥用的潜在风险
			IR1.1.2.13 新增设备，授权过程不明确，造成新设备无法识别
			IR1.1.2.14 缺少记录移动存储介质的申请-审批-授权的全过程（包括授权人，授权使用范围，被授权人以及授权清除等记录）
			IR1.1.2.15 有关移动存储介质申请-审批-授权审计信息，缺少安全措施，造成篡改和擦除
		(IR1.1.3)	IR1.1.3.4 重要文件的读、写、修改、传输等过程中出现信息泄漏的风险
			IR1.1.3.5 外来的重要文件进入内网，使其满足本地使用要求，过程中导致信息泄漏的风险
		信息共享(IR1.1.4)	IR1.1.4.1 没有监控终端随意设置共享文件的情况
			IR1.1.4.2 没有对终端共享情况进行审计
			IR1.1.4.3 不能及时关闭共享
		(IR1.1.5)	IR1.1.5.3 重要应用系统截屏，造成信息泄漏

基于技术平台由人工协助处理类是指终端安全风险的发现和管控是基于技术平台，在人工协助下进行的。这种方式包括半自动和半人工两类。

1）自动发现，人工协助处理：指终端安全风险是自动发现，由平台执行防护措施，但是否执行防护措施，或执行哪个防护措施由相关系统管理员依据实际情况确定。基于技术平台发现这类风险后提示系统管理人员或终端用户发现风险，并给出备选防护措施，以供选择。基于操作人员的选择，将相关执行结果信息显示给系统管理人员或终端用户，系统自行记录以备日后审计分析，具体见表 9-2。

表 9-2 基于技术平台由人工协助处理的安全风险列表_1（自动发现，人工协助处理）

风险大类	风险类	风 险 子 类	风 险 点
基础安全风险(BR)	终端自身安全风险（BR1.1）	BIOS 弱密码风险(BR1.1.2)	BR1.1.2.1 BIOS 密码强度设置不符合要求
			BR1.1.2.5 BIOS 密码强度不符合要求，提示用户修改，用户修改后自己忘记 BIOS 密码
		杀毒软件检查风险(BR1.1.3)	BR1.1.3.5 终端防病毒软件程序和病毒库不能升级到最新状态
			BR1.1.3.6 终端防病毒程序处于未运行状态
			BR1.1.3.7 终端防病毒程序处于未运行状态后不能启动防病毒程序
			BR1.1.3.8 防病毒程序处于未运行状态，没有告警信息
		终端系统补丁风险(BR1.1.5)	BR1.1.5.5 不能对终端补丁安装前进行验证
		终端软件自动分发风险(BR1.1.6)	BR1.1.6.6 分发的应用软件不能自动安装
			BR1.1.6.7 分发的应用软件不能自动安装没有告警信息

（续）

风险大类	风险类	风险子类	风险点
基础安全风险(BR)	终端环境安全风险（BR1.2）	终端网络运行环境风险(BR1.2.1)	BR1.2.1.6 终端使用多网卡后，不能控制哪块网卡的禁用或者启用
	终端外设安全风险(BR1.3)	外设设备管理(BR1.3.2)	BR1.3.2.19 光盘刻录机使用禁止，导致光盘只读应用受到影响
		终端注册表风险(BR1.3.3)	BR1.3.3.8 对终端下发的注册表监控策略与某些终端的注册表内容冲突
		终端系统驱动风险(BR1.3.4)	BR1.3.4.15 下发策略与某些终端冲突
			BR1.3.4.16 下发策略被停止或被删除
		基本配置风险(BR1.3.5)	BR1.3.5.6 从终端上获取的基本配置信息不完整，无法配置基线比较
终端安全运行风险(RR)	网络运行安全(RR1.1)	网络设备运行风险(RR1.1.1)	RR1.1.1.9 不能自动发现终端设备之间、终端设备与关键业务资产的连接关系
			RR1.1.1.10 没有根据发现的连接关系自动绘制并更新拓扑图
			RR1.1.1.11 管理平台不能远程监控管理全部网络设备和终端
		终端流量异常风险(RR1.1.2)	RR1.1.2.4 没有事先对实际的网络流量按照 IP、时间、端口分别统计得出流量白名单
			RR1.1.2.5 没有事先对实际的网络流量按照 IP、时间、端口分别统计得出连接白名单
			RR1.1.2.12 发现终端的 P2P 下载行为但是不能控制
		终端违规网络访问风险(RR1.1.3)	RR1.1.3.9 策略失效禁用或被卸载
	终端运行安全(RR1.2)	进程/服务运行的风险(RR1.2.1)	RR1.2.1.10 白名单进程/服务运行不完整
			RR1.2.1.14 白名单进程/服务运行不完整，没有通过策略启用进程/服务
			RR1.2.1.16 白名单机制不完整
			RR1.2.1.17 白名单机制不完整，相应的策略内容不完整
			RR1.2.1.19 黑名单进程/服务运行，导致 CPU 占用率持续高
		违规软件安装风险(RR1.2.2)	RR1.2.2.7 违规软件列表不完整
			RR1.2.2.8 违规软件列表不完整，相应的策略内容不完整
			RR1.2.2.16 必须安装软件列表不完整
			RR1.2.2.17 必须安装软件列表不完整，相应的策略内容不完整
		异常资源占用风险(RR1.2.3)	RR1.2.3.13 当终端 CPU 使用率持续过高时，将 CPU 占用率高的进程信息上报管理员，管理员禁止了该进程，但该进程不应禁止
			RR1.2.3.17 对终端的 CPU 使用率进行了监控，但由于终端操作系统的问题，获取的 CPU 使用率信息不准确
			RR1.2.3.18 对终端的内存用率进行了监控，但由于终端操作系统的问题，获取的内存使用率信息不准确
			RR1.2.3.19 对终端的磁盘空间进行了监控，但由于操作系统的问题，获取的磁盘剩余空间信息不准确
		操作系统用户管理风险(RR1.2.4)	RR1.2.4.20 对操作系统用户和用户组信息进行检测，由于操作系统的问题，获取的用户信息不准确，无法进行相应的用户控制
	网络边界风险(RR1.3)	违规内联(RR1.3.1)	RR1.3.1.3 登录终端用户没有合法登记的违规内联
			RR1.3.1.11 产生违规内联后，不能识别终端身份信息
			RR1.3.1.27 授权终端，开启未经系统管理员允许的服务端服务（DHCP、代理）
		违规外联(RR1.3.2)	RR1.3.2.7 发生违规外联事件时，不能发现并准确定位违规外联的途径

（续）

风险大类	风险类	风险子类	风险点
终端安全运行风险(RR)	网络边界风险(RR1.3)	违规外联(RR1.3.2)	RR1.3.2.8 发现违规外联的状态时，无法界定内外网互联和离线上网的不同情况
			RR1.3.2.9 不能对终端违规接入其他网络（非互联网）进行检测
			RR1.3.2.10 不能对终端违规接入其他网络（非互联网）进行阻断
			RR1.3.2.11 不能对终端违规接入其他网络（非互联网）进行审计记录和告警
			RR1.3.2.12 不能对违规外联的行为准确取证
		漫游管理(RR1.3.3)	RR1.3.3.6 在所有服务器均启用 802.1X 认证的情况下，终端在漫游状态时，不能静默通过 802.1X 认证和接入网络
信息安全风险(IR)	信息扩散风险(IR1.1)	信息传输的风险(IR1.1.1)	IR1.1.1.5 不限定终端只能在指定的打印机上打印文件
			IR1.1.1.9 存在国家秘密文件的终端未按提示删除相应涉密文件
		信息文档保护(IR1.1.3)	IR1.1.3.1 重要文档没有加密存储
			IR1.1.3.3 存储重要文件的终端安全防护措施不达标，造成文件泄密

2）人工发现，平台协助处理：指终端安全管理人员基于技术支撑平台所提供的监控信息分析发现终端安全风险，并依赖或部分依赖技术平台来执行防护措施，具体见表 9-3。

表 9-3 基于技术平台由人工协助处理的安全风险列表_2（人工发现，平台协助处理）

风险大类	风险类	风险子类	风险点
基础安全风险(BR)	终端自身安全风险（BR1.1）	终端应用软件检查风险(BR1.1.4)	BR1.1.4.1 不能统计终端安装应用软件的情况统计
	终端环境安全风险（BR1.2）	终端防火墙风险(BR1.2.2)	BR1.2.2.7 终端防火墙程序处于未运行状态后不能启动防火墙程序
	终端外设安全风险(BR1.3)	外设设备管理(BR1.3.2)	BR1.3.2.14 光盘驱动器使用禁止，导致虚拟光驱无法使用
			BR1.3.2.23 照相机/MP3/智能手机类设备禁用，导致无线鼠标受到影响
			BR1.3.2.24 照相机/MP3/智能手机类设备禁用，导致 USB 电源类设备无法提供电源
			BR1.3.2.28 3G 手机禁用，导致手机充电功能受到影响
			BR1.3.2.47 传真功能禁用，导致网络业务受到影响
终端安全运行风险(RR)	网络运行安全(RR1.1)	网络设备运行风险(RR1.1.1)	RR1.1.1.6 没有对在用网络设备的规定使用周期进行追溯
			RR1.1.1.7 没有对网络运行环境，网络运行拓扑等基础信息做详细的调查了解，或者没有及时更新
			RR1.1.1.12 管理平台事件记录不全，导致某些事件后续无法追溯
	终端运行安全(RR1.2)	进程/服务运行的风险(RR1.2.1)	RR1.2.1.7 黑名单机制不完整
			RR1.2.1.8 黑名单机制不完整，相应的策略内容不完整
			RR1.2.1.9 黑名单进程/服务运行，不能用已有的黑名单机制来检测，导致黑名单进程/服务不能检测
	网络边界风险(RR1.3)	违规内联(RR1.3.1)	RR1.3.1.4 终端身份标识符被篡改、冒用的风险
			RR1.3.1.5 终端身份标识符被冒用，在应用控制措施之后，可能导致原来的合法终端的身份标识因无法识别而无法使用网络

全人工处理是指完全依赖终端安全管理人员发现和处理，具体见表 9-4。

表 9-4　全人工处理类终端安全风险列表

风险大类	风险类	风 险 子 类	风　险　点
基础安全风险(BR)	终端自身安全风险（BR1.1）	密码口令风险(BR1.1.1)	BR1.1.1.17　因工作或维修需要，终端用户将密码告知他人
			BR1.1.1.18　因工作或维修需要，终端用户将密码告知他人。在相关工作完成后未及时修改密码
		BIOS 弱密码风险(BR1.1.2)	BR1.1.2.11　采取技术措施获取终端的 BIOS 强度情况，但不同厂商主板不尽相同，获取的 BIOS 强度情况不精确
		杀毒软件检查风险(BR1.1.3)	BR1.1.3.4　终端安装防病毒软件后，和系统冲突
			BR1.1.3.9　管理员不能远程调用其杀毒软件对发现的病毒进行杀毒
			BR1.1.3.10　终端杀毒软件不能查杀病毒
		终端系统补丁风险(BR1.1.5)	BR1.1.5.6　安装补丁后引发系统崩溃不能进行补丁回退
	终端环境安全风险（BR1.2）	终端防火墙风险(BR1.2.2)	BR1.2.2.4　终端安装防火墙软件后，和系统冲突
	终端外设安全风险(BR1.3)	外设设备管理(BR1.3.2)	BR1.3.2.13　光盘驱动器使用禁止，导致 U 盘移动存储介质无法使用
			BR1.3.2.32　蓝牙网络禁用，导致办公辅助设备无法使用
			BR1.3.2.36　红外连接禁用，导致办公辅助设备无法使用
			BR1.3.2.40　便携式 WIFI 和无线网卡禁用，导致网络无法连接
			BR1.3.2.43　打印机禁用，导致文档镜像输出受到影响
			BR1.3.2.44　复印机随意使用
			BR1.3.2.52　投影仪/电视机/电子显示屏功能禁用，导致显示器识别异常
			BR1.3.2.53　投影仪/电视机/电子显示屏功能禁用，导致工作应用受到影响
终端安全运行风险(RR)	网络运行安全(RR1.1)	网络设备运行风险(RR1.1.1)	RR1.1.1.1　温度、湿度等环境因素导致网络设备运行风险
			RR1.1.1.2　设备老化导致网络设备运行风险
			RR1.1.1.5　不能及时获取温度、湿度等环境因素
		终端流量异常风险(RR1.1.2)	RR1.1.2.9　下发策略与某些业务冲突
		IP/MAC 地址篡改风险(RR1.1.4)	RR1.1.4.9　终端的 IP/MAC 地址绑定模块加载后与某些程序和应用冲突
信息安全风险(IR)	信息扩散风险(IR1.1)	信息的非技术泄漏(IR1.1.5)	IR1.1.5.1　不能禁止用户携带照相设备
			IR1.1.5.2　不能禁止用户对终端显示信息进行记录
			IR1.1.5.4　屏幕电磁泄漏，造成信息泄漏
			IR1.1.5.5　采用信号干扰措施，造成正常的无线通信故障
			IR1.1.5.6　物理线路上的电磁窃听，造成信息泄漏
			IR1.1.5.7　采用视频监控，仍存在死角，不可避免非技术类的信息泄密
		人为灾害(IR1.1.6)	IR1.1.6.1　关机状态下，拆除硬盘
			IR1.1.6.2　人为造成的设备损坏，如淋水、明火、磕碰等
			IR1.1.6.3　人为造成设备盗窃、丢失

第 10 章　终端安全风险日常运维管理

10.1　重要风险监控

安全风险根据其对业务系统、商业利益、公司声誉与社会影响、法律法规符合度等造成的影响和损失，一般分为高、中、低三个级别。信息安全风险管理的主要目的是及时发现安全风险，评估安全风险，响应安全风险，以期降低或规避风险，并基于风险管理工作实践改进安全防护系统。

信息安全风险管理过程中根据不同的安全风险事件的等级采用不同的方式进行告警，对事件处理和事件沟通的过程和规程作详细说明。由于目前无论是 IDS，还是其他安全监测设备，都存在误报现象，终端安全相关的防护和管理系统也不例外，对于纷繁复杂的安全告警，管理人员不可能对每一条安全风险和事件都要关注，只有关注高级别的安全风险。这样才能在有限的资源下最大可能地保障被保护对象的安全。

因此，终端安全管理人员要依托相关的技术手段和支撑平台对终端系统的异常现象进行检测，该技术平台一旦检测到高级风险事件，要做到实时告警提示使用和管理人员，要有邮件、短信等及时有效的方式及时通知到安全管理员，并能实时展现本地范围和管辖范围的高级别的安全风险及事件，并以弹出窗口的方式显示详细信息内容和解决建议。管理员可以通过评估检查确认该风险的真实性。如果确实属于确定的安全事件，启动应急预案，对该风险做出响应，并对处理结果跟踪，事后根据处理结果和分析形成知识经验方案，添加经验库，以支持后续工作。

日常运维中需要关注的重要风险主要包括信息安全类风险、引起大面积终端无法正常使用的风险。

具体参见表 10-1。

表 10-1　重要风险列表

风险大类	风险类	风险子类	风险点
基础安全风险（BR）	终端自身安全风险(BR1.1)	密码口令风险(BR1.1.1)	BR1.1.1.1　密码复杂性不符合要求
			BR1.1.1.2　密码复杂性不符合要求的，没有提示终端用户修改
			BR1.1.1.3　密码复杂性不符合要求的，审计信息没有上报管理员
			BR1.1.1.4　用户并未按照密码复杂性不符合要求的提示信息进行修改
			BR1.1.1.5　密码最小长度不符合要求
			BR1.1.1.6　密码最小长度不符合要求的，没有提示终端用户修改
			BR1.1.1.7　密码最小长度不符合要求的，审计信息没有上报管理员
			BR1.1.1.8　用户并未按照密码最小长度不符合要求提示信息进行修改

（续）

风险大类	风险类	风险子类	风险点
基础安全风险（BR）	终端自身安全风险(BR1.1)	密码口令风险(BR1.1.1)	BR1.1.1.9 密码最长存留周期不符合要求
			BR1.1.1.10 密码最长存留周期不符合要求的，没有提示终端用户修改
			BR1.1.1.11 密码最长存留周期不符合要求的，审计信息没有上报管理员
			BR1.1.1.12 用户并未按照密码最长存留周期要求提示信息进行修改
			BR1.1.1.13 终端未设置屏保、屏保密码
			BR1.1.1.14 终端未设置屏保、屏保密码的信息未提示终端用户进行修改
			BR1.1.1.15 终端未设置屏保、屏保密码的审计信息未上报管理员
			BR1.1.1.16 用户并未按照提示对终端设置屏保和屏保密码
			BR1.1.1.17 因工作或维修需要，终端用户将密码告知他人
			BR1.1.1.18 因工作或维修需要，终端用户将密码告知他人。在相关工作完成后未及时修改密码
		BIOS弱密码风险(BR1.1.2)	BR1.1.2.1 BIOS 密码强度设置不符合要求
			BR1.1.2.2 BIOS 密码强度不符合要求的，没有提示终端用户修改
			BR1.1.2.3 BIOS 密码强度不符合要求的，审计信息没有上报管理员
			BR1.1.2.4 BIOS 密码强度不符合要求，没有产生告警信息
			BR1.1.2.5 BIOS 密码强度不符合要求，提示用户修改，用户修改后自己忘记 BIOS 密码
			BR1.1.2.6 BIOS 密码设置为空
			BR1.1.2.7 BIOS 密码设置为空没有提示终端用户
			BR1.1.2.8 BIOS 密码设置为空没有产生告警信息
			BR1.1.2.9 BIOS 密码设置为空，审计信息没有上报管理员
			BR1.1.2.10 BIOS 密码设置为空，提示终端用户修改，用户修改后自己忘记 BIOS 密码
			BR1.1.2.11 采取技术措施获取终端的 BIOS 强度情况，但不同厂商主板不尽相同，获取的 BIOS 强度情况不精确
		(BR1.1.3)	BR1.1.3.10 终端杀毒软件不能查杀病毒
		(BR1.1.6)	BR1.1.6.8 不能对分发的软件分发成功数、分发成功率、安装成功数、安装成功率等信息进行统计
		(BR1.2.1)	BR1.2.1.7 终端 IP/MAC 地址绑定后，不能发现终端克隆其他 IP、MAC 地址
		(BR1.2.2)	BR1.2.2.4 终端安装防火墙软件后，和系统冲突
		外设设备管理(BR1.3.2)	BR1.3.2.1 U 盘/移动存储卡使用，没有提示终端用户
			BR1.3.2.2 U 盘/移动存储卡使用，审计信息没有上报管理员
			BR1.3.2.3 U 盘/移动存储卡使用，没有产生告警
			BR1.3.2.4 移动硬盘使用，没有提示终端用户
			BR1.3.2.5 移动硬盘使用，审计信息没有上报管理员
			BR1.3.2.6 移动硬盘使用，没有产生告警
			BR1.3.2.7 软盘使用，没有提示终端用户
			BR1.3.2.8 软盘使用，审计信息没有上报管理员
			BR1.3.2.9 软盘使用，没有产生告警
			BR1.3.2.10 光盘驱动器使用，没有提示终端用户
			BR1.3.2.11 光盘驱动器使用，审计信息没有上报管理员

（续）

风险大类	风险类	风险子类	风险点
基础安全风险（BR）	终端自身安全风险(BR1.1)	外设设备管理(BR1.3.2)	BR1.3.2.12 光盘驱动器使用，没有产生告警
			BR1.3.2.15 光盘刻录机使用，没有提示终端用户
			BR1.3.2.16 光盘刻录机使用，审计信息没有上报管理员
			BR1.3.2.17 光盘刻录机使用，没有产生告警
			BR1.3.2.18 光盘刻录机刻录光盘内容没有上报管理员
			BR1.3.2.19 光盘刻录机使用禁止，导致光盘只读应用受到影响
			BR1.3.2.20 照相机/MP3/智能手机类设备使用，没有提示终端用户
			BR1.3.2.21 照相机/MP3/智能手机类设备使用，审计信息没有上报管理员
			BR1.3.2.22 照相机/MP3/智能手机类设备使用，没有产生告警
			BR1.3.2.25 3G 手机使用，没有提示终端用户
			BR1.3.2.26 3G 手机使用，审计信息没有上报管理员
			BR1.3.2.27 3G 手机使用，没有告警
			BR1.3.2.29 蓝牙使用，没有提示终端用户
			BR1.3.2.30 蓝牙使用，审计信息没有上报管理员
			BR1.3.2.31 蓝牙使用，没有告警
			BR1.3.2.33 红外使用，没有提示终端用户
			BR1.3.2.34 红外使用，审计信息没有上报管理员
			BR1.3.2.35 红外使用，没有告警
			BR1.3.2.37 便携式 WIFI 和无线网卡使用，没有提示终端用户
			BR1.3.2.38 便携式 WIFI 和无线网卡使用，审计信息没有上报管理员
			BR1.3.2.39 便携式 WIFI 和无线网卡使用，没有告警
			BR1.3.2.41 打印机使用，审计信息没有上报管理员
			BR1.3.2.42 打印机使用，没有告警
			BR1.3.2.44 复印机随意使用
			BR1.3.2.45 传真机使用，审计信息没有上报管理员
			BR1.3.2.46 传真机使用，没有告警
			BR1.3.2.48 未经过准入控制的终端使用打印机
			BR1.3.2.49 投影仪/电视机/电子显示屏功能使用，审计信息没有上报管理员
			BR1.3.2.50 投影仪/电视机/电子显示屏功能使用，没有告警
			BR1.3.2.51 投影仪/电视机/电子显示屏功能使用，没有提示终端用户
		(BR1.3.3)	BR1.3.3.8 对终端下发的注册表监控策略与某些终端的注册表内容冲突
		(BR1.3.4)	BR1.3.4.15 下发策略与某些终端冲突
			BR1.3.4.16 下发策略被停止或被删除
		基本配置风险(BR1.3.5)	BR1.3.5.1 通过安全配置中心给终端下发了基本配置策略，终端修改了基本配置
			BR1.3.5.2 终端修改了基本配置，没有提示终端用户
			BR1.3.5.3 终端修改了基本配置，审计信息没有上报管理员
			BR1.3.5.4 终端修改了基本配置，没有产生告警
			BR1.3.5.5 安全配置中心给终端下发的基本配置策略没有及时更新
			BR1.3.5.6 从终端上获取的基本配置信息不完整，无法配置基线比较

（续）

风险大类	风险类	风险子类	风险点
终端安全运行风险(RR)	网络运行安全(RR1.1)	网络设备运行风险(RR1.1.1)	RR1.1.1.1 温度、湿度等环境因素导致网络设备运行风险
			RR1.1.1.2 设备老化导致网络设备运行风险
			RR1.1.1.5 不能及时获取温度、湿度等环境因素
		(RR1.1.2)	RR1.1.2.9 下发策略与某些业务冲突
		(RR1.1.3)	RR1.1.3.10 管理平台不能及时发现所有的上述违规的终端网络访问行为
			RR1.1.3.11 管理平台发现了上述违规的终端网络访问行为，但是不能对所有的违规及时告警或处理
		IP/MAC 地址篡改风险(RR1.1.4)	RR1.1.4.1 没有记录所有网卡的 MAC 地址和对应的 IP 地址
			RR1.1.4.9 终端的 IP/MAC 地址绑定模块加载后与某些程序和应用冲突
	终端运行安全(RR1.2)	进程/服务运行的风险(RR1.2.1)	RR1.2.1.1 黑名单进程/服务运行
		(RR1.2.2)	RR1.2.2.18 必须安装软件的检测，不能用已有的必须安装软件列表来检测，导致必须安装的软件检测无法进行
	(RR1.3)	(RR1.3.2)	RR1.3.2.6 终端离网状态下不能进行阻断，产生信息外泄
信息安全风险(IR)	信息扩散风险(IR1.1)	信息传输的风险(IR1.1.1)	IR1.1.1.1 不能对发送邮件行为进行控制
			IR1.1.1.2 不能对发送邮件行为进行审计
			IR1.1.1.3 邮件发送行为的控制导致某些内容不违规邮件无法发送
			IR1.1.1.4 不能对打印管理
			IR1.1.1.5 不限定终端只能在指定的打印机上打印文件
			IR1.1.1.6 不审计终端的打印行为（包括终端属性、打印时间、打印文件、份数、打印机等）
			IR1.1.1.7 终端通过传输文件带来的安全风险
			IR1.1.1.8 终端（包括移动存储设备）上存在国家秘密级或以上密级的文件的安全风险
			IR1.1.1.9 存在国家秘密文件的终端未按提示删除相应涉密文件
		移动存储介质违规使用的风险(IR1.1.2)	IR1.1.2.1 移动存储介质没有进行资产登记管理对移动存储介质缺乏管理
			IR1.1.2.2 U 盘没有进行单独注册和授权
			IR1.1.2.3 移动存储介质没有进行安全等级划分
			IR1.1.2.4 光盘介质使用没有进行禁止、限制范围的管理
			IR1.1.2.5 移动存储介质格式化，授权信息被更改
			IR1.1.2.6 移动存储介质被重新分区，授权信息被更改
			IR1.1.2.7 移动存储介质授权信息被更改，没有报警提示和禁止
			IR1.1.2.8 外部移动存储，传输外部信息进内网的风险
			IR1.1.2.9 外部信息使用内部移动介质，没有进行安全检查
			IR1.1.2.10 采用控制措施后，外部移动介质使用，没有报警、提示和禁止
			IR1.1.2.11 新增内网使用的移动存储介质，管理流程，无法确定其生命周期中的使用情况
			IR1.1.2.12 新增申请流程不明确，造成移动介质滥用的潜在风险
			IR1.1.2.13 新增设备，授权过程不明确，造成新设备无法识别
			IR1.1.2.14 缺少记录移动存储介质的申请-审批-授权的全过程（包括授权人，授权使用范围，被授权人以及授权清除等记录）
			IR1.1.2.15 有关移动存储介质申请-审批-授权审计信息，缺少安全措施，造成篡改和擦除

（续）

风险大类	风险类	风险子类	风险点
信息安全风险(IR)	信息扩散风险(IR1.1)	信息文档保护(IR1.1.3)	IR1.1.3.1 重要文档没有加密存储
			IR1.1.3.3 存储重要文件的终端安全防护措施不达标，造成文件泄密
			IR1.1.3.4 重要文件的读、写、修改、传输等过程中出现信息泄漏的风险
			IR1.1.3.5 外来的重要文件进入内网，使其满足本地使用要求，过程中导致信息泄漏的风险
		信息共享(IR1.1.4)	IR1.1.4.1 没有监控终端随意设置共享文件的情况
			IR1.1.4.2 没有对终端共享情况进行审计
			IR1.1.4.3 不能及时关闭共享
		信息的非技术泄漏(IR1.1.5)	IR1.1.5.1 不能禁止用户携带照相设备
			IR1.1.5.2 不能禁止用户对终端显示信息进行记录
			IR1.1.5.3 重要应用系统截屏，造成信息泄漏
			IR1.1.5.4 屏幕电磁泄漏，造成信息泄漏
			IR1.1.5.5 采用信号干扰措施，造成正常的无线通信故障
			IR1.1.5.6 物理线路上的电磁窃听，造成信息泄漏
			IR1.1.5.7 采用视频监控，仍存在死角，不可避免非技术类的信息泄密
		人为灾害(IR1.1.6)	IR1.1.6.1 关机状态下，拆除硬盘
			IR1.1.6.2 人为造成的设备损坏，如淋水、明火、磕碰等
			IR1.1.6.3 人为造成设备盗窃、丢失

10.2 运维全过程管理

为了实现终端安全从零散管理到整体保障的转变，一定要解决管理信息化问题，依托终端安全防护和管理技术平台，支撑终端安全管理运维流程和管理制度的执行，实现运维工作全过程的管理。

根据信息安全管理体系要求，建立《终端安全管理日常运维管理办法》，基于该办法设计《终端安全日常运维流程》，并在技术平台中为其提供支撑，实现人、操作、技术的有效结合，见表 10-2。

表 10-2 终端安全管理日常运维管理办法列表

工作类别	规范类别	规范内容概要	技术平台支撑
日常工作管理	日常工作规范	必须保持手机 7×24 小时开机，预留紧急联系方式	○
		禁止在上班时间从事与工作无关的其他事情	○
		禁止在终端安全监控终端上安装、下载与工作无关的各种软件	•
		随时检查工作相关信箱	◎
		及时更新相关人员的接口通信簿	◎
		禁止私自拆装、更换运营中心内机器配件，机房内电脑主机均应有易破损标签保护	○

（续）

工作类别	规范类别	规范内容概要	技术平台支撑
日常工作管理	日常工作规范	对于参观视察人员，由值班人员填写《监控机房出入记录单》等	○
		机房出现失火、停电或其他意外情况，及时按重大故障处理流程进行处理，并迅速与相关部门及人员通报、联系	○
	考勤管理	终端安全运维人员上班下班时必须签到，如无故不签到或找人代签到，则均视为迟到并按行政管理制度进行处理	●
		工作期间禁止因私外出，如发现均视为早退并按行政管理制度进行处理	○
		如需请假，需至少提前一天申请，并告知相关人员进行记录，如因临时事件请假，则需在9点前电话或短信请假	○
值班工作管理	交接班管理	终端安全管理人员应按规定时间上下班，未经批准不得调换班次和离开岗位，接班人员未到交班人员不得离岗	○
		值班时，不得做与工作无关的事	○
		值班期间须在系统中详细准确地记录值班工作情况	•
		交班人员应提前作好交班准备，填好交接班记录	◎
		交接班应做到手续清楚，责任明确，上下衔接。值班期间的事件处理、问题发现、事件通知及未了事宜等，均应写入值班记录表并交接清楚	◎
		交接班时，如发生严重事故或网络中断时，交班人员应在保证接班人员了解清楚事件的全部过程、后续工作情况下，方可以交接下班，接班人员在未了解事件的过程、进展情况、后续的工作情况下有权拒绝进行交接	◎
		因漏交或错交而产生的问题责任由交班人承担，由漏接或错接而产生的问题责任由接班人承担，交接班双方均未发现的问题责任则应由双方承担	○
	值班工作规范	终端安全管理值班人员工作流程： 1）登录技术支撑平台 2）进入内部工单系统，查看并处理工单 3）登录终端安全管理系统监视平台，查看并处理重要风险预警及告警 4）登录终端安全工作邮箱 5）定期完成规范要求的周报及月报 6）安全通告（预警）的制作和发送	●
		终端安全管理值班人员日常检查项： 1）终端安全值班人员工作检查项 2）系统状态和资源使用情况 3）每日需查看的监视仪表板、活动列表等 4）工单系统 5）基于关联规则的安全事件告警 6）系统的安全预警或外部接收的安全预警信息 7）工作邮件等	●
	安全事件定义及处理方法规范	安全事件是指所有的终端系统及技术平台自身，由于终端（或服务器）系统的硬件、软件、数据因设备故障、偶然、恶意的原因而遭到的系统破坏、更改、信息泄漏或者导致系统不能连续正常运行的事件。如发生以下情况，可以定义为安全事件： 1）系统性能严重下降，或者宕机，导致系统无法正常运行 2）客户代理掉线 3）非授权访问，通过入侵的方式进入未被授权访问的网络中，而导致数据信息泄漏 4）信息泄密，数据在传输中因数据被截取、篡改而造成信息的更改 5）拒绝服务，正常用户不能正常访问服务器提供的相关服务 6）大面积感染计算机病毒或蠕虫 7）设备故障导致系统崩溃 8）误操作导致系统崩溃 9）任何在监控中或日常工作中发现的可疑、不确定的事件等	◎
		安全预警或安全事件信息的获取方式： 1）日常监控的发现 2）用户电话申告 3）用户邮件申告 4）外部信息获取 5）其他方式	◎

（续）

工作类别	规范类别	规范内容概要	技术平台支撑
值班工作管理	安全事件监控与处理流程	安全事件的处理依据安全事件响应流程说明进行处理	◎
		对于严重或复杂事件，在规定的时间内无法提供解决方案时，转入更高一级处理流程	◎
		安全事件处理完成的后续步骤： 1）完善知识库系统 2）修订问题发现规则	●
考核管理		按照《终端安全日常运维管理考核要求》定期对全体终端安全管理人员进行考核并计算考核分数，该考核结果作为奖惩依据 考核的范围包括：考勤、日常监控、日常维护、工时、报表、知识贡献等，具体考核标准需依据相关规范要求	◎
终端接入管理	终端接入流程	终端接入网络相关流程，包括所有表格模板	◎
	终端接入规范	接入网络终端所需满足的要求规范	◎
	终端配置初始化	终端接入网络前需进行的配置要求规范	◎
账户管理	账号的申请、更改和撤销	终端用户进行账号申请和审批，终端安全管理相关领导负责审批创建、变更和撤销员工的账号及权限，具体操作由终端安全管理员执行	●
		日常运维、分析等人员以及安全业务相关人员应严格按照审批后的账号、权限维护和管理系统，按要求生成、变更和删除相关账号。相关工作人员在离职或调转后应在指定时间内删除其所有账号和权限	◎
		终端安全管理负责人应负责登记、备案用户账号，并定期对用户账号和权限进行监督、检查	◎
	账号规范及管理	应根据不同的角色确定用户账号	○
		各账号应能标识系统访问的不同角色，应尽量避免使用系统默认账号，账号的设定应易于审计	◎
		各级系统管理员应当对系统中存在的账号进行定期审计，系统中不应存在无用或匿名账号	◎
		终端安全技术支撑系统应开启系统安全日志功能，能够记录系统的登录和访问时间、操作内容	●
	密码、口令规范及管理	根据密码、口令所属的不同系统和应用进行分类要求，包括长度、复杂度和变更时间要求等	●
		密码不能以明文的方式通过电子邮件或者其他网络传输方式进行传输	○
		任何人不得将密码告诉他人，如系统密码泄漏，必须立即更改	○
		未经批准任何权限管理人员不能共享权限及口令	○
		所有系统在建设和维护期间设立的默认密码在系统投入使用之前都要修改	○
		密码在输入系统时，不能在显示屏上明文显示出来	●
		系统应该强制指定密码的策略，包括密码的最短有效期、最长有效期、最短长度、复杂性等	●
		除了系统管理员外，一般用户不得具有改变其他用户口令的权限	●
		针对第三方人员的账号，应再分配时明确指定创建时间及撤销时间，并由终端安全管理负责人进行记录、跟踪及监督，到期应理解停止试用	●
	权限管理	应根据“最小授权”的原则设定账户访问权限，控制用户仅能够访问到工作需要的信息	●
		终端安全管理负责人应具有对各系统用户的审计权限，应具备比较完整的读权限，应当能够读取系统关键文件，检查系统设置、系统日志等信息	◎
		针对第三方人员的访问权限，应进行定期的检查和审计	◎
		账号口令的审批、授权、分发和使用应遵循本规定的要求，对于违反规定，造成账号口令的滥用、失窃，导致信息系统安全风险的，须追查并追究相应环节责任人的责任，将根据情节轻重采取责令期限整改、通报批评等处罚措施	◎
	账号命名要求	针对自有工作人员，账号名称需采用所在地区、省市的拼音第一个字母　具体人员名字全拼组成，对于地区首字母重合的依次向后取至不再重合为止，对于姓名全拼重合的加 1 位阿拉伯数字以区分	◎

（续）

工作类别	规范类别	规范内容概要	技术平台支撑
账户管理	账号命名要求	针对第三方人员（主要指有临时需要的各种人员的权限分配），账号名称为：L+预计撤销时间的年月日组成（如建立使用期限到 2011 年 12 月 1 日的账号：L20111201）	◎
报告编写与发布规范	安全运维报告	依据安全运维报告模板进行编写	◎
	安全预警报告	依据安全预警报告模板进行编写	◎
	安全事件分析报告	依据安全事件报告模板进行编写，每个步骤都要求详细具体	◎
	安全评估报告	依据安全评估工作情况和相关模板，编写安全评估报告	◎
知识管理	知识共享管理	具有知识库平台，支持知识积累和知识共享	●

备注：

技术平台支撑标识符含义：

完全由技术平台支撑为●

部分由技术平台支撑为◎

不需要技术平台支撑为○

终端安全日常维护中常用到的流程有表 10-3 中的 8 个，具体流程需要结合应用单位的实际行政管理情况进行完善。

表 10-3　终端安全日常维护流程列表

流　程　名	涉 及 人 员	输入输出文档	说　　明
日常监控流程	主机系统管理员	《重要风险监控及处理结果》 《系统日常工单及处理情况表》 《系统日常监控情况表》 《日常安全事件处理情况表》 《交接班文档》	日常监控包括的主要内容有： 1）早接班工作 2）日常监控工作 3）总结及交班工作
安全预警处理流程	主机系统管理员 安全管理员	《安全（预警）通告文档》	主要是安全预警信息的获取，整理和发布
安全事件处理流程	主机系统管理员 安全管理员 安全审计员	《安全事件工单》 《安全事件处理过程说明书》 《安全事件处理案例说明书》（可选） 《安全（事件）通告》（可选）	主要包括： 1）发现安全事件后派发的工单 2）安全事件处理 3）安全事件处理经验总结和丰富知识库
安全故障处理流程	主机系统管理员 安全管理员 安全审计员 安全主管	《安全事件工单》 《安全事件处理过程说明书》 《安全事件升级处理申请》 《安全故障处理过程说明书》 《安全故障处理案例说明书》（可选） 《安全（故障）通告》（可选）	主要包括： 1）安全事件升级 2）升级为安全故障后的处理 3）安全故障处理经验教训总结，丰富知识库，并全员通告以加强安全意识
终端入网管理流程	终端使用者（申请者） 主机系统管理员（实施者） 安全管理员（审核者）	《终端入网申请单》 《入网终端检查单》 《终端入网处置单》	主要包括： 1）终端入网申请 2）终端入网前检查 3）终端入网实施

（续）

流 程 名	涉 及 人 员	输入输出文档	说 明
终端维护管理流程	终端使用者（提出维护申请） 主机系统管理员 安全管理员（监督审核者）	《终端维护申请单》 《终端维护记录单》 《终端入网申请单》 《入网终端检查单》 《终端入网处置单》	主要包括： 1）终端维护申请 2）终端维护过程记录和审计 3）终端维护结束后重新入网
账号申请、修改、撤销流程	终端使用者（或主机系统管理员，申请终端安全防护和管理技术平台的账号） 安全管理员； 安全主管；	《账号申请单》 《账号修改申请单》 《账号撤销申请单》 《账号操作记录单》	主要包括： 1）账号申请 2）账号修改 3）账号撤销 4）账号操作实施及相关工作记录
变更流程	终端使用者 主机系统管理员 安全管理员 安全主管	《终端硬件配置变更申请单》 《终端资产使用人变更申请单》 《终端使用范围变更申请单》 《终端安全防护及管理系统配置变更申请单》	主要包括 1）终端软、硬件、使用人等变更 2）服务器软、硬件、维护人员变更 3）终端安全防护和管理技术平台配置等变更

10.3 日常统计分析

通过终端安全防护平台和管理平台对管理范围内终端管理信息进行实时采集，统一汇总、级联、统计和分析，及时了解所管理范围内的终端状态，对终端管理数据进行安全评估，对终端安全进行分析。终端系统的管理信息包括基础管理数据、安全事件信息。

基础管理数据包括终端数量、操作系统类别、终端硬件配置、在线/离线状态、防病毒软件安装及升级状态、安装软件、终端弱口令、操作系统日志等。

安全事件信息包括终端异常运行、系统补丁检测更新、终端用户权限变化、非法软件操作、违规外联、非注册终端违规接入等影响终端及网络正常运行的各种行为事件信息。

基于管理信息，各单位通过级联对以下指标进行对比分析：

1）信息内网终端注册数量和比率　各单位已注册（安装了客户端）信息内网终端数量与信息内网终端总数，以及信息内网终端注册数量与信息内网终端总数量的比率。数据采集周期：实时。

2）信息内网终端使用数量和比率　各单位信息内网在线终端数量，信息内网在线终端数量与终端总数的比率。数据采集周期：实时。

3）安装各种操作系统信息内网终端数量　各单位管理范围内安装 Windows 98/NT/2000/2003/XP/Vista/7 等操作系统的信息内网终端数量。

4）补丁更新率　各单位管理范围内及时更新操作系统补丁的信息内网终端数量与信息内网终端总数的比率。数据采集周期：每天。

5）违规外联报警数量　各单位管理范围内信息内网终端违规外联的报警数量。数据采样方式：违规外联事件产生后触发。

6）安装各种防病毒软件信息内网终端数量　各单位管理范围内安装各种防病毒软件的信息内网终端数量。数据采集周期：实时。

通过与上级终端系统的级联，上级终端系统将通过下级终端系统采集各单位终端管理信息。未部署终端系统的单位，要通过内部信息系统运行维护月报将本单位终端管理信息上报上级信息化工作部门，上级信息化工作部门将综合对各单位的终端管理信息采集情况和统计分析情况，形成整个信息内网终端安全有关通报进行发布。

10.4 日常工作的实现

日常运维的主要目的是通过实时监控终端系统，及时发现终端系统存在的安全风险并处理，规避重大终端安全风险问题或降低终端安全风险问题的损害。

日常运维工作的基本框架如图 10-1 所示。

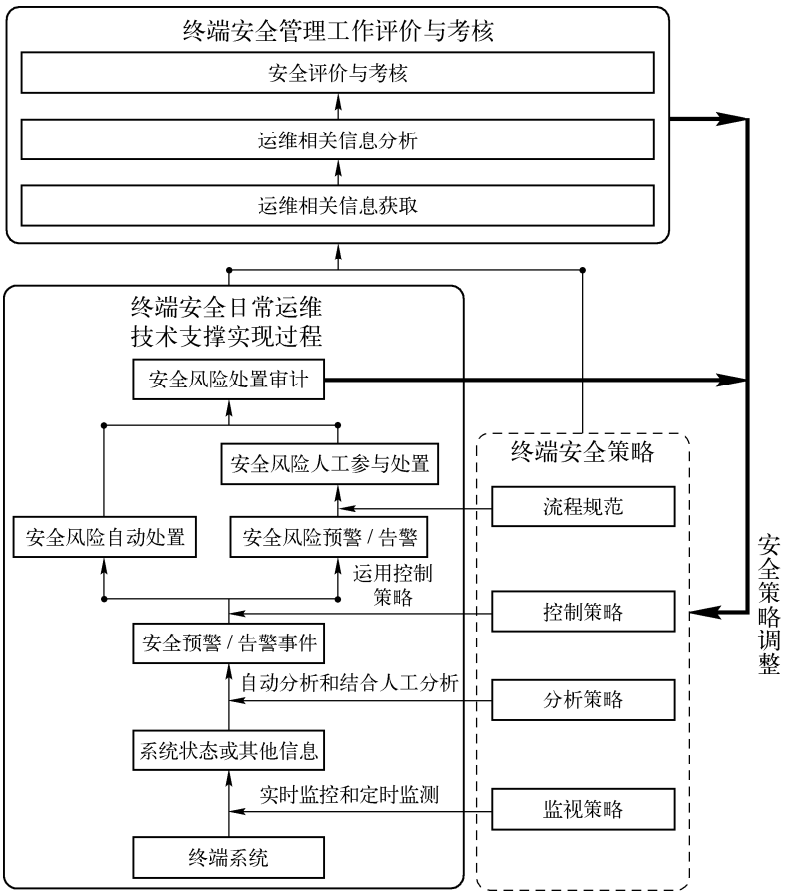

图 10-1 终端安全日常运维工作框架图

作为信息网络中的接入节点，终端系统数量大，应用多，如不采用有效的技术手段，单纯依靠人工进行系统的监视和风险处置是无法实现的。

从以上终端日常运维工作框架图的的技术支撑实现可见：

1）终端系统状态及安全信息的获取是运维实施的基础，信息获取主要通过技术检测手段实时或定期获得。

2）基于终端安全分析策略检测分析出终端安全风险事件（包括预警和告警事件）。

3）运用安全控制策略，自动或提醒终端安全管理人员手工对安全风险事件进行处置。

4）对于安全风险处置工作（包括自动和人工）进行记录，以供后续审计工作需要。

5）基于日常运维全过程信息进行分析，支撑对终端安全管理人员考核和终端系统的安全状况进行评价。

6）基于 4）和 5）的工作对于现行的安全策略进行评估和调整，以实现终端安全体系的保障能力螺旋式上升。

以上 1）到 6）的过程是在终端安全策略体系的指导下，基于终端安全技术平台实现的。通常的实现框架主要由防护框架和管理框架两部分组成，如图 10-2 所示。其中置为灰色的为终端安全防护技术框架部分，其他为终端安全管理技术框架部分。

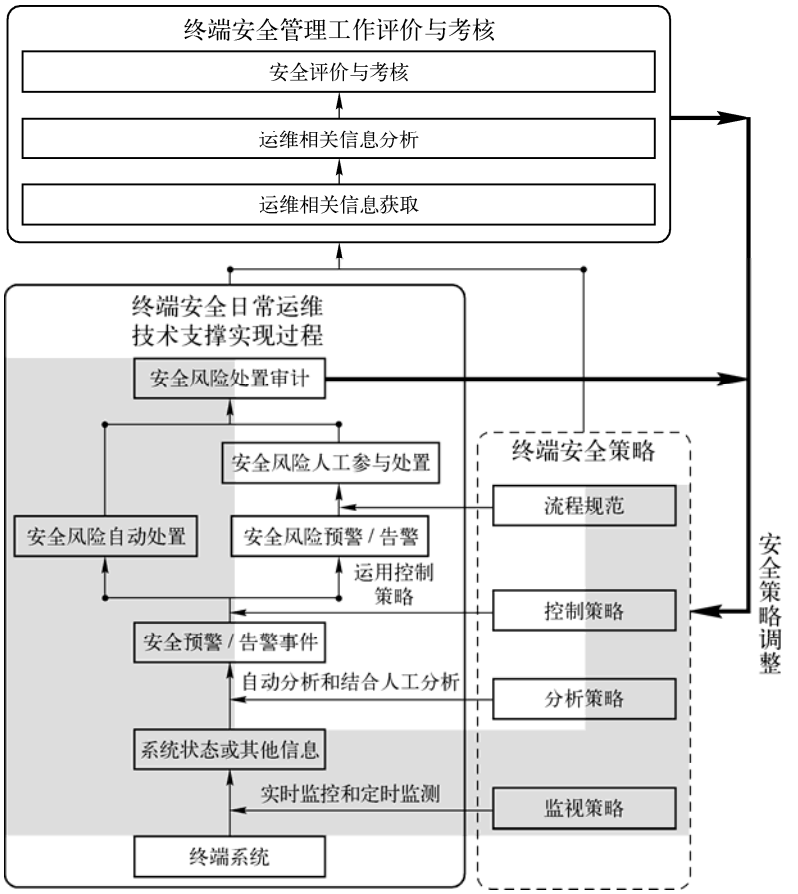

图 10-2　终端安全日常运维过程安全防护及管理框架示意图

以上两大防护框架不仅可以自行提供相关的技术支撑工具，也可以集成其他终端安全防护工具，完善技术平台和体系。如系统状态或其他信息监控中可以集成终端病毒防护产品，实现对病毒相关状态和特征的监测、分析与控制。

第 11 章　终端安全风险深度分析

11.1　分析数据准备

分析数据的目的主要是根据获取的事件信息，揭示可能已知或未知的趋势，为终端安全管理工作提供管理和监督的实际数据支持。通过对数据的深入分析，可以对终端安全的工作情况深入了解，并对后续的整改提供分析的依据，或为计划提供可靠的实际数据支持。

要进行深度分析，首先要进行分析数据的准备工作。分析数据的来源与分析数据的目标密切相关。结合终端安全管理体系的内容，分析的数据来源可列举如下：

✓ 终端本身的安全事件

✓ 与终端相关的设备上对终端记录的安全事件

✓ 相关应用系统上对终端记录的安全事件，包括但不限于审计系统、行为分析系统等

✓ 其他设备或系统记录的终端相关的安全事件

由于有如此之多的数据来源，且这些数据来源提供的安全事件在内容上必然存在极大的差别，为了能够对这些安全事件进行统一的管理和分析，需要对这些事件进行归一化的处理。一般而言，数据归一化处理可以分为数据格式化与数据语义映射两个部分。

（1）数据格式化

数据格式化，将数据通过格式化的方式，转换为统一的表现形式。其处理过程又可细分为数据预处理、数据处理与数据填充。

1）数据预处理，将原始数据解析为信息元（有特定含义的数据单元，信息元的划分一般与归一化事件字段有关）。如：

CISCO 交换机 UDP 日志：

<39>233159: *Mar 26 04:04:10: UDP: rcvd src=192.168.101.239(137), dst=192.168.101.255(137), length=58

CISCO PIX 防火墙 UDP 日志：

<166>%PIX-6-302016: Teardown UDP connection 12385695 for outside:61.171.177.212/16405 to inside: 192.168.101.255/40560 duration 0:02:01 bytes 70

处理后的信息元如表 11-1 所示。

表 11-1　处理后的信息元

CISCO 交换机 UDP 日志		PIX 防火墙 UDP 日志	
39	Syslog 日志标准格式字段，表示优先级，可通过计算公式进一步处理获得设备字段和严重级别字段	166	Syslog 日志标准格式字段，表示优先级，可通过计算公式进一步处理获得设备字段和严重级别字段
233159	事件号	PIX	PIX 日志标志
Mar 26 04:04:10	日志产生时间	6	日志严重级别，可通过 166 计算获得

（续）

CISCO 交换机 UDP 日志		PIX 防火墙 UDP 日志	
UDP	协议类型，这里可以有其他类型，如：IP ARP 协议等，这里的协议不同，日志后面的内容也不同，可提取得信息元也不相同。在示例日志中，IP ARP 协议中没有了端口信息，但是多了 MAC 地址信息	302016	事件号
192.168.101.239	源 IP 地址，可以从日志中的 src 部分推理得到	UDP	表示协议类型，根据协议的不同，日志描述的内容也有差别，可获取的信息元也会发生变化
137	源端口号	12385695	表示连接 ID
192.168.101.255	目的 IP 地址，可以从日志中 dst 部分推理得到	outside	源接口的名字
137	目的端口号	61.171.177.212	源 IP 地址，可以从日志中的 outside…to 部分推理得到
58	表示源发送了 58 个字节	16405	源端口
		inside	目的接口的名字
		192.168.101.255	目的 IP 地址
		40560	目的端口
		0:02:01	连接持续时间，这个时间需要被格式化为秒
		70	表示源发送了 70 个字节

2）数据处理，对信息元的数据进行处理，将相同类型的数据处理为统一的格式。比如时间，它可以有非常多的表现形式，如“Dec 3 11:00:00 2007”，“2007-12-3 11:00:00”或“Mon Dec 3 11:00:00 CST 2007”等，它们表示的都是同一个时间，但表现形式上有差别。计算机无法自动认知这些差别，所以为了后续的数据表现及数据处理，需要对时间进行格式化，统一其表现形式。除时间外，还有 MAC 地址、IP 地址等需要格式化的数据类型。除了格式上的统一外，还需要对数值型数据的度量进行统一，如文件或空间的大小，可能用 MB（兆字节）、KB（千字节）或 BYTE（字节）等任意一个度量做单位，单位的不同会造成数据的巨大差异，因此也需要对数值型的数据进行度量统一。

3）数据填充，将经过数据处理的信息元填充到相应语义的归一化数据字段中。通过正确分析原始数据的整体语义，正确地理解信息元的含义。如即使都是 IP 地址，但根据语义不同可以区分为源 IP 地址和目的 IP 地址，根据语义可以知道数据是谁发出的等，在确定语义后，将信息元分别填充到归一化事件对应的字段中。

（2）数据语义映射

数据语义映射用于统一数据的语义表述，即将表示相同语义的不同内容统一为同一的表述形式。该过程将不同原始数据中，表示相同语义的内容统一为同一的语义表示。这里有别于格式化的是，这里强调的是对数据内容语义的统一。如数据的级别，在 Syslog 标准中定义了 8 个级别，而 Windows 的 Event Log 日志中定义了 5 个级别，它们分别如表 11-2 所示。

因为二者在划分级别的个数上不统一，而且定义不统一，势必造成后续的数据表示及处理的不一致，所以必须对它们级别的内容进行数据映射，统一它们的语义。上面表格的映射

部分给出了数据映射的对照关系。像这样需要进行数据映射的内容还包括病毒信息、漏洞信息、补丁信息、IDS 攻击信息等，以上的信息均会因为厂商或标准的不同，信息的描述上存在差异。如不同的反病毒厂商会给同一种病毒定义不同的名字，这里就需要将不同的名字映射为同一个名字，以便后续的数据处理。

表 11-2　常用标准的数据级别定义

Syslog				Event Log			
数值	解释	映射值	映射解释	数值	解释	映射值	映射解释
0	紧急	4	非常高	1	信息	1	低
1	报警	3	高	2	警告	2	中
2	严重	3	高	4	错误	3	高
3	错误	2	中	8	审核成功	3	高
4	警告	2	中	16	审核失败	4	非常高
5	通知	1	低				
6	信息	1	低				
7	调试	0	非常低				

11.2　深度分析建模

所谓终端安全风险的深度分析实质上是对终端安全风险进行的由浅入深、由表及里的全方位分析。结合终端的安全现状，如补丁情况、有无脆弱性等，与不断发生的、终端相关的安全事件一起来评价终端的整体风险情况。终端安全风险的深度分析需要建立在对终端相关的安全事件的认识与理解的基础之上。在有了上一小节对安全事件的准备之后，读者应该已经对每种安全事件的含义有了初步的认识。下面需要结合安全知识的理解、终端安全的现状以及安全事件的认知三者来构建终端安全风险的分析模型。

下面以安全事件为主视角，分别对单一安全事件、多个相关安全事件及海量安全事件进行分析建模。

（1）单一安全事件

在安全事件知识的认知体系中，除了如 IDS、IPS 等报出的具有明确安全意义的，可能造成具体终端风险上升的单一安全事件需要关注外，其他还有很多级别较低的，容易被忽视的，却存在一定安全隐患的单一安全事件需要关注。如一个在午夜的登录某一业务系统的安全事件，这个安全事件本身属于一个正常的业务登录事件，其级别并不高，但由于它是午夜的发生的，而这个时间段不属于正常的业务系统访问时间，也就是该事件反映了一个非常态的登录行为，那么这个安全事件就必须引起关注。即使经过最终确认，这是一个合法用户临时加夜班时的合理登录行为。

另外，即便是如 IDS、IPS 等报出的具有明确安全意义的安全事件，但由于终端当前的安全状态是已经修补了系统，打上了补丁或有其他安全产品防护。则该安全事件所反映的问题根本无法影响到终端，不会造成终端风险的上升。此时应该忽略掉这个安全事件，从而节省处理安全事件所需的成本。

以上两类安全事件分析模型都是用于确认安全事件是否会对终端的风险造成影响。下面描述如何对两类安全模型进行建模。

第一类模型的建模需要根据预先掌握的安全知识或实际应用情况（如真实应用系统的应用环境）设定一个正常或异常的模型描述。然后确认应用此模型安全事件需要具备的安全特征，如安全事件中必须有时间信息且它必须是登录事件才能应用到“异常时间段访问”的分析模型中。最后需要确认模型的应用范围，如指明究竟是哪些系统的登录安全事件应用到这个分析模型。

第二类模型的建模需要首先根据安全知识对安全事件类型与补丁、漏洞等的信息关系进行模型描述。然后确认哪些具体的安全事件属于该安全事件类型。最后需要明确该安全模型应用于哪些终端。

（2）多个相关安全事件

在安全事件知识体系中，很多时候，单个安全事件本身所体现的安全行为不值得关注，但将多个安全事件串在一起分析就很值得关注了。如一个外部地址在一个时间段内频繁访问一个主机的不同端口，而外部地址与该主机间的防火墙记录了所有这些访问事件。这里的每一个访问事件都是正常的事件，且事件本身被标记的级别也不高。但将这一段时间内发生的所有访问事件关联在一起分析时，就会发现这是一个外部地址扫描内部主机端口的扫描行为，是一个值得密切注意的安全行为。

另外，如 IDS 这样的安全设备，其在产生安全事件时有很多情况下会误报，信噪比比较高。这将加大终端安全事件的处理成本及干扰终端安全风险的正确评估。针对这种情况也可以通过关联多个安全事件来确认该安全事件是否真的发生，是否值得关注。如 IDS 发现了一个针对某一终端的 DDOS 攻击，并报告了一个安全事件。在这一段时间内防火墙也报告了很多源地址不同而目标地址皆为某一终端的通信事件。且终端上的 CPU 利用率已超过 80%。此时可以确认 IDS 报的安全事件是一个真实的安全事件；否则这个安全事件不值得关注。

以上两类多个安全事件相关的风险分析模型与单一安全事件的风险分析模型的目标一致，主要是用来确认安全事件对终端的风险是否有影响，借此评估终端安全的风险情况。多个安全事件的风险模型可以分为通用风险分析模型和专用风险分析模型。通用风险分析模型的普适性好，但建模周期长，需要经过长时间的知识积累。多数通用风险分析模型已被其他的安全产品提供，如 IDS 就提供了端口扫描的风险分析模型。可以直接借鉴这类模型来对安全事件进行分析建模。而专用风险分析模型对实际应用的环境有较高的依赖，这有别于通用的风险分析模型。但专用风险分析模型正因为对环境有较高的依赖，所以它的应用效果更好，安全事件分析准确率更高。下面描述如何对专用风险分析模型进行建模。

首先需要充分了解终端所处的环境。比如外网是否能访问到终端？终端能否访问到外网？外网到终端的网络通路上都部署了什么安全产品？是否已经部署了防火墙或 IDS？二者的部署顺序是什么？终端能访问和被哪些内网访问？这些网络通路上都部署了什么等。在充分了解了终端的部署环境后，根据所知的安全知识提出一个共知的安全问题，如 IDS 在报告 DDOS 攻击时有较大的信噪比。针对此问题，结合实际环境设定一个模型描述（模型描述会根据环境中有无防火墙而不同）。然后确定满足这一模型的安全事件都应具备的特征。最后确认模型的应用范围，如指明该场景应用于哪些终端。

（3）海量安全事件

海量安全事件分析主要用于终端的风险统计分析。它可以分析一段时间以来的终端的总体风险趋势、终端中各类安全事件的比率及趋势、造成终端风险的安全事件来源的分布情况及全网终端风险趋势等等。这些分析模型一般基于数据库构建。

11.3 深度分析方法与实现

上一节以安全事件为主视角讨论了风险深度分析的建模。本节将针对上一节的描述着重阐述如何用不同的深度分析方法来实现不同的分析模型。

（1）单一安全事件----基于规则匹配的分析方法

基于规则匹配的分析方法是一种条件匹配分析方法。它通过预先设定好匹配条件完成对安全事件的分析。当一个安全事件匹配了规则预先设定的条件，其分析结果就为真，否则就为假。

基于规则匹配的分析方法需要具备灵活的语法，可以尽最大可能地描述各类匹配条件，并具有很好的可扩展性，可以扩展语法尚不满足的条件规则。至少需要支持 AND、OR、NOT 等逻辑运算并支持逻辑运算的嵌套应用，还需要支持“=”、“<>”、“>”、“>=”、“<”、“<=”、“BETWEEN..AND”“IS”、“IN”、“LIKE”及正则表达式等匹配运算。

基于规则匹配的分析方法需要支持多个匹配规则同时运行，并需要具备良好的运行效率。

下面尝试用一段伪规则匹配语法描述一下 11.2 节中单一安全事件中提到的两个分析模型。

1）异常时间段访问（InTimeRange(evt.time,'19:00:00','8:00:00')AND evt.type='登录'）；该规则表示的含义是如果事件的时间在 19 点到第二天早晨 8 点钟之间并且事件的类型为登录，则该事件匹配此规则。InTimeRange 是一个函数，用于判断给定的时间在不在指定的时间范围内。

2）IDS 事件确认（Validate(evt.dstIp,evt.technology)AND evt.dvcType='IDS'）；该规则表示的含义是如果事件的目标 IP 所表示的终端会被该事件记录的攻击手段侵害且事件的设备类型为 IDS 时规则被匹配。Validate 是一个函数，用于判断指定 IP 所表示的终端是否会被指定的技术侵害，该函数在实现时会读取终端当前的安全状态信息及安全事件技术与漏洞补丁的关系，综合计算出是否被侵害的结论。

（2）多个相关安全事件----基于状态机的关联分析方法

基于状态机的关联分析方法是一种基于有限状态机（Finite-State Machine, FSM）理论的事件分析方法。有限状态机是一种表示有限个状态以及在这些状态之间的转移和动作等行为的数学模型。状态用于存储关于过去的信息，即它反映从系统开始到现在的输入变化。转移指示状态变更，它使用转移发生时必须满足的条件来进行描述。动作是在给定时刻要进行的活动的描述。有多种类型的动作。

- ✓ 进入动作（Entry Action） 在进入状态时进行
- ✓ 退出动作 在退出状态时进行
- ✓ 输入动作 依赖于当前状态和输入条件进行
- ✓ 转移动作 在进行特定转移时进行

FSM 可以使用图 11-1 那样的状态图（或状态转移图）来表示。

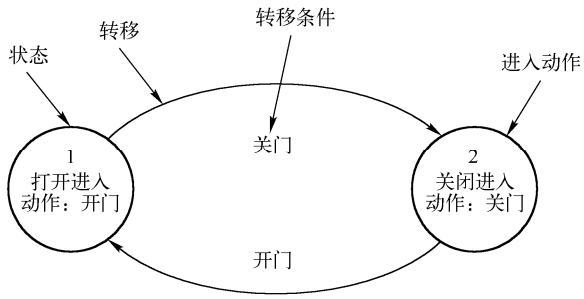

图 11-1　开关门的状态图

采用基于状态机的关联分析方法来实现多个相关安全事件的分析模型。如在 11.2 节中多个相关安全事件中提到的 DDOS 事件确认模型。图 11-2 是该模型假定的网络拓扑图。

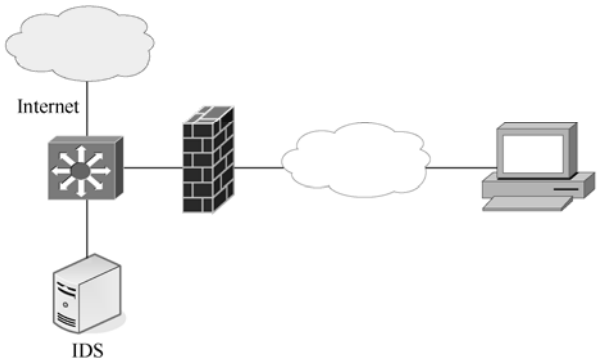

图 11-2　网络拓扑图

将该模型表示为图 11-3 所示的状态机图。

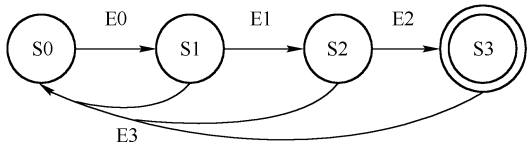

图 11-3　状态机图

1）状态 S0 表示状态机的初始状态，即没有任何安全事件触发状态机的状态。

2）状态 S1 表示收到了 IDS 报出的一个目标为终端 T 的 DDOS 相关的安全事件。

3）状态 S2 表示收到了在 IDS 报告事件之后一段时间里防火墙报出的目标为终端 T 的 N 个通信连接。

4）状态 S3 表示终端 T 的 CPU 利用率超过了 80%。该状态是整个状态机的接收状态，此时状态模型规约并会滚回 S0 的状态。

5）E0 表示当一个 IDS 报出的 DDOS 相关的安全事件。

6）E1 表示有 N 个由防火墙报出的通信事件，其目的与 E0 报出的安全事件的终端 IP 一致。N 为常数，在具体应用时可以设置，如可以设为 10 个，即表示收到 10 个目标 IP 为终端 IP 的通信连接就满足条件了。

7）E2 表示有 CPU 利用率超过 80%的安全事件的 IP 地址与 E0 报出的终端 IP 地址一致。

8）E3 表示状态在 N(N 为可设定的常数，同 E1)秒内若不能迁转到下一状态，则状态超时，状态迁转为 S0。

本模型中，当状态 S0 收到了 IDS 报告的 DDOS 安全事件后迁转到状态 S1。 S1 有两个迁转条件，一个是满足 E1 当有 N1 个防火墙通信事件发生时；一个是满足 E3 在 N2 秒后超时。若在 N2 秒的范围内，没有 N1 个安全事件发生，则 S1 满足 E3 的迁转条件，状态迁转到 S0 状态而不是 S2 状态。这个迁转表示已发生的这些安全事件不符合该安全分析模型。若在 N2 秒的范围内有 N1 个安全事件发生，则 S1 状态在第 N1 个事件发生时立刻迁转到 S2 状态，并在 S2 状态等待迁转条件被满足，要么迁转到 S3 状态，要么迁转到 S0 状态。在本模型中，只有当状态机到达 S3 状态时，才认为这些安全事件符合安全分析模型，并可最终确认 IDS 报出的 DDOS 事件是一个会影响终端风险的安全事件。

基于状态机的关联分析方法需要支持灵活的语法描述，方便不断添加新发现和总结的风险分析模型。其语法应完全支持有限状态机中列举的概念，应包括状态的定义、迁转条件的定义以及动作的定义。状态定义语法需要支持一个状态可以迁转到不同的状态上。迁移条件定义语法需要支持在条件设置中引用状态信息，需要支持 AND、OR、NOT 等逻辑运算及逻辑运算的嵌套应用，还需要支持“=”、“<>”、“>”、“>=”、“<”、“<=”、“BETWEEN..AND”“IS”、“IN”、“LIKE”及正则表达式等匹配运算。另外，对于尚未包含的匹配条件可以通过函数方式进行扩展。最后还需要支持超时定义。行为定义语法需要支持有限状态机所描述的四种行为发生条件的设置。支持行为内容的函数方式扩展，并可将状态信息作为参数传给函数。

基于状态机的关联分析方法需要能同时支持多个状态机分析模型并行运行。需要拥有良好的执行效率和稳定性。需要能够设置每个状态分析模型的实例对象数目，防止因状态机对象实例数目过多导致系统内存耗尽而引起系统工作异常。

（3）海量安全事件----基于多维数据的分析方法

基于多维数据分析的方法是一种以数据库或数据仓库为基础的数据分析方法，也称为联机分析处理 (On-Line Analytical Processing, OLAP)。联机分析处理(OLAP)的概念最早是由关系数据库之父 E. F. Codd 于 1993 年提出的。当时，Codd 认为联机事务处理(OLTP)已不能满足终端用户对数据库查询分析的需要，SQL 对大数据库进行的简单查询也不能满足用户分析的需求。用户的决策分析需要对关系数据库进行大量计算才能得到结果，而查询的结果并不能满足决策者提出的需求。因此 Codd 提出了多维数据库和多维分析的概念,即 OLAP。

OLAP 数据库分为一个或多个多维数据集，每个多维数据集也被称为立方体。它是数据的集合，通常从数据仓库的子集构造，并组织成一个一组维度和度量值定义的多维结果。多维数据集包含以下几个主要概念。

✓ 维（Dimension）是人们观察数据的特定角度，是考虑问题时的一类属性，属性集合

构成一个维（时间维、地理维等）

- ✓ 维的层次（Level）是人们观察数据的某个特定角度（即某个维）还可以存在细节程度不同的各个描述方面（时间维：日期、月份、季度、年）
- ✓ 维的成员（Member）是维的一个取值，是数据项在某维中位置的描述。（“某年某月某日”是在时间维上位置的描述）
- ✓ 度量值（Measure）是多维数组的取值（2000 年 1 月，上海，登录，100KB）
- ✓ 事实表是度量值所在的表
- ✓ 维度表是包含维度信息的表
- ✓ 联机分析处理的主要分析操作有钻取（Drill-up 和 Drill-down）、切片（Slice）和切块（Dice）、以及旋转（Pivot）等。
- ✓ 钻取是改变维的层次，变换分析的粒度。它包括向下钻取（Drill-down）和向上钻取（Drill-up）/上卷(Roll-up)。Drill-up 是在某一维上将低层次的细节数据概括到高层次的汇总数据，或者减少维数；而 Drill-down 则相反，它从汇总数据深入到细节数据进行观察或增加新维
- ✓ 切片和切块是在一部分维上选定值后，关心度量数据在剩余维上的分布。如果剩余的维只有两个，则是切片；如果有三个或以上，则是切块
- ✓ 旋转是变换维的方向，即在表格中重新安排维的放置（例如行列互换）

利用多维数据分析方法来实现 11.2 节海量安全事件中提到的各种终端风险分析模型。根据风险分析模型抽取模型可能的维度，如 11.2 节中提到的关于时间的统计和关于安全事件类型的统计等。将时间和安全事件类型作为两个维度，并构建与其相关的维度表。修正 11.1 数据准备小节中提到的数据准备过程，让每一个归一化后的数据都包含与维度表相关的维度信息。修订安全事件表的结构，存储安全事件，并将这张表看作是安全事件的事实表。利用 OLAP 数据库工具，在工具中建立维度表与事实表的关系，将维度表与事实表的数据导入多维数据模型，生成多维数据集。结合多维数据展示工具及多维表达式(MultiDimensional Expressions, MDX)，对多维数据进行钻取、切片、切块等分析操作，实现基于海量安全事件的终端安全风险统计分析。

第 IV 部分

终端安全风险行业化管理及应用案例

第 12 章　终端安全风险行业化管理模式

12.1　行业化的需求

本节主要介绍几个比较典型的行业信息化建设过程中对于终端安全风险的处理情况，包括政府部门、公检法行业、大型商业企业、能源行业等。

政府部门的信息化建设往往目标和规划变化比较频繁，但是每个阶段都是以国家总体规划为基础原则。各级行政区域的政府部门，对于信息化的建设十分重视，并且强调所在区域的互联互通，因此相对的信息来源和信息交互非常频繁。在这种情况下，对终端的管理往往要以使用者为单位进行重点区分，区分使用者的身份、数据查询的权限、数据操作的权限、信息传递的审计和监控。政府部门有健全的行政管理体系，对于设备和人员的管理很细致，分级和分类都很清晰，设备的针对性很强，较少出现一机多用的情况，甚至可以实现按需分配使用不同设备，从根本上提高了设备使用的安全性，减少了交叉使用和工作疏忽带来的风险。但是政府部门的人员往往身兼多职，且权限较高，所涉及信息跨领域的情况也非常普遍，因此对于人员身份的识别和行为的审计在终端的管理过程中显得尤为重要，但是对于操作的限制较少，功能的管控不多。

公检法行业的信息化建设规范很明确，行业的分布式倾向很强，工作内容也比较敏感，对于信息安全要求极高，往往需要物理隔离不同的网络。公检法的工作时间比较有弹性，因此工作时段比较难以明显限定，而且移动办公情况较多，数据的传递情况非常频繁，而且不同的人员即使是在相同的部门下都会存在较大的差别，数据会要求严格区分读/写权限并且是以使用者为单位。公检法行业在追求工作效率方面，强调安全为基本原则，但是工作流程不可以任意调整，相关的工作制度和规范都有国家的统一标准，因此即使在分布式的管理模式下也是如此，而各个区域的管理也都能够保持相对的一致。从已知的成功案例中，可以发现适合该行业的信息化，通常都把工作重点放在信息安全方面，尤其是移动办公的安全性和移动存储介质的管理，在强调人员的个人身份认证和识别基础上，要求相关信息的操作时另外需要权限的认证和工具的操作口令判断。该行业属于典型的以强制流程和规范保护信息安全，即使工作效率受到影响，也要保障工作秘密的安全性。

大型商业企业的信息化建设由于起步不同和风格不同，往往千差万别，以电子商务类公司为例，工作业务不可避免地与互联网进行直接接触，无须像上两个行业一样进行网络的物理隔离，受到国家制度和规范的影响较小，因为国家较少直接对企业进行制度和规范性的要求，没有明确的指标限制。不过也正因如此，导致终端面临的安全问题十分严峻，网络攻击和病毒木马的侵袭，信息的外泄和丢失屡见不鲜。商业企业以追求利益为前提，片面强调安全会失去信息化建设的意义。因此在保障工作的基础上，进行终端的安全管控，这在很大程度上是对管理工作的灵活性提出了更高的要求。管理策略的阶段性变化是企业信息化建设中不可忽略的重点，企业自身的建设通常是强调效率至上和利益优先，终端的管理应该尽可能

配合，不应该成为阻碍，更不能制约企业的发展。

能源行业属于大型商业企业的特例，尤其是国有大中型企业，特点很鲜明，风格介于政府和一般商业企业之间，既有国家安全制度和规范的约束，也有企业追求效率和利益的压力，在这两者间直接的平衡是该行业面临的重要问题。国家安全制度和规范是能源行业的终端安全管理基础，是国有大中型企业立足的根本和长远发展的必要保障，效率和利益的压力是国有大中型企业生存和成长的重要支柱。该行业的终端安全管理属于应用终端安全管理最典型的情况，管控措施非常细，阶段性调整非常大，对于整体规划和安全管理的灵活性要求很高。

终端安全管理作为一个泛化的课题，不好脱离实际去研究其理论上的意义，因为终端的灵活性和针对性只有在对应的行业内才具有实际意义。

终端安全管理的目的是保障终端的安全发展，只有实现终端的安全发展，才能最大限度地体现终端的价值。所以，需要研究的是选择最有效的方式实施终端安全管理，寻找最有效的途径来实现终端安全管理目的。经过终端安全的多年发展，各个行业形成自有的特色，既是发展的进步，也是能力的提升。这期间，终端安全管理的行业特点更加明显，终端行业化管理已形成发展趋势，成为实现终端安全管理目的有效途径的必然选择。

终端行业化管理的意义，在于明确终端在实际使用中的具体应用边界和范围，根据终端的用途形成分类的行业制度和规范，结合行业特点和需求制定终端安全管理的规划，避免由于泛化的安全管理概念阻碍行业的自身发展。终端行业化管理的途径也是它的目标，就是构建终端行业化管理体系，通过行业制度和规范来保障终端的安全发展。

终端行业化管理不是简单的人力投入或者设备投入，而是要实现人员的思想和工作模式转变，使之达到有效的管理。而有效的管理是建立在大量数据和信息的分析基础之上。管理方法再先进，没有足够的技术和工具支撑，都是无意义的空谈，这就对终端安全管理工具提出了较高的要求。但是仅仅依赖工具去实现终端行业化管理，又会走回以往失败建设的老路上去。“学而不思则罔，思而不学则殆”，想要实现行之有效的管理，离不开信息化手段的支撑，要通过搭建相应的平台，设定科学严谨的管理流程，形成一个完整的管理循环，使得管理工作在不断地循环中变得更加完善。

具体来讲，终端行业化管理需要通过终端防护平台和终端安全管理平台两部分来实现，终端防护平台负责终端的具体信息采集和安全防护措施应用，终端安全管理平台负责数据的分析和管理的调整。从风险的视角来看，已知可控风险在防护平台上进行发现和预防，经过监控进行整理和汇总，在管理平台进行分类分级的处理和分析，通过整体趋势的判断和控制，以及重点风险的实时掌控，重要人员和重要设备的专项关注，形成安全策略的调整，进行终端安全管理的细节调整。从管理工作的视角来看，防护平台和管理平台区分管理工作的重心，防护平台侧重在终端的细节管控，包括终端的基础安全、运行安全和信息安全，对于网络的安全和设备安全实时监控和分析，对于特殊情况和个别情况的甄别和直接处理，管理平台侧重在区域的安全态势，对于安全的整体要求和发展发现进行规划、调整和评价，不同的工作平台需要的工作技能不同，对应的工作视角和工作要求也不同，各自思考问题的层面和思路也是不同的。

12.2 行业化管理的技术支撑

行业化终端安全防护的管理内容是针对终端资产的安全风险进行的，各行业同类终端资

产在其业务专网中所面对的安全风险基本相同。其差异部分在于行业化终端安全管理的管理对象终端资产因不同的行业略有差别，行业业务相关部分资产会有差异。比较典型的例子如税务系统的专用业务 U 盘、公安的干警身份证书等。

税务系统的专用业务 U 盘是面向非税务系统内部的人员使用的，U 盘的使用范围主要是税务信息申报的各个单位和个人，而使用的环境和终端与税务系统本身无关，且无法进行统一的管理和约束。因此税务系统的专用业务 U 盘，属于典型的外用型工具。这种外用型工具，使用环境复杂，使用方式比较难以进行规范，但是，在传递到税务系统之后，仍需要再进行信息的传递，这就是为什么要采用专用业务 U 盘的意义，因为管理上的要求往往需要技术的配合，技术上如果不能够满足，则管理上的要求往往形同虚设。专用业务 U 盘是可以区分出使用者和使用范围的，在安全的使用环境中，是会提前进行安全检查，并且记录操作行为，而且当专用业务 U 盘使用在非指定的环境中，可以像普通 U 盘一样进行操作，既解决了兼容性的问题，又可以提高安全性。

公安的干警身份证书是面对公安内部人员使用的，主要使用范围是公安内部的设备，可以区分人员身份，进行快速识别和认证。这就要求公安内部设备具备该身份证书的认证能力，可以区分和判断该身份证书的使用权限，并且记录下该身份证书认证之后所进行的操作，用于事后的审计。该身份证书在其他设备上应该具备自我保护功能，避免被复制和破解，使之能够达到自身安全防护的效果。

终端安全防护平台的主要功能在各行业具有通用性，与其特定资产相关部分略有不同，主要表现在接入参数和防护内容。例如税务行业的信息化要求比较高，相关的信息维护很到位，可以实现所有设备的先登记后接入，完整地实现终端设备的全生命周期管理，在终端防护过程中就可以实现每个阶段的关联处理和跟踪审计。

12.3 行业化管理模式

组织机构的规划是行政体系建设中的核心，不同的组织机构在工作职能、工作方式上有着一定的差异，这种差异就为机构提供了选择自己适合的模式的方法，根据国内企、事业单位行业职能的不同，管理模式有一定的区分，总体上包含以下 3 种：垂直管理、分布式管理、混合型管理。

12.3.1 垂直管理

垂直管理体现了管理体系的直接性和整体性，通常这种管理模式出现在管理体系建设的初期或者管理要求很集中的地方，管理建设的初期特别是从上至下建立的时候，下级管理往往很不完善，需要上级的直接管控，下级仅需要处理信息的收集和上报，业务独立且应用很少与其他业务交叉，基本上呈现上下两层的管理模式，下层管理模式虽然也可以继续分层，但是并不具备管理能力；而管理要求很集中的地方，往往强调对下层的监管，例如政府职能部门实行垂直管理，就意味着脱离地方政府管理序列，不受地方政府监督机制约束，直接由高一级或者更高级别的主管部门统筹管理“人、财、物、事”。不同部门的垂直管理机制在具体运作过程中，还有很多差别，如部分业务职能独立出来实行垂直管理，不是全部事务实行垂直管理，垂直管理层延伸到地级市、区县或者乡镇街道。图 12-1 为典型的职能体系中

的垂直管理模式。

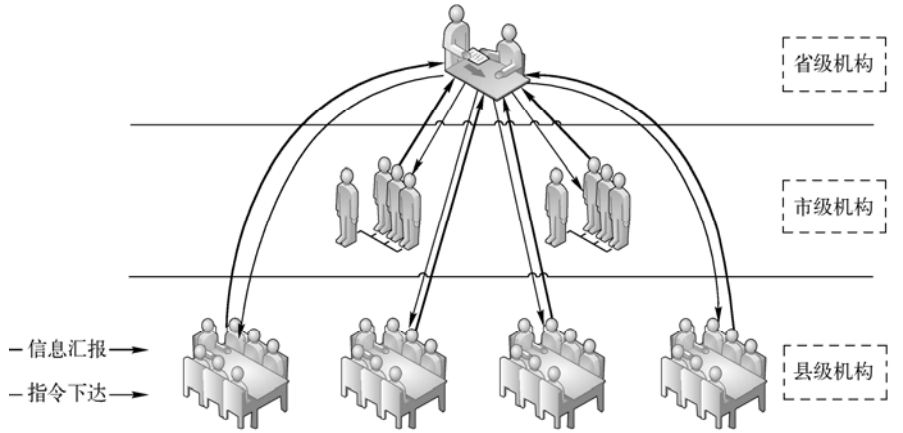

图 12-1　职能体系中的垂直型结构管理模式

12.3.2　垂直管理实例

垂直管理是一种重要的组织的管理形式，目前在多个行业的部门中采用垂直的管理模式进行管理，上级部门对下级各机构具有绝对的领导与管理权力，这种模式能较好体现上级指令下达的及时性和快速反应的特点，同时也存在下级机构不受同级行政机构的管理，具有较大的自由度和管理困难等问题。

终端管理平台在职能体系为垂直管理的行业中，受其行业自身的行政化管理体系差异以及行业中的管理特点，也较多采用垂直管理的方式管理平台部署在总部节点，所有分支节点均为接入节点。总部节点承担全部的管理功能，接入节点作为整个系统的数据采集点或共享数据的使用者。

以国税行业为例，终端安全防护平台和管理平台的部署方式是管理平台部署在系统中心位置，防护平台部署在各级节点位置；所有安全防护平台作为监视、防护数据的接入端接入总部终端安全管理平台。安全管理策略由总部统一制定，并通过系统下发。监控数据和防护结果信息上传至总部安全管理中心进行统一存储和处理。中心节点直接对二三级节点的防护平台下发安全策略，下发的策略类型分为 3 类：查询策略、关联分析策略、预警告警策略。查询策略是系统中与查询相关的所有策略信息，关联分析策略是关联分析场景相关策略信息的集合，预警告警信息策略是产生预警信息的各种阈值配置的内容，二三级节点根据策略执行的情况，实时向中心节点上报结果信息；中心节点管理员完成全局终端的状态监控和策略制定，二三级节点的管理员仅完成本地防护平台的系统维护。该项目中垂直管理体现在下发终端进程监控告警与统计分析策略上，通过安全管理中心，统一向所有的下级节点下发该策略，当终端发现有违规的进程运行，系统发生告警并同时将告警信息实时上传至管理平台中心，管理中心经过集中分析引擎，统计出进程违规运行最多的终端，并结合管理制度与操作流程进行相应的处置。以中心向二、三级终端下发策略的垂直管理方式，达到了策略多点快速下发、信息迅速集中反馈的效果，为安全管理工作高效开展提供了有效的支撑。中心与下级的信息传递方式参见图 12-2。

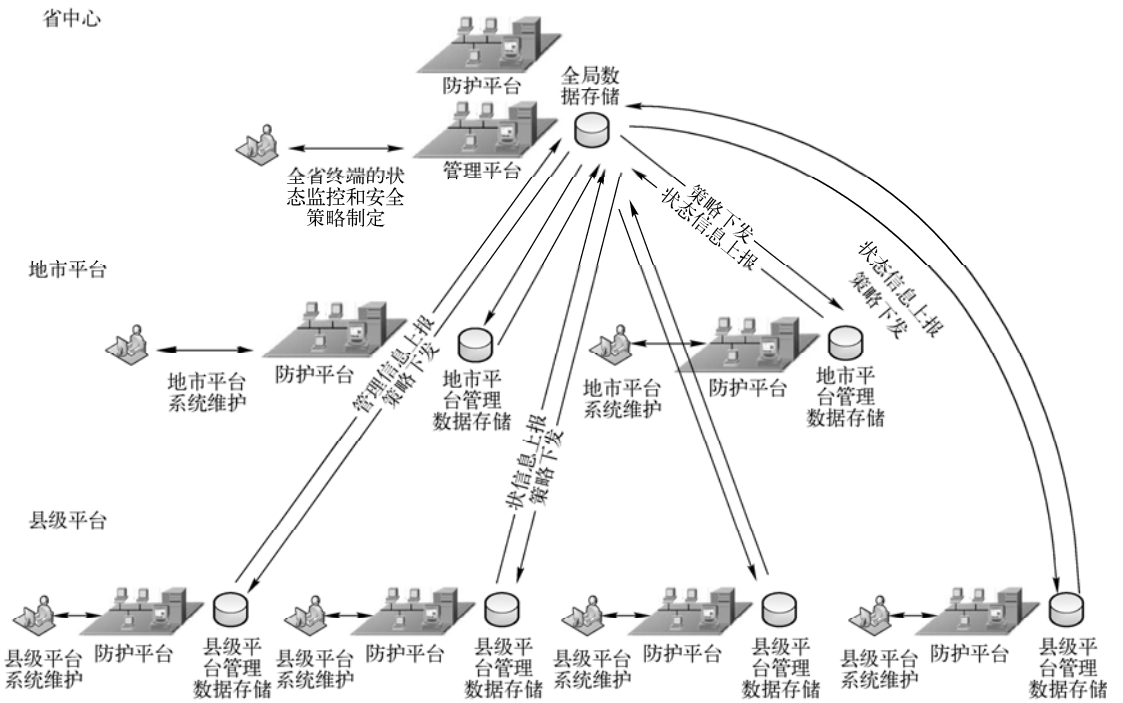

图 12-2　垂直管理示意图

12.3.3　分布式管理

相对的，采用分布式管理机制的行业的职能部门通常实行地方和上级的“双重领导”，上级主管部门负责管理业务“事权”，地方负责管理“人、财、物”，且纳入同级相关部门监督。分布式管理模式往往出现在从下至上的管理建设初期，每个下级自行建设，强调区域自我管控。这种管理模式也出现在管理要求相对分散的地方，例如联合国的管理模式就很典型，分布式保护各级和各个区域的内部完整性，上级对下级不直接进行干预。但是得益于整体框架，又可以保证互相之间的连通性和结构性，达到分散管理的目的。图 12-3 为典型的职能体系中的分布式管理模式。

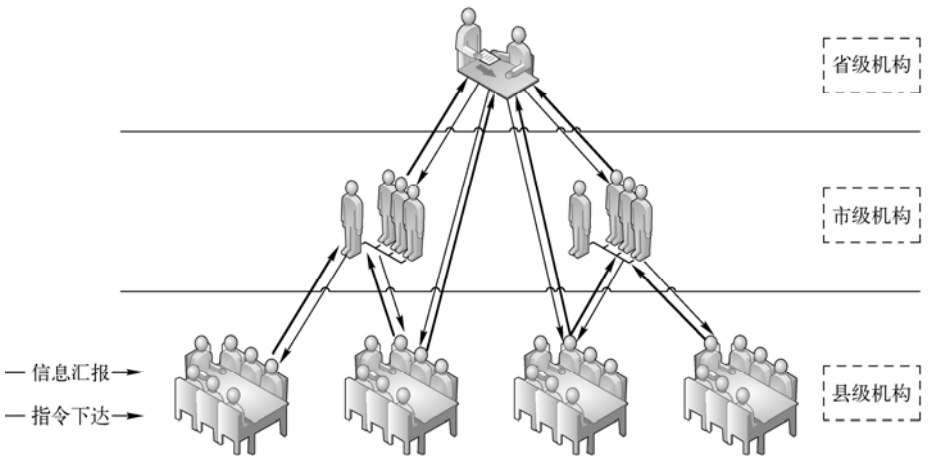

图 12-3　职能体系中的分布式结构管理模式

12.3.4 分布式管理实例

分布式管理业务，管理平台和防护平台部署在各级节点上，所有分支节点为管理及防护功能完全的自主节点。总部节点仅承担全局状态的展示，下级节点作为独立的管理防护节点，按照谁运营谁管理的原则实现对各级节点的防护管理。

分布式管理模型的终端管理系统，各级节点均部署管理平台和防护平台；监控数据和防护结果信息由各级管理平台进行存储和处理；三级节点按预定周期定期向二级节点上报状态信息，二级节点按预定周期定期向中心节点上报状态信息；各级管理员完成本地终端的状态监控的和策略制定。

在国内某军工集团项目建设中，其行政管理上分为集团、院、厂三级组织结构，项目涉及集团及下属各院、厂所终端近 50 000 点，分布在全国多个省、市、自治区。项目一期，针对集团各厂所部属终端防护与终端管理系统，以各厂所为单位，自主对内部终端进行安全管理、维护，由服务器直接对各个终端下发安全策略，对终端接口、外设、用户打印、刻录等操作行为进行安全管控。二期项目开始后，建设完成院管理平台与集团中心管理平台。各院级管理平台向上连接集团中心，向下连接院内各厂管理平台，各厂内管理端部属为三级管理平台继续使用，由院信息中心二级管理平台对其下发平台策略，下属各个厂所日志收集上传处理。二期建设完成后，在集团下属院、厂所本地，乃至全国已初步形成分布式管理模式。集团设立的一级平台，限制并明确二级平台权限、策略范围，二级平台再次在本权限内对三级平台下发平台策略，设置日志转发模式。对于终端日志与报警信息，全部逐级转发，汇总至集团信息中心进行安全事件处理。这样就在全国范围内形成了一个涵盖所有终端，分三级部署、管理的分布式终端管理平台。各个服务器权限清晰，流程明确。分布式管理模式参见图 12–4。

12.3.5 混合型管理

混合管理模式即垂直管理和分布式管理的结合。结合的方式往往不是固定的，常规的方式是非垂直管理业务由上级指导，当地负责组织管理，也有一些混合管理的模式是部分地区由上级直属管理，其他地区当地自行管理。混合管理模式是在垂直管理和分布式管理中找寻一种合适的解决方案，通过变通两者的管理模式达到管理要求的平衡点。这种管理模式往往是根据实际情况进行的必要调整，有时也是灵活的管控调整，尤其是相对规模比较大的和管理要求相对比较复杂的行业。通过上面的分析，不难看出实际实践过程中，完全的垂直管理和分布式管理，多出现在管理模式建设的初期，差别在建设的方式是从上而下还是从下而上；而到了建设的后期，都不约而同地转向了混合管理模式，但是这种转向有些是预先的设计，有些其实是向现实妥协的结果。图 12–5 为典型的职能体系中的混合型管理模式：

垂直管理的特点就是垂直性和相对独立性，业务运行基本上脱离同级行政管理框架，封闭在系统的体系内，而且特别强调业务的敏感性和保密性。分布式管理其管理分布在各个所属单位，混合型管理组织业务分为垂直管理业务和非垂直管理业务，不同业务具有其不同的特点。行业自身的管理模式不同，必然对各级终端安全管理建设造成影响，需要加以综合考虑。管理模式不是针对某个行业或者业务进行设计的，而是根据管理形态进行理论总结的，因此不存在固定的选择和搭配，任何行业和业务，甚至在不同的地域和不同的时间段，选择的管理模式都可能是不同的。通过管理特点和管理效果与实际管理要求相结合，选择适合的

管理模式，这也是混合型管理模式越来越广泛应用的主要原因。

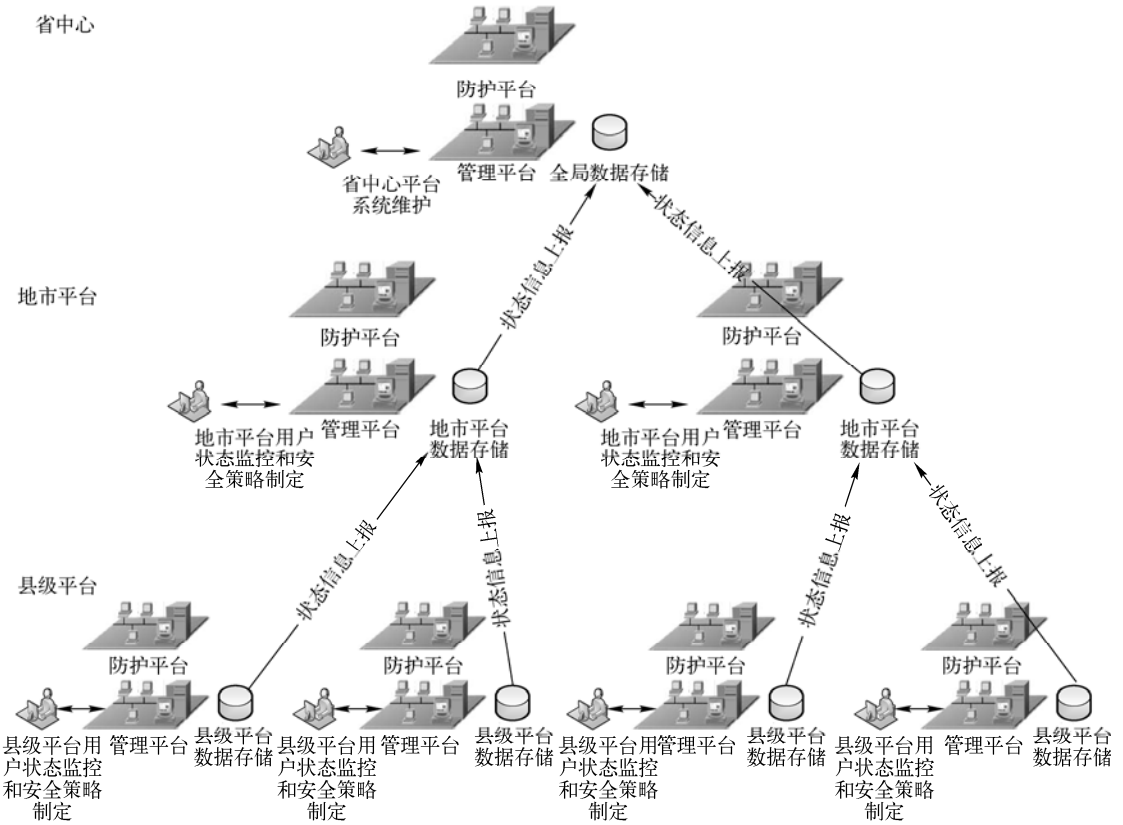

图 12-4　分布式管理示意图

12.3.6　混合管理实例

混合式管理业务，管理平台和防护平台部署在各级节点上。总部节点承担全局状态的展示，并制定全局策略，下级节点接受全局策略并根据本地管理需要进行本地策略的配置。

混合式式管理模型的终端管理系统，各级节点均部署管理平台和防护平台；监控数据和防护结果信息由各级管理平台分别进行存储和处理，并由中心平台统一展现；三级节点按预定周期定期向二级节点上报状态信息，二级节点按预定周期定期向中心节点上报状态信息；中心管理员完成全局终端的状态监控的和全局策略制定，二三级管理员完成本地终端的状态监控和本地策略的制定。

某省局终端防护项目为例，在省、省辖市、市辖县分别部署一级、二级、三级管理平台，分别由一级、二级管理平台对下级平台进行策略制定，通过安全管理平台将策略下发至各个终端计算机，在终端计算机使用过程中，一旦意图违背策略规定（如：试图使用被禁用的计算机接口、连接国际互联网等），报警信息将上传至上级管理中心，并逐级上报至位于省会城市的一级管理平台，一级管理中心进行综合报警分析、处理，一旦发现二级或三级平台出现网络断点，一级平台将自动接管断点下辖所有的管理服务器及终端，为终端分配应急响应策略，防止计算机终端发生脱离管控现象。

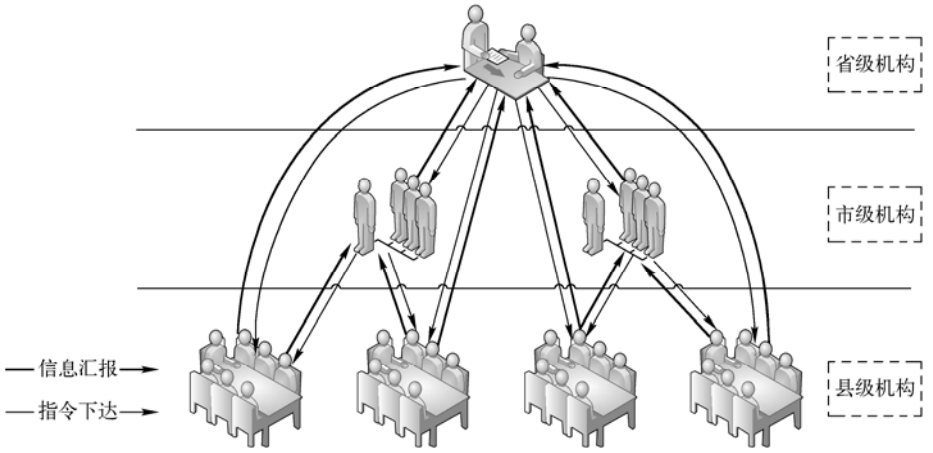

图 12-5　职能体系中的混合型结构管理模式

混合管理模式参见图 12-6。

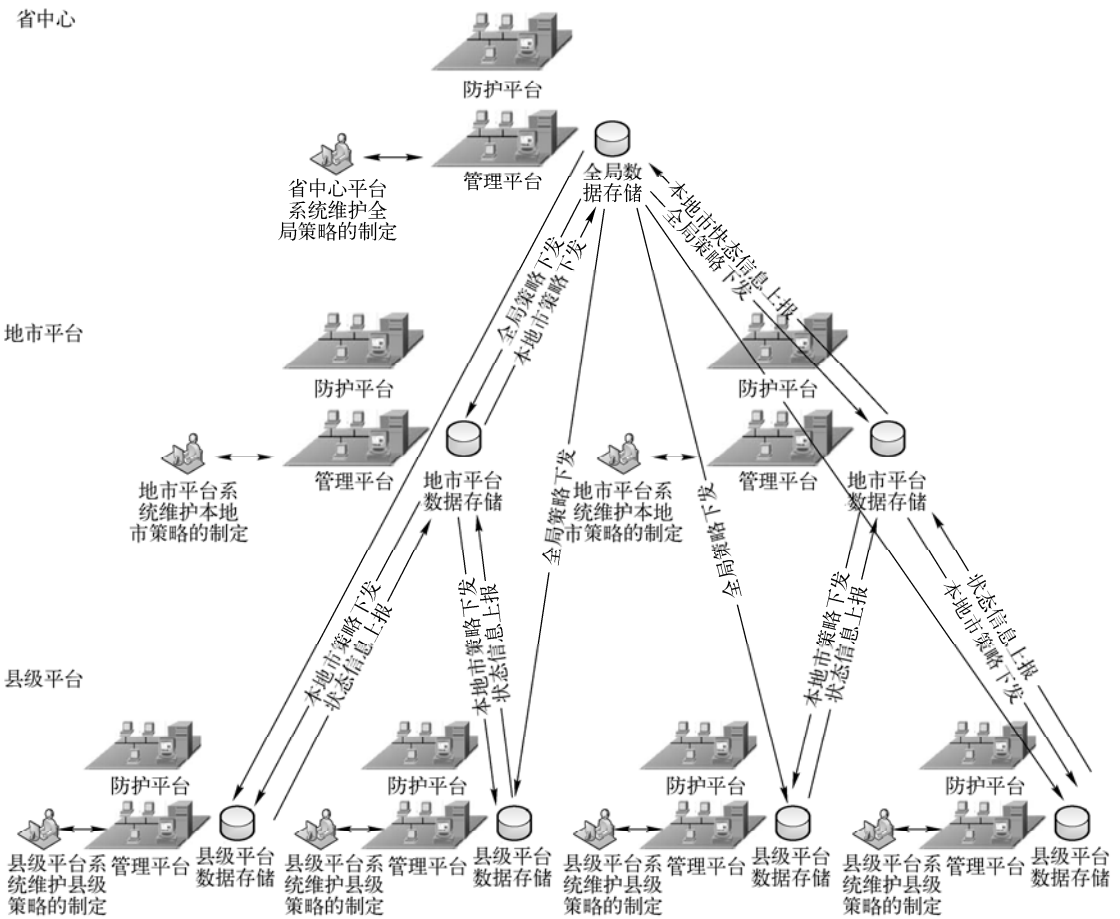

图 12-6　混合管理模式示意图

第13章 经典案例

13.1 项目背景

近年来，税务行业的信息化建设突飞猛进，信息化服务能力也有了更进一步的提升。在建设逐渐完善的业务系统过程中，伴随而来的是信息的安全、有效、合理的监管问题，怎么管理好与业务系统相伴的安全问题，是关系到整个税务行业信息化建设进一步发展的重要因素。

江苏省地税局作为税务行业信息化建设的领先者之一，近年在安全建设上取得了一系列重大突破，各地市征管系统顺利完成了由地级市集中处理模式向省级集中处理模式的转换。省级大集中系统的全面上线，标志着江苏地税税收管理最重要的省级一体化信息平台初步建成。随着征管系统的管理机构、工作模式、岗位职责、人员分工等变化，征管系统面临的安全风险也发生了变化。从以往各地的风险仅仅是局部影响，到现在的互动影响，各地问题相互交替，范围扩大，继而影响全省，出现了各地小风险会导致全局大风险，甚至可能演变成全省灾难性风险。为了能够系统地研究分析各地自身终端信息安全，从而达到保证省级大集中系统安全的目的，依据目前安全规范要求，更需要重点关注大集中后各地终端运行安全和信息安全管控，关注应急防范处置，解决安全认识不到位、技术手段的管控力度低、信息资料的定密不清、外来人员的监控不力等问题。而基于人工方式对出现的问题和风险进行排查和处置，已无法应对人手少、范围广、事件多的困难局面，更无法适应面对全省征管大集中新形势下的终端安全需要。

为解决出现的安全管理问题，江苏省地税局计划建立终端安全管理体系，建设终端安全防护平台和终端安全管理平台，逐步形成具有地税特色的功能成熟并能切实发挥作用的终端安全防护和管理平台，促进业务与安全的协调发展，满足省级大集中后全省信息安全有效管控的需要。

13.2 项目需求

江苏地税局在安全教育培训、技术防范、规章制度建立、安全检查评估及整改等方面做了大量的工作，在一定程度上提高了终端安全管理水平。但是，终端系统数量大、应用多，加之安全管理人员少，缺乏完备的技术手段，无法掌握终端安全风险状况，安全管理人员难以对真正紧急的事件进行快速响应。

因此，江苏地税局需要建立终端安全管理体系，通过完善相关管理制度、流程、规范组织机构职责、构建终端安全防护和安全管理平台实现以下终端安全管理功能：

✓ 实时对内网终端的软硬件、移动介质、接入访问、补丁更新、病毒防范等状况进行

统一监控。

- ✓ 实现对终端资产全生命周期的管理
- ✓ 采集终端安全相关安全事件和日志信息，进行整合和关联分析，提供终端安全态势展示
- ✓ 评估终端安全风险，实现终端全生命周期的安全风险管理
- ✓ 审计终端用户行为，重点实现对第三方接入终端的用户行为审计
- ✓ 产生安全事故和告警，提供自动告警和响应手段
- ✓ 接收并处理相关单位发来的终端相关的安全预警
- ✓ 生成各种安全报告并及时进行应急响应
- ✓ 进行终端相关安全知识管理
- ✓ 为相关部门的信息安全审计和考核提供技术手段和依据，实现全内网终端系统的安全集中监控、审计和应急响应，全面提升江苏地税内网终端安全管理能力，提升江苏地税整体信息安全保障能力。

终端安全防护和安全管理平台将是江苏地税信息安全管理团队非常必要的技术支撑系统之一。

13.3 项目目标

基于终端安全防护和安全管理平台的建设落实在江苏地税终端安全管理体系内，实现终端安全管理工作的信息化，为全省终端安全管理提供技术手段，提高终端安全管理、维护的水平，优化终端安全工作流程，缩短终端安全事件处理的响应处理时间，进而保障全省税务业务网络、支撑网络、业务系统以及整个信息化系统安全高效的运行，系统有如下的建设方向与目标。

- ✓ 搭建终端安全防护和安全管理平台，实现三级机构终端管理
- ✓ 建设终端安全管理体系的基本组织框架，确保终端安全管理相关工作的有效落实
- ✓ 推进内网终端安全管理标准化　对内网终端的安全访问、非法内联、非法外联、补丁更新、桌面管理、病毒防范等安全策略进行标准化管理
- ✓ 推进安全事件管理规范化　对安全事件的采集、汇总及处理规范化管理，规范安全事件的响应措施
- ✓ 终端安全策略框架和策略脚本建立，构建符合安全策略的基本运作流程，结合终端安全防护和管理平台实现内网终端安全维护管理流程化，对终端安全实施设备及使用的全生命周期管理、风险全过程管理和重要风险系统管理，并配合行政管理，实现终端安全管理流程化管理
- ✓ 终端安全态势可视化　对各类安全事件进行统一展现，从各种角度进行分析，针对不同的安全事件，提供安全预警分析
- ✓ 推进内网终端运行管理自动化　增强终端管理的自动化，事件响应自动化，安全告警管理和安全工单自动派发
- ✓ 实现内网终端运行管理指标化　对终端安全事件量化处理，实现终端运行监测点及相关考核指标标准化

13.4 建设方法

江苏地税安全管理平台建设从三个层面考虑：终端安全防护平台、终端安全管理平台、终端安全防护体系，如图 13-1 所示。

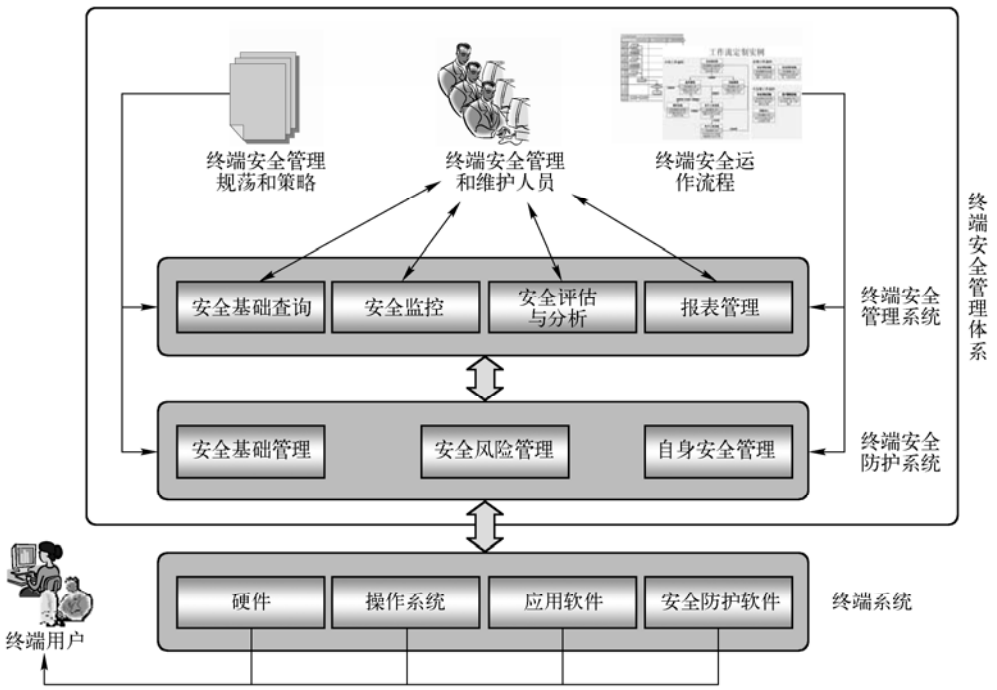

图 13-1　系统三层示意图

终端安全防护平台负责终端信息的采集和维护、终端安全风险的管理和防护、终端安全事件的监测和控制，为管理平台提供所需要的各类数据的采集和传输。实现各类安全事件的“事前防范、事中防御、事后处理”的立体化、流程化防御，是构建综合的、完整的内网终端安全防护体系的基础。

终端安全管理平台在终端安全防护平台提供的数据基础上，提供安全管理人员（系统管理员、安全主管）所需要的管理、监控、风险分析功能，各类管理报表的制作，同时满足省、市、县分布式环境下的行业安全管理要求，是构建完整的终端内网安全管理体系的技术支撑平台。

终端安全管理体系由终端安全组织体系、终端安全运作体系、终端安全策略体系和终端安全技术体系构成。其中终端安全技术体系主要由终端安全防护平台和终端安全管理平台构成。

终端安全防护平台是核心组件，是终端安全管理体系的基础部件。

终端安全管理平台在采取集中监控管理的方式，在更高层面上接收来自终端安全防护平台的安全事件和安全风险监测数据，负责对这些事件进行深层的分析、统计和关联，提供处理方法和建议。

防护平台和管理平台采用联合部署的方式，可以通过同机或者双机的方式进行部署，联

合实现终端安全风险管理的有效控制。由于江苏地税的行业特性和网络结构，决定了在不同的网络类型上采用不同的部署方式和部署要求。在部署方式上，同机部署适用于小型网络（区县级网络），双机部署适用于中型网络（县市级网络），多级联合部署适用于大型网络（省市级网络），因为不同的网络级别安全性保障要求也不同。

13.4.1 部署模型

从逻辑上总体架构包括 4 部分：两个业务平台（安全防护和安全管理）、一个业务支撑子系统、一个自身管理子系统，见图 13-2。

业务支撑子系统包括安全防护和安全管理业务所需的资产管理、认证授权、报表和工作流引擎。

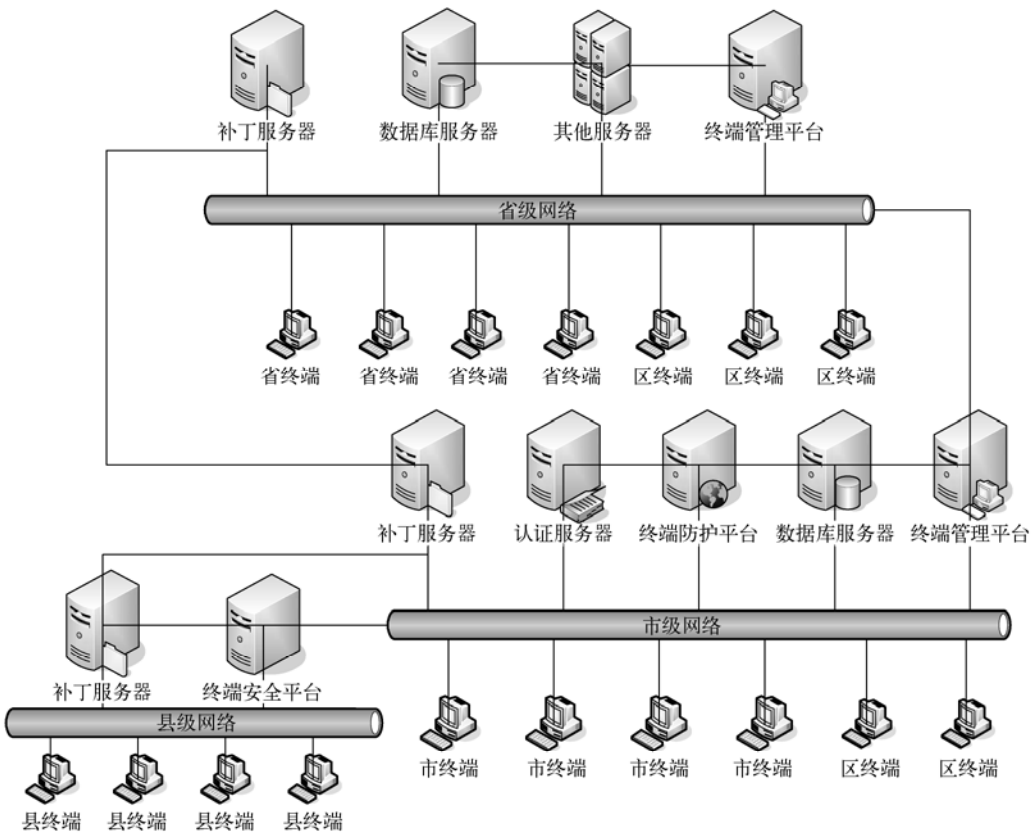

图 13-2 部署示意图

自身管理支撑子系统包括健康管理、存储管理、系统审计和多级管理。

小型网络（县级网络）可以采用同机部署方式，把安全防护平台和安全管理平台部署集成，解决少量终端的网络安全风险管理管控，同时部署补丁服务器。

中型网络（市级网络）采用多级联合部署方式，防护平台和管理平台分开，数据库服务器独立，针对网络情况选择指定方位部署认证服务器和补丁服务器。

大型网络（省级网络）兼容其他终端安全管理系统（省局采用第三方终端安全接入系

统），汇总下级防护和管理的数据，统一在安全管理平台进行分析、挖掘和统计，最终形成全局的管控。

13.4.2 部署方案

江苏省地税终端安全管理体系平台的总体结构如图所示。系统由 3 个层次组成，包括省局、地市局（园区）和县局（保税区）终端安全防护与安全管理平台。

3 个层次组成树形结构，从逻辑上看，省局中心节点只有 1 个，地市局节点共 15 个（其中包括 13 个地市局、省局自身管理和苏州园区），县节点共 68 个（其中包括 67 个县和 1 个张家港保税区）；各地市局节点连接到省局中心节点，各县节点连接到所属地市局节点（其中张家港保税区连接到苏州地税局节点），如图 13-3 所示。

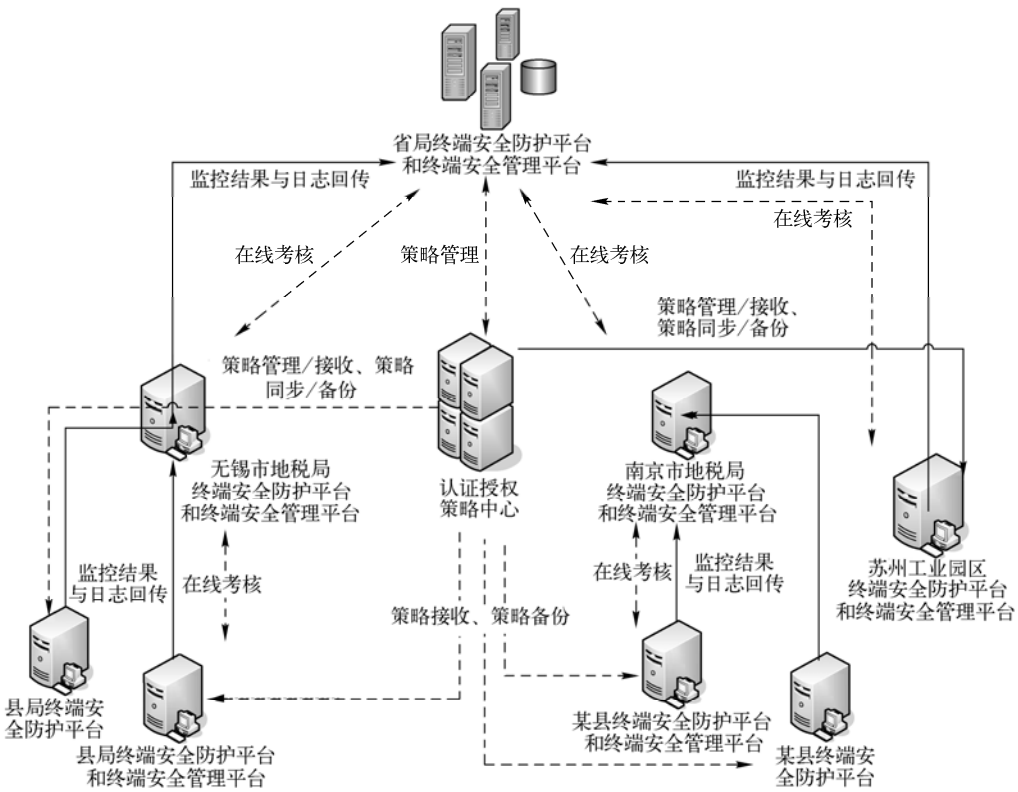

图 13-3　江苏省地税终端安全防护与管理系统总体部署示意图

省局中心节点：最顶层是省局终端安全防护与安全管理平台，其中省局终端安全防护平台管理全省统一安全策略，省局终端安全管理平台不仅基于省局终端安全防护平台管理省局内网终端，而且是全省终端安全管理平台的总中心，负责全局终端安全策略的管理和下发，接收全局上报信息，具有全省数据综合分析和与其他系统协同联动的功能。

地市局节点：负责本地市内终端的安全防护和安全管理工作，同时对所管辖的下级县局安全防护平台和安全管理平台有监管功能，具体包括接收省中心策略配置或进行本地配置，收集监控信息并产生事件并上报，同时具有数据分析的能力。

县局节点：负责本县内终端的安全防护和安全管理工作，包括接收省中心和地市局中心策略配置或进行本地配置，收集监控信息并产生事件并上报，同时具有一定的数据分析的能力。

认证授权策略中心：负责全网所有的认证、授权、策略信息，所有服务器的管理角色集中在一起，由省级配发区域管理权限，区域根据自身情况进行使用者信息的管理，并且对所有使用者信息进行区域化限定，既满足全网管理要求的统一性，又兼顾了本地管理的灵活性，统一性保障终端信息与使用者信息，以及风险信息在全网是一致的，灵活性保障管理角色和使用者具备本地管理属性。对所有节点的认证进行统一维护和备份，当任意节点的服务器出现故障，可以直接从认证中心恢复认证信息。对所有节点的策略信息进行集中管控，可以保障全省安全策略的统一，也支持全省策略的地区差异化，并且上级可以掌握下级差异化的管理详情。

所有节点都与它们的父节点、中心节点以及所有的子节点进行通信。中心节点用于统一安全策略，所有节点根据策略的性质配发适用的范围，父节点能够对所有的子节点进行管理和查询，包括策略应用情况、终端安装情况、补丁安装情况查询和报警信息等，如果下级有选配管理中心，还可以对其进行在线考核。每个节点的认证和策略都是本地配置，这些本地配置将只影响本地的终端安全防护，不影响上级或者平级部署的平台，同时由于这些信息都在中心节点备份，所以可以实时进行同步和恢复。

在管理上漫游属于特殊情况，分为两种：资产漫游和人员漫游。

人员漫游比较常见，在现有的部署方案中，人员漫游可以采用人员的管理链接方式，即人员的管理属性不变，还是由其直属上级进行管理，但是资源属性支持共享，即漫游地的上级也可以查看他的属性，并且可以对其的认证和授权信息进行分配。例如：张三从南京调动到盐城工作，他的工作申请在经过管理审批之后，除了南京的领导可以维持对其的管理，盐城的领导也可以看到张三的信息，并且可以分配资产到张三的名下，并且对其的安全策略进行对应配置，而张三可以继续使用自己在南京的认证信息使用盐城的网络，不需要盐城重新配发认证账号和登记人员信息。

资产漫游分为两种：借用和设备调拨。借用时，保持资产的原有信息借用到另外区域，终端在两地的信息都会汇总到上级，而上级进行统计和分析的时候，该终端发生的所有事件都是前后关联在一起的。设备调拨时，根据规定会结束原有的生命周期，重新按照流程入网。

13.4.3 行业管理策略

以江苏地税为例，为保障行业管理的一致性，兼顾各地网络安全管理的灵活性，对全局管理的策略进行了如下的设计：

1）省级中心统一配发安全策略，各地根据实际情况选择策略的应用范围，各地会定时上报统一策略的应用范围和应用状态。

2）省级中心分析全省的安全事件，同时可以根据分析结果下发安全预警和告警。

3）省级中心可以查看全省的管理日志，按区域进行管理工作评估（KPI 考核）。

4）各节点可以转发上级的安全策略到下级服务器，也可以根据本地情况对于本地的特殊终端，在一定范围内采用本地安全策略，在保持整体安全基本一致的情况下，灵活处理本

地的部分特殊业务要求。

5）各节点会自动上传上级策略产生的报警，同时上报管理日志。

13.5 建设效果

江苏地税项目按照终端安全防护平台、终端安全管理平台、终端安全防护体系三层结构模型的建设，达到了终端风险可管、可控，安全状态可视的效果。

实现内网终端的“全程全网”安全状态可视化（Visualization）。体现在三级机构的内网终端系统相关安全状态信息可以非常直观地可视化监视，安全策略执行情况可感可知，有能力进行事后的分析和追查，提供可以“呈堂”的证据。

内网终端的安全风险处于可管理、可控制状态下。对内网终端系统安全风险的不间断的评估和控制措施调整，使得全内网终端的整体安全状况和风险情况以定性或半定量的形式及时展现出来。帮助安全管理层和终端安全管理维护人员清晰、准确、及时地了解终端所处的风险状况。

使全网的安全保障能力处于国内领先地位。在病毒爆发、违规操作以及其他不可预见的威胁出现时，内网终端安全防护和管理系统有能力及时发现，并迅速进行响应和恢复，保障业务工作的正常运行。

保证内网终端相关业务活动在网络安全方面的法律法规符合性。规范、管理和审计内网终端安全状态和用户的行为，在整个体系中将建立法律法规符合性审核制度，保证终端系统安全管理工作的有效性及终端系统合法合规的使用。

附　　录

终端安全风险分析报告

附录 A　终端安全基础风险

附录 B　终端安全运行风险

附录 C　终端安全信息风险

附录 A　终端安全基础风险

终端安全基础风险（BR:Basic Risk）是终端自身存在风险，包括 BIOS 等硬件配置隐含的风险，也包含软件配置的风险，例如操作系统本身存在的漏洞和用户口令安全，杀毒软件和应用软件的安装使用风险，终端对于补丁和软件管理的风险，以及网络相关参数配置和网络防护措施的管理风险，终端自身包含的外设、端口、注册表、驱动、操作系统等的使用风险。

终端安全基础风险是针对终端计算机的基础情况进行管理，此类管理不涉及各类具体安全风险事件，强调终端安全基础的安全性，侧重于自身安全的加固和风险的预防，为系统的基础管理类。

终端安全基础风险管理（防护）系统的所有安全基础管理功能类可以划分为自身安全风险、环境安全风险、外设安全风险，具体如图 A-1 所示。

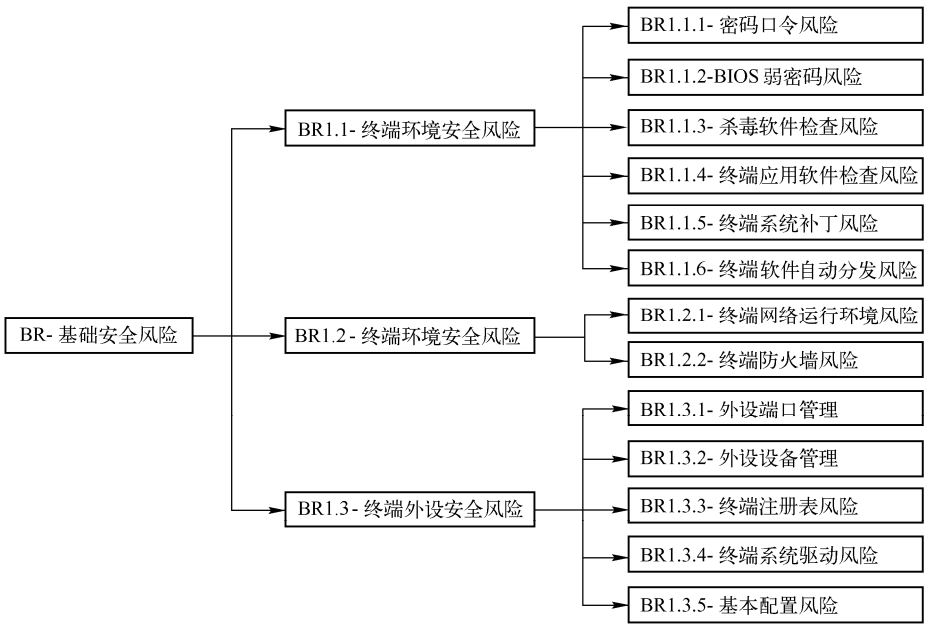

图 A-1

A.1　终端自身安全风险（BR1.1）

A.1.1　密码口令风险（18 个风险点）

1．风险分析

（1）风险描述

密码口令风险包括终端代理准入账号密码、终端安全管理系统密码和操作系统密码。密

码口令风险主要表现为密码复杂度不够，密码没有定期修改，屏幕没有设置密码保护等，由此带来口令被轻易窃取和破解，导致用户账户被冒用，引起终端安全中的信息扩散和信息外泄、被攻击等不可控风险。

简单密码容易被破解和猜测，轻易被获取用户身份，常见情况有：

1）密码与用户名类似或者关联。

2）密码为字母或者数字的单一组合。

3）密码是常用词汇的拼写等。

4）密码是固定电话和手机号码。

口令的长度不足，容易使用工具在短时间之内以穷举方式破解。

口令的修改周期过长，或者没有建立密码修改周期管理制度，增加了密码破解的风险。

屏幕保护设置和限制口令解除的缺失，容易产生他人冒用身份，因为终端用户已经进行了身份验证，但是因为临时离开终端，而他人可以在这个时间冒用身份，获取信息，或者执行非法操作，引发信息安全的风险。

（2）相关风险点

操作系统终端密码口令风险点见列表 A-1。

表 A-1

	序　号	风　险　点	风 险 属 性	隐患/风险
密码口令	1	密码复杂性不符合要求	原生风险	隐患
	2	密码复杂性不符合要求的，没有提示终端用户修改	衍生风险	隐患
	3	密码复杂性不符合要求的，审计信息没有上报管理员	衍生风险	风险
	4	用户并未按照密码复杂性不符合要求的提示信息进行修改	残余风险	隐患
	5	密码最小长度不符合要求	原生风险	隐患
	6	密码最小长度不符合要求的，没有提示终端用户修改	衍生风险	隐患
	7	密码最小长度不符合要求的，审计信息没有上报管理员	衍生风险	风险
	8	用户并未按照密码最小长度不符合要求提示信息进行修改	残余风险	隐患
	9	密码最长存留周期不符合要求	原生风险	隐患
	10	密码最长存留周期不符合要求的，没有提示终端用户修改	衍生风险	隐患
	11	密码最长存留周期不符合要求的，审计信息没有上报管理员	衍生风险	隐患
	12	用户并未按照密码最长存留周期要求提示信息进行修改	残余风险	隐患
	13	终端未设置屏保、屏保密码	原生风险	隐患
	14	终端未设置屏保、屏保密码的信息未提示终端用户进行修改	衍生风险	隐患
	15	终端未设置屏保、屏保密码的审计信息未上报管理员	衍生风险	隐患
	16	用户并未按照提示对终端设置屏保和屏保密码	残余风险	隐患
	17	因工作或维修需要，终端用户将密码告知他人	原生风险	风险
	18	因工作或维修需要，终端用户将密码告知他人。在相关工作完成后未及时修改密码	衍生风险	风险

以下将分别从资产使用生命周期、资产使用人员、资产承载的信息和合规性 4 个方面对以上 18 个风险点进行详细阐述，包括风险发生的阶段、风险检测的条件和风险损害等。

（a）基于资产使用生命周期分析

该类风险涉及入网前、运行和维护阶段，入网前由于终端资产不包含敏感信息和数据，密码口令风险较低。入网后，由于运行过程中涉及敏感信息和生产数据，如果不对终端密码

口令风险进行有效管控，导致的损失较大，风险较高。终端资产进入维护阶段后，通常为了维护需要，需将终端资产的密码口令交给维护人员。如果直接将终端资产的密码交给维护人员且事后不及时进行更改，就存在密码外泄，系统被非法入侵和使用的风险。在报废阶段，终端不能使用，此时不存在该类风险。

风险点（1-12）：密码复杂性、长度、留存周期不符合要求，这些风险在入网前，因为终端资产不包含敏感信息和数据，风险较低；入网后，密码复杂性不符合要求，密码泄漏会导致终端的数据泄漏，风险较高。

风险点（13-16）：未按照要求设置屏保，在终端未入网前，只会影响单个终端，对单个终端的信息和数据造成泄漏，风险较低；入网后，如果是核心主机，不是终端的操作用户可以进入终端，对终端进行操作，会对终端的信息和数据造成泄漏，风险高。

风险点（17-18）：未按照规定告知密码，告知后未及时更改密码，主要发生在终端的维护阶段。必须严格制度，要求对告知密码的操作进行详细记录，并在告知密码维护工作完成后，及时更改密码，并进行备案。

（b）与信息安全关系

密码口令风险涉及在线信息安全风险和存储信息风险。

风险点（1-8）：如果终端资产存在弱口令，包括口令复杂度不够、密码长度不够等，容易造成口令被破解，系统被非法入侵，导致存储在计算机中的信息外泄。如果弱口令被破解，别有用心的人利用破解的用户名和密码对业务服务器进行操作，进而对在线的信息篡改或窃取，下载业务服务器的敏感信息，可能造成严重社会恶劣影响以及其他不可预测的风险。

风险点（9-12）：密码留存周期不符合要求的，密码长时间不更改，导致密码泄漏，该风险可能造成终端的存储信息被篡改或泄漏，如果是泄漏的密码被利用，终端的在线信息也面临被下载、泄漏、篡改和外泄的风险。

风险点（13-16）：如果屏幕不设置屏保和密码，有可能被别人偷窥到一些敏感信息或者被人通过屏幕拍照等方式截取重要信息，造成信息外泄。存储信息也容易在登录用户离开电脑时，因为没有屏保的密码，被非授权人员轻易获取导致外泄。

风险点 17-18）：未按照规定告知他人密码，告知后未及时更改的风险，对存储信息来说，密码信息泄漏，会造成存储信息外泄；如果告知后未及时更改，非法用户利用先前的密码信息进入终端，并进行操作，会造成在线信息被篡改的风险。

（c）基于资产使用人分析

风险点 1-12）：任何岗位角色都可能存在密码口令不按规定使用的问题。因此，这些风险与内部人员相关时，高级管理岗位（如高层领导）的终端资产存在以上风险，由于其终端含有企业核心信息和涉密信息，风险级别高。当部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员的终端存在以上风险，由于该类终端对业务支撑非常关键，且一般包含关键业务信息，风险级别较高。当生产人员、办公人员等终端存在该风险，尽管该类终端支持业务和对正常运营起保障作用，但因不涉及重要信息和关键业务，风险为中。与临时人员有关时，该类风险发生在辅助人员岗位，如食堂、车队、绿化等人员，则该类终端一般不涉及业务、不包含敏感信息，风险为低。与外来人员有关时，因外来人员不涉及组织内部信息和业务系统。此类人员终端发生该风险时，对于组织的影响很小，风险为低。

风险点 13-16）：任何岗位角色都可能存在不按规定设置屏保的问题。这些风险与内部人

员有关，高级管理岗位和部门主管等人员必须严格对终端设置屏保，否则其重要终端因为不设置屏保，容易造成信息泄漏或篡改的风险，风险较高；临时人员和外来人员的终端不涉及核心业务和敏感数据，风险较低。

风险点 17-18）：这两个风险点主要涉及的是内部人员，如果在维修过程中需要使用密码，应尽量采取陪同操作的方式，避免将密码告知他人。如果不得不采取告知密码的方式，必须将密码告知人的使用时间和使用操作记录在案，便于事后问题追踪，同时在他人使用密码后，及时修改密码。

（d）合规性要求

合规性要求详见表 A-2。

表 A-2

序　号	安 全 类	等级保护（三级）要求	符 合 程 度
1	主机安全	7.1.3.1 身份鉴别（S3） b) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换 c) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施 d) 当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听 e) 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性	符合

基于以上风险点分析，如采取相关技术和管理手段管控 18 个风险点，终端密码口令部分管理将符合等级保护相关要求。

相关技术和管理的风险管控措施参见以下阐述。

2．风险管控

每类风险在管控过程中，针对风险的事前、事中和事后 3 种状态进行监控，做到事前预防，事中控制、事后审计追查。下面的风险管控处理流程，尽量从事前、事中和事后 3 方面对风险进行管控。

风险点（1-4）：密码复杂度不符合要求的管理控制流程

（1）事前处置

1）制定操作系统密码管理制度，包括密码口令不能为空、密码复杂度、密码最小长度、密码更新周期。如强行规定密码复杂度达到 8 个以上字符，至少包含大小写字母、数字和特殊符号三种类型字符等。

2）制定终端屏幕管理保护要求，包括必须设置屏保、设置屏保最长多久保护、恢复时需要用户密码解开屏锁。

（2）事中处置

发现弱口令包括密码复杂性不够、长度不够、没有按期修改、未设置屏幕保护密码等，对该用户首先在终端进行提示，并将该信息上报管理中心，对于逾期不修改的用户，通报批评，行政扣分，仍然不改正的用户，下发断网策略。具体措施如下：

1）修改密码时，如果密码复杂度不符合要求，则提示密码的复杂度，如果不符合要求，则提示用户修改或者无法保存新的密码。

2）修改密码时，如果密码长度不符合要求，则提示密码的长度，如果不符合要求，则

提示用户修改或者无法保存新的密码。

3）密码超期使用，提示密码需要修改，如果不修改密码，则发送报警到防护平台，并且记录日志用于审计。

4）屏幕保护的设置不符合要求，提示重新配置屏幕保护设置，如果不修改配置，则发送报警到防护平台，并且记录日志用于后续跟踪。

（3）事后处置

1）对操作系统密码违规设置查询，了解内网终端操作系统密码设置安全性，了解不安全终端密码的台数，可以提醒修正。

2）对于该类风险，保留日志记录，如果出现安全事件，则可以追溯责任人。

控制流程详见图 A–2。

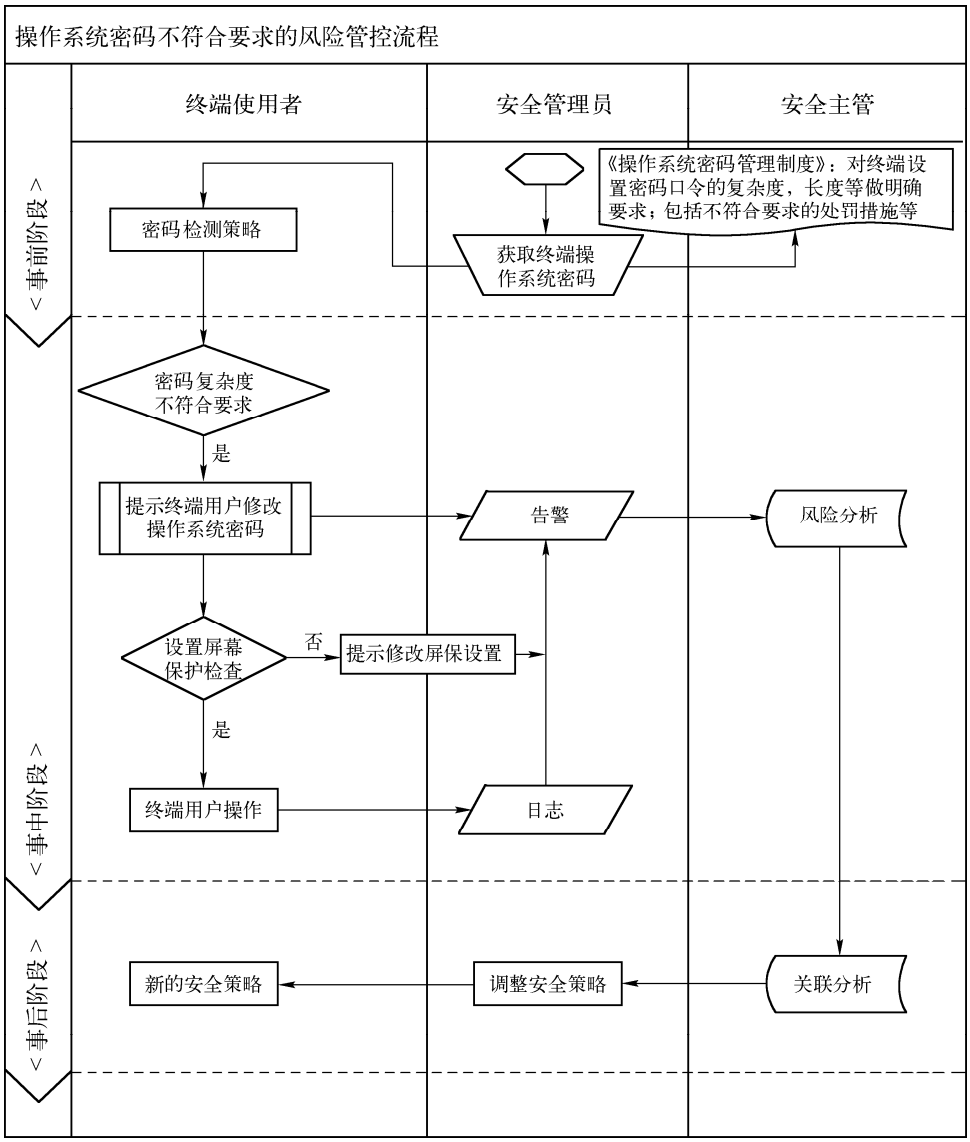

图　A–2

风险点（5-8）：密码长度不符合要求的管理控制流程，与风险点（1-4）类似，检测的主要内容是密码长度，其余管控过程类似。

风险点（9-12）：密码留存周期不符合要求的管理控制流程，与风险点（1-4）类似，检测的主要内容是密码留存周期，其余管控过程类似。

风险点（13-16）：终端没有按规定设置屏保的管理控制流程，与风险点（1-4）类似，检测的主要内容是屏保的有无和屏保密码的复杂度，其余管控过程类似。

风险点（17-18）：必须在制度上严格规定，不允许将密码随意告诉他人。告知密码随意告知别人的风险，同时提醒用户，因自己密码泄漏造成的风险将由个人承担。

3．残余风险处理

在对终端的密码和口令风险管理工作中存在以下几种情况：

1）针对密码口令复杂度、长度和定期修改的提示并未被终端用户执行。

2）其审计信息报给管理员后，也未得到及时的关注和处理。

3）系统因工作或维修需要将口令直接交由他人，事后又未及时修改。

因此，尽管部署了完备的检测和管理技术手段，却会因人的操作习惯和安全意识造成密码口令被破解的风险继续存在。

针对该问题，建议增加以下几方面工作：

1）加强安全意识培训和教育，使终端用户意识到密码口令的重要性，督促其养成定期修改密码和主机信息密码保护的好习惯。

2）提供制度保障，要求因工作或维护需要密码的统一处理方法，如不能继续使用个人密码，应该更换成维护密码，重新领用后再换回个人密码等。

3）建立定期检查和整改制度，定期对组织内终端的密码口令状况进行集中检查，集中整改。

4）设立针对密码口令相关的考核管理措施，将该项工作作为终端使用人、终端所有单位安全工作考评中的考核指标。

4．技术管控中存在的问题和对策

由于 Windows 密码都采用加密保存，在开机阶段不能主动探测到密码复杂度，建议最好采用专业密码口令探测器扫描，另外，从密码保护和法律的角度，不建议采用暴力破解的工具。

5．风险控制效果

能保护终端操作系统的口令安全，实现口令的安全管理，防范终端在正常使用情况下的信息扩散和信息外泄风险，杜绝终端用户的身份被冒用的风险。

A.1.2 BIOS 弱密码风险（11 个风险点）

1．风险分析

（1）风险描述

设置 BIOS 密码可以为终端带来一定程度的保护。设置 BIOS 密码的目的有两个：一是防止别人擅自更改终端的 BIOS 设置；二是防止别人非法进入终端（包括进入操作系统等）。

合理利用 BIOS 密码可以给终端的安全带来很大的益处。需要结合不同的终端进行 BIOS 密码的设置规定。

公用的计算机，比如只作为查询作用的终端，一般会采取 BIOS 密码不公开的方式，此时允许他人进入操作系统使用计算机，但不允许他人进入 BIOS 画面随意修改 BIOS 设置，以保护计算的正常运行。

比较重要的个人终端，如果不允许其他人使用，则必须设置 BIOS 密码不公开，此时别人无法进入 BIOS 设置，也无法进入操作系统。

个人终端，允许指定的几个人使用，可以设置 BIOS 密码，并将密码告知指定的使用人，但需要保留“管理员密码”，日后可以根据需要取消或修改掉 BIOS 密码，这样，终端 BIOS 主动权掌握在高级管理员手中。

BIOS 密码设置为空或者较弱，很容易被别人猜中，从而控制硬件启动顺序，主机很可能被别人控制不能操作，使而失去可用性。也可能被别人利用软盘、光盘和 U 盘等外部引导方式或远程启动方式控制电脑。由于现在 CPU 多提供智能控制功能，因此通过 BIOS 就可以开启远程控制，并且可以在操作系统启动之前进行控制，实现操作系统的修复和重新安装，功能上方便了，但是安全风险也增加了。

（2）相关风险点

终端 BIOS 弱密码风险点见表 A-3。

表 A-3

	序　号	风　险　点	风 险 属 性	隐患/风险
密码口令	1	BIOS 密码强度设置不符合要求	原生风险	隐患
	2	BIOS 密码强度不符合要求的，没有提示终端用户修改	原生风险	隐患
	3	BIOS 密码强度不符合要求的，审计信息没有上报管理员	原生风险	风险
	4	BIOS 密码强度不符合要求，没有产生告警信息	原生风险	隐患
	5	BIOS 密码强度不符合要求，提示用户修改，用户修改后自己忘记 BIOS 密码	次生风险	风险
	6	BIOS 密码设置为空	原生风险	隐患
	7	BIOS 密码设置为空没有提示终端用户	原生风险	隐患
	8	BIOS 密码设置为空没有产生告警信息	原生风险	风险
	9	BIOS 密码设置为空，审计信息没有上报管理员	原生风险	风险
	10	BIOS 密码设置为空，提示终端用户修改，用户修改后自己忘记 BIOS 密码	次生风险	风险
	11	采取技术措施获取终端的 BIOS 密码强度情况，但不同厂商的主板不尽相同，获取的 BIOS 密码强度情况不精确	残余风险	隐患

（a）基于资产使用生命周期分析

该类风险涉及入网、运行阶段。

风险点（1-11）：终端 BIOS 密码不设置或者为空、较弱都极有可能被轻易获得，从而终端被控制利用，导致终端无法启动，不可用，设置被通过 U 盘等其他虚拟驱动登录方式或者远程控制的方式登录终端主机，造成终端数据信息被复制、外泄等风险。

（b）与信息安全关系

密码口令风险涉及在线信息安全风险和存储信息风险。

由于 BIOS 弱口令的存在，使得 BIOS 口令容易被破解。其损害有：引起终端的启动顺

序变化，使用外接系统引导，绕开终端的监控和防护，直接读取终端的文件信息，导致存储在计算机中的信息外泄；可以利用主动控制等远程操作方式监视主机与业务服务器的连接，下载服务中的敏感信息，引发信息外泄风险。

（c）基于资产使用人分析

BIOS 风险对所有人均有可能发生，但该类风险主要还是在内部人员中发生，当内部别有企图的人员接近终端的时候，很容易进入 BIOS，重新设置密码，导致操作系统不能正常启动，或者通过设置硬件启动顺序，通过 USB 中虚拟操作系统启动，导致终端被控制，信息外泄；其他人员的终端往往由于制度和规范保护，经过统一处理，可以有效降低该类风险。

（d）合规性要求

合规性要求详见表 A-4。

表 A-4

序　号	安 全 类	等级保护（三级）要求	符 合 程 度
1		等级保护中没有明确的对 BIOS 密码的要求	

2．风险管控

风险点（1-5）：BIOS 密码强度不符合要求的风险管控流程。

1）事前处置　所有终端领用时初始化 BIOS 密码，对于拥有修改 BIOS 权限的使用者，制定 BIOS 密码管理要求，包括密码口令不能为空、密码复杂度、密码最小长度、密码更新周期。如强行规定密码复杂度达到 8 个以上字符，包含大小写、数字、符号等。

2）事中处置　定期检查终端资产的 BIOS 密码设置情况。

发现 BIOS 密码为空时，警告终端用户，管理员记录违规情况。

BIOS 密码复杂度不符合要求，警告终端用户，管理员记录违规情况。

如果经提醒不修改密码，则记录日志用于后期审计和行政处罚。

3）事后处置　管理员保留违规记录，如果出现安全事件，可以追溯责任人，逾期不修改的，结合行政扣分管理措施等。

控制流程详见图 A-3。

风险点（5-10）：管控流程与（1-5）类似，主要是判断 BIOS 密码是否为空。

风险点（11）：残余风险。BIOS 密码由于属于底层主板厂商设置，和不同厂商主板特性有关系，还没有有效的技术手段能探测到不同主板厂商的 BIOS 密码设置复杂度。

3．残余风险处理

BIOS 弱密码的残余风险与操作系统密码口令的残余风险类似，其处理措施可一并考虑。针对该问题，建议增加以下几方面工作。

1）加强安全意识培训和教育，使终端用户意识到密码口令的重要性，督促其按照规定设置 BIOS 密码。

2）提供制度保障，规定维护时使用 BIOS 密码的统一处理方法，如在维护时不能继续使用原 BIOS 密码，应该更换成维护密码，在重新领用后再更换回原终端 BIOS 密码等。

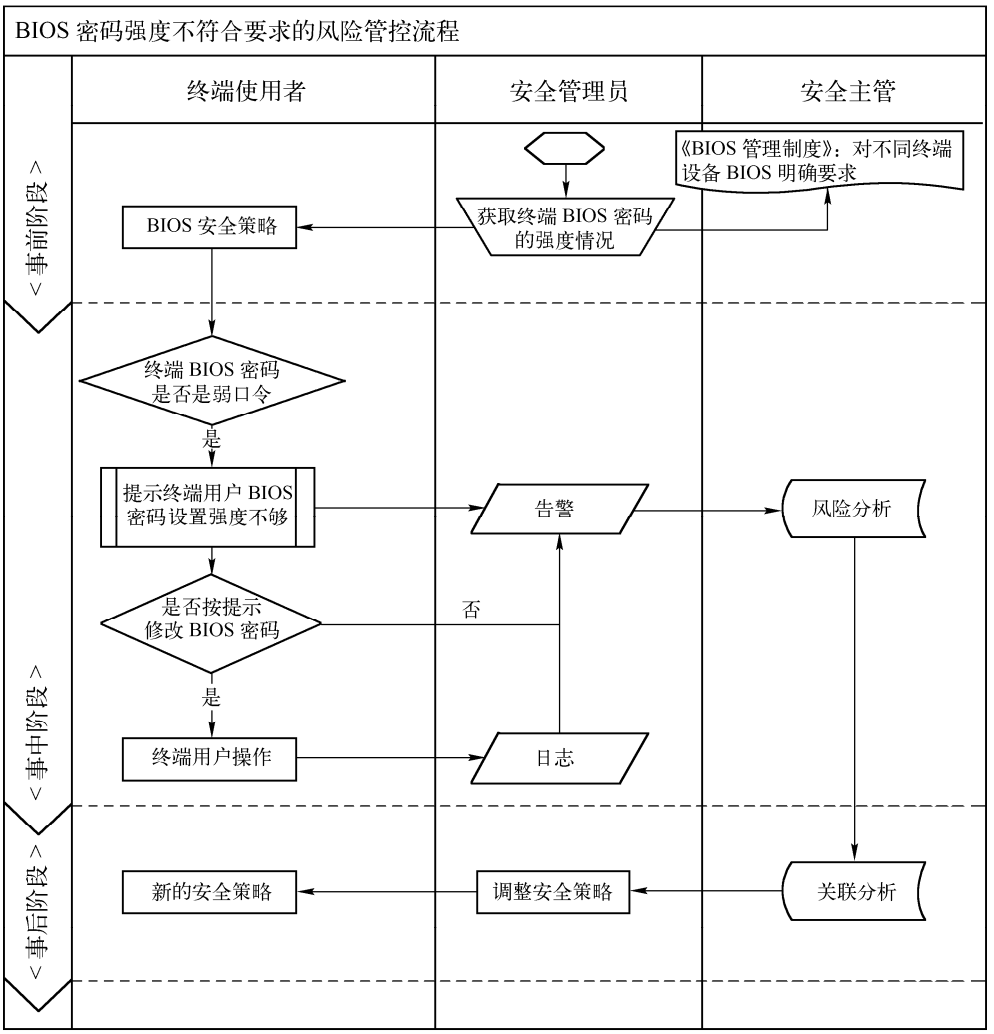

图 A-3

3）建立定期检查和整改制度，定期对组织内终端的 BIOS 密码状况进行集中检查，集中整改。

4）设立针对密码的考核管理措施，将该项工作作为终端使用人、终端所有单位安全工作考评中的考核指标之一。

4．风险控制效果

保护终端 BIOS 的口令安全，实现口令的安全管理，防范终端在正常使用过程中通过底层获得终端控制权限，防范终端被从底层 BIOS 泄密和破坏的风险。

A.1.3 杀毒软件检查风险（10 个风险点）

1．风险分析

（1）风险描述

1）终端不安装防病毒软件，不能对病毒进行查杀，终端的数据流面临不可控的风险，

终端上运行的病毒不能及时查杀，终端安全性得不到保证，进而威胁整个网络系统。

2）终端安装了防病毒软件后，如果不及时获取防病毒软件的新版本和病毒库等信息，就不能对防病毒软件进行有效的升级，进而影响防病毒软件的正常使用。安装的防病毒软件如果不按照要求启用，相当于没有安装防病毒软件，会导致病毒事件的发生。安装的防病毒软件还需要验证是否具备查杀病毒的功能，如果不能，需要重新查验防病毒的相关配置信息。

（2）相关风险点

终端杀毒软件检查风险见表 A-5。

表 A-5

	序 号	风 险 点	风险属性	隐患/风险
杀毒软件检查风险	1	终端没有安装防病毒软件	原生风险	隐患
	2	终端未安装防病毒软件，没有告警信息	次生风险	隐患
	3	终端安装防病毒软件后，防病毒软件的型号、版本、病毒库信息不能发现	原生风险	隐患
	4	终端安装防病毒软件后，和系统冲突	原生风险	风险
	5	终端防病毒软件程序和病毒库不能升级到最新状态	原生风险	隐患
	6	终端防病毒程序处于未运行状态	原生风险	隐患
	7	终端防病毒程序处于未运行状态后不能启动防病毒程序	次生风险	风险
	8	防病毒程序处于未运行状态，没有告警信息	次生风险	风险
	9	管理员不能远程调用其杀毒软件对发现的病毒进行查杀	次生风险	风险
	10	终端杀毒软件不能查杀病毒	次生风险	风险

（a）基于资产使用生命周期分析

资产使用生命周期包含入网前、运行阶段、维修阶段、报废阶段，终端防病毒软件检测风险在资产使用生命周期的体现如下。

风险点（1-2）：如果终端未安装防病毒软件就接入网络，可能会导致病毒在网络蔓延，如果没有在入网前进行控制，将会带来很大的风险；在运行阶段，如果终端都安装了防病毒软件并且正确使用，将不会带来更大的风险，如果没有做好控制措施，会带来更大的安全风险。

风险点（3-10）：出现在系统运行阶段，如果不能发现防病毒软件的版本病毒库等信息，就不能对防病毒软件进行有效的升级，进而影响防病毒软件的正常使用。如果防病毒软件停止启动，而又不能恢复启动，就相当于没有安装防病毒软件，终端会感染病毒、木马等恶意程序，导致终端运行异常、终端宕机、网络异常、甚至引起网络瘫痪的风险，导致的损失较大，风险较高。

（b）相关信息风险

ⓐ 在线信息风险

风险点（1-2）：防病毒软件能对终端运行的病毒进行查杀，未安装防病毒软件的终端容易被病毒木马等感染，进而导致在线信息相关系统不能正常工作，严重的还能引起网络瘫痪。

风险点（3-10）：防病毒软件的正常运行，与程序版本和病毒库版本的实际情况密切相关，在线信息与这些风险关系更为密切，如果不及时更新防病毒软件程序版本和病毒库，可能无法有效查杀新出现的病毒。防病毒软件不正常启用和运行，病毒可能感染终端，而导致在线信息相关系统不能正常工作，甚至引起网络瘫痪。

ⓑ 存储信息风险

风险点（1-10）：该风险可能导致终端上存储的信息丢失或者被破坏，或者破坏业务系统导致存储的信息无法读取，更严重的影响操作系统或者磁盘系统，导致存储信息的环境异常。

（c）基于资产使用人分析

ⓐ 内部人员

风险点（1-10）：该类风险发生在内部人员高级管理岗位（如区域负责人等高层领导），由于其终端含有企业核心信息和涉密信息，风险非常高。该类风险发生在地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，由于该类终端对业务支撑非常关键，且一般包含关键业务信息，风险较高。如果该类风险发生在开发人员、研发人员等，则由于该类终端支持业务和对正常运营起保障作用，相当重要，风险为中。

ⓑ 临时人员

风险点（1-10）：如果该类风险发生在辅助人员岗位（如食堂、车队、绿化等人员），则该类终端一般不涉及业务、不包含敏感信息，风险为低，如果临时人员的用的终端接入网络系统的话，该类风险等级就会很高，因为临时人员的终端病毒控制不好，可能会在网络内爆发病毒。

ⓒ 外来人员：

风险点（1-10）：该风险一般不涉及此类人员，但是如果外来人员有终端接入到网络，风险等级就会很高，因为临时人员的终端病毒控制不好，可能会在网络内爆发病毒。

（d）合规性要求见表 A-6。

表 A-6

序　号	安 全 类	等级保护（三级）要求	符 合 程 度
1	主机安全	7.1.3.6 恶意代码防范（G3） a) 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库 b) 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库 c) 应支持防恶意代码的统一管理	符合
2	系统运维管理	7.2.5.8 恶意代码防范管理（G3） a) 应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查 b) 应指定专人对网络和主机进行恶意代码检测并保存检测记录 c) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定 d) 应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报	符合

2．风险控制

（1）风险点（1-2）

事前处置：终端在接入系统前，必须安装终端防病毒软件，并且满足软件版本和病毒库的检查要求，然后才能接入到网络使用；没有安装防病毒的软件的终端或者软件版本和病毒库版本不符合检查要求不允许接入到网络，并通知管理人员安装防病毒软件。

事中处置：在运行中发现终端未安装防病毒软件（包含入网之前已经安装但是入网之后卸载或者停用），马上将该终端断开网络访问，并上报管理人员，恢复后再接入网络。

事后处置：对于该类风险，保留日志记录，如果出现安全事件，可以追溯责任人。

控制流程见图 A-4。

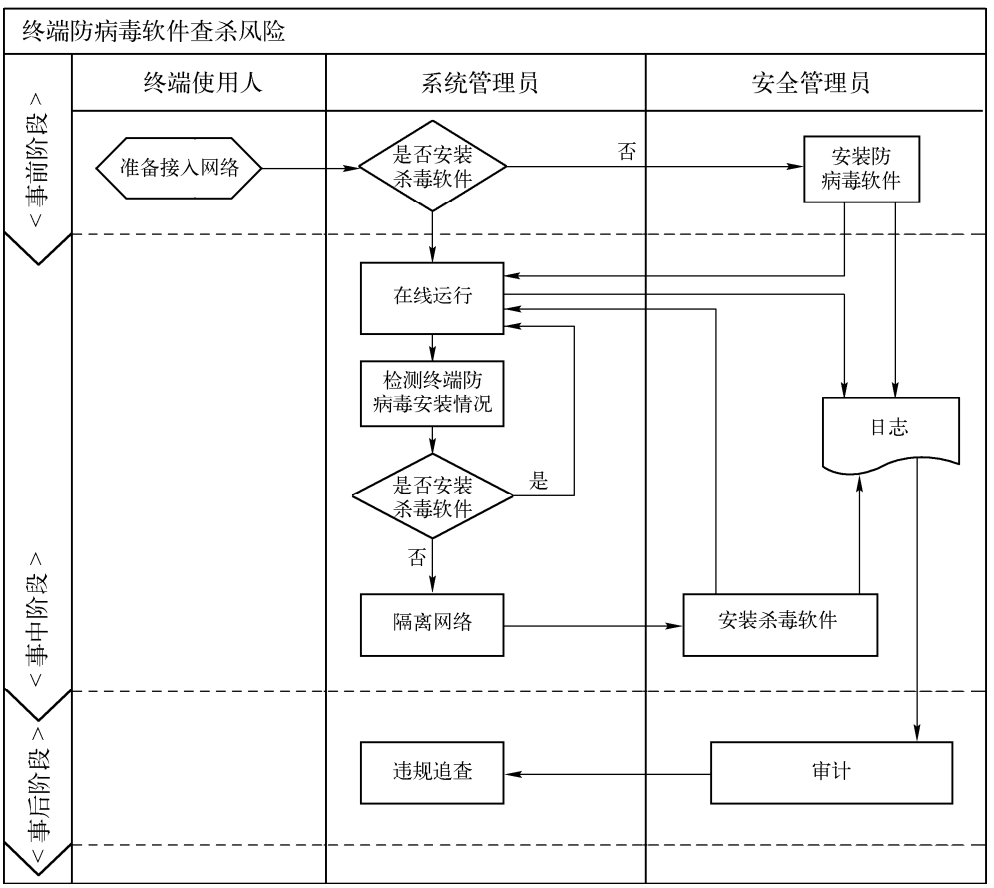

图 A-4

（2）风险点（3-9）

事前处置：终端入网前先统一规范防病毒的软件版本和病毒库升级要求，经过安全检查验证符合规范的终端才能接入网络。

事中处置：接入网络后，如果发现终端未保持一直启用防病毒程序，则立即禁止访问网络，待恢复启用后再准入网络；规定病毒检查策略，统一按照规范进行病毒的处理；同时，病毒库要保持定时更新，若未按照规范更新病毒库，则应提醒终端使用者，提醒多次未处理

的终端限制网络使用，隔离到受限区域防止影响整个网络的安全。

事后处置：对于该类风险，保留日志记录，如果出现安全事件，可以追溯责任人。

控制流程见图 A-5。

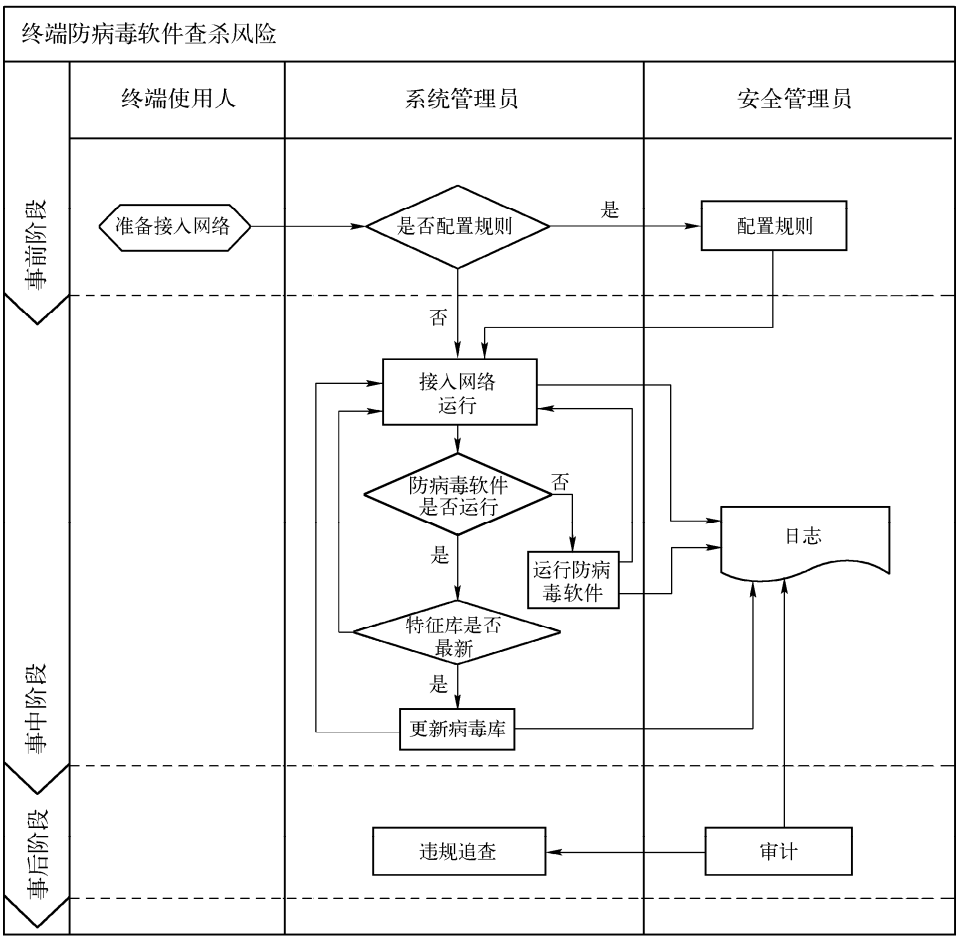

图 A-5

（3）风险点（10）

事前处置：终端安装前安全管理人员应该评估多种防病毒软件的功能与性能，统一防病毒软件的使用，定期考察防病毒软件的功能，确认正常后再推广应用。

事前处置：防病毒病毒查杀能力失效后，先暂时采取断网处理并通知安全管理人员然后检查原因，排查故障，处理完成后再接入网络运行。

事后处置：对于该类风险，保留日志记录，如果出现安全事件，可以追溯责任人。

控制流程见图 A-6。

3．风险控制效果

1）可以保证接入网络的终端均安装统一要求的防病毒软件。

2）可以保证接入网络的终端防病毒软件的版本和病毒库版本保持与安全策略定义一致。

3）可以保证接入网络的终端上的防病毒软件始终正常运行。

4）如果用户或管理员怀疑某台终端已经感染病毒或木马，既可以由终端使用者自行在终端上通过杀毒软件进行查杀，又可以由管理员远程调用终端上的杀毒软件进行查杀。这种方式能够提供更进一步的保证。

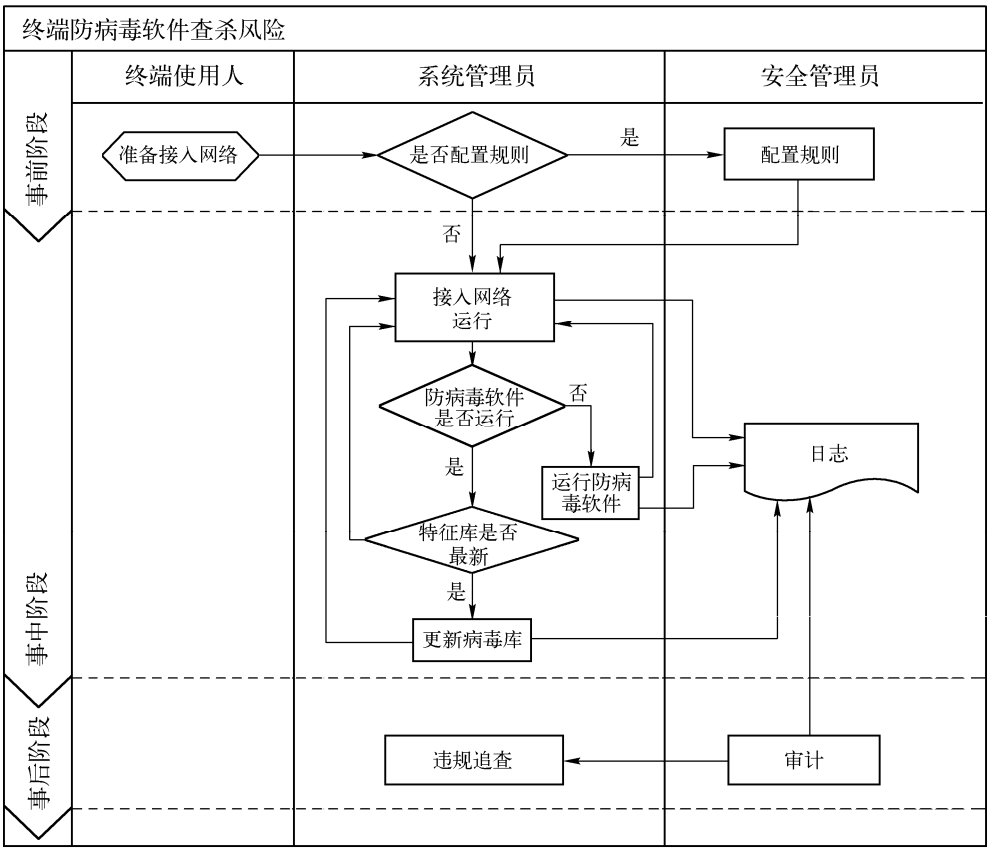

图 A-6

A.1.4 终端应用软件检查风险（8 个风险点）

1. 风险分析

（1）风险描述

终端应用软件是终端使用者日常应用接触最多的部分，用户的大部分工作都需要通过应用软件完成。如果不对应用软件进行管控，由用户随意安装、卸载、使用，存在如下风险：

1）如果用户日常工作需要的软件没有安装，会导致用户无法正常进行工作。

2）如果用户日常工作需要的软件被卸载，同样会导致用户无法正常进行工作。

3）如果用户安装了与工作无关的某些软件并使用，可能会在工作时间做与工作无关的事情，影响工作效率。

4）如果用户安装了某些占用带宽严重的下载软件，在使用时会对网络带宽造成严重影响，使得网络的可用性下降。

（2）相关风险点

终端应用软件检查风险见表 A-7。

表 A-7

	序　号	风 险 点	风 险 属 性	隐患/风险
应用软件检查	1	不能对终端安装应用软件的情况统计	原生风险	隐患
	2	终端安装了非法软件	原生风险	风险
	3	终端安装了非法软件不告警	次生风险	风险
	4	禁止终端安装非法软件，但终端仍安装	次生风险	风险
	5	终端安装非法软件后不能卸载	次生风险	风险
	6	卸载正常的应用软件	原生风险	隐患
	7	卸载正常的应用软件不告警	次生风险	隐患
	8	禁止终端卸载正常的应用软件，但终端仍卸载	次生风险	风险

（a）基于资产使用生命周期分析

风险点（1-8）：这些风险主要涉及资产的入网前和运行阶段，维修和报废阶段，终端不运行，这些风险的影响较小。入网前，如果终端上安装了非法软件，只会影响终端自身的使用，不会对整个网络造成大的影响，风险较低。入网后，如果终端必须安装的软件安装不完整，会导致相关工作无法开展；如果终端上安装了非法软件，会导致信息泄漏，如果安装了下载类的软件，会导致网络流量异常，影响网内其他用户的带宽使用。如果安装的是与工作无关的软件，还会影响终端用户的工作效率。运行时，如果不能对终端进行软件安装和卸载，会导致终端应用软件使用不可控制，不能为终端安装需要安装的软件，会导致需要使用的软件无法使用；不能为终端卸载非法软件，造成信息泄漏，或者影响业务正常使用等风险。

（b）相关信息风险

ⓐ 在线信息风险

风险点（1-8）：不能统计应用软件的安装情况，会导致终端出现需要安装的软件没有安装，禁止安装的软件被安装等情况。如果不能管控软件的安装，当非法软件被安装时，就不能卸载，影响工作效率，会影响在线信息的处理；如果是恶意软件被安装，还有可能引发在线信息泄漏的风险。

ⓑ 存储信息风险

风险点（1-8）：恶意软件被安装，可能会引发存储信息泄漏的风险。

（c）基于资产使用人分析

ⓐ 内部人员

该类风险发生在高级管理岗位（如高层领导），由于其终端含有企业核心信息和涉密信息，风险非常高。该类风险发生在部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，则由于该类终端对业务支撑非常关键，且一般包含关键业务信息，风险较高。如果该类风险发生在生产人员、办公人员等，则由于该类终端支持业务和对正常运营起保障作用，相当重要，风险为中。

ⓑ 临时人员

如果该类风险发生在辅助人员岗位（如食堂、车队、绿化等人员），则该类终端一般不涉及业务、不包含敏感信息，风险为低。

ⓒ 外来人员

风险点 1-8：该风险不涉及此类人员。

（d）合规性要求

合规性要求见表 A-8。

表 A-8

序　号	安 全 类	等级保护（三级）要求	符 合 程 度
1	系统运维管理	7.2.5.5 监控管理和安全管理中心（G3） 应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存	符合

2．风险控制

事前处置：在终端接入网络之前，检查应用软件的安装和运行情况，作为准入条件的一部分。只有符合准入条件的终端才允许接入网络正常使用。

事中处置：在终端接入网络运行后，定期检查应用软件安装和运行情况。当终端安装新软件时，需要进行新软件安装审批流程，并对终端下发安全策略，安全策略规定哪些软件不能随意卸载，并对已安装限制网络内使用的软件，终端应该提示终端用户卸载，当终端根据工作需要必须运行安装和运行某些软件，需要进行申请，得到主管领导和信息安全的审核之后才能放开限制。

事后处置：统计应用软件的种类、版本等信息，对违反软件安装策略的行为予以汇总通报，并且记录安装日志，为日后安全事件溯源提供依据。

控制流程见图 A-7。

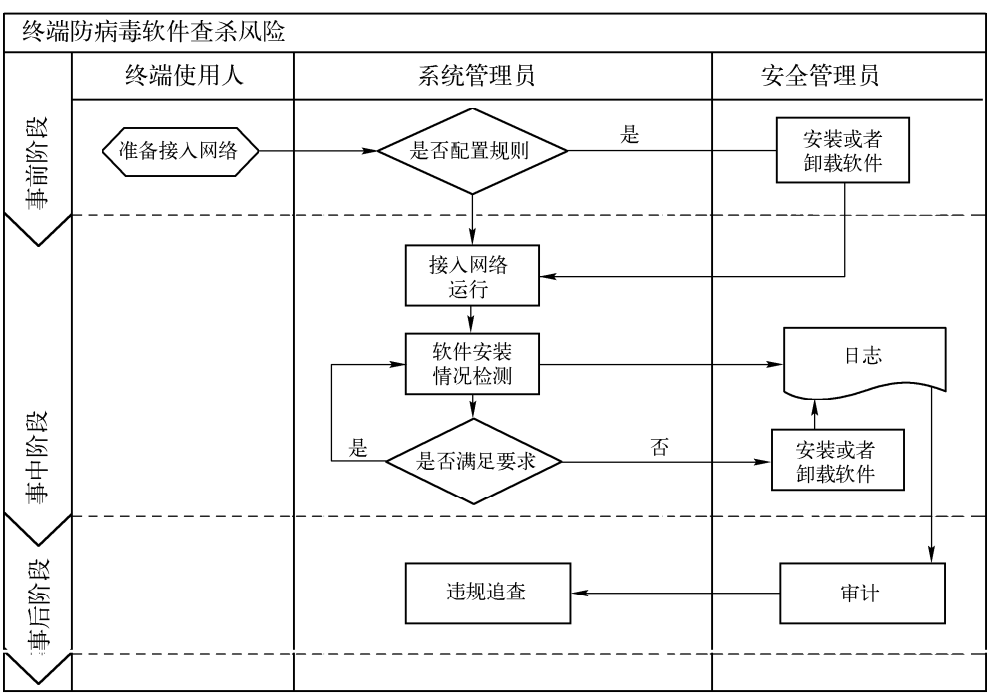

图 A-7

3．风险控制效果

通过终端应用软件检查控制确保终端能够安装必需的软件、保证终端不安装禁止使用的软件，为终端的正常工作提供有力的技术保障。

A.1.5 终端系统补丁风险（6 个风险点）

1．风险分析

（1）风险描述

根据调查表明，病毒、蠕虫、木马的肆虐以及频出的网络攻击行为大部分都是利用了操作系统或者应用软件的漏洞。因此终端系统的补丁是否及时打上，与终端的安全程度密切相关。如果终端没有及时打上补丁，病毒木马可能就会利用该漏洞，使终端机器感染病毒程序，一些别有用心的人也会利用该漏洞窃取网络内的信息，造成泄密事件的发生。

（2）相关风险点

终端系统补丁风险点详见表 A-9。

表 A-9

	序　号	风 险 点	风 险 属 性	隐患/风险
补丁管理	1	不能识别终端已经安装的补丁的补丁号、补丁描述、补丁级别、补丁类型和安装时间等信息	原生风险	隐患
	2	不能识别终端尚未安装的补丁信息，具体包括补丁号、补丁描述、补丁级别、补丁类型等信息的风险	原生风险	隐患
	3	对没有安装补丁的终端不告警	次生风险	风险
	4	不能统一安装补丁	原生风险	风险
	5	不能对终端补丁安装前进行验证	原生风险	隐患
	6	安装补丁后引发系统崩溃不能进行补丁回退	次生风险	风险

（a）相关资产使用生命周期

风险点（1-4）：该类风险涉及入网前与运行阶段。入网前，如果不打补丁，会带来运行阶段的安全风险；运行中，可能会出现新的各种补丁，不及时打上，会导致安全事件的发生，影响生产系统业务稳定的运行。平台如果不能发现终端是否安装了补丁信息，就不能及时为系统打上补丁。如果系统不打补丁，可能被人利用，造成病毒、蠕虫、木马以及网络攻击事件的发生，进而引发泄密事件的发生。如果不加以防范，导致的损失较大，风险较高。

风险点（5-6）：该类风险主要出现在运行阶段，如果平台不能对终端将要安装的补丁进行验证，可能会导致终端安装补丁后崩溃，造成终端不可用，影响业务的正常运行。如果终端安装安装完补丁后出现系统崩溃，不能够进行补丁回退，造成终端不可用，会影响业务的正常运行。

（b）相关信息风险

ⓐ 在线信息风险

风险点（1-4）：如果不能获取终端已经安装或者未安装补丁的信息，就不能及时给终端

或者提醒终端安装最新的补丁。如果补丁未安装就在线运行，系统很容易被病毒木马控制。如果病毒在网络内泛滥，引起网络堵塞，造成在线信息无法使用。如果终端被木马控制，可能会造成泄密事件的发生。

风险点（5-6）：如果平台不能进行补丁验证以及补丁回退，终端安装补丁后可能会引起崩溃，造成终端不可用，进而影响业务工作正常的在线信息的处理。

ⓑ 存储信息风险

风险点（1-4）：该风险可能导致终端上存储的信息或者网络上传输的信息被恶意代码窃取，造成信息泄漏。

风险点（5-6）：该风险可能会导致存储信息丢失。

（c）相关人员风险

ⓐ 内部人员

风险点（1-6）：该类风险发生内部人员，在高级管理岗位（如区域负责人等领导），由于其终端含有企业核心信息和涉密信息，风险非常高。该类风险发生在地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，则由于该类终端对业务支撑非常关键，且一般包含关键业务信息，风险较高。如果该类风险发生在开发人员、研发人员等，则由于该类终端支持业务和对正常运营起保障作用，相当重要，风险为中。

ⓑ 临时人员

风险点（1-6）：如果该类风险发生在临时人员岗位（如食堂、车队、绿化等人员），该类终端一般不涉及业务、不包含敏感信息，风险为低。

ⓒ 外部人员

风险点（1-6）：一般不会涉及外部人员。

（d）合规性要求

合规性要求见表 A-10。

表 A-10

序　号	安　全　类	等级保护（三级）要求	符 合 程 度
1	系统运维管理	7.2.5.7 系统安全管理（G3） c) 应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装	符合

2．风险管控

事前处置：对于终端系统补丁的风险，在终端入网前，需要进行补丁的安装，在大面积给终端安装重要补丁包前要搭建测试环境，人工验证补丁无误后再行在终端上安装。

事中处置：终端入网后，平台采集识别补丁包信息，对未安装补丁的终端及时提示告警信息，并详细向客户描述补丁包情况、威胁等级等，提醒用户下载安装或者强制用户安装补丁。

事后处置：对于该类风险，保留日志记录，如果出现安全事件，可以追溯责任人。

控制流程见图 A-8。

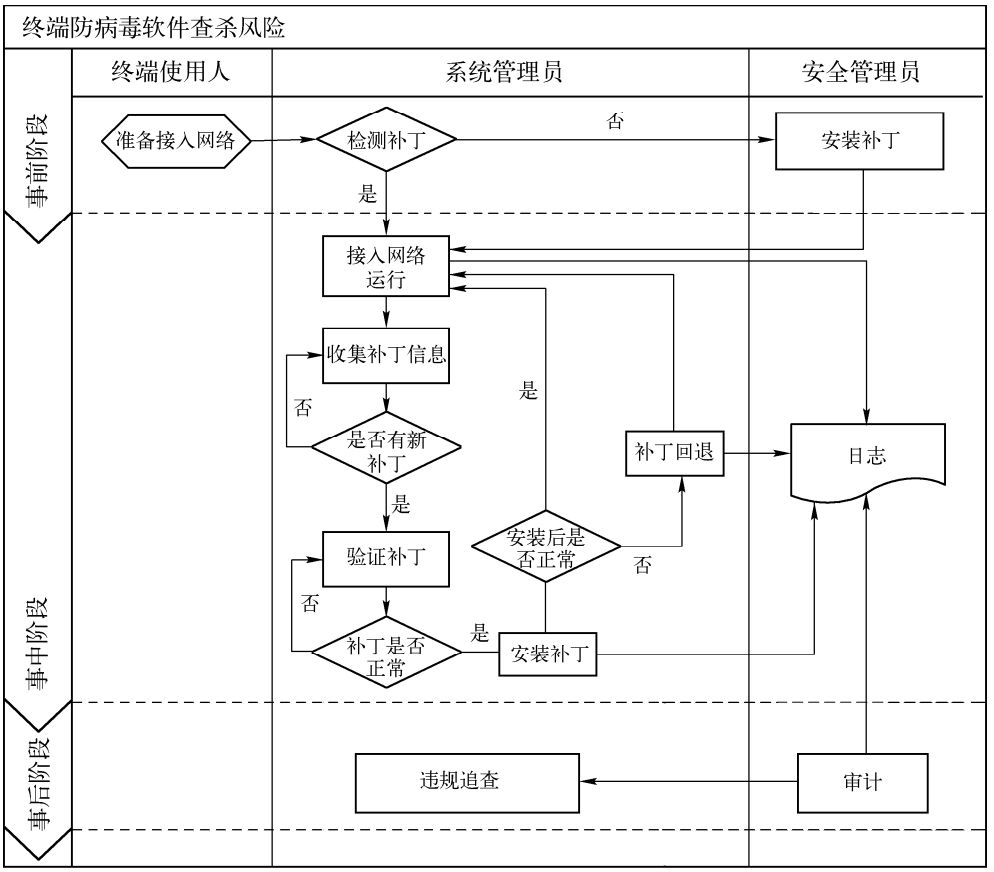

图 A-8

3. 风险控制效果

通过补丁管理，可以及时进行补丁安装，减少系统脆弱性，预防蠕虫、病毒、木马的攻击。

A.1.6 终端软件自动分发风险（8 个风险点）

1. 风险分析

（1）风险描述

当需要为终端统一安装新的应用软件时，管理员需要到终端处手工安装，并且手工统计安装结果。手工给终端安装软件存在的风险有人工安装软件占用管理员大量时间，另外也可能会漏装软件，降低了工作效率。管理员手工统计安装结果，有可能统计错误。

为了解决上述问题，可以采取终端软件自动分发的方式，集中统一为终端需要安装的软件进行自动分发，并自动在终端上运行。但软件的自动分发也存在下面的风险：

1）统一进行了软件自动分发，并显示成功分发，但终端还是没有安装该软件；造成必要的软件没有安装。

2）统一进行了软件自动分发，并成功分发，但分发的软件在终端上不能安装，造成分

发软件安装不成功。

必须对需要进行自动分发的软件做严格规定和统一管理，只有那些工作和业务必需的软件，才应归到自动分发的软件范围中来。

（2）相关风险点

终端软件自动分发风险点见表 A-11。

表 A-11

	序　号	风　险　点	风险属性	隐患/风险
应用软件分发检查	1	应用软件不能自动分发	原生风险	隐患
	2	应用软件不自动分发没有告警信息	次生风险	隐患
	3	应用软件自动分发后没有分发成功	原生风险	隐患
	4	应用软件自动分发后没分发成功无告警信息	次生风险	隐患
	5	不能设定软件自动分发时间	原生风险	隐患
	6	分发的应用软件不能自动安装	原生风险	隐患
	7	分发的应用软件不能自动安装没有告警信息	次生风险	隐患
	8	不能对分发的软件分发成功数、分发成功率、安装成功数、安装成功率等信息进行统计	原生风险	隐患

（a）基于资产使用生命周期分析

风险点（1-8）：这些风险主要出现在资产使用生命周期中的入网后运行阶段。入网前，终端不接入网络，无法对该终端进行软件自动分发操作；维护和报废阶段，终端不运行，也不存在这些风险。终端入网运行后，如果没有应用软件自动分发与自动安装，会增加管理员的工作量而降低工作效率。另外终端如果自行安装软件也可能安装不正确或者安装非法软件，轻则降低终端的工作效率，重则可能会造成终端泄密事件的发生。

（b）相关信息风险

ⓐ 在线信息风险

风险点（1-8）：不能进行软件分发，终端可能会存在由于没有统一的软件，影响对在线信息的处理，另外如果软件分发的时间不能控制，可能会增加网络流量，影响对在线信息的处理。

ⓑ 存储信息风险

风险点（1-8）：对存储信息的影响不是很大，需要注意的就是当下发的软件较多时，会占用终端的存储空间，可能会影响后续的存储信息。

（c）基于资产使用人分析

ⓐ 内部人员：该类风险发生在高级管理岗位（如区域负责人等高层领导），由于其终端含有企业核心信息和涉密信息，风险非常高；该类风险发生在部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，则由于该类终端对业务支撑非常关键，且一般包含关键业务信息，风险较高；如果该类风险发生在生产人

员、办公人员等，则由于该类终端支持业务和对正常运营起保障作用，相当重要，风险为中。

ⓑ 临时人员：如果该类风险发生在辅助人员岗位（如食堂、车队、绿化等人员），该类终端一般不涉及业务、不包含敏感信息，风险为低。

ⓒ 外来人员：该风险不涉及此类人员。

（d）合规性要求

合规性要求详见表 A-12。

表 A-12

序　号	安 全 类	等级保护（三级）要求	符 合 程 度
1		等级保护中没有明确对软件分发的要求	

2．风险控制

事前处置：在终端接入网络之前，检查应用软件的安装和运行情况。作为准入条件的一部分，只有符合准入条件的终端才允许接入网络正常使用业务，不符合准入条件的终端，需要安装指定的软件。对于可能引起冲突的软件，先进行小范围的测试，避免未经过验证的大范围直接处理，导致影响业务工作和网络安全。

事中处置：在终端接入网络运行后，根据工作和业务需要为不同的终端分发不同的软件，保证终端的应用，在分发中要根据软件的数量来确定分发时间，避免因分发给网络带来额外的负担，影响正常业务的处理。

事后处置：统计软件包分发及运行的结果进行检测和记录与否，包括软件的分发成功总数、分发成功数、分发成功率、安装成功数、安装成功率。

3．风险控制效果

软件分发时可以根据网络带宽使用情况和网络流量的大小，灵活设定软件分发所占用的网络带宽，避免软件分发对正常应用产生影响。

为不同的应用分发不同的软件包，软件分发支持用户按不同的应用、部门、客户机等制定不同的软件包分发策略，以满足不同的应用对不同应用软件的需求。

A.2　终端环境安全风险（BR1.2）

A.2.1　终端网络运行环境风险（7 个风险点）

1．风险分析

（1）风险描述

终端网络设备管理主要体现在对网卡设备的管理和网络参数的配置。

网卡设备随着科技的发展，形状越来越小，且出现了支持热插拔的网卡设备。随着网卡设备的发展，其便携性和可热插拔性给网卡的应用带来了很大的方便。个别终端用户或者别有用心的人员就可能在终端设备上增加多个网卡，同时实现终端的外联和内联，这必将带来

信息外泄的风险。同时在联网的过程中，个别人员通过网络大量下载文件，或者由于客户端带蠕虫病毒、木马等，攻击别的设备和服务器，这都会造成信息外泄、网络带宽占用、病毒感染传播等风险。

网络参数的配置应该遵循统一的规范。网络规划是网络安全的基础，也是网络管理过程中跟踪和定位的前提，终端使用者自行修改网络参数的配置，是混淆管理员跟踪的常用方式，也是变更网络使用权限的常见操作。

（2）相关风险点

表 A-13

	序　号	风　险　点	风险属性	隐患/风险
终端网络环境	1	不能监控终端异常网络流量	原生风险	隐患
	2	终端出现异常网络流量不告警	原生风险	风险
	3	不能监控终端使用多网卡	原生风险	隐患
	4	发现终端使用多网卡不告警	原生风险	风险
	5	不能对终端 IP/MAC 地址进行绑定	原生风险	隐患
	6	终端使用多网卡后，不能控制哪块网卡的禁用或者启用	次生风险	风险
	7	终端 IP/MAC 地址绑定后，不能发现终端克隆其他人 IP、MAC 地址	次生风险	风险

（a）相关资产使用生命周期

风险点（1-5）：该类风险主要出现在资产使用生命周期的运行阶段，异常的网络流量会影响正常的业务运行；终端多网卡现象会导致非法外联，控制不力将导致泄密事件的发生；IP/MAC 地址不绑定会出现 IP 地址盗用的现象。该类风险如果不加以防范，会导致安全事件的发生，导致的损失较大，风险较高。入网前、维护和报废阶段，终端独立运行，不接入网络，不存在该类风险。

风险点（6-7）：该类风险主要出现在资产使用生命周期的运行阶段，平台发现终端使用多网卡后，如果不能控制哪块网卡的启停，而采用全部断网的方式解决问题，可能会影响终端正常的业务行为，因此平台能够单独控制哪块网卡的启停，禁掉非法安装的网卡，启用正常的网卡。如果终端克隆其他人的 IP、MAC 地址信息，可能会导致非授权的访问行为发生，一旦出现安全事件，也会影响日后的溯源。入网前、维护和报废阶段，终端独立运行，不接入网络，不存在该类风险。

（b）相关信息风险

ⓐ 在线信息风险

风险点（1-5）：如果平台不能对终端的异常流量、使用多网卡以及对 IP/MAC 地址进行绑定等控制，异常的网络流量会影响在线运行的业务系统；终端多网卡现象会导致非法外联，控制不力将导致在线信息泄密；IP/MAC 地址不绑定会出现 IP 地址盗用的现象，影响在线信息的外泄，该类风险如果不加以防范，会导致安全事件的发生，导致的损失较大，风险较高。

风险点（6-7）：如果平台不能对终端使用的多网卡进行单独的控制，会影响在线信息及

时处理，多网卡行为也会导致非法外联事件的发生，可能会引起在线信息泄密事件的发生。如果别有用心的人克隆其他人的 IP、MAC 地址信息，可能会导致在线信息非授权的访问行为发生，进而引发在线信息泄密事件的发生。

ⓑ 存储信息风险

风险点（1-5）：主要影响的是在线的信息，对存储信息的影响较小。

风险点（6-7）：对存储信息影响较大，如果控制不好，可能导致非授权的访问行为，导致存储的信息外泄。

（c）相关人员风险

ⓐ 内部人员

风险点（1-7）：该类风险发生在内部人员高级管理岗位（如区域负责人等高层领导），由于其终端含有企业核心信息和涉密信息，风险非常高；该类风险发生在地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，则由于该类终端对业务支撑非常关键，且一般包含关键业务信息，风险较高；如果该类风险发生在开发人员、研发人员等，则由于该类终端支持业务和对正常运营起保障作用，相当重要，风险为中。

ⓑ 临时人员

风险点（1-7）：如果该类风险发生在辅助人员岗位（如食堂、车队、绿化等人员），该类终端一般不涉及业务、不包含敏感信息，风险为低。

ⓒ 外来人员

风险点（1-7）：该风险不涉及此类人员。

（d）合规性要求

合规性要求见表 A-14。

表 A-14

序　号	安 全 类	等级保护（三级）要求	符 合 程 度
1		等级保护中没有明确对 IP 地址和网络流量管理相关的要求	

2．风险管控

事前处置：入网前检查终端是否安装了多网卡，配置了多网卡的终端必须禁用超出指定网络连接需求的网卡后才允许接入网络，另外还要预先配置 IP/MAC 地址绑定策略，限制 BT 类工具运行，以免影响网络流量。

事中处置：采集网卡状态信息，发现私自修改 IP 地址或者 IP 不对应则告警并禁用该网卡。采集网卡流量与并发链接数，如果超出阈值则告警，并禁用该网卡。发现终端安装多网卡，直接隔离该终端，并立即派专人进行查处。

事后处置：对于该类风险，保留日志记录，如果出现安全事件，可以追溯责任人。

控制流程见图 A-9。

3．风险控制效果

通过有效监控网卡和网络流量，可以及时发现网络中 IP 地址变动信息，有效防止非授权用户连接网络，防止病毒、木马攻击进程，有效预防网络异常流量和进程。

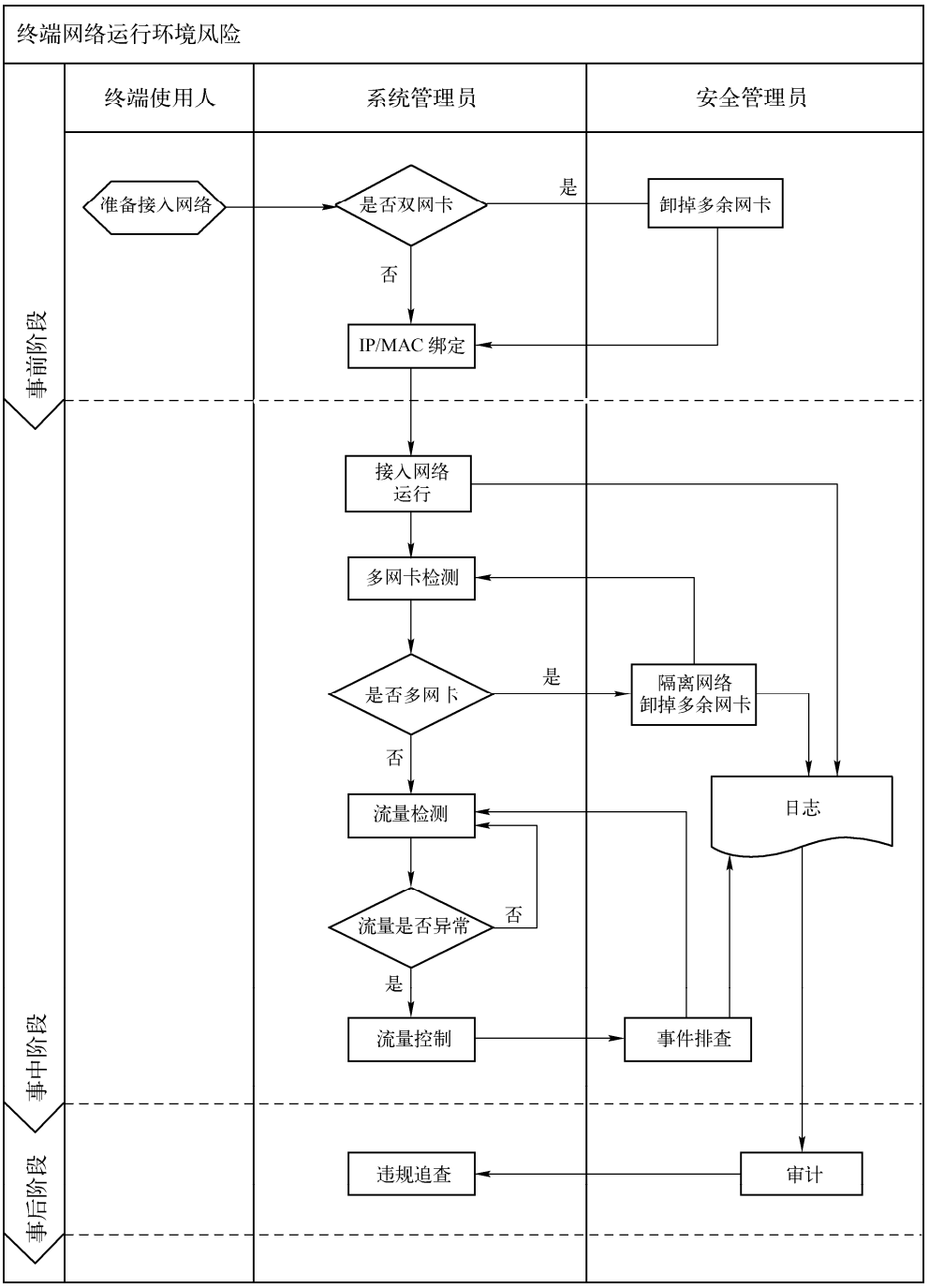

图 A-9

A.2.2 终端防火墙风险（14 个风险点）

1. 风险分析

（1）风险描述

终端未安装软件防火墙软件：如果终端不安装软件防火墙软件，就不能对终端的访问端

口与应用协议进行控制，终端将面临数据流不可控的风险。恶意进程、端口、协议不加以及时阻断，终端安全性得不到保证，会威胁整个网络系统。

终端安装软件防火墙软件：如果终端安装了软件防火墙软件，但不能检测软件防火墙软件的版本和规则特征库等信息，就不能对软件防火墙软件进行有效的升级，进而影响软件防火墙软件的正常使用。如果软件防火墙软件停止启动，而又不能恢复启动，就相当于没有安装软件防火墙软件，可能会导致泄密事件的发生。此外，如果防火墙软件不能进行 IP、端口和协议的有效访问控制，就会给恶意进程可乘之机，引起泄密事件的发生；如果软件防火墙配置了访问控制规则，但访问控制规则没有生效，防火墙将形同虚设。

（2）相关风险点

终端防火墙风险点见表 A-15。

表 A-15

	序　号	风　险　点	风险属性	隐患/风险
终端防火墙风险	1	终端未安装防火墙软件	原生风险	隐患
	2	终端未安装防火墙软件，没有告警信息	次生风险	风险
	3	终端安装防火墙软件后，防火墙软件的型号、版本、特征库信息不能发现	原生风险	隐患
	4	终端安装防火墙软件后，和系统冲突	次生风险	风险
	5	终端防火墙软件程序和特征库不能升级到最新状态	次生风险	隐患
	6	终端防火墙程序处于未运行状态	原生风险	隐患
	7	终端防火墙程序处于未运行状态后不能启动防火墙程序	原生风险	风险
	8	防火墙程序处于未运行状态，没有告警信息	次生风险	风险
	9	终端防火墙不能进行 IP 地址控制	原生风险	隐患
	10	终端防火墙软件采用了 IP 地址控制，但控制不生效	次生风险	风险
	11	终端防火墙不能进行端口控制	原生风险	隐患
	12	终端防火墙软件采用了端口控制，但控制不生效	次生风险	风险
	13	终端防火墙不能协议控制	原生风险	隐患
	14	终端防火墙软件采用了协议控制，但控制不生效	次生风险	风险

（a）基于资产使用生命周期分析

资产使用生命周期包含入网前、运行阶段、维修阶段、报废阶段，终端防火墙风险在资产使用生命周期的体现如下：

风险点（1-2）：这些风险主要出现在运行阶段，入网前、维护和报废阶段，不安装软件防火墙软件只会影响终端本身，且因为终端未接入网络，不会给网络造成威胁。如果终端未安装软件防火墙软件就接入网络，可能会导致终端泄密事件的发生，如果在入网前阶段如果没有进行控制，将会带来很大的风险；在运行阶段，如果终端都安装了防火墙软件并且正确使用，将不会带来更大的风险，如果没有做好控制措施，会带来更大的安全风险。

风险点（3-8）：这些风险主要出现在运行阶段。入网前、维护和报废阶段，软件防火墙软件不更新只会影响终端本身，且因为终端未接入网络，不会给网络造成威胁。这些风险出现在系统运行阶段，如果不能发现防火墙软件的版本特征库等信息，就不能对软件防火墙软件进行有效的升级，进而影响防火墙软件的正常使用。如果防火墙软件停止启动，而又不能

恢复启动，就相当于没有安装防火墙软件。恶意程序可能会控制终端系统，造成泄密事件的发生。该类风险如果不加以防范，会导致安全事件的发生，导致的损失较大，风险较高。

风险点（9-14）：这些风险主要出现在运行阶段。入网前、维护和报废阶段，终端不接入网络，不会对外访问，不存在这些风险。这些风险出现在系统运行阶段，如果终端软件防火墙不能启用 IP 地址、端口以及协议控制规则，很容易导致安全隐患，恶意程序可能会控制终端系统，造成泄密事件的发生。该类风险如果不加以防范，会导致安全事件的发生，导致的损失较大，风险较高。

（b）相关信息风险分析

ⓐ 在线信息风险

风险点（1-2）：软件防火墙软件对于终端运行的所有工作均起到保护作用，未安装软件防火墙软件的终端容易被恶意程序控制，进而导致在线信息相关系统不能正常工作，或者导致敏感信息泄漏。

风险点（3-14）：软件防火墙软件的正常运行，与程序版本和特征库版本的实际情况相结合，在线信息与此关联更为明显，不能及时更新软件防火墙软件程序版本和特征库版本，可能无法有效针对新发现的攻击。软件防火墙在不运行或者访问控制规则不合理时，恶意程序可能控制终端或者有意无意地进行非授权的访问，进而导致在线信息相关系统不能正常工作，或者导致敏感信息泄漏。

ⓑ 存储信息风险

风险点（1-14）：该风险可能导致终端上存储的信息被恶意代码窃取，造成信息泄漏。

（c）基于资产使用人员风险分析

ⓐ 内部人员

风险点（1-14）：该类风险发生在内部人员高级管理岗位（如区域负责人等高层领导），由于其终端含有企业核心信息和涉密信息，风险非常高；该类风险发生在地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，则由于该类终端对业务支撑非常关键，且一般包含关键业务信息，风险较高；如果该类风险发生在开发人员、研发人员等，则由于该类终端支持业务和对正常运营起保障作用，相当重要，风险为中。

ⓑ 临时人员

风险点（1-14）：如果该类风险发生在辅助人员岗位（如食堂、车队、绿化等人员），该类终端一般不涉及业务、不包含敏感信息，风险为低。

ⓒ 外来人员

风险点（1-14）：该风险不涉及此类人员。

（d）合规性要求

合规性要求见表 A-16。

表 A-16

序　号	安 全 类	等级保护（三级）要求	符 合 程 度
1	网络安全	7.1.2.5 入侵防范（G3） a) 应在网络边界处监视以下攻击行为：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 碎片攻击和网络蠕虫攻击等	符合

2．风险管控

（1）风险点（1-2）

事前处置：终端在接入网络前，必须安装终端防火墙软件，并根据业务需要配置合理的访问控制规则，然后才能接入到网络中使用。没有安装防火墙的软件的终端不允许接入网络，并通知相关管理人员给终端安装防火墙软件。

事中处置：在运行中发现终端未安装防火墙软件（可能是被人卸载或者禁用），马上将该终端断开网络访问，并上报管理人员。

事后处置：对于该类风险，保留日志记录，如果出现安全事件，可以追溯责任人。

控制流程见图 A-10。

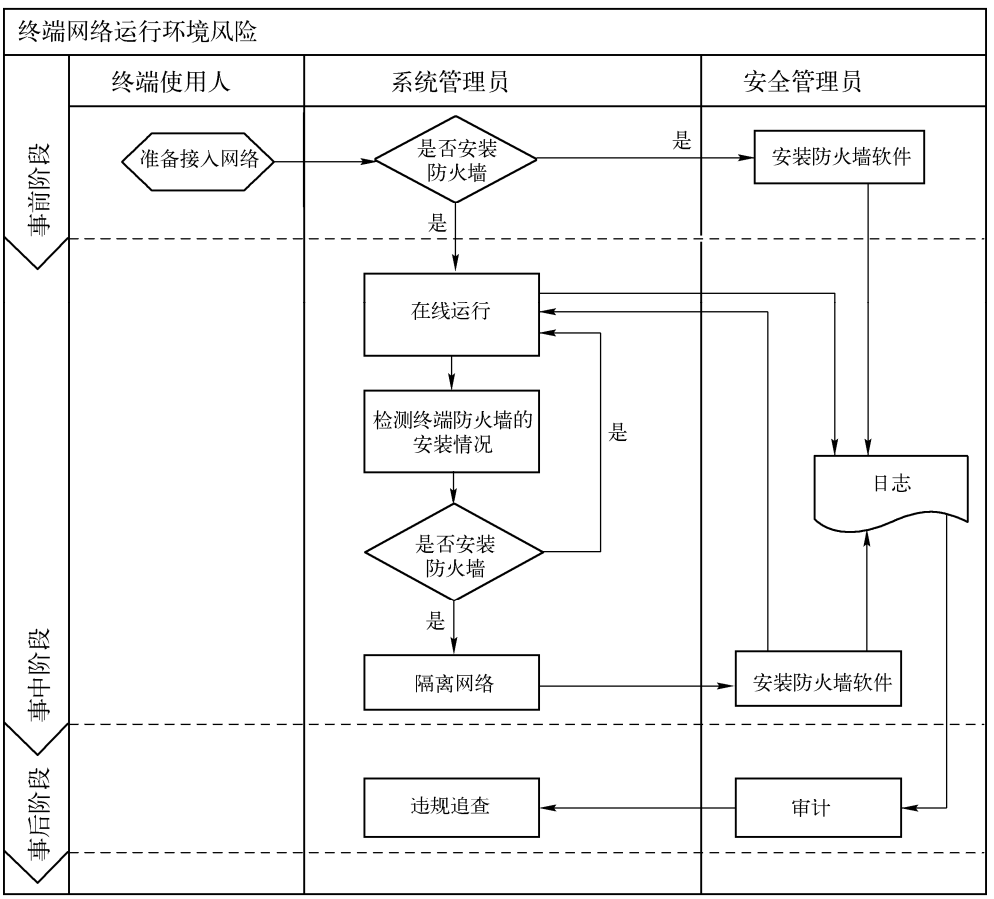

图 A-10

（2）风险点（3-8）

事前处置：终端入网前按照实际业务需求情况，先配置好访问控制策略和软件防火墙特征库升级策略，然后接入网络。

事中处置：接入网络后，关闭与业务系统无关的端口，除授信的 IP 地址可以访问重要（敏感）信息终端外，其他 IP 地址全部禁止访问。重要（敏感）信息终端只能访问授信的 IP

地址及端口，指定终端仅开放与业务系统相关的应用协议。如果终端未启用软件防火墙，应该禁止访问网络，待启用后再准入网络；终端有未授权的访问行为，应禁止访问网络并及时通知管理员；另外，软件防火墙特征库要及时更新，未更新的采取强制更新的措施。

事后处置：对于该类风险，保留日志记录，如果出现安全事件，可以追溯责任人。

控制流程见图 A-11。

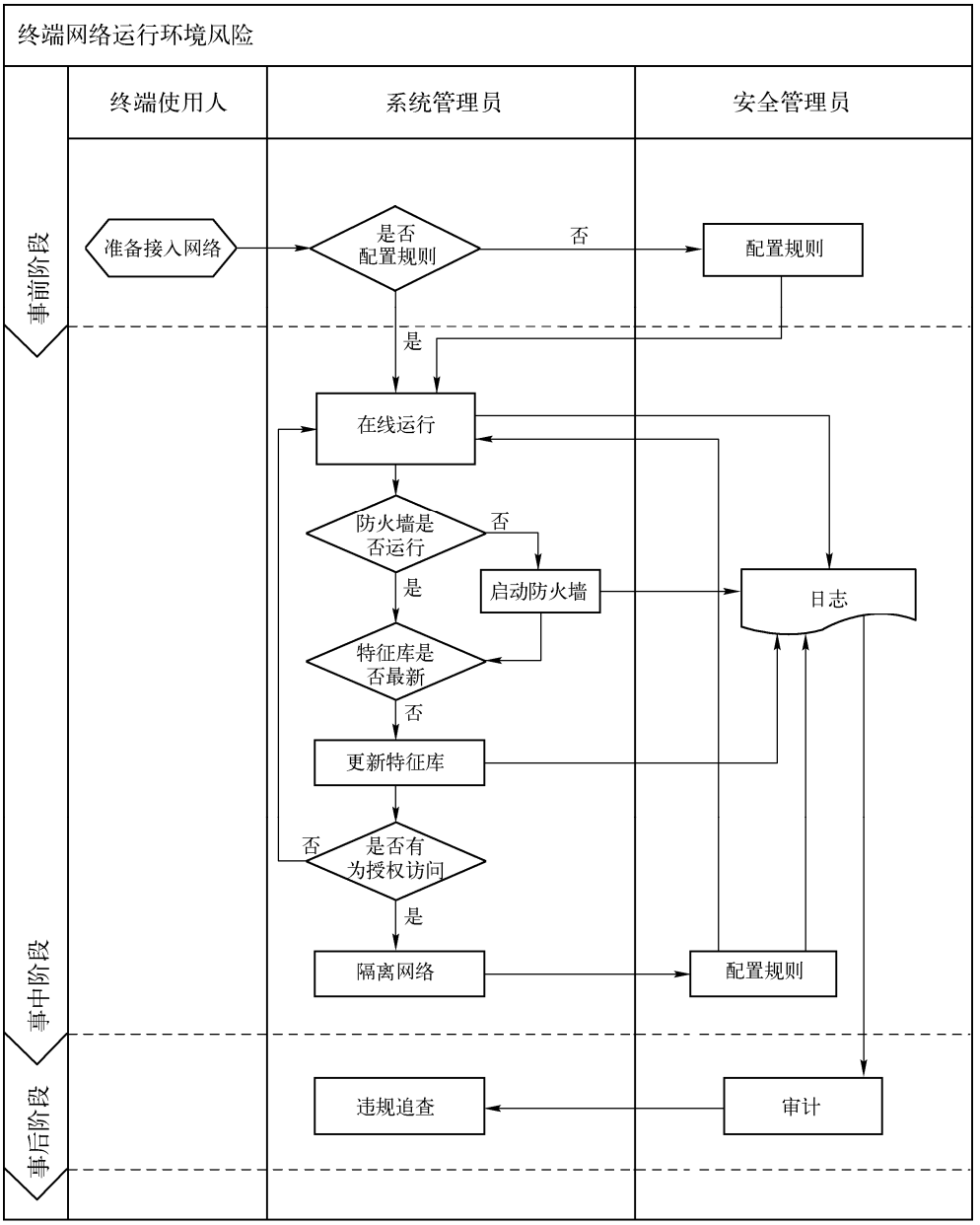

图 A-11

（3）风险点（9-14）

事前处置：终端安装前安全管理人员应评估软件防火墙软件的功能与性能，保障软件防

火墙软件的功能正常后再安装并接入网络。

事前处置：软件防火墙访问控制规则失效后，先暂时断网处理并通知安全管理人员，然后检查原因，排查故障，处理完成后再接入网络运行。

事后处置：对于该类风险，保留日志记录，如果出现安全事件，可以追溯责任人。

控制流程见图 A-12。

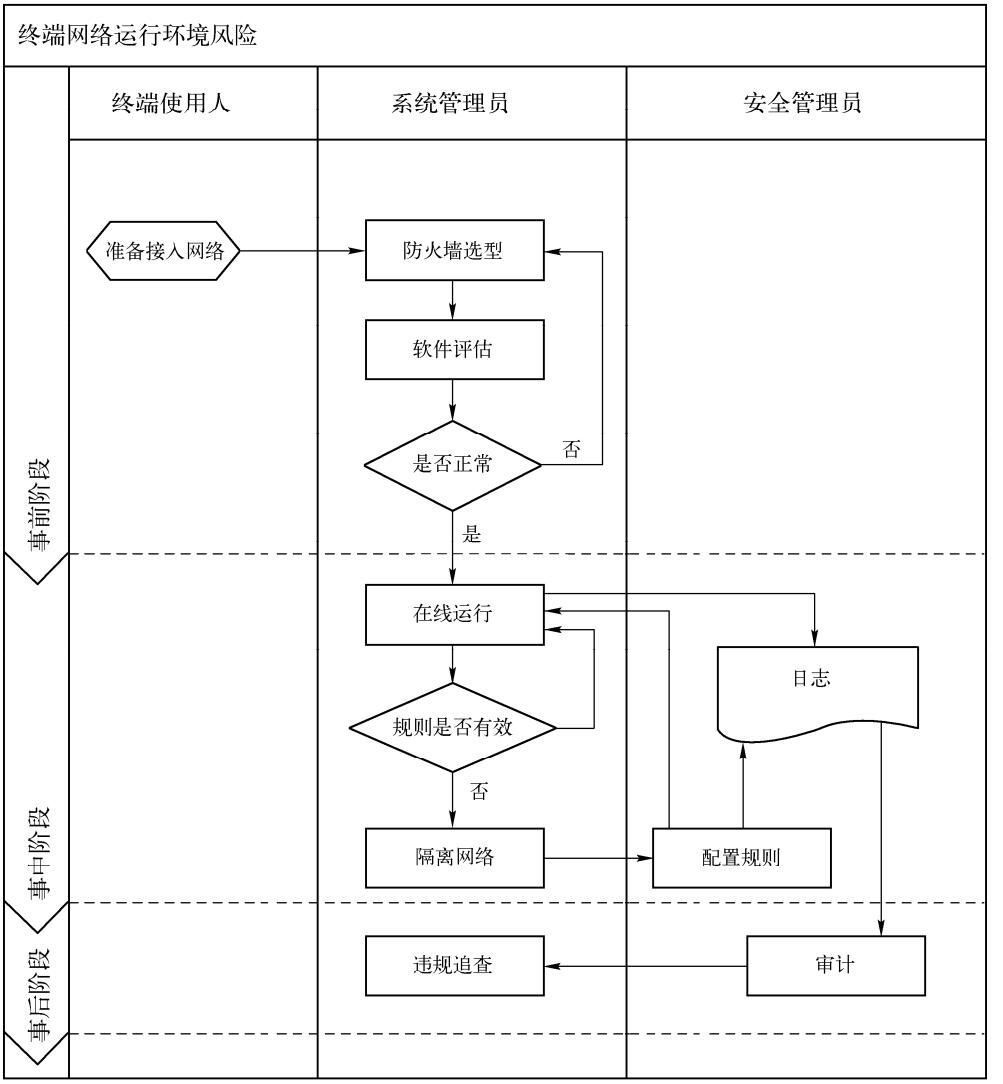

图 A-12

3. 风险控制效果

终端软件防火墙软件，可以对终端的 IP 访问、端口访问、协议访问、共享服务访问等进行限制。管理员可对远程 IP 地址、本地端口、远程端口、网络协议、是否开启共享端口等进行设置，确保终端仅能访问指定的合法 IP、端口和协议，从而可以有效应对非法访问和保障业务数据安全。

A.3 终端外设安全风险（BR1.3）

A.3.1 外设端口管理（15 个风险点）

1．风险分析

（1）风险描述

内网终端都有存储设备接口，例如光驱、软驱、 USB 接口、串并口和红外接口等。从终端保护的角度来看，通过外设端口很容易造成信息泄漏，这类风险主要表现在以下两个方面：

1）内部员工通过外设端口把业务信息违规带离业务网络，对外扩散或者泄密，严重的可能造成社会事件；或者随意将软件、游戏、电影等复制到内网终端运行，极有可能将病毒、木马、后门等带到内网当中，从而造成对网络和信息安全的破坏。

2）通过外设端口进行非法外联，打通内网与其他网络的连接。

从外设端口保护的角度来看，保护不足的风险主要表现在以下几个方面：监控缺失风险，由于缺少对外设端口的监控，将导致关键主机数据的保护失控的风险；标准基线风险，由于事先没有对各种终端的外设端口作出详细统计，根据不同品牌的终端和工作的具体情况做出允许的外设端口黑白名单列表，会造成不能有效地识别终端的可以使用和不允许使用的外设端口，进而不能有效控制外设端口的使用风险；加载了外设端口监控策略后，导致一些需要使用特殊端口的业务无法使用，或造成终端蓝屏、宕机严重影响业务，造成终端业务持续有效运行的风险。因此这类风险的可知、可控、可管十分重要。下面对终端系统驱动风险进行详细的分解。

（2）相关风险点

终端外设端口管理风险点见表 A-17。

表 A-17

	序　号	风　险	属　性	隐患/风险
外设端口管理	1	光驱端口没有管控	原生风险	隐患
	2	软驱端口没有管控	原生风险	隐患
	3	红外设备端口没有管控	原生风险	隐患
	4	蓝牙设备端口没有管控	原生风险	隐患
	5	PCMCIA 设备端口没有管控	原生风险	隐患
	6	串口没有管控	原生风险	隐患
	7	并口没有管控	原生风险	隐患
	8	1394 端口没有管控	原生风险	隐患
	9	USB 端口接入普通设备没有管控	原生风险	隐患
	10	USB 端口接入存储介质没有管控	原生风险	隐患
	11	加载策略后导致正常业务无法使用	次生风险	风险
	12	加载策略后导致终端死机、宕机	次生风险	风险
	13	USB 端口接入普通设备禁用，导致人机交互类设备无法使用	次生风险	风险
	14	USB 端口接入普通设备禁用，导致 USB Key（硬件、数字证书载体）类设备无法使用	次生风险	风险
	15	USB 端口接入存储设备禁用，导致照相机、MP3 等设备无法使用	次生风险	风险

以下将分别从资产使用生命周期、相关信息安全、资产使用人员和合规性 4 个方面对以上 15 个风险点进行详细描述。

（a）基于资产使用生命周期分析

资产使用生命周期包含入网前、运行阶段、维修阶段、报废阶段，终端违规网络访问风险按照资产使用生命周期的分析如下：

风险点（1-8）：该类风险涉及资产使用生命周期阶段为运行阶段和维修阶段。终端外设端口管理的目的在于通过外设使用控制、监控、审计等安全控制措施，防止通过外设接口造成的网络边界完整性的破坏，最终导致敏感信息的泄漏。因此，终端外设端口类风险主要发生在运行阶段；同时，设备维修阶段为特殊阶段，许多在线监控措施和管理规定将会失效，也会造成敏感信息的泄漏。

风险点（9-10）：此类风险由于涉及目前使用十分普遍的 USB 端口的管控，特别单独分析。此类风险涉及资产使用生命周期阶段为运行阶段和维修阶段。在运行阶段，如果 USB 端口不能得到有效管控的话，用户可以违规使用 U 盘、移动硬盘复制文件，出现数据泄漏的风险；另外通过 USB 端口，用户可以违规连接 Modem、手机导致出现违规外联的风险，导致数据外泄无法管控、无法追踪，破坏系统安全边界，违背系统整体安全防护策略。

风险点（11-12）：此类风险涉及资产使用生命周期阶段为入网前和运行阶段。由于没有在入网前期对所有的在用终端设备进行充分调查，就设备的外设端口情况、外设端口与业务的关联情况得出一套白名单，并且进行充分测试验证，一旦集中加载策略，可能会造成部分终端的业务不可用，更为严重的会造成终端蓝屏、死机。

风险点（13-15）：此类风险涉及资产使用生命周期阶段为入网前和运行阶段。由于临时或特殊的情况，需要开启管控的端口，而端口已经被禁用，就会造成人机交互类设备、照相机、MP3 等设备不能使用，最严重的是需要使用身份识别的 USBKey（硬件数字证书载体）类设备无法使用，导致以此相关的业务无法开展。

（b）基于相关信息安全关系分析

相关信息安全分为在线信息风险和存储信息风险，终端端口管理按照相关信息安全关系的分析如下：

风险点（1-8）：如果缺失有关外设端口的监控措施，一旦被利用，可能造成文件外泄，因此涉及在线信息风险和存储信息风险。

风险点（9-10）：USB 端口是目前使用最为广泛的外设端口，如果其监控措施缺失，当终端通过 USB 端口违规外联时，终端的在线信息会通过外联泄漏。对存储信息来说，终端通过 USB 端口可以将终端上的存储信息进行篡改和泄漏，风险较高。

风险点（11-12）：此类风险主要涉及在线信息和存储信息风险。当终端正在处理在线信息时，一旦加载的外设端口策略影响到业务的正常进行，在线信息的处理和存储都会受影响。

风险点（13-15）：此类风险不涉及信息风险。信息风险是在从事业务的时候出现的，业务已经不能开展了，因此不会涉及信息风险。

（c）基于资产使用人分析

资产（终端）使用人包括内部人员、临时人员和外部人员 3 大类，而内部人员可以再细分为高级管理者、关键业务人员和网络管理人 3 种角色，临时人员主要是辅助人员岗位（如食堂、车队、绿化等人员），而外部人员包括外来厂商运维人员和系统内外来人员。终端的

使用者因为不同的角色和不用的操作意图，一个相同的风险点对应不同身份的终端使用人风险级别也不同。将外设端口风险按照终端使用人角色分析如下：

风险点（1-8）：该类风险与内部人员的角色级别有关。

1）高级管理岗位

（如区域负责人等高层领导），其终端一般都为核心终端，终端上的信息重要程度也较高，如果其终端的管控措施不力，将导致终端上的信息泄漏或篡改，风险较高。

2）地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，对终端和网络有比较高的操作权限，如果对外设端口的管理不到位，会影响整体业务的运行，风险较高。

3）对网络管理员来说，主要体现在对外访问的端口，如果不进行管控，会导致一些端口在网络上开放，风险较高；对于临时人员和外来人员，一般情况下要禁止外设端口的使用，不允许其随意打开终端的端口。

风险点（9-10）：该类风险与内部人员的角色级别有关。

1）高级管理岗位（如区域负责人等高层领导），对 USB 端口存储和复制一定要实施管控，否则其掌握的重要信息容易泄漏，尽量做到专门的终端和专门的移动存储介质使用，这类风险较高。

2）地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，也必须做到 USB 端口的管控，否则重要信息容易外泄，这类风险较高。

3）对网络管理员来说，必须限制其 USB 端口及介质的使用，否则一些端口在网络上开放，风险较高；对临时人员和外来人员来说，因为对其携带的介质不好管控，应限制这类人员对 USB 端口的使用，在制度上就规定该类人员不允许使用 USB 外设端口。否则，USB 端口被利用，风险难以掌控。

风险点（11-12）：对于临时人员和外部人员，因无法事先作出驱动程序基线，风险较大；对于地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，以及高级管理岗位（如区域负责人等高层领导），如果不能及时全面地做出外设端口管理列表，对于贸然加载策略导致业务遭到影响的风险较大。

风险点（13-15）：该风险对于高级管理岗位（如区域负责人等高层领导）的终端的正常使用风险较大；对于网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员的终端的使用风险较大；对于临时人员和外部人员风险不大。

（d）合规性要求

合规性要求见表 A-18。

表 A-18

序　号	安 全 类	等级保护（三级）要求	符 合 程 度
1	系统运维管理	7.2.5.3 介质管理（G3） c) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点	符合

2．风险管控

每类风险在管控过程中，针对风险的事前、事中和事后 3 种状态进行监控，做到事前预防，事中控制、事后审计追查。下面的外设端口风险管控处理流程，尽量从事前、事中和事

后 3 方面对风险管控进行描述。

（1）风险点（1-10）：外设端口风险管控流程

事前处置：对于外设端口管理的风险，需要制定一系列的管理措施，如《主机安全管理制度》，其中需要针对现有不同的品牌终端，按照不同的外设端口的风险高低，做出相应的外设端口监控策略。

事中处置：根据风险控制策略，实施控制措施，并进行实施监控，违规行为及时告警，通过策略/人工方式阻断，并进行系统日志信息的安全存储。

事后处置：对于违规行为，进行后续安全审计和操作追踪，并进行违规分析，进行策略调整。

风险管控流程见图 A-13。

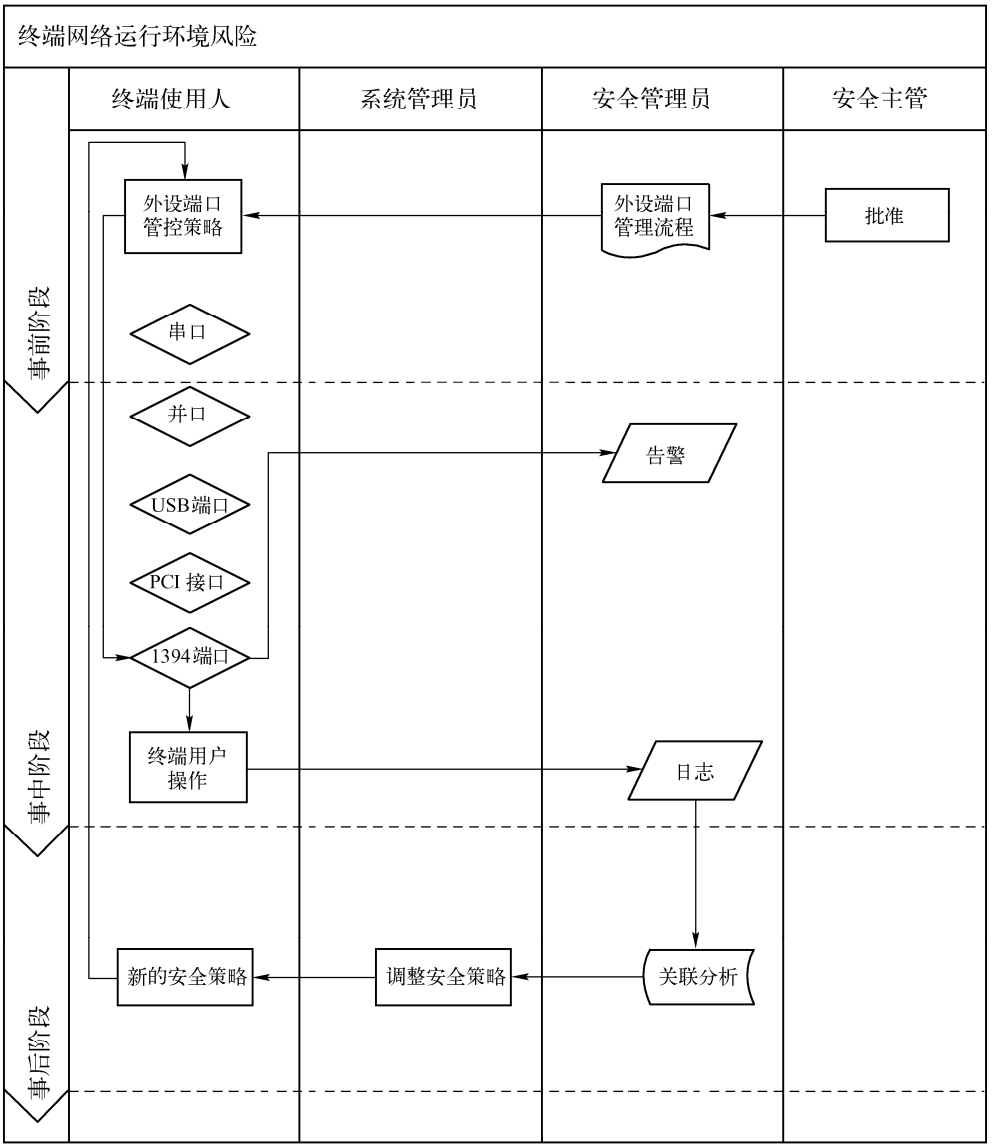

图 A-13

（2）风险点（11-12）：外设端口监控技术本身风险

事前处置：需要制定有关的应急响应预案，并且定期演练，确保一旦加载策略导致出现意外，影响业务时，能够及时启动。

事中处置：一旦出现策略与业务的兼容性问题，需要有逃生机制，即通过人工卸载策略，确保业务的顺利进行。

事后处置：在安全主管的认可下启动应急预案。首先在确保业务顺利进行的前提下，在本地人工更新或卸载策略。在此基础上再考虑其他问题，如策略不能更新的故障原因、涉及的部门和人员，造成问题的是平台本身的性能原因，还是其他问题，这些问题是否在管理制度中作出了相关规定，是否需要完善或补充等。

风险管控流程见图 A-14。

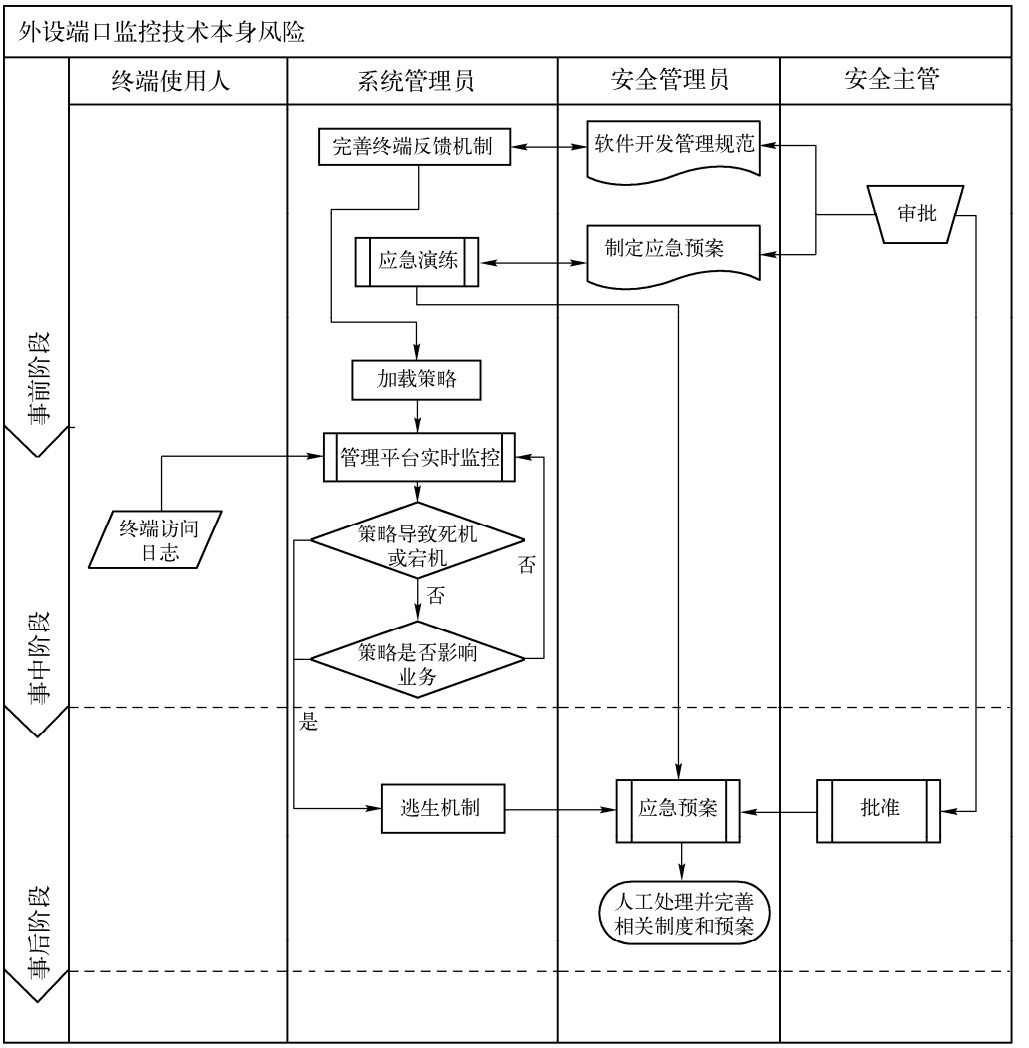

图 A-14

（3）风险点（13-15）：外设端口临时开启管控流程

事前处置：在常规情况下，被禁用的端口不允许随意开启。若因工作原因，需要开启相

应的端口时，应提交申请，由管理员进行审核，并由相关领导进行批准，方能开启使用。

事中处置：可以采取两种流程。

1）普通申请流程，终端使用者登录相关申请页面，按照要求填写申请，逐级提交申请。在整个申请过程中，依据实际业务流程进行自动化管理，系统后台自动记录申请的全过程，并将申请批准的整个过程写入数据库，便于安全管理负责人员统一管理。

2）应急申请流程，该应急申请流程主要适用于主管领导不在现场时的特殊情况。申请者在提交申请后，由管理员审核后先进行功能的开放和处理。待主管领导回来后，管理员将临时处理的端口申请事件提交主管领导重新查阅审批，对不合格的申请进行事后处理和责任追查。

事后处置：对临时开启端口后的端口使用行为进行日志记录并对其进行关联分析，找出可能的问题并对下发策略进行完善，然后重新加载更新后的策略。

风险管控流程见图 A-15。

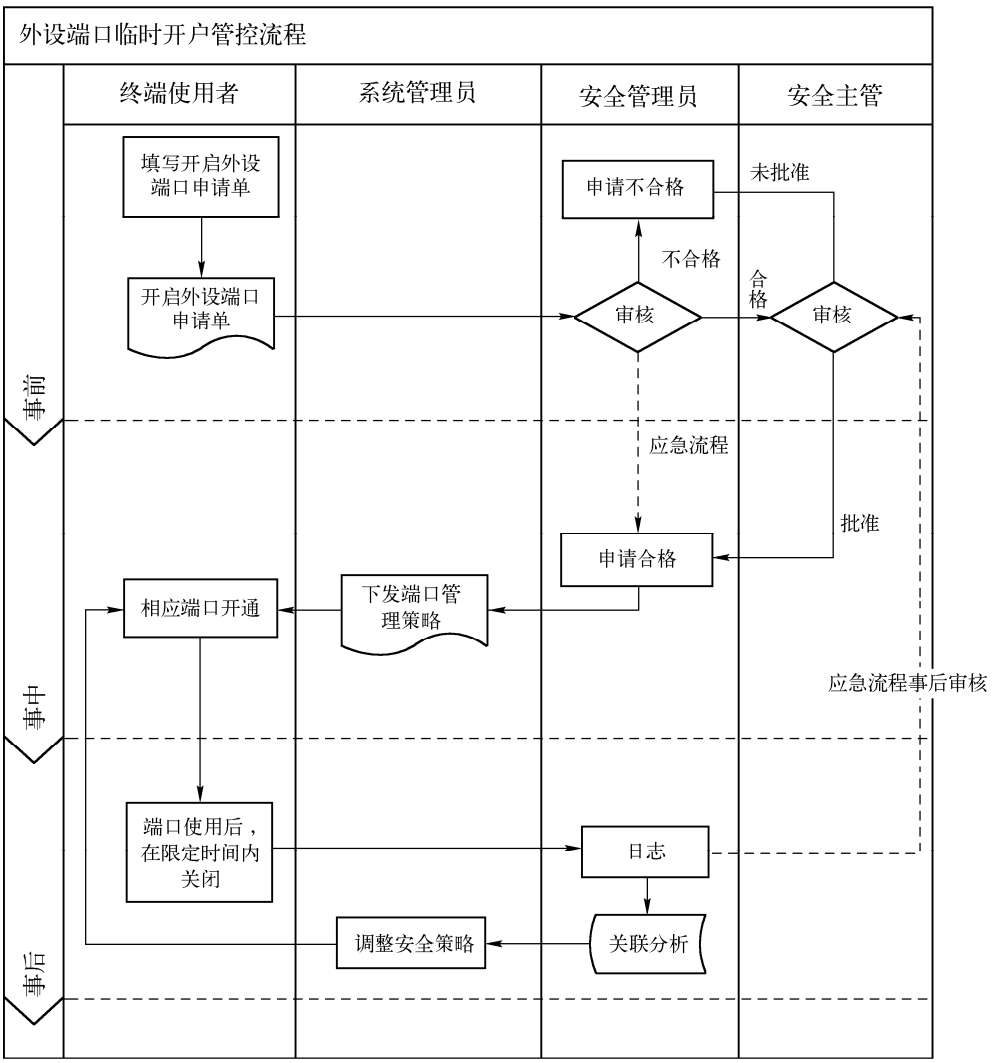

图 A-15

3．风险控制效果

对于此类风险涉及的终端流量异常风险，通过采取管理、规范、流程、技术不同的措施，分别从事前、事中、事后 3 个方面来加以控制，可以基本达到风险管控的目的。

通过事前对不同角色的用户，不同时间的业务所需要的外设端口的调查，逐步建立各种终端的外设端口列表，这些端口包括软盘驱动器、光盘驱动器、串行通信口、并行通信口、1394、红外通信口等不同类型的端口。

另外在事前还要有针对端口临时开启的审批流程和制度，避免不能临时开启一些被禁止的端口而影响业务的风险。

由于加载的安全策略可能给业务带来风险，需要根据可能出现的场景，如策略与业务冲突、终端死机等场景，制定应急预案并做定期演练，努力确保业务的连续性和可靠性。

A.3.2 外设设备管理

1．风险分析

（1）风险描述

外设设备主要包括 U 盘、移动硬盘、光盘刻录机、软盘；蓝牙/3G 手机、便携 WIFI 和无线网卡；打印机、图形仪、复印机、传真机等。这些设备如果不进行合理管控使用，极有可能将病毒、木马、后门等带到内网当中，从而造成难以预见的破坏；外来人员和内部人员也可能利用这些设备，将内网敏感信息复制打印等传播到外网，造成泄密事件的发生。

根据这些外设的用途，我们将这些设备分成 3 类，具体分类如下：

1）存储设备，如 U 盘、移动硬盘、光盘刻录机、软盘。

2）外联设备，如蓝牙/3G 手机、便携 WIFI 和无线网卡。

3）打印设备，如打印机、图形仪、复印机、传真机。

（2）相关风险点

存储设备管理风险点见表 A-19。

表 A-19

	序　号	风 险 点	风险属性	隐患/风险
外设设备管理	1	光盘刻录机随意使用	原生风险	隐患
	2	光盘刻录不记录	次生风险	风险
	3	软盘随意使用	原生风险	隐患
	4	软盘使用刻录不记录	次生风险	风险
	5	U 盘随意使用	原生风险	隐患
	6	U 盘使用不记录	次生风险	风险
	7	移动硬盘随意使用	原生风险	隐患
	8	移动硬盘使用不记录	次生风险	风险
	9	移动存储卡随意使用	原生风险	隐患
	10	移动存储卡使用不记录	次生风险	风险

外联设备管理风险点见表 A-20。

表 A-20

	序 号	风 险 点	风 险 属 性	隐患/风险
外设设备管理	1	3G 手机随意使用	原生风险	隐患
	2	3G 手机使用不记录	次生风险	风险
	3	蓝牙红外随意使用	原生风险	隐患
	4	蓝牙红外使用不记录	次生风险	风险
	5	便携式 WIFI 和无线网卡随意使用	原生风险	隐患
	6	便携式 WIFI 和无线网卡使用不记录	次生风险	风险

打印设备管理风险点见表 A-21。

表 A-21

	序 号	风 险 点	风 险 属 性	隐患/风险
外设设备管理	1	打印机随意使用	原生风险	隐患
	2	打印机使用不记录	次生风险	风险
	3	扫描仪随意使用	原生风险	隐患
	4	扫描仪使用不记录	次生风险	风险
	5	复印机随意使用	原生风险	隐患
	6	复印机使用不记录	次生风险	风险
	7	传真机随意使用	原生风险	隐患
	8	传真机使用不记录	次生风险	风险

（a）基于资产使用生命周期分析

ⓐ 存储设备基于资产使用生命周期分析

该类风险涉及生命周期阶段为入网阶段、使用阶段、维修阶段及报废阶段。由于存储设备保留有相关信息，因此，在各个阶段保留的相关信息都存在篡改和泄漏的风险。入网前，存储设备在分配的时候就要根据领用人的责职和权限指定分配，没有权限的人禁止领用可存储设备，并做到专盘专用，通过工具进行标签化管理，明确公示管理制度和领用人的责任，不得随意借用。运行过程中，对于存储类设备，尤其是移动存储介质如 U 盘的使用，不仅做到对 USB 接口的管控，还要对 U 盘在网络中的使用严格监视、审计。防止这些存储类设备将外面的病毒、木马在使用的过程中带入内网，也要防止某些人利用这些存储介质私自传递已经开启 USB 接口的终端设备中的敏感信息。因此要对 USB 移动存储设备加强审计，审计其是否修改、删除或者传递过哪些文件夹或者文件。同时，设备维修阶段为特殊阶段，许多在线监控措施和管理规定将会失效，因此，该类设备在维修过程中首先要做脱敏检查，即擦除存储设备中的敏感信息，防止维修过程中敏感信息的泄漏；其次，在设备报废阶段，必须将存储设备消磁，使得其中存储的信息不可能恢复。

ⓑ 外联设备基于资产使用生命周期分析

该类风险涉及生命周期阶段为入网阶段和使用阶段。外联设备关系到网络是否真正隔离，是否存在违规内联和外联的风险。因此，入网阶段，对外联设备就要严格禁止使用，明

确公示管理制度，告知随意通过外联设备接入对内外网隔离是严重违背的，并且存在严重安全风险。运行过程中，对于外联类设备，尤其是 3G 手机的使用，不仅做到对外联设备及时发现和管控，还要对 3G 设备在网络中的使用严格监视、审计。防止这些存储类设备将外面的病毒、木马在使用的过程中带入内网，也要防止某些人利用这些外联设备将内网的终端设备中的敏感信息外传，引发信息泄密风险。

ⓒ 打印设备基于资产使用生命周期分析

该类风险涉及生命周期阶段为运行阶段。由于打印设备涉及敏感信息可能被打印后携带出去的风险。因此，需要对打印设备严格管理。对敏感信息的打印，要指定打印机，不允许将敏感信息通过普通非指定打印机打印，对打印的内容要标记，对打印出来后的敏感信息要管理，临时使用或者弃用的内容要及时粉碎销毁。防止打印设备没有管控以及打印的纸张没有管控造成敏感信息外泄的风险。

（b）相关信息风险分析

ⓐ 在线信息风险

存储设备在线信息风险：特定生产系统需对移动存储介质进行读取和写入，因此，对于该类 U 盘应放开使用，否则会造成业务不可用，同时，又要能识别和禁止其他类别的 U 盘的使用，因此需要对内部使用的 U 盘进行标签化管理，区分 U 盘的类别和使用范围。对于数据需要在外网使用的情况，可以生成文件通过摆渡机和专用 U 盘复制到外网。因为日常工作中需要经常利用 U 盘将内网数据发布到外网，如果不严格管理，业务数据被窃取、篡改，造成的恶劣社会影响，外网感染的病毒、木马也会随着 U 盘的无序使用而进入内网，造成对内网业务系统的威胁，风险非常高。而该类风险如果发生在公文处理系统、单位财务处理系统，以上业务受到影响可能局部范围可控，不会造成重大社会和经济损失，只对内部工作造成影响，因此风险为中。如果该类风险发生在内网网站、档案管理软件中，由于该类信息资产是业务运转不依赖或较少依赖的，脱离该信息资产完全可以生产或开展业务活动，以上业务对实时性要求不高，一般不会对企业和社会造成影响，风险较低。

外联设备在线信息风险：外联设备使用，和内外网隔离的策略是严重违背的，是被严格禁止的。该类风险不仅存在信息外泄和扩散的风险，同时也存在其他所有可能的安全风险和隐患。对整个网络和业务都是极端危险的行为。目前 3G 手机非常流行，而终端设备也具备蓝牙、红外、无线网卡等接口，任何拥有 3G 手机的员工，都可以通过 3G 手机利用手机蓝牙和终端设备的蓝牙链接，使得原本不能上外网的终端通过 3G 手机获得访问外网的途径。同样，利用手机 WIFI，或者手机数据线，一旦手机和终端有了连接通道，就可以搭建手机访问外部网络的通道，而一旦外联通道打通，内联也就随时可能发生了，整体网络的信息安全也就得不到保证。

打印设备在线信息风险：打印设备使用，和整个业务系统都相关，根据业务的重要性要严格管理打印设备的使用。对于重要的生产系统来说，如果不严格管理外设，在日常工作中和需要打印过程中，很容易将客户的个人信息和业务敏感信息打印出来，如果不对打印出来的信息加以管控，就容易导致纸张信息和数据被带出而造成信息外泄，给客户和企业的形象造成恶劣影响，风险较高。因此对于敏感信息打印需要指定打印机和终端。而对于不重要的或者不涉及敏感信息的系统，其影响相对较低。不需要指定 IP 和打印设备。而对于打印出来的包含敏感信息的纸张，对数量和内容都要管理，废弃时必

须彻底粉碎，对该信息的复印也要经过批准，严禁未经批准私自复印敏感文件，防止信息外泄。

ⓑ 存储信息风险：

存储设备存储信息风险：存储在终端设备中的信息可能通过存储设备泄漏出去。

外联设备存储信息风险：存储在终端设备中的信息可能通过外联设备泄漏出去。

打印设备存储信息风险：存储的信息可能通过打印机或者图形仪打印而被携带出去，造成信息外泄。

（c）基于资产使用人员风险分析

ⓐ 存储设备基于资产使用人员风险分析

内部人员：如果高级管理岗位（如高层领导），其存储设备丢失，由于其存储外设中极有可能含有企业核心信息和涉密信息以及个人的敏感文档，可能造成的社会影响非常大，风险非常高。而该类风险发生在部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，则由于像网络管理人员存储介质往往中含有网络拓扑、配置策略、运行业务数据等，由于该类数据一般包含敏感信息，随意传递、刻录极易造成信息外泄，风险较高。而如果光盘刻录，存储设备随意使用风险发生在生产人员、办公人员等，则可能将程序带出，造成知识产权的泄漏，由于该类终端支持业务和对正常运营起保障作用，相当重要，风险为中。

临时人员：如果该类风险发生在临时人员岗位（如食堂、车队、绿化等人员），则该类终端一般不涉及业务、不包含敏感信息，风险为低。

外部人员：如果该类风险发生在外部人员身上，可能造成信息外泄的风险，因此应严格控制外来人员存储设备的使用。外来人员要求任何操作外设的动作必须经过审批，降低可能导致信息外泄的风险。

ⓑ 外联设备人员风险

内部人员：对于高级管理岗位（如高层领导），使用 3G 手机开通网络功能，由于目前 3G 手机安全防护能力薄弱，手机病毒木马犯罪呈现上升趋势。手机一旦中了木马，就可能成为外部控制的监视设备，随时可能被黑客利用，手机和终端设备也会自动搜索蓝牙和 WIFI 智能设备，这样很有可能被别人利用，而一旦被利用，则由于其终端含有涉及企业核心信息和涉密信息，风险非常高。该类风险发生在部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，则由于该类终端对业务支撑非常关键，终端中一般有网络拓扑、配置策略信息等，且一般包含关键业务信息，风险较高。如果该类风险发生在生产人员、办公人员等，则由于该类终端支持业务和对正常运营起保障作用，相当重要，风险为中。

临时人员：如果该类风险发生在临时人员岗位（如食堂、车队、绿化等人员），则该类终端一般不涉及业务、不包含敏感信息，风险为低。

外部人员：如果该类风险发生在外部人员身上，可能造成信息外泄的风险，因此应严格控制外来人员外联设备的使用。外来人员要求任何操作外设的动作必须经过审批，降低可能导致信息外泄的风险。

ⓒ 打印设备人员风险

内部人员：该类风险发生在高级管理岗位（如高层领导），则由于其终端含有企业核心

信息和涉密信息，风险非常高。该类风险发生在部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，则由于该类终端对业务支撑非常关键，且一般包含关键业务信息，风险较高。如果该类风险发生在生产人员、办公人员等，则由于该类终端支持业务和对正常运营起保障作用，相当重要，风险为中。

临时人员：如果该类风险发生在临时人员岗位，如食堂、车队、绿化等人员，则该类终端一般不涉及业务、不包含敏感信息，风险为低。

外部人员：如果该类风险发生在外部人员身上，可能造成信息外泄的风险，因此应严格控制外来人员打印设备的使用。外来人员要求任何操作外设的动作必须经过审批，降低可能导致信息外泄的风险。

（d）合规性要求

合规性要求见表 A-22。

表 A-22

序　号	安 全 类	等级保护（三级）要求	符 合 程 度
1	系统运维管理	7.2.5.4 设备管理（G3） c) 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等 d) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作	符合

2．风险管控

（1）存储设备风险管控

事前处置：常规情况下，建议对移动存储外设采取指定品牌和型号，统一采购和标签化管理的方式。指定的设备只能使用指定的存储设备，非指定的移动存储外设不允许在内网使用。必须建立外设的采购和领用审批流程存，对外设使用进行严格规定，对敏感信息和设备，在存储和传递过程中，必须加密数据用于指定的专用设备，并且只有授权和审批的设备和人才有权限登录，复制下载信息。未经审批的存储设备不允许接入网络，即使接入也无法使用。

事中处置：根据存储设备使用规定下发主机外设控制策略，实施控制措施，并对存储类外设监控。当存储类外设接入时，首先检测是否为符合策略中规定的指定存储类外设，如果不属于指定存储类外设，应向管理中心及时报警，不允许其使用，并记录发生时间，进行系统日志信息的安全存储。对于符合策略要求，属于指定应用类的外设，则允许其使用，但是记录其读、写、删除操作信息，如果数据存储过程中有越权操作或者下载了非授权敏感信息，则应将日志安全存储到管理平台，并提示管理中心。如果存储类外设使用过程中出现问题（如损毁等），则走相应的维护流程。

事后处置：对于违规读写数据行为，进行后续安全审计和操作追踪，并进行违规分析，如果确实属于越权行为，则采取一定的惩罚措施；如果属于误报，则进行策略调整。

管控流程如图 A-16 所示。

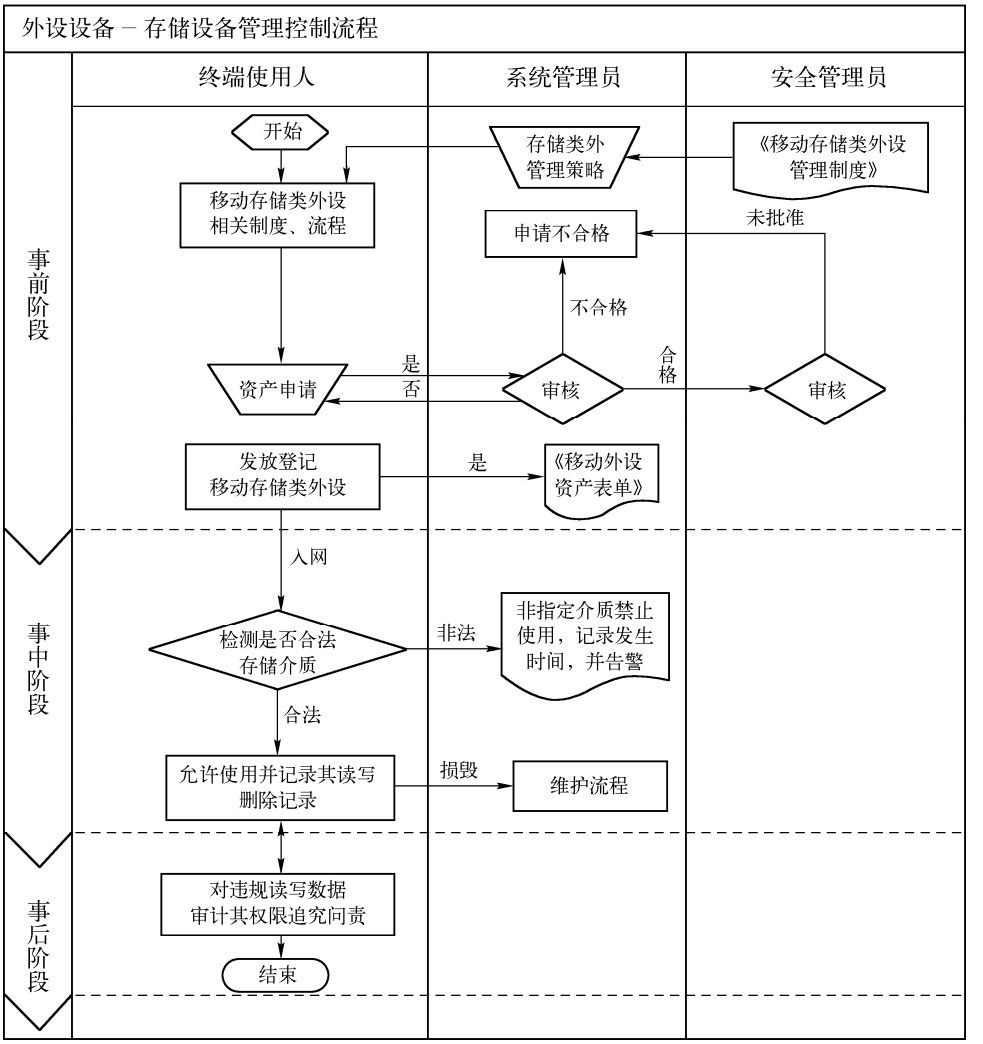

图　A-16

（2）外联设备风险管控

事前处置：外联类设备主要有小巧、使用普遍、不易察觉的特点。比如 3G 手机，应用非常普遍，几乎人手一个，接入信息外网的途径很多，可以通过蓝牙和电脑对接，可以通过手机 PC 套件和电脑连接，也可以通过 WIFI 和电脑连接，管理难度较大。因此终端在入网时必须严格执行端口管理规定，严格管理蓝牙、红外、WIFI、USB 模块，对这一类设备端口下发策略默认关闭，如果需要打开必须经过严格审批。对违反规定擅自使用 3G 手机和电脑连接的责任人一律严肃处理。

事中处置：根据安全需要，下发主机控制策略，实施网络链接控制措施，监控外联类外设，尤其是 3G 手机。首先禁止不必要的端口（如蓝牙、红外端口），尽量切断其接入途径。其次禁止安装手机 PC 套件和相关驱动，通过软件检查，发现违规安装 PC 套件的则禁止使用并告警。最后，主动探测接入网络设备和网卡、Modem，判断是否为手机类设备，如果是，则切断并记录接入时间并告警。

事后处置：对于违规使用 3G 手机和终端联网行为，一经发现则需严格处理，必须建立

后续安全审计和操作追踪，查看是否有信息外泄等违规分析，严重违规的则必须追究其责任，形成高压线，不得触犯。

管控流程见图 A-17。

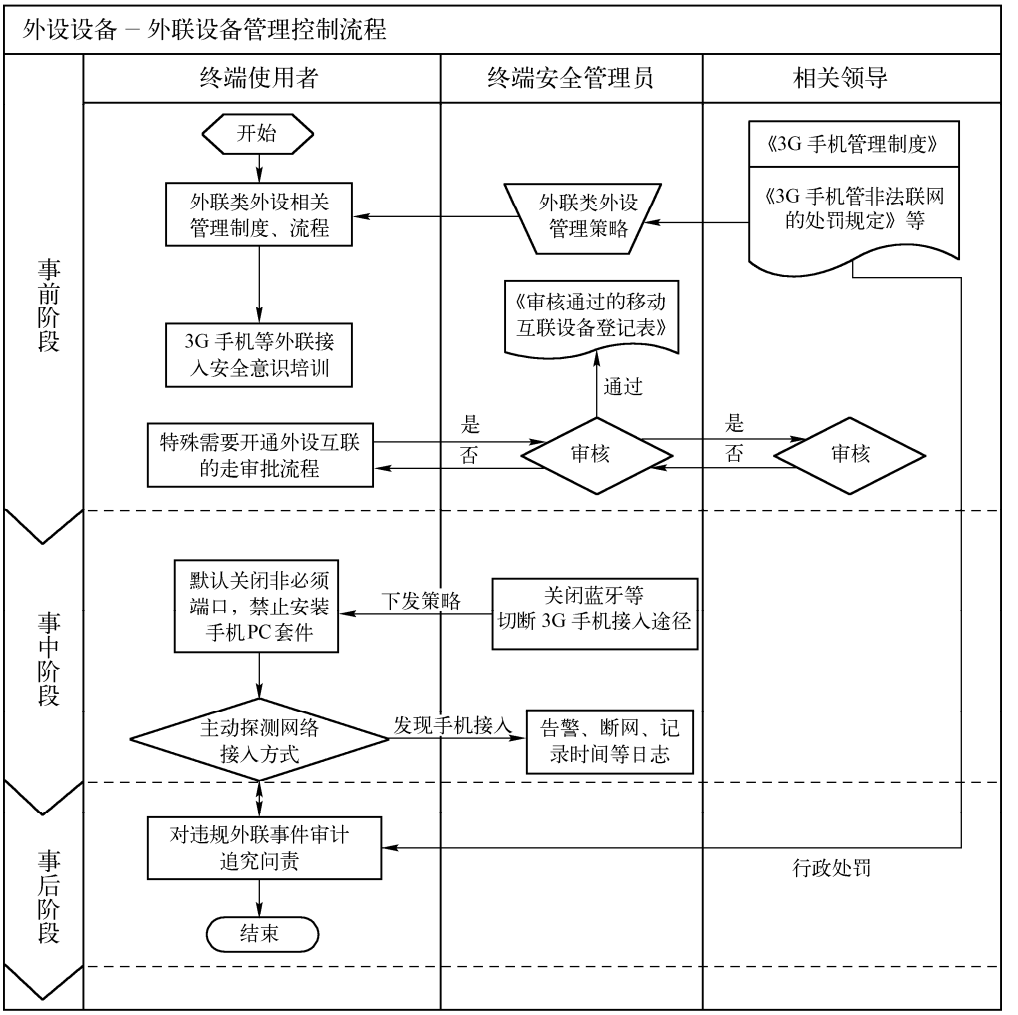

图 A-17

（3）打印设备风险管控

事前处置：打印类设备在办公中普遍使用，如果涉及敏感信息文件的打印和传递就必须指定打印设备，对打印文档的数量、纸张也要严格管控。所以需要建立相应的敏感信息打印设备管理规定。对于敏感信息的打印要指定打印区域，指定打印设备，并且要限定规定地址的终端设备才能访问该打印机。打印出来的文档要建立严格的处置保管制度。

事中处置：根据安全需要，下发主机访问控制策略，未授权的终端不能访问指定的打印设备。对任何企图尝试连接指定打印机的终端应记录其尝试次数，超出规定的，向管理平台告警，并记录日志。

事后处置：对于打印出来的含有敏感信息的文档要登记，记录打印人。文档借出时要登记借阅人，最终销毁要记录销毁时间、销毁人。

终端安全风险管理

对于授权使用外设人员自身违规，擅自将移动存储设备带走，或者将保存有敏感信息的外设和打印的纸张、图片带出单位等情况，终端无法发现。敏感信息接触者通过非技术类手段的泄漏（如拍照、摘抄、电话泄漏等），都无法通过技术手段做到监控。

对策：

1）长期的安全意识培训。

2）适当的人员监督机制。

3）严厉的惩罚措施。

4）保留事件调查、起诉的权利。

5）加强审计追踪。

管控流程见图 A-18。

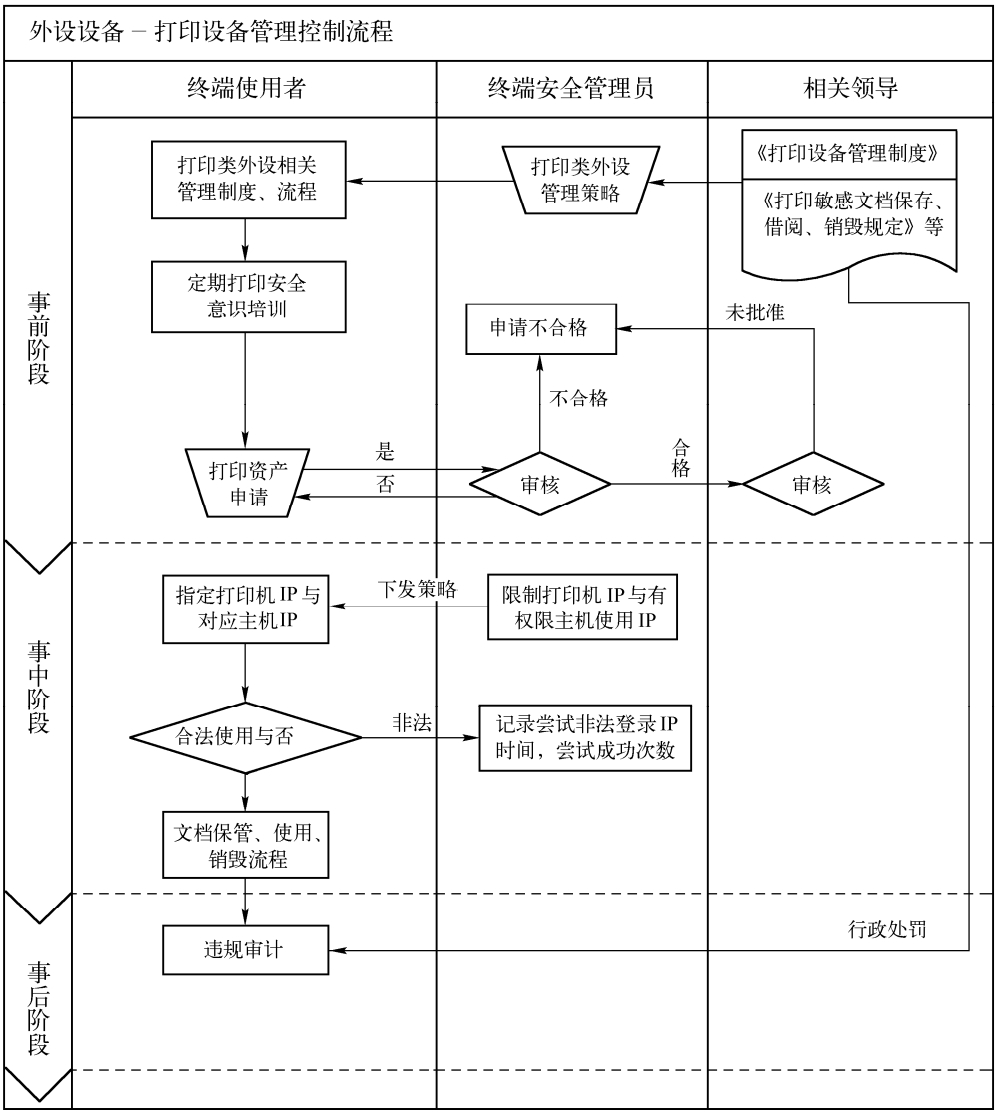

图　A-18

3．风险控制效果

通过对外设设备使用控制流程，能够对外设设备的使用和审批全程进行监控，对常用的存储类外设设备如 U 盘、移动存储等能发现，对读写修改能审计。对 3G 手机、蓝牙、WIFI 接入能发现非法外联，能审计其外联网络。建立对本地打印机、数码图形仪、复印机等设备的指定管理和敏感文件打印的监控。

所有这些控制，都必须建立一套完整的外设管理审批流程和终端防护发现机制。只有实现制度和技术的结合，才能有效管控外设设备的使用。

A.3.3 终端注册表风险（9 个风险点）

1．风险分析

（1）风险描述

注册表是为 Windows 操作系统中所有硬件/驱动和应用程序设计的数据文件。在没有注册表的情况下，操作系统不会获得必需的信息来运行和控制附属的设备和应用程序及正确响应用户的输入。当操作系统需要存取硬件设备，就会使用驱动程序，驱动程序是独立于操作系统的，但是操作系统需要知道从哪里找到它们，包括其文件名、版本号、其他设置和信息，没有注册表对设备的记录，它们就不能被使用。当一个用户准备运行一个应用程序，注册表提供应用程序信息给操作系统，这样应用程序可以被找到，正确数据文件的位置被规定，其他设置也都可以被使用，注册表保存关于缺省数据和辅助文件的位置信息、菜单、按钮条、窗口状态和其他可选项。它同样也保存了安装信息（如日期）、安装软件的用户、软件版本号和日期、序列号等。根据安装软件的不同，它包括的信息也不同。一般来说，注册表控制所有应用程序和驱动，控制的方法是基于用户和计算机的，而不依赖于应用程序或驱动，每个注册表的参数项控制了一个用户的功能或者计算机功能。

注册表作为系统必不可少的组成部分，成为黑客与安全专家们关注的焦点，如果不能对注册表进行很好的管理（如访问、增加、删除、注册表项等操作），终端的安全就得不到保障，黑客或恶意程序就可以轻松地控制终端系统的某些功能或窃取或某些信息。

从终端保护的角度来看，主要的风险主要表现在以下几个方面：

1）监控缺失风险。由于缺少对访问、增加、删除注册表项等操作的监控，会导致关键主机的保护失控的风险。

2）标准基线风险。由于事先没有对注册表项作出详细分析，根据不同的终端做出注册表项白名单，或没有及时更新注册表的监控白名单，导致不能有效地识别终端的异常注册表项，造成不能有效监控注册表项的风险。

3）加载注册表项监控策略导致终端蓝屏，严重影响业务，造成终端业务无法持续有效地运行的风险。

4）控制平台本身风险。发现了异常访问、增加、删除注册表项等操作，但是技术措施不到位，不能及时准确地处理，如采取告警、限制连接等控制措施，实现有效监控的风险。

因此这类风险的可知、可控、可管十分重要。下面对终端注册表风险进行详细的分解。

（2）相关风险点

终端注册表风险点见表 A-23。

表 A-23

风险分类	序　号	风　险　点	风险属性	隐患/风险
终端注册表风险	1	没有对终端注册表系统关键项访问进行监控	原生风险	隐患
	2	没有对终端注册表系统关键项增加进行监控	原生风险	隐患
	3	没有对终端注册表系统关键项删除进行监控	原生风险	隐患
	4	没有对终端注册表用户关键项访问进行监控	原生风险	隐患
	5	没有对终端注册表用户关键项增加进行监控	原生风险	隐患
	6	没有对终端注册表用户关键项删除进行监控	原生风险	隐患
	7	对终端下发的注册表监控策略没有根据需要及时更新	次生风险	隐患
	8	对终端下发的注册表监控策略与某些终端的注册表内容冲突	次生风险	风险
	9	对终端下发的注册表策略被停止或被删除	次生风险	风险

以下将分别从资产使用生命周期、相关信息安全、资产使用人员和合规性 4 个方面对以上 9 个风险点进行详细描述。

（a）基于资产使用生命周期分析

资产使用生命周期包含入网前、运行阶段、维修阶段、报废阶段。终端违规网络访问风险按照资产使用生命周期的分析如下：

风险点（1-6）：涉及入网前、运行阶段。由于微软并没有完全公开关于注册表正确设置的支持信息，这样使得注册表看上去更不可琢磨。处理和编辑注册表如同“黑色艺术”一样，它在系统中的设置让用户感觉象在黑暗中摸索一样找不到感觉。这样，因为用户对这方面的缺乏了解使得注册表更多地出现故障，也正因为如此当前注册表成为黑客与安全专家们关注的焦点，如果不能对注册表进行很好的管理，如访问、增加、删除、注册表项等操作，就不能使终端得到更好的保障，黑客或恶意程序就可以轻松地控制终端系统的某些功能或窃取某些信息，例如控制面板操作功能、桌面外观和图标、网络配置参数、浏览器功能和特征存取控制、登录确认功能、文件和打印机共享功能、网卡设置和协议、系统性能和虚拟内存设置等。

风险点（7-9）：涉及入网前、运行阶段。由于注册表涉及各种硬件和应用，如不能及时和全面地对终端系统做分析，建立系统关键项和用户关键项的注册表白名单，并且该注册表白名单没有随驱动升级和应用改变而及时更新，可能导致注册表监控的基线不准确，控制措施难以实施，甚至会严重影响业务的顺利进行。

（b）基于相关信息安全关系分析

相关信息安全分为在线信息风险和存储信息风险，终端注册表风险按照相关信息安全关系的分析如下：

风险点（1-6）：如果缺失有关注册表的监控措施，一旦注册表被恶意访问、增加、删除，可以导致终端系统所有文件操作都受影响，势必造成业务运行中的在线信息风险和存储信息风险。

风险点（7-9）：如果系统关键项和用户关键项的注册表白名单不能及时升级，一旦造成无法检测遗漏注册表的恶意操作，也会造成业务运行中的在线信息风险和存储信息风险。

（c）基于资产使用人分析

终端使用人包括内部人员、临时人员和外部人员 3 大类，而内部人员可以再细分为高级管理者、关键业务人员和网络管理人 3 种角色，临时人员主要是辅助人员岗位，如食堂、车

队、绿化等人员，而外部人员包括外来厂商运维人员和系统内外来人员。终端的使用者因为不同的角色和不同的操作意图，一个相同的风险点对应不同身份的终端使用人风险级别也不同。以下将终端注册表风险按照终端使用人角色分析如下：

风险点（1-6）：该类风险与内部人员的角色级别有关。

1）高级管理岗位，如区域负责人等高层领导，风险很大。

2）地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，风险较大。

3）网络管理员，风险较大。

对于临时人员和外来人员，如果自带终端的话，风险极大。

风险点（7-9）：该风险对于高级管理岗位，如区域负责人等高层领导的终端的正常使用威胁极大；对于网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员的终端的使用威胁较大；而对于临时人员和外部人员，因无法事先作出注册表基线，风险较大。

（d）合规性要求

合规性要求见表 A-24。

表 A-24

序　号	安 全 类	等级保护（三级）要求	符 合 程 度
1		等级保护要求中没有对此做明确的要求	

2．风险管控

每类风险在管控过程中，针对风险的事前、事中和事后 3 种状态进行监控，做到事前预防、事中控制、事后审计追查。下面的风险管控处理流程，尽量从事前、事中和事后 3 方面对风险管控进行描述。

（1）风险点（1-6）：终端系统注册表监控缺失和基线风险

事前处置：在安全系统被安装前，提前备份注册表内容，并且对系统注册表关键项和用户关注的注册表项进行跟踪，将相关的获取到的信息进行基本的安全分析，主要是对需要关注的注册表数据的正确性、安全性、完整性进行基本的分析，由此确定要被关注的数据是不是正常的或安全的数据。分两种情况处理：安全数据——对于此种数据将进行管理，统一制作系统安全基线，用于规范全网终端系统的安全；

风险数据——对于存在风险的数据，将其作为系统安全相关的事件上报到服务器进行记录，并将此信息告知相关的系统管理人员，同时提醒终端使用者当前存在的信息，要求用户对系统进行彻底的安全检查，特别是注册表的内容。通过以上两种处理方式，保证了系统中安全的注册表数据作为系统的安全恢复依据，同时也能在注册表中存在风险时保证了事件的记录行为，并向用户提示了系统当前的基本安全情况。

事中处置：在安全管理系统被正确安装后，在系统运行期间通过应用层与内核层两层体系结构，对注册表进行全面的保护，任何恶意篡改或未经许可的访问动作都将被禁止并通过报警的方式上报至服务器，由此不仅可以对注册表数据做到有效的保护还可以将存在的风险及时上报到相关的管理人员，相关的管理人员可能通过报警的信息及时发现风险、追查风险的来源，最终将其修复。

事后处置：对于个别情况下所出现的未能及时禁止或处理的操作，由此引发的注册表数据被篡改行为，可以通过事前对于安全的数据所做的备份进行恢复，基本可以保证注册表数据的正常与完整，而对于未经许可的读取数据，则要求通过对于网络数据包审计（网络访问读取）或内核驱动（本地访问读取）来进行控制，最终达到保护数据的安全。

控制流程见图 A-19。

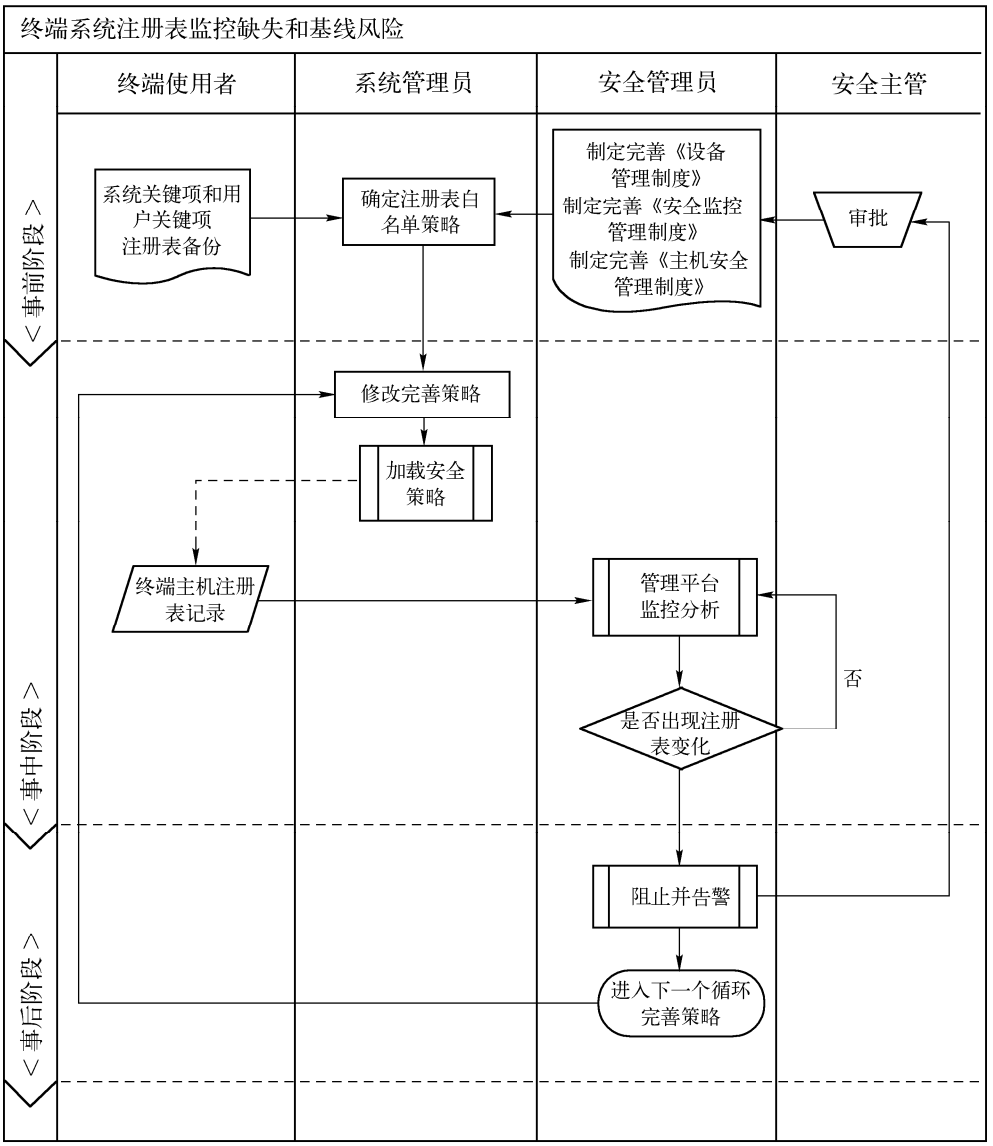

图 A-19

（2）风险点（7-9）：终端系统注册表技术控制风险

事前处置：需要不断完善“从终端上得到反馈”的技术机制，测试验证该机制可以实现；需要制定有关的应急响应预案，一旦出现策略与业务发生冲突时，需要启动；另外，如果有关策略一旦被停止和被删除不能及时更新而技术手段无法实现时需要启动。

事中处置：通过分析实时的通信日志，及时了解注册表白名单策略与某些业务是否冲

突，注册表白名单策略停止和被删除，或者注册表白名单策略已经得到更新，如果在规定的时间内得不到反馈信息，需要启动应急预案；一旦出现策略与业务的兼容性问题，需要有逃生机制，即通过人工卸载策略，确保业务的顺利进行。

事后处置：一旦前面的技术手段都失效，需要在安全主管的认可下启动应急预案。首先在确保业务顺利进行的前提下，人工在本地更新或卸载策略。在此基础上再考虑其他问题，如策略不能更新的故障原因、涉及的部门和人员，造成问题的是平台本身的性能原因，还是其他问题，这些问题是否在管理制度中作出了相关规定，是否需要完善或补充等。

控制流程见图 A-20。

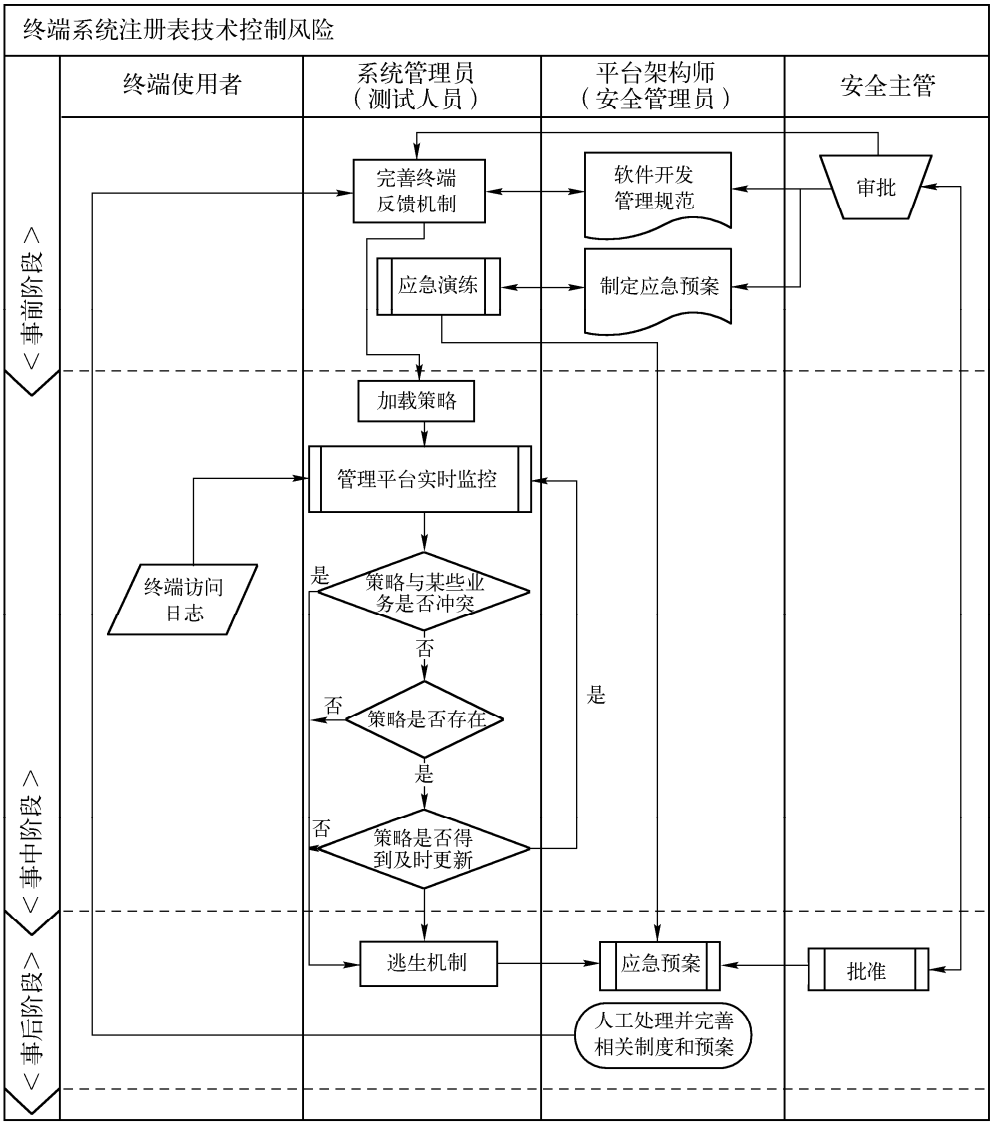

图 A-20

3. 风险控制效果

根据之前在风险管理部分的描述，通过对注册表分别在应用层与内核层两层监视与控制

体系结构，基本上可做到大部分的注册表非法篡改或读取行为在开始修改注册表之前就被禁止，如果有少数操作在篡改数据之前没有被禁止，也可以通过恢复机制在最短的时间内将被修改的数据恢复，最终达到注册表中数据与信息的安全与保密。

A.3.4 终端系统驱动风险（16 个风险点）

1．风险分析

（1）风险描述

驱动程序是添加到操作系统中的一小块代码，其中包含有关硬件设备的信息。有了此信息，计算机就可以与设备进行通信。驱动程序是硬件厂商根据操作系统编写的配置文件，可以说没有驱动程序，计算机中的硬件就无法工作。操作系统不同，硬件的驱动程序也不同，凡是安装一个原本不属于电脑中的硬件设备时，系统就会要求安装驱动程序，将新的硬件与电脑系统连接起来。驱动程序扮演沟通的角色，把硬件的功能告诉电脑系统，并且也将系统的指令传达给硬件，让它开始工作。在 Windows 系统中，需要安装主板、光驱、显卡、声卡，文件系统、网络通信等一套完整的驱动程序。如果需要外接别的硬件设备，则还要安装相应的驱动程序，驱动程序按系统中工作的层次来分，有用户态驱动程序、核心态驱动程序，中间层驱动程序、硬件总线驱动等。

从以上的描述中可以看到驱动程序的种类非常多，且对于终端机器的控制能力也比应用层程序更强，再基于其加载于系统的内核地址空间中，没有任何界面，更增加了驱动恶意程序的隐蔽性，目前流行的黑客软件或病毒程序大部分都是利用驱动的强控制能力与隐蔽性等应用层程序所不具备的特性进行攻击或窃取保密数据。从终端保护的角度来看，主要的风险主要表现在以下几个方面：

1）监控缺失风险。由于缺少对终端驱动程序的监控，这将会导致关键主机的保护失控的风险。

2）标准基线风险。由于事先没有对终端的驱动程序作出详细分析，根据不同的品牌终端做出驱动白名单，可能会造成不能有效地识别终端的异常驱动程序，造成不能有效监控驱动的风险。

3）加载驱动程序监控策略导致终端蓝屏，严重影响业务，造成终端业务无法持续有效运行的风险。

4）控制平台本身风险。发现了异常驱动程序，但是技术措施不到位，不能及时准确地处理，如采取告警、限制连接等控制措施，实现有效监控的风险。

因此这类风险的可知、可控、可管十分重要。下面对终端系统驱动风险进行详细分解。

（2）相关风险点

终端系统驱动风险点见表 A–25。

以下将分别从资产使用生命周期、相关信息安全、资产使用人员和合规性 4 个方面对以上 16 个风险点进行详细描述：

（a）基于资产使用生命周期分析

资产使用生命周期包含入网前、运行阶段、维修阶段、报废阶段。终端违规网络访问风险按照资产使用生命周期的分析如下：

风险点（1-7）：涉及入网前、运行阶段。由于驱动程序的种类繁多，且对于终端机器的

控制能力也比应用层程序更强，再基于其加载于系统的内核地址空间中，没有任何界面，更增加了驱动恶意程序的隐蔽性，目前流行的黑客软件或病毒程序大部分都是利用驱动的强控制能力与隐蔽性等应用层程序所不具备的特性进行攻击或窃取保密数据。通过驱动可以轻松完成以下的工作，如监控终端系统的所有文件操作；监控终端系统的所有网络数据包发送或接收；监控终端系统的打印文档；如果将驱动与应用层程序结合，更是可以做到几乎任何任务，如窃取用户口令、窃取用户隐私数据、拦截系统视窗的消息。

表 A-25

风险分类	序号	风险点	风险属性	隐患/风险
终端流量异常风险	1	没有监控终端系统的打印机驱动程序驱动文件加载、修改、删除操作	原生风险	隐患
	2	没有监控终端系统的显卡/声卡驱动程序驱动文件加载、修改、删除操作	原生风险	隐患
	3	没有监控终端系统的网卡驱动程序驱动文件加载、修改、删除操作	原生风险	隐患
	4	没有监控终端系统的总线驱动程序驱动文件加载、修改、删除操作	原生风险	隐患
	5	没有监控终端系统的硬盘驱动器驱动程序驱动文件加载、修改、删除操作	原生风险	隐患
	6	没有监控终端系统的文件系统驱动程序驱动文件加载、修改、删除操作	原生风险	隐患
	7	没有监控终端系统的扫描仪、数码相机驱动程序驱动文件加载、修改、删除操作	原生风险	隐患
	8	没有对终端系统的打印机驱动程序做分析，建立白名单	原生风险	隐患
	9	没有对终端系统的显卡/声卡驱动程序做分析，建立白名单	原生风险	隐患
	10	没有对终端系统的网卡驱动程序驱动程序做分析，建立白名单	原生风险	隐患
	11	没有对终端系统的总线驱动程序做分析，建立白名单	原生风险	隐患
	12	没有对终端系统的硬盘驱动程序做分析，建立白名单	原生风险	隐患
	13	没有对终端系统的文件系统驱动程序做分析，建立白名单	原生风险	隐患
	14	没有对终端系统的扫描仪、数码相机驱动程序做分析，建立白名单	原生风险	隐患
	15	下发策略与某些终端冲突	次生风险	风险
	16	下发策略被停止或被删除	次生风险	风险

风险点（8-14）：涉及入网前阶段。由于终端涉及的品牌，种类繁多，操作系统不一，而驱动程序又涉及各种硬件和应用，不能及时和全面地对终端系统的各种驱动程序做分析，建立白名单，一旦驱动升级和改变，白名单也没有及时升级，导致驱动监控的基线不准确，控制措施难于实施。

风险点（15-16）：涉及入网前阶段和运行阶段。一旦下发的驱动程序监控策略与终端发生冲突，或策略被删除或强行停止，均可能导致终端不能正常运行，给业务连续性带来风险。

（b）基于相关信息安全关系分析

相关信息安全分为在线信息风险和存储信息风险，终端流量异常风险按照相关信息安全关系的分析如下：

风险点（1-7）：如果缺失有关驱动程序的监控措施，一旦被驱动恶意程序加载，可以监控终端系统的所有文件操作，因此必将造成业务运行中的在线信息风险和存储信息风险。

风险点（8-14）：如果驱动程序白名单不能及时升级，一旦遗漏驱动恶意程序，也会造成业务运行中的在线信息风险和存储信息风险。

风险点（15-16）：该风险点最大的威胁在于可能造成蓝屏、外设不能正常使用，导致终端不能正常使用，因此必将造成业务运行中的在线信息风险和存储信息风险。

（c）基于资产使用人分析

资产（终端）使用人包括内部人员、临时人员和外部人员三大类，而内部人员可以再细分为高级管理者，关键业务人员和网络管理人三种角色，临时人员主要是辅助人员岗位，如食堂、车队、绿化等人员，而外部人员包括外来厂商运维人员和系统内外来人员。终端的使用者因为不同的角色和不同的操作意图，一个相同的风险点对应不同身份的终端使用人风险级别也不同。以下将终端系统驱动风险按照终端使用人角色分析如下。

风险点（1-7）：该类风险与内部人员的角色级别有关。

1）高级管理岗位，如区域负责人等高层领导，风险很大。

2）地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，风险较大。

3）网络管理员，风险较大。

对于临时人员和外来人员，如果自带终端的话，风险极大。

风险点（8-14）：该风险对于高级管理岗位，如区域负责人等高层领导的终端的正常使用威胁极大，对于网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员的终端的使用威胁较大，而对于临时人员和外部人员，因无法事先作出驱动程序基线，风险较大。

风险点（15-16）：该风险还是跟内部人员的角色级别有关。

a）高级管理岗位，如区域负责人等高层领导，风险很大。

b）地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，风险较大。

c）网络管理员，风险较大。

d）合规性要求

合规性要求见表 A-26。

表 A-26

序　号	安 全 类	等级保护（三级）要求	符 合 程 度
1		等级保护要求中没有对终端驱动做出明确的要求。	

2．风险管控

每类风险在管控过程中，针对风险的事前、事中和事后 3 种状态进行监控，做到事前预防、事中控制、事后审计追查。下面的风险管控处理流程，尽量从事前、事中和事后 3 方面对风险管控进行描述。

（1）风险点（1-14）：终端系统驱动监控缺失和基线风险

事前处置：对于类似风险，需要制定一系列的管理措施，如《主机安全管理制度》，其中需要针对现有不同的品牌终端，按照不同的操作系统、外设、存储做出驱动文件的白名单文件，形成驱动监控策略。

事中处置：安装终端防护工具，在终端系统运行期间，监控和防护在终端系统的关键位置，结合主动防御技术，进行全面的监控，任何访问或数据的修改都将被记录在案，而对于管理人员所关注的内容或被管理人员定义为违规的行为将被禁止。但因为在驱动中有许多动

作发生没有关联性，所以对于驱动中的行为难以甚至无法进行行为关联分析，所以有些情况会需要用户配合进行，由用户来决定禁止或允许。

事后处置：如果存在个别的驱动不能被禁止也不能被自动卸载，可以通过报警的方式通知管理人员，由管理人员进行人工卸载或处理，如果人工也不能处理则可以尝试用以前的驱动备份进行恢复。

控制流程见图 A-21。

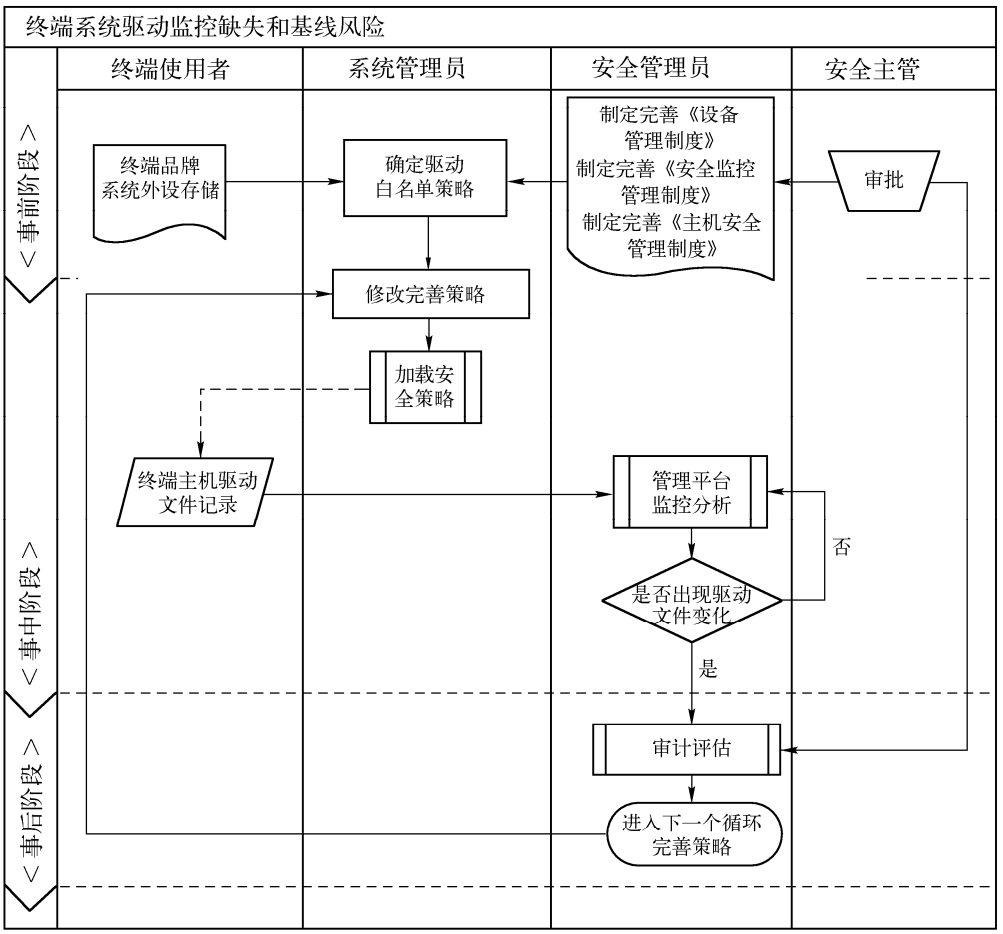

图 A-21

（2）风险点（15-16）：终端系统驱动技术控制风险

事前处置：需要不断完善“从终端上得到反馈”的技术机制，测试验证该机制可以实现；需要制定有关的应急响应预案，一旦出现策略与业务发生冲突时，需要启动；另外，如果有关策略一旦被停止和被删除不能及时更新而技术手段无法实现时需要启动。

事中处置：通过分析实时的通信日志，及时了解驱动程序白名单策略与某些业务是否冲突，驱动程序白名单策略停止和被删除，或者了解驱动程序白名单策略已经得到更新，如果在规定的时间内得不到反馈信息，需要启动应急预案；一旦出现策略与业务的兼容性问题，需要有逃生机制，即通过人工卸载策略，确保业务的顺利进行。

事后处置：一旦前面的技术手段都失效，需要在安全主管的认可下启动应急预案。首先

在确保业务顺利进行的前提下，人工在本地更新或卸载策略。在此基础上再考虑其他问题，如策略不能更新的故障原因、涉及的部门和人员，造成问题的是平台本身的性能原因，还是其他问题，这些问题是否在管理制度中作出了相关规定，是否需要完善或补充等。

控制流程见图 A-22。

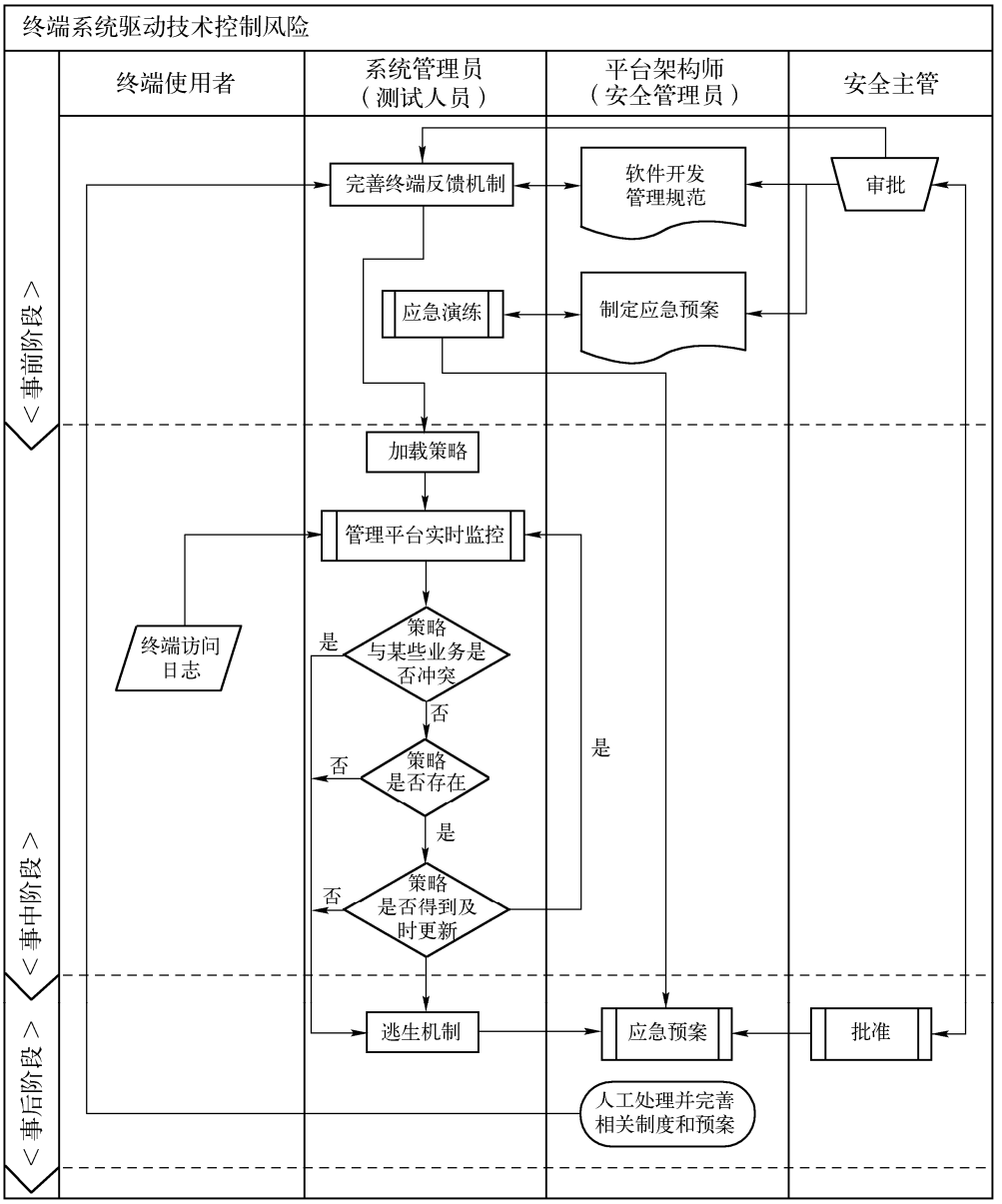

图　A-22

3．风险控制效果

在通过以上所描述的全面监控结合主动防御技术的安全管理控制下，基本上能保证当前系统中的正常合法驱动不被破坏，同时非法的恶意驱动程序不能被安装，即使安装了在进行数据访问或修改时也会被禁止，同时被禁止的动作也会被上报到服务器，以供管理人员进行

分析与处理，如果确实存在个别的驱动难以控制或处理，也可以通过报警的方式上报给管理人员，进行人工卸载或恢复，通过以上一系列的处理，基本可以做到终端机器在面对恶意驱动程序时能够对关键或保密的数据进行有效的保护，同时对难以处理的驱动向管理人员报警，要求人工协助或操作。

A.3.5 基本配置风险（6 个风险点）

1．风险分析

（1）风险描述

客户端计算机安全配置的选项非常多而且复杂，如果配置不好，往往会造成重要数据的泄漏；不能及时跟踪和发现潜在的安全配置问题，将导致终端一直处于数据泄漏状态。终端安全配置选项繁多，并且配置时需要专业的安全技术，单靠终端使用者的自行配置，很难达到安全标准。而一个局域网内有上百台终端，单靠网络管理人员很难对网络内的终端进行快速配置和检查。目前对于终端的配置，推荐使用终端安全配置中心的方式，通过终端安全配置中心根据用户角色对终端实现全方位的安全等级配置，从而降低因为终端配置而带来的安全风险。

终端的安全配置中心保存着多种整体的安全配置策略，每个配置策略涉及了整个终端的安全；一个配置策略对应一个安全等级，等级分为高级、中级、一般。终端的配置中心会根据网络管理员的指令自动应用相应的等级配置。

配置中心安全等级分类：高级、中级、一般。配置的选项可以根据用户要求定制，目前根据行业里的安全标准优先定义如表 A-27。

表 A-27

配 置 项	描 述	高级	中级	一般
补丁升级	系统补丁升级配置选项应该打开	必选	必选	可选
软件防火墙	软件防火墙开启	必选	必选	可选
用户身份	对用户权限的设置（如 Guest，User）；远程用户登录的设置	必选	必选	可选
网络设置	IP/MAC 的绑定	必选	必选	可选
IE 浏览器的设置	IE 里的设置选项很多（如禁止 BHO 的加载，非法弹出广告等）	必选	可选	可选
启动项的设置	自启动列表里启动项的设置和控制	必选	可选	可选
屏保的设置	屏保的目的是当使用者离开终端时，避免其他人员绕开身份认证，直接以当前已登录的身份操作，而采取的一种保护方式。	必选	可选	可选
用户定制的安全设置	定制设置根据用户特定的安全需求来对机器的设置	必选	可选	可选

（2）相关风险点

终端基本配置风险点见表 A-28。

表 A-28

	序号	风 险	属 性	隐患/风险
基本配置风险	1	通过安全配置中心给终端下发了基本配置策略，终端修改了基本配置	原生风险	隐患
	2	终端修改了基本配置，没有提示终端用户	原生风险	隐患
	3	终端修改了基本配置，审计信息没有上报管理员	原生风险	风险
	4	终端修改了基本配置，没有产生告警	原生风险	风险
	5	安全配置中心给终端下发的基本配置策略没有及时更新	次生风险	风险
	6	从终端上获取的基本配置信息不完整，无法配置基线比较	残余风险	风险

（a）基于资产使用生命周期分析

该类风险涉及入网前、运行阶段。入网前由于终端资产不包含敏感信息和数据，风险较低。入网后，由于运行过程中涉及敏感信息和生产数据，如果不加以控制，导致的损失较大，风险较高。基本配置风险对终端的影响在资产使用生命周期的体现如下。

风险点（1-6）：入网前，不能对终端下发配置策略，此时终端的配置完全取决于终端本身，如果配置的策略不合理，会导致终端的一些信息泄漏或服务开放，但因为其还没有接入到网络，风险较低。

进入运行阶段后，可以通过配置中心给其下发策略，如果终端配置的基本配置策略不合理，会导致终端上一些信息泄漏，开放的服务可以为其他不合法的终端访问，风险较高。

维护阶段和报废阶段，基本配置不合理，风险较低。

（b）与信息安全关系

基本配置的风险涉及在线信息安全风险和存储信息风险。

风险点（1-6）：基本配置不合理，如果配置开放了一些端口或服务，会造成在线信息泄漏的风险。对存储信息而言，因为配置不合理，一些端口或服务开放，可以对存储信息进行查看或修改，存在信息泄漏或篡改的风险。

（c）基于资产使用人分析

风险点（1-6）：任何岗位角色都涉及终端的基本配置不合理的风险。因此，该风险与内部人员相关：

a）高级管理岗位，如区域负责人等高层领导。

b）地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员。

c）开发人员、研发人员等，需要根据业务和工作需要对不同的终端执行不同的终端基本配置策略。

临时人员：辅助人员岗位（如食堂、车队、绿化等人员），该类人员在使用终端的过程中，不允许改变终端的基本配置。

外来人员：外来厂家人员、外来维护人员一般情况下，是不赋予基本配置的更改权限的，如果因为工作需要，需要先将更改的配置项报批，在基本配置变更中备案后，再根据相关的政策对终端的基本配置做修改。

d）合规性要求

合规性要求见表 A-29。

表 A-29

序　号	安 全 类	等级保护（三级）要求	符 合 程 度
1	系统运维管理	7.2.5.7 系统安全管理（G3） d) 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定	符合

2．风险管控

每类风险在管控过程中，针对风险的事前、事中和事后 3 种状态进行监控，做到事前预防、事中控制、事后审计追查。下面的风险管控处理流程，尽量从事前、事中和事后 3 方面

对风险进行管控。

（1）风险点（1-4）：终端用户对下发的基本配置进行修改的管理控制风险

事前处置：根据用户的角色来给出安全配置等级，如高层领导，则由于其终端含有企业核心信息和涉密信息，配置等级应该是高级，还有部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，也应该是高级。终端配置等级的配置项必须严格遵循国家的等级保护条款，只能增加新的配置选项，而不能漏掉等保里要求的设置选项。自动配置能识别当前系统环境，并能成功应用等级配置策略，终端能正确安装设置运行。

事中处置：配置中心根据当前终端配置信息对比应用的等级配置策略来发现配置上的漏洞，及时通知管理员；管理员必须立即作出回复等级配置操作。

事后处置：对于该类风险，保留日志记录，如果出现安全事件，可以追溯责任人。

控制流程见图 A-23。

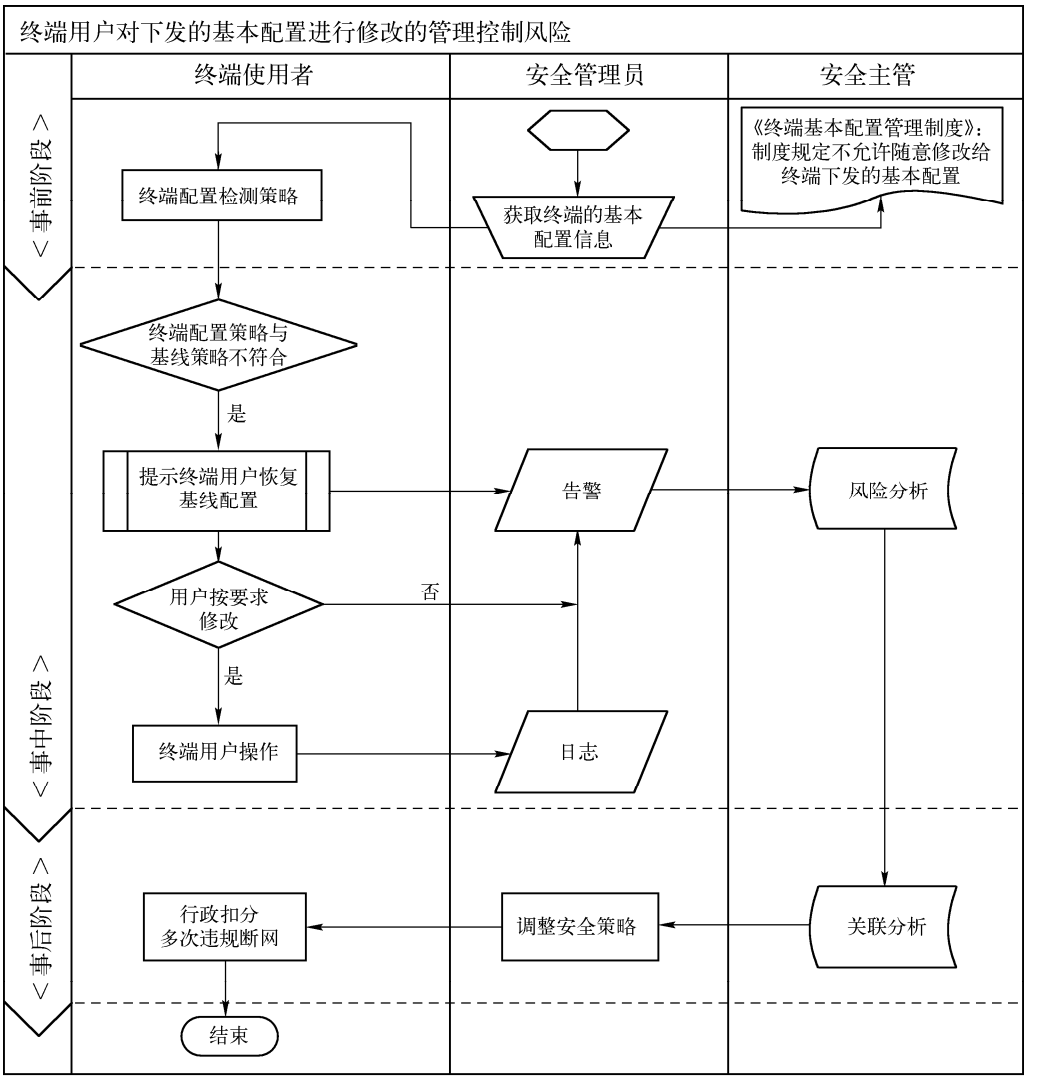

图 A-23

（2）风险点（5）

对这块风险的控制主要是制度上的管控，及时调整给不同终端下发的策略，保证这个基线的策略是符合实际要求的。

（3）风险点（6）

残余风险，对终端的配置信息进行了获取，但获取的配置信息不准确，导致后续与基线的比较结果不准确。属于技术管控下的残余风险。

3．风险控制效果

配置中心快速解决掉局域网内的终端因为配置上存在的安全漏洞而泄漏重要信息。所有的配置操作都是自动完成，方便快速地提高了终端的安全。

附录 B　终端安全运行风险

终端安全运行风险（RR:Running Risk）管理是终端在运行过程产生的风险，包括网络运行安全风险、终端运行安全风险和网络边界风险 3 大类。

终端安全运行风险管理为整个终端安全管理平台所需要管理的核心部分，主要包括在终端安全防护平台中涉及的所有有关风险的事件。

终端安全运行风险详见图 B-1。

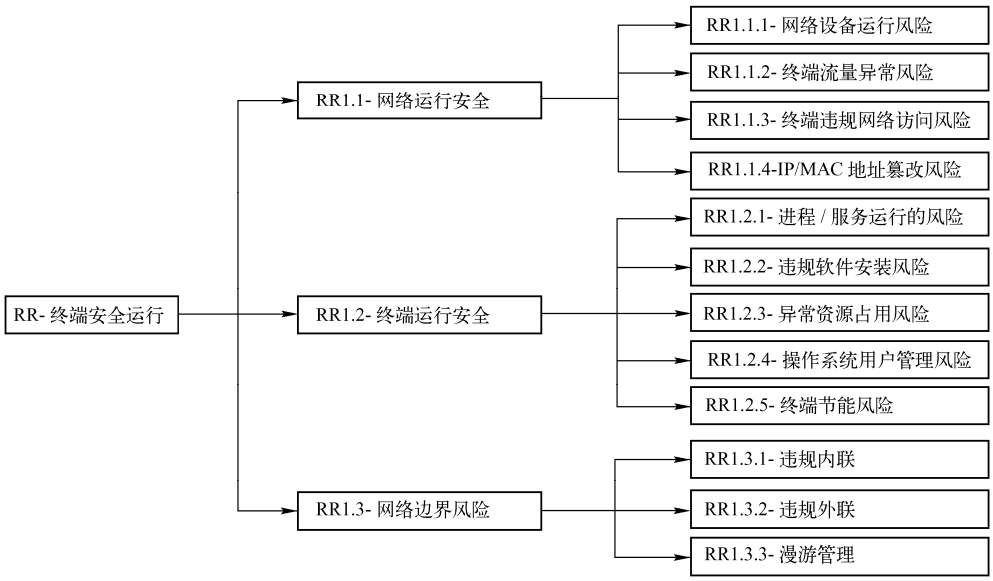

图　B-1

B.1　网络运行安全（RR1.1）

B.1.1　网络设备运行风险（12 个风险点）

1．风险分析

（1）风险描述：

网络逐渐扩大，设备越来越多，网络设备信息的收集和设备管理变得日益复杂和繁重，对网络管理也提出了更高的要求。网络管理中最常用的管理方式是网络拓扑发现，通过网络拓扑发现，可以获取和维护网络节点的存在信息和它们之间的连接关系信息，可以收集网络设备的信息，并在此基础上绘制出整个网络拓扑图。在遇到紧急情况时，能根据网络拓扑及

时定位终端的位置并做出相应的调整。对网络设备的运行实行可知、可控、可管十分重要。

该类风险主要表现为，因为环境、硬件、通信等方面缺少管理制度、流程和技术监控，造成网络设备运行的无序，具体表现为以下 4 个方面:

1）环境风险。由于一般的接入层网络设备没有单独的机房，一般就安装在办公室和走廊的角落，灰尘、温度、湿度、线路布置等方面的考虑不够，因此可能在这些方面出现运行风险。

2）硬件风险。这里主要是指设备本身器件老化导致设备可用性下降，出现经过一段时间的使用后的死机，转发速率下降的情况。

3）通信风险。网络通信具有交互性、传播性，连通性，如果不能及时、有效地知晓终端与终端之间、终端与业务服务器之间的连接关系，进而将这些连接关系以视图的方式提供给管理员，在大型网络中一旦某台主机发生故障例如主机感染蠕虫等传播性、攻击性病毒导致断网事件，由于缺乏基础的网络设备布局或拓扑图，则网络管理人员去定位故障机器物理位置连接情况将是非常耗费人力和时间的，如果遇到紧急情况未能及时定位主机的位置并做出调整，就会给整个网络造成影响和危害，造成依赖网络的业务不能及时恢复。

4）监控工具本身性能风险，由于使用工具监控网络运行状态的技术手段的不足，不能收集到所有的网络事件，或者不能全部分析，造成监控不能及时发现所有的网络运行，或者不能对所有的违规网络运行及时告警或处理，造成安全策略执行不到位甚至给业务带来极大的安全风险。

下面将对网络设备运行风险进行详细的分解。

（2）相关风险点

网络设备运行风险点详见表 B-1。

表 B-1

	序号	风险点	风险属性	隐患/风险
网络设备运行风险	1	温度、湿度等环境因素导致网络设备运行风险	原生风险	隐患
	2	设备老化导致网络设备运行风险	原生风险	隐患
	3	网络通信状态、拓扑不明	原生风险	隐患
	4	缺乏基本的网络运行基线	原生风险	隐患
	5	不能及时获取温度、湿度等环境因素	次生风险	隐患
	6	没有对网络设备的规定使用周期进行追溯	次生风险	隐患
	7	没有对网络运行环境、网络运行拓扑等基础信息做详细的调查了解，或者没有及时更新	次生风险	隐患
	8	没有及时获取网络设备的运行情况和联网信息	次生风险	隐患
	9	不能自动发现终端设备之间、终端设备与关键业务资产的连接关系	次生风险	隐患
	10	没有根据发现的连接关系自动绘制并更新拓扑图	次生风险	隐患
	11	管理平台不能远程监控管理全部网络设备和终端	残余风险	隐患
	12	管理平台事件记录不全，导致某些事件后续无法追溯	残余风险	隐患

以下将分别从资产使用生命周期、相关信息安全、资产使用人员、和合规性 4 个方面对以上 12 个风险点进行详细描述。

（a）基于资产使用生命周期分析

资产使用生命周期包含入网前、运行阶段、维修阶段、报废阶段，网络设备运行风险按照资产使用生命周期的分析如下。

风险点（1、5）：涉及运行阶段，在这个阶段，需要保证终端运行的温度和湿度在国家标准的范围之内。否则可能引起终端运行不正常。

风险点（2、6）：涉及资产的整个生命周期。终端在入网前，需要登记该设备的 IP、MAC 地址，CPU、主板、硬盘的型号和序号以及登记日期，并确定正常的使用寿命期限；在运行阶段，需要判断是否已经超出了使用寿命期限，一旦超过，需要向管理员上报，并且要求管理员反馈是否已经接收并及时处理；在维修阶段，需要在资产管理平台中及时更新硬件变化的信息，入网前重新走入网流程。

风险点（4、7）：涉及入网前、运行阶段、维修阶段。由于缺乏基础的网络设备布局或拓扑图，一旦出现断网情况，不能及时找到故障点。在入网前，没有了解网络设备或终端的 IP 地址、机器名、接入网络设备端口号、具体地理信息（单位、楼层、房间号等）、关键业务服务器名称等，或者是有这些信息但是没有及时更新这些基线信息，导致不能掌握及时的网络态势。

风险点（3、8、9、10）：涉及运行阶段。如果不能及时、有效地知晓终端与终端之间、终端与业务服务器之间的连接关系，一旦网络出现蠕虫爆发、大规模攻击造成网络瘫痪的局面，就会给严重依赖网络的关键业务带来严重的风险。具体情况分为有网络设备的运行情况和联网信息不能获取，终端与终端之间的信息不能获取，终端和服务器之间的信息不能获取 3 类，或者这些信息不能及时传送给管理员，不能及时绘制并更新拓扑图，势必带来业务中断的风险。

风险点（11、12）：涉及运行阶段，如果技术上监控网络运行状态的技术手段的不足，不能收集到所有的网络事件，或者不能全部分析，则造成监控不能及时发现所有的网络运行，或者不能对所有的违规网络运行及时告警或处理，造成安全策略执行不到位。将会给业务带来极大的安全隐患。

（b）基于相关信息安全关系分析

相关信息安全分为在线信息风险和存储信息风险，网络设备运行风险按照相关信息安全关系的分析如下。

风险点（1、2、5、6）：如果环境条件和硬件信息不能及时知晓并采取相应措施，则网络设备运行会面临威胁，涉及在线和存储信息风险。

风险点（3、8、9、10）：如果不能及时、有效地知晓终端与终端之间、终端与业务服务器之间的连接关系，一旦网络出现蠕虫爆发、大规模攻击造成网络瘫痪的局面，就会给严重依赖网络的关键业务带来严重的风险，影响在线信息的正常处理，涉及在线信息安全风险。

风险点（4、7）：如果没有能够及时反映网络环境的拓扑，一旦出现网络事件，会带来无法及时、准确定位的风险，涉及在线信息和存储信息风险。

（c）基于资产使用人分析

资产（终端）使用人包括内部人员、临时人员和外部人员 3 大类，而内部人员可以再细分为高级管理者、关键业务人员和网络管理人 3 种角色，临时人员主要是辅助人员岗位（如食堂、车队、绿化等人员），而外部人员包括外来厂商运维人员和系统内外来人员。终端的使用者因为不同的角色和不同的操作意图，一个相同的风险点对应不同身份的终端使用人风险级别也不同。将网络设备运行风险按照终端使用人角色分析如下。

风险点（1-2）：人员风险，涉及内部人员、临时人员、外部人员相关，如果没有及时有效的机房防护措施和机房管理制度，一旦出现临时人员、外部人员因为不熟悉环境，就可能

出现磕碰网线、电源造成断网风险。

风险点（3-4）：对于内部人员，需要对其使用的机器名、IP 地址、MAC 地址、接入网络设备的端口号等基本信息做出详细的调查和统计，否则一旦出现网络运行故障，不能及时定位到人。

风险点（3-4）：对于临时人员和外来人员，如果自带电脑入网，没有及时将机器名、IP 地址、MAC 地址、接入网络设备的端口号等基本信息收集下来更新拓扑的话，一旦因这些电脑的问题导致内部断网的话，给内部网络环境带来较大风险。

风险点（5-6）：对于内部人员的使用终端的环境及时获取，并需要追溯其使用周期，否则会出现风险。

风险点（7，8，9，10）：对于内部人员来说，他们之间的访问，他们跟业务主机之间的访问、运行情况和联网信息需要及时掌控，否则会给内部环境带来较大的风险；对于外部人员来说，更要严密监控其网络行为，避免给内部网络带来严重的风险。

风险点（11-12）：如果平台性能不足，不能监控管理全部网络设备和终端，最大可能的风险还是会来自外来人员，其次是内部关键业务人员和网络管理员，再次是临时人员。

（d）合规性要求

合规性要求见表 B−2。

表 B−2

序号	安全类	等级保护（三级）要求	符合程度
1	网络安全	7.1.2.1 结构安全（G3） a) 应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要 b) 应保证网络各个部分的带宽满足业务高峰期需要 c) 应在业务终端与业务服务器之间进行路由控制，建立安全的访问路径 d) 应绘制与当前运行情况相符的网络拓扑结构图 e) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段 f) 应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段 g) 应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主机	符合
2	网络安全	7.1.2.3 安全审计（G3） a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录 b) 审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息 c) 应能够根据记录数据进行分析，并生成审计报表 d) 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等	符合

2．风险管控

每类风险在管控过程中，针对风险的事前、事中和事后 3 种状态进行监控，做到事前预防、事中控制、事后审计追查。下面的风险管控处理流程，尽量从事前、事中和事后 3 方面对风险进行管控

（1）风险点（1、5）：网络设备运行环境风险

事前处置：根据有关标准，制定《设备管理制度》、《资产管理制度》等管理制度，详细规定如湿度和温度的具体设定值；并且在相应的应急预案中明确一旦环境因素超出了规定值后需要采取的应急措施，并且有关人员需要按照应急措施定期演练，以达到熟悉的程度。

事中处置：根据设定的湿度和温度值，周期检测，当发现环境因素风险时，及时采取技术手段处理，并记录。

事后处置：一旦技术手段采取后无法取得效果，或人工发现技术手段已经失效，需要通过人工流程加以干涉。

控制流程见图 B-2。

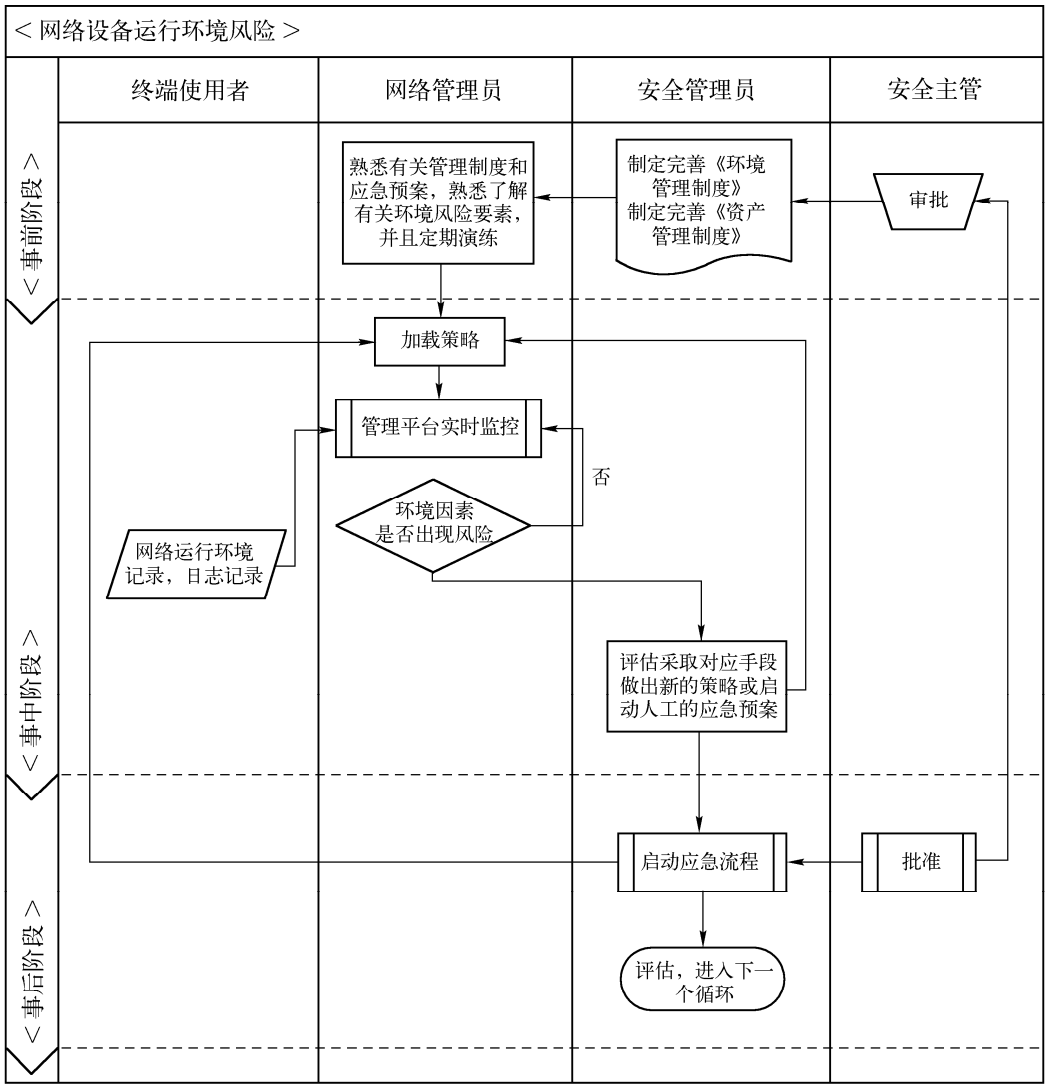

图 B-2

（2）风险点（2、6）：网络设备老化风险

事前处置：对于类似风险，需要针对现有终端和其他网络设备做出周密调查和检测，严格执行《资产管理制度》和《设备管理制度》，在入网前,需要在登记入网时记录该设备的 MAC 地址、CPU、主板、硬盘的型号和序号，以及登记日期，并确定正常的使用寿命期限。

事中处置：在运行阶段需要判断该设备是否已经超出了使用寿命期限。一旦超过，需要向管理员上报，并且要求管理员反馈是否已经接收并及时处理。在维修阶段需要在资产管理

平台中及时更新硬件变化的信息，入网前重新走入网流程。

事后处置：监控平台需要将在网设备即将到期或已经到期的设备列出清单，供安全主管拟定设备更新计划。

控制流程见图 B-3。

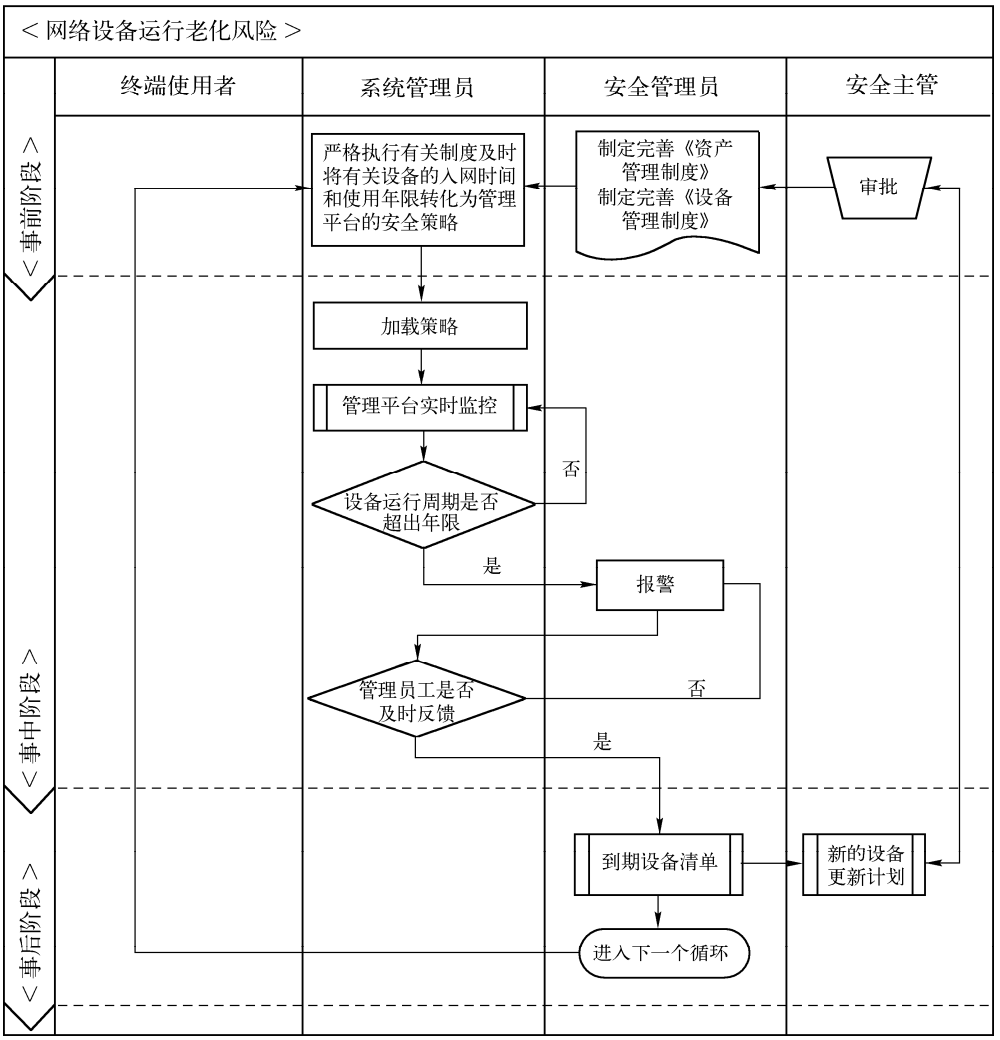

图 B-3

（3）风险点（3、4、7、8、9、10）：网络设备运行基线和通信风险

事前处置：对于类似风险，需要针对现有终端和其他网络设备做出周密调查和检测，将其网络属性如 IP 地址、主机名和 MIB 信息完整收集上来，根据不同类型的设备，分别用基于 SNMP 的网络拓扑发现方法，基于通用协议（ping，ARP，telnet）的网络拓扑发现方法，基于路由协议的网络拓扑发现方法这 3 种方法，最终映射为拓扑自动发现系统的策略。需要了解和掌控终端与终端之间，终端与业务主机之间的访问，运行情况和联网信息。以此作为监控终端通信的基线。

事中处置：将上述的拓扑和基线映射为安全策略并加载到管理平台中；通过管理平台对网

络设备的运行情况进行监控，发现设备拓扑是否变化，是否出现新的节点，一旦发现异常，需要及时报警。如果可以通过技术手段解决，就通过技术手段解决，否则需要向主管及时报警。

事后处置：一旦技术手段采取后无法取得效果，或人工发现技术手段已经失效，需要通过人工流程加以干涉。安全主管根据实际情况启动应急流程，通过管理和人工的办法消弭风险。

控制流程见图 B-4。

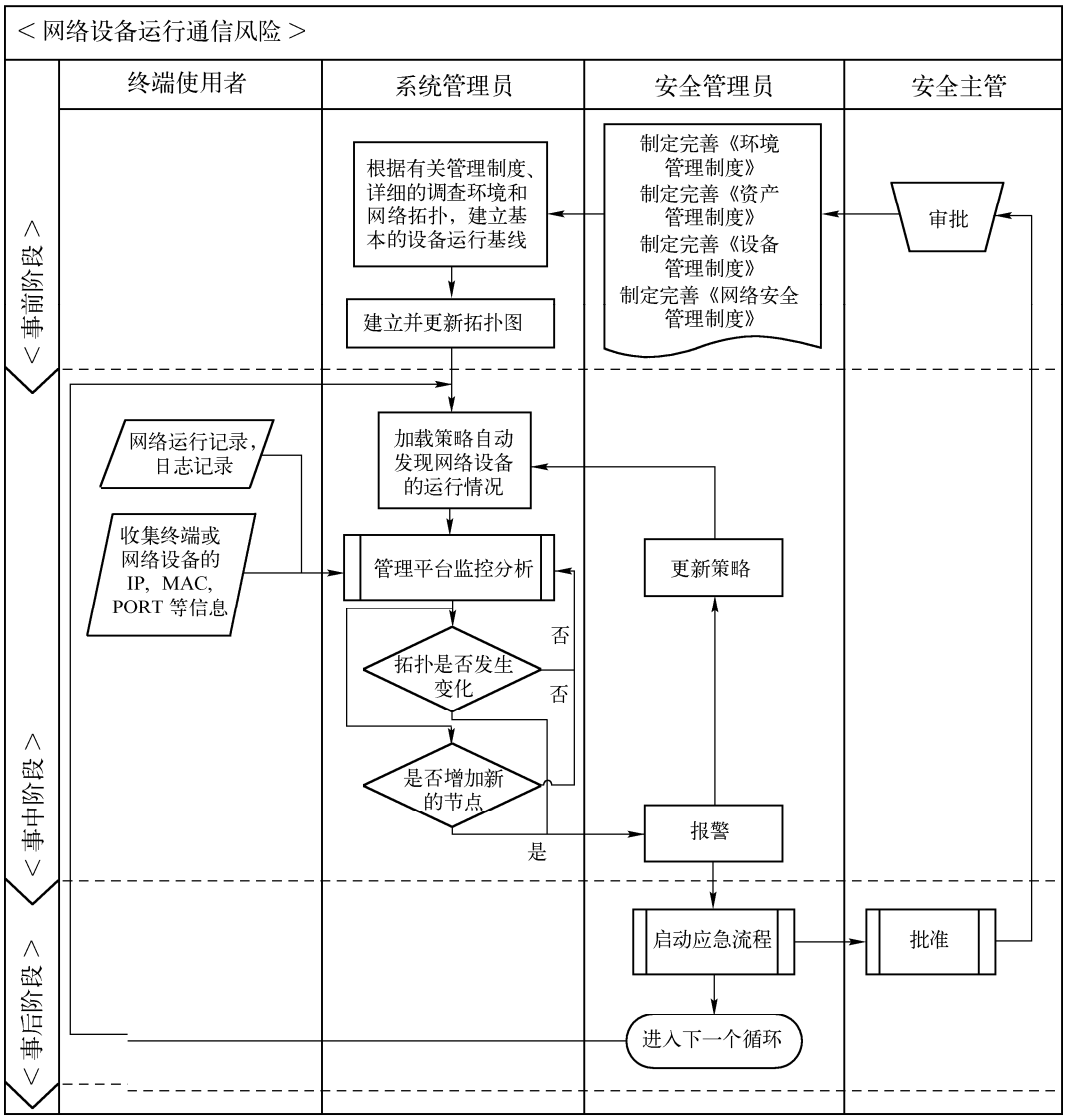

图 B-4

（4）风险点（11、12）网络设备运行监控平台自身风险

事前处置：严格执行软件开发管理规范，明确功能需求，严格审核测试方案和测试用例，并且确保软件能够解决现有工作中的问题。充分预见到可能的失效场景，拟定对应的应急预案，其中明确一旦由于平台的性能出现瓶颈，导致业务停止的状况下，需要采取的应急措施。有关人员需要按照应急措施去定期演练，以达到熟悉的程度。

事中处置：平台的健康自诊断系统需要及时检测平台的资源使用情况，如果超出预先规定的阈值，则需要及时向管理员报警，要求管理员必须及时反馈；通过分级部署的方式来规避集中部署的性能瓶颈。

事后处置：一旦平台出现问题导致严重影响业务，安全主管必须及时启动应急预案，确保业务本身的安全。在此基础上再考虑其他问题，如故障现象、可能的故障原因、涉及的部门和人员，造成问题的是平台本身的性能原因，还是其他问题，这些问题是否在管理制度中做出了相关规定，是否需要完善或补充等。

控制流程见图 B-5。

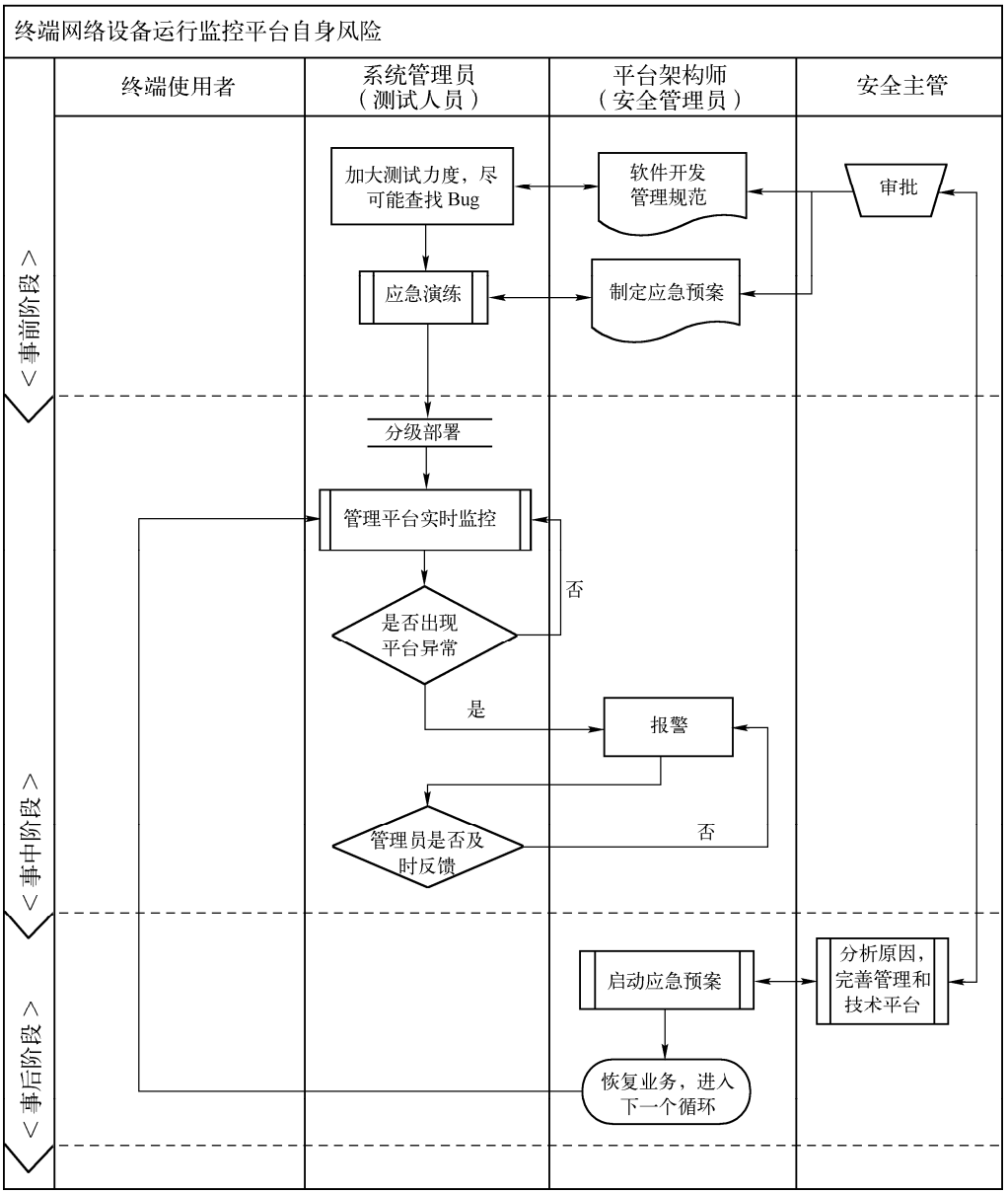

图 B-5

3．风险控制效果

对于此类风险涉及的环境、设备老化和通信的风险，通过采取管理、规范、流程、技术不同的措施，分别从事前、事中、事后 3 个方面来加以控制，可以基本达到风险管控的目的。

通过事前调查各种网络设备，包括终端的网络属性，确定不同的拓扑发现方式，从而拓扑发现系统的策略也得到了确定，进而事中自动拓扑发现和拓扑示意图自动绘制以及事后效果的分析和改善，最终实现了 PDCA 的最佳实践，为有效地控制网络设备运行风险起到很好的效果，提供网络运行的稳定性，记录网络设备和资源的使用情况，保证当前网络的高效性。

由于控制平台本身的性能可能会造成风险事件在采集、汇集、分析、展示等不同阶段的遗漏和误判，这一点还需要按照残余风险的处理办法去加以处理。

B.1.2 终端流量异常风险（12 个风险点）

1．风险分析

（1）风险描述

现在的业务系统都严重依赖网络的系统，比如核心业务、管理办公业务等都需要运转正常的网络基础设施来支撑。一旦网络出现拥塞，就会导致网络带宽不足，出现数据传输速率下降，从而给业务的正常运行带来严重风险。在终端联网的过程中，个别人员违规通过迅雷、BT 等 P2P 网络下载软件、在线播放流媒体以及玩网络游戏，这些非工作流量会抢占有限的带宽资源，影响网络传输性能，导致语音和视频会议、OA、ERP 等业务系统运行不稳定；另外，客户端感染蠕虫病毒也会造成网络带宽的占用。如果对终端流量使用的情况包括流量大小、发包数、连接数等流量信息不及时监控、上报和采取有效措施，就会严重威胁业务持续有效的运行。因此这类风险的可知、可控、可管十分重要。

该类风险主要表现在于以下 3 个方面：

1）监控缺失风险。由于缺少对终端发送和接收数据包的数量以及连接数的监控，就会导致关键主机的保护失控的风险。

2）标准基线风险。由于事先没有对终端的正常业务流量（连接数）、异常流量（连接数）和非法流量（连接数）做出仔细分析得出流量（连接数）的白名单，就可能造成无法有效地识别终端的异常流量（连接数）从而不能有效监控的风险。

3）控制平台本身风险。出现了异常流量（连接数），但是技术措施不到位，不能及时、准确地处理，如采取告警、限制流量和连接数等控制措施，实现有效监控的风险。

下面对终端流量异常风险进行详细的分解：

（2）相关风险点

终端流量异常风险点详见表 B-3。

表 B-3

风险分类	序号	风险点	风险属性	隐患/风险
终端流量异常风险	1	没有监控终端发送和接收数据包的数量	原生风险	隐患
	2	没有监控终端并发连接数的数量	原生风险	隐患
	3	不能自动识别终端的 P2P 下载行为	原生风险	隐患
	4	没有事先对实际的网络流量按照 IP、时间、端口分别统计得出流量的白名单	原生风险	隐患
	5	没有事先对实际的网络流量按照 IP、时间、端口分别统计得出连接数的白名单	原生风险	隐患
	6	不能下发流量和连接数的白名单策略	原生风险	隐患
	7	白名单策略被停止或被删除	原生风险	隐患
	8	发现白名单策略丢失后不能及时恢复	原生风险	风险
	9	下发策略与某些业务冲突	原生风险	风险
	10	发现终端连接数过大但不能控制	原生风险	风险
	11	发现终端流量过大但不能控制	原生风险	风险
	12	发现终端的 P2P 下载行为但是不能控制	原生风险	风险

以下将分别从资产使用生命周期、相关信息安全、资产使用人员和合规性 4 个方面对以上 12 个风险点进行详细描述。

（a）基于资产使用生命周期分析

资产使用生命周期包含入网前、运行阶段、维修阶段、报废阶段。网络设备运行风险按照资产使用生命周期的分析如下。

风险点（1-3）：涉及资产使用生命周期的运行阶段。如果缺失有关的流量异常的监控措施，一旦网络出现拥塞，带宽下降，就将对业务的正常运行带来严重风险；另外如果缺少这类监控措施，就不能及时识别和控制网络中的 P2P 下载软件，一旦出现病毒蠕虫也不能及时发现。

风险点（4-5）：涉及入网前、运行阶段。如果没有预先了解当前网络中的业务情况，包括业务高峰周期、每天的业务流量峰值、每个终端的流量模型、每个终端基于端口的流量模型，就不能准确地了解网络的态势，建立基于实际情况的并按照 IP、时间、端口的连接白名单，也就不能提供当前终端流量是否异常的标准，这将对流量异常监控带来风险。

风险点（6-8）：涉及运行阶段，如果不能对所有的终端统一下发流量（连接数）的白名单策略，势必造成流量和连接数异常监控的不全面，造成遗漏；如果不能及时发现流量（连接数）的白名单策略停止或被删除的情况，或者发现了不能及时恢复，也会对统一的安全监控环境带来监控的缺失风险。

风险点（9）：涉及入网前和运行阶段。如果在入网前没有仔细测试下发策略与当前业务的兼容性，一旦加载可能给业务带来极大的风险；另外即使在入网前已经测试了策略与业务的兼容性符合，一旦业务发生改变，也有可能与策略不兼容导致业务连续性风险。

风险点（10-12）：涉及运行阶段。如果技术上监控有关流量或连接数变化的技术手段性能不足，不能及时发现所有的违规，或者不能对所有的违规及时告警或处理，造成安全策略执行不到位，将会给业务带来极大的安全隐患。

（b）基于相关信息安全关系分析

相关信息安全分为在线信息风险和存储信息风险，终端流量异常风险按照相关信息安全关系的分析如下。

风险点（1-3）：如果缺失有关的流量异常的监控措施，一旦网络出现拥塞，带宽下降，必将造成业务运行中的在线信息风险和存储信息风险。

风险点（4-5）：如果不能建立基于实际情况的并按照 IP、时间、端口的连接白名单，也就不能提供当前终端流量是否异常的标准，这将对流量异常监控带来风险，必将造成业务运行中的在线信息风险和存储信息风险。

风险点（6-9）：如果没有一套闭环的，从下发、监控到恢复一系列的策略的监控机制，并且能够发现策略与业务的兼容性，可能会造成在线信息风险和存储信息风险。

风险点（10-12）：如果管理平台的技术能力不够，不能及时发现所有的违规，或者不能对所有的违规及时告警或处理，造成安全策略执行不到位。将会给业务带来在线信息风险和存储信息风险。

（c）基于资产使用人分析

资产（终端）使用人包括内部人员、临时人员和外部人员 3 大类，而内部人员可以再细分为高级管理者，关键业务人员和网络管理人 3 种角色，临时人员主要是辅助人员岗位（如食堂、车队、绿化等人员），而外部人员包括外来厂商运维人员和系统内外来人员。终端的使用者因为不同的角色和不同的操作意图，一个相同的风险点对应不同身份的终端使用人其风险级别也不同。将终端流量异常风险按照终端使用人角色分析如下。

风险点（1-3）：任何岗位角色都会使用网络，并涉及终端违规网络访问风险问题，因此，该风险与内部人员相关：

a）高级管理岗位，如区域负责人等高层领导，风险不大。

b）地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，风险较大。

c）网络管理员等。

该风险也与临时人员相关：辅助人员岗位（如食堂、车队、绿化等人员等），可能利用网络下载游戏，观看网络视频，造成带宽拥堵，其风险重大。

该风险与外来人员相关：外来厂家人员、特别是外来维护人员网络知识丰富，也有可能利用内部网络下载资料，造成流量异常，其风险重大。

风险点（4-5）：内部人员在使用网络时，必须对其正常的网络应用流量做出详细的了解，作出正常的流量基线，否则，无法判断其流量是否属于异常，从而不能进行有效控制；重点需要了解高级管理岗位，如区域负责人等高层领导的流量情况和地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员的流量情况。而对于临时人员和外部人员，因无法事先作出基线，风险较大。

风险点（6-8）：对于高级管理岗位，如区域负责人等高层领导的流量策略需要重点保证，一旦策略不能及时有效下发，或不能了解当前策略是否有效，就会造成重要业务不能及

时审批，给业务的有效性造成风险；对于地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，一旦策略不能生效或与业务冲突，就会对业务造成风险。

风险点（9）：该风险对于高级管理岗位较大，一旦策略与领导的业务冲突，导致不能上网，必然给业务带来严重风险；当然这个风险也会给内部管理人员如地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员的业务带来威胁；这个风险与临时人员和外来人员的风险级别不大。

风险点（10-12）：这个风险主要跟临时人员和外来人员有关，一旦发现辅助人员岗位，如食堂、车队、绿化等人员等，可能利用网络下载游戏，观看网络视频，造成带宽拥堵的情况，要首先采用技术措施去限制其利用带宽流量，一旦技术措施失效，可能对内部网络运行带来失控，给业务带来较大的风险。

（d）合规性要求

合规性要求见表 B-4。

表 B-4

序号	安全类	等级保护（三级）要求	符合程度
1	网络安全	7.1.2.2 访问控制（G3） b) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级 e) 应限制网络最大流量数及网络连接数 h) 应限制具有拨号访问权限的用户数量	符合
2	网络安全	7.1.2.3 安全审计（G3） 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录	符合

2．风险管控

每类风险在管控过程中，针对风险的事前、事中和事后 3 种状态进行监控，做到事前预防，事中控制、事后审计追查。下面风险管控处理流程，尽量从事前、事中和事后 3 方面对风险管控进行描述

（1）风险点（1-3）：终端流量异常监控缺失风险

事前处置：对于类似风险，需要制定一系列的管理措施，如《网络安全管理制度》，其中需要针对现有终端按照不同的使用角色做出不同的带宽策略，包括内部高级管理员、关键岗位业务人员、外部厂家人员、临时人员 4 种角色策略。

事中处置：加载策略后，需要定期轮询终端网卡流量，发现是否存在终端流量异常。一旦发现异常，需要及时报警。可以通过技术手段解决，上报管理中心或由管理员根据当时影响业务的重要情况决定采用是否及时阻断占用带宽的终端，或在终端桌面上弹出警告提示信息等措施。

事后处置：一旦技术手段采取后无法取得效果，或人工发现技术手段已经失效，需要通过人工流程去加以干涉。安全主管根据实际情况启动应急流程，通过管理和人工的办法消弭风险。

控制流程见图 B-6。

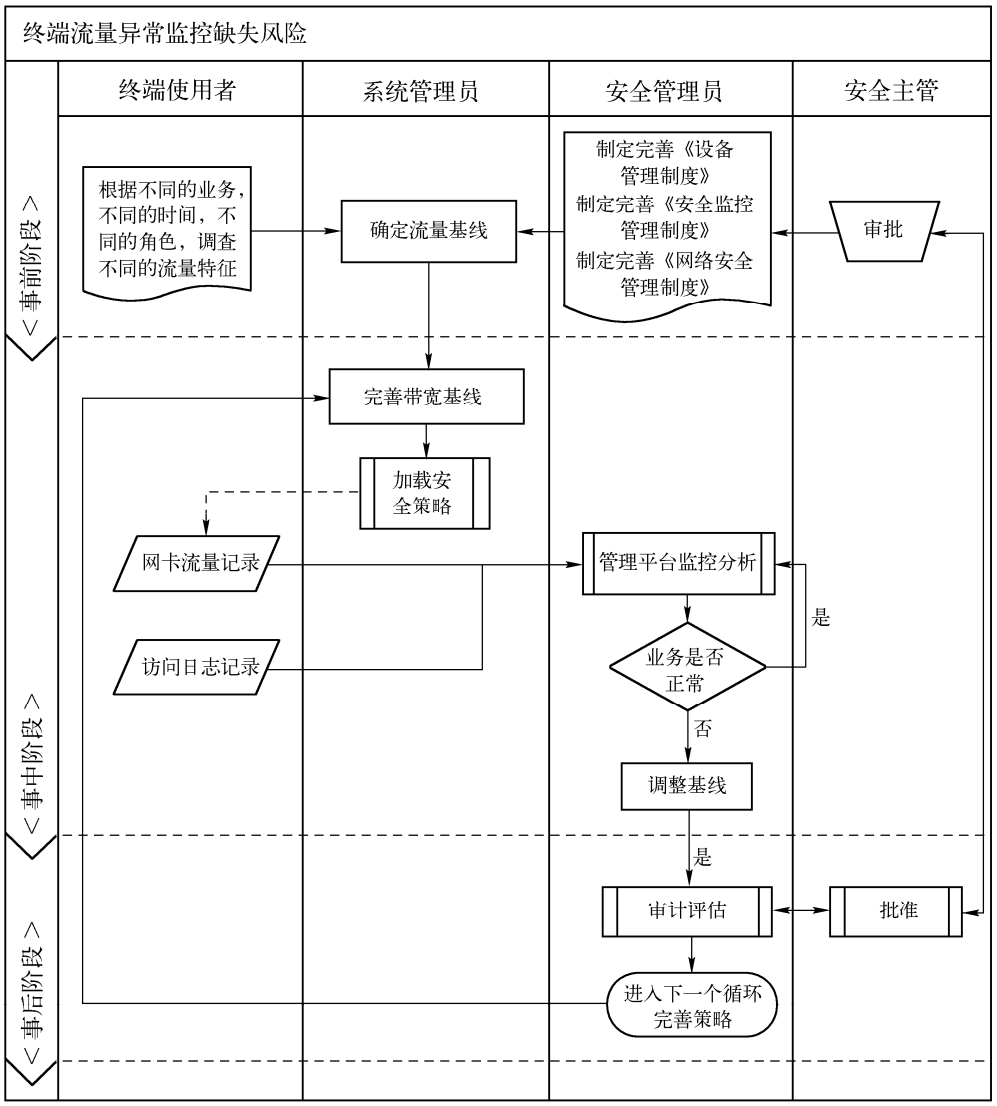

图 B-6

（2）风险点（4-5）：终端流量异常基线风险

事前处置：通过事先建立的网络流量监控机制，以不同的业务为中心，来了解内部各个终端的正常的业务流量，即建立符合业务特色的流量管理制度，制定不同角色不同业务终端的正常的带宽流量标准。通过这类流量基线，建立流量策略。

事中处置：通过网络流量监控机制，定期评估当前的带宽策略是否符合当前的业务情况、是否会影响业务的正常进行、是否符合不同的角色情况、是否符合不同的时间段正常业务的变化情况，根据这些要素，及时调整策略。

事后处置：对于该类风险，需要按照有关管理制度和流程，定期审计评估，找出造成兼容性的原因，尽量规避直至消除，把因策略的因素导致业务的影响降到可以接受的范围。

控制流程见图 B-7。

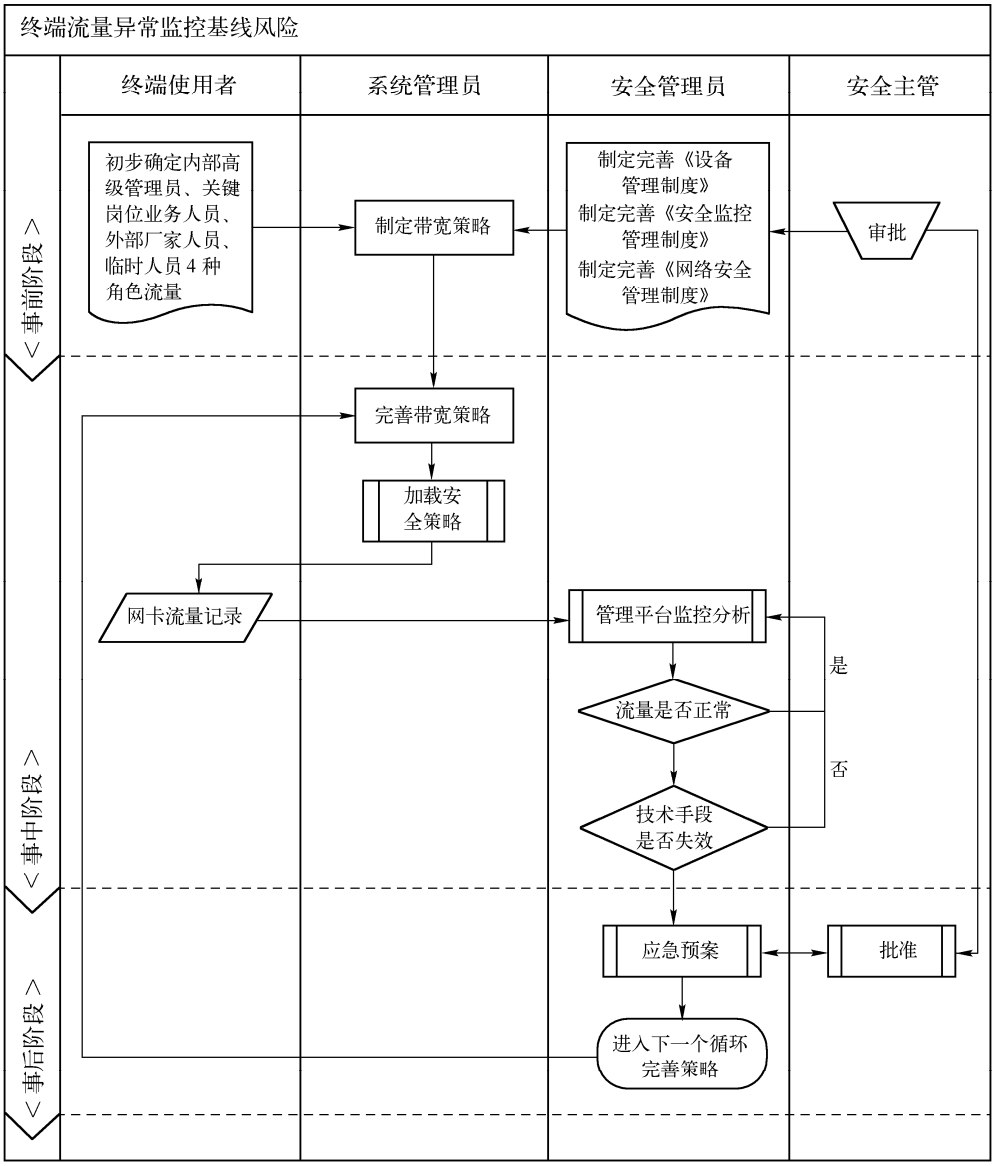

图 B-7

（3）风险点（6-12）：终端流量异常控制风险

事前处置：收集终端流量信息，定义终端流量的正常边界和连接黑白名单。需要制定有关的应急响应预案，一旦出现策略不能及时更新而技术手段无法实现时需要启动。

事中处置：通过分析实时的通信日志，来确认策略是否已经得到更新；及时了解流量和连接数白名单策略已经得到更新，或者及时发现流量和连接数白名单策略停止和被删除，或者了解流量和连接数白名单策略与某些业务是否冲突；如果在规定的时间内得不到反馈信息，需要启动应急预案。

一旦出现策略与业务的兼容性问题，就需要有逃生机制，即通过人工卸载策略，确保业务的顺利进行。

事后处置：一旦前面的技术手段都失效，就需要在安全主管的认可下启动应急预案。首先在确保业务顺利进行的前提下，人工在本地更新或卸载策略。在此基础上再考虑其他问题，如策略不能更新的故障原因、涉及的部门和人员、造成问题的是平台本身的性能原因还是其他问题，这些问题是否在管理制度中做出了相关规定，是否需要完善或补充等。

控制流程见图 B-8。

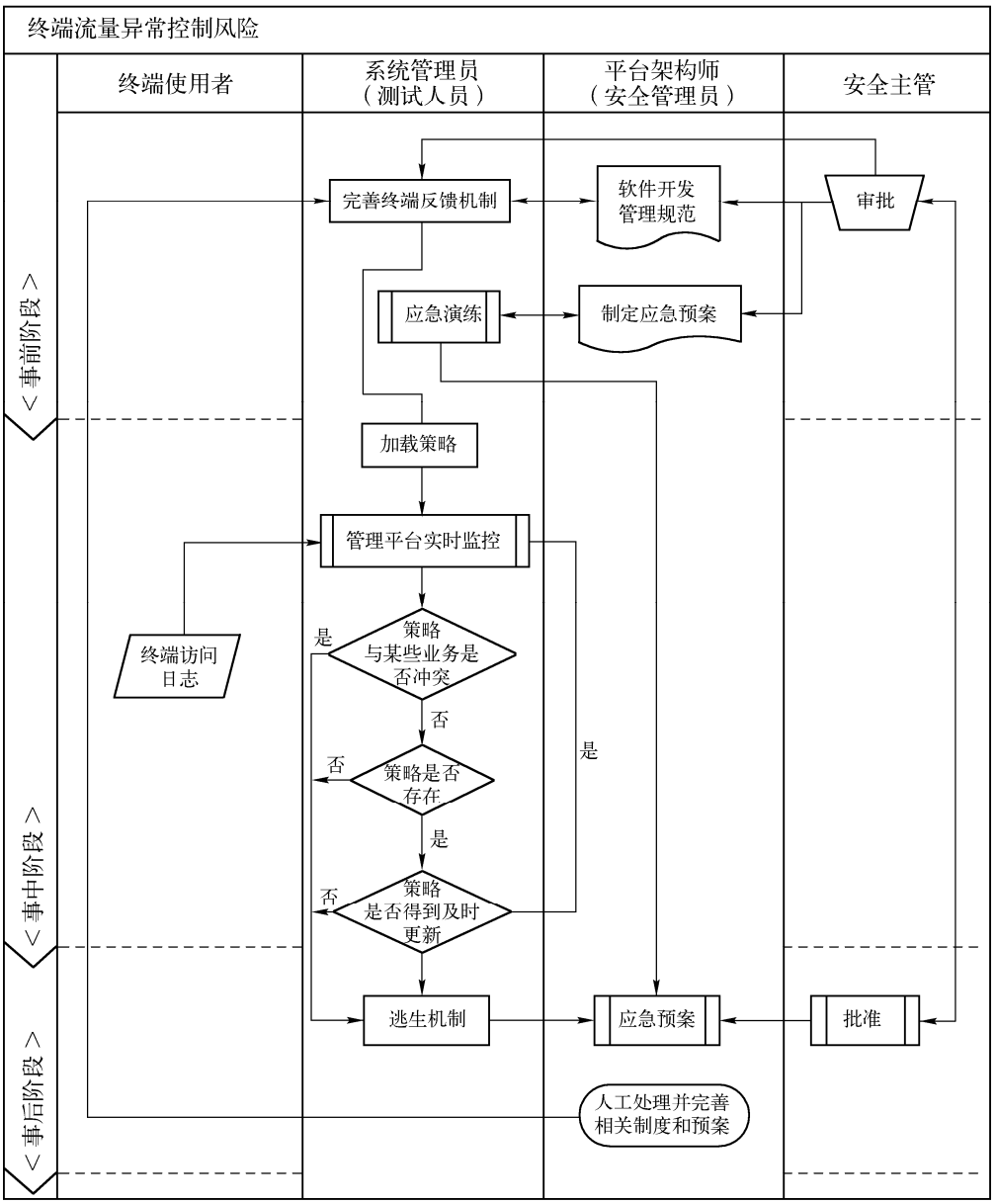

图 B-8

3. 风险控制效果

对于此类风险涉及的终端流量异常风险，通过采取管理、规范、流程、技术不同的措施，分别从事前、事中、事后 3 个方面来加以控制，可以基本达到风险管控的目的。

通过事前对不同角色的用户，不同时间的业务所需要的带宽调查，逐步建立标准流量基线，事中根据这个基线进行监控和事后效果的分析和改善，实现了 PDCA 的最佳实践，为有效控制网络流量异常风险达到了效果。事后通过日志审计，可以查找风险源，追溯到终端责任人，可以给后续的考评管理提供依据。

由于控制平台本身的性能可能会造成风险事件在采集、汇集、分析、展示等不同阶段的遗漏和误判，可能给业务带来风险，需要根据可能出现的场景，如策略与业务冲突，定制的技术处理手段失灵等，制定应急预案并做定期演练，以确保业务的连续性和可靠性。

B.1.3 终端违规网络访问风险（11 个风险点）

1．风险分析

（1）风险描述

网络通信是现今基于信息化业务的基础。由于担心业务不能顺利开展，一般对内部终端的访问不做控制，这样就导致内部终端能随时随意访问本不应该访问的资源，出现扫描端口、嗅探密码等黑客行为。如果不对该终端网络访问风险进行严格管理和控制，将会导致信息外泄、资源滥用甚至全网范围内的灾难性事件。

该类风险主要表现在因终端网络访问缺少有关 IP、端口、协议的管理制度、流程和技术监控，造成终端网络访问的无序。另外尽管增加了 IP、端口、协议的黑白名单,但是没有及时更新完善访问策略，造成应该允许的访问不能进行，给业务开展带来风险。由此带来 4 类问题：

1）没有终端访问的 IP、端口、协议范围，这将会导致关键主机的保护失控的风险。

2）存在终端访问的 IP、端口、协议限定策略，但是由于策略本身没有及时更新完善，导致不能正常开展业务，这是用户十分担心的风险。

3）加载的策略没有生效，或被卸载，导致安全策略不能有效贯彻，将导致内部网络运行失控的风险。

4）违规访问记录没有及时发送给管理平台，或者管理平台不能及时处理如采取告警，阻断等控制措施。

下面将对终端违规使用风险进行详细的分解：

（2）相关风险点

终端违规网络访问风险点见表 B-5。

表 B-5

	序号	风险点	风险属性	隐患/风险
终端违规网络访问风险	1	没有终端访问的 IP 范围	原生风险	隐患
	2	没有终端访问的端口范围	原生风险	隐患
	3	没有终端访问的业务服务器范围	原生风险	隐患
	4	没有终端访问使用的协议范围	原生风险	隐患
	5	策略本身没有及时更新完善导致终端访问的 IP 范围与限定的不一致	次生风险	隐患
	6	策略本身没有及时更新完善导致终端访问的端口范围与限定的不一致	次生风险	风险
	7	策略本身没有及时更新完善导致终端访问的业务服务器与限定的不一致	次生风险	风险
	8	策略本身没有及时更新完善导致终端访问使用的协议与限定的不一致	次生风险	风险
	9	策略失效禁用或被卸载	次生风险	风险
	10	管理平台不能及时发现所有的上述违规的终端网络访问行为	残余风险	隐患
	11	管理平台发现了上述违规的终端网络访问行为，但是不能对所有的违规及时告警或处理	残余风险	隐患

以下将分别从资产使用生命周期、相关信息安全、资产使用人员和合规性 4 个方面对以上 11 个风险点进行详细描述。

（a）基于资产使用生命周期分析

资产使用生命周期包含入网前、运行阶段、维修阶段、报废阶段，终端违规网络访问风险按照资产使用生命周期的分析如下：

风险点（1-4）：涉及资产使用生命周期的运行阶段，如果一台没有作任何访问控制的终端遭到僵尸木马的入侵，成为外部控制的僵尸，它就会成为外部攻击内部的桥头堡，内部所有机器的脆弱性都会被其利用，内部单位机密信息甚至国家机密信息都遭到极大威胁。著名的 conficker 病毒就是这类例子；涉及维修阶段，如果在维修以后的访问控制策略被删除，可能再次入网后对内部安全带来风险。

风险点（5-8）：涉及入网前阶段，在该阶段需要对业务行为进行分析，形成策略并逐步细化，如果我们加载的访问控制策略没有充分验证测试，可能导致业务不能顺利进行的严重风险；涉及运行阶段，由于业务改变，涉及的 IP、端口、协议信息也相应发生了改变，如果加载的策略没有及时变化，就会导致业务不能顺利进行的严重风险；涉及维修阶段，如果在维修以后的访问控制策略被修改，也会导致再次入网后业务不能顺利进行的严重风险。

风险点（9）：涉及入网前、运行阶段、维修阶段，一旦策略被无意或恶意卸载导致失效，而管理平台不能及时发现，势必导致安全策略不能有效贯彻，将导致内部网络运行失控的风险。

风险点（10-11）：涉及运行阶段，如果监控有关地址、端口和协议变化的技术手段的性能不足，不能及时发现所有的违规，或者不能对所有的违规及时告警或处理，就造成安全策略执行不到位，给业务带来极大的安全隐患。

（b）基于相关信息安全关系分析

相关信息安全分为在线信息风险和存储信息风险，终端违规网络访问风险按照相关信息安全关系的分析如下。

风险点（1-4）：对网络的威胁极高，可能遭到攻击、成为僵尸和信息外泄的风险，在线信息系统和存储信息系统由于涉及重要信息和数据，往往对于安全要求较高，因此使在线信息系统、存储信息系统存在风险。

风险点（5-8）：由于加载策略和实际的业务情况不匹配，不能及时访问在线信息系统，存储信息系统也不能及时更新，因此使在线信息系统、存储信息系统存在风险。

风险点（9）：对网络的威胁极高，可能遭到攻击、成为僵尸和信息外泄的风险，因此使在线信息系统、存储信息系统存在风险。

风险点（10-11）：由于技术能力不足，不能及时、充分获取终端违规网络访问风险事件，按照当前的业务及时调整策略并下发，同时做出及时的告警、阻断等处理措施，因此使在线信息系统、存储信息系统存在风险。

（c）基于资产使用人分析

资产（终端）使用人包括内部人员、临时人员和外部人员 3 大类，而内部人员可以再细分为高级管理者、关键业务人员和网络管理人 3 种角色，临时人员主要是辅助人员岗位（如食堂、车队、绿化等人员），而外部人员包括外来厂商运维人员和系统内外来人员。终端的使用者因为不同的角色和不同的操作意图，一个相同的风险点对应不同身份的终端使用人风

险级别也不同。将终端违规网络访问风险按照终端使用人角色分析如下。

风险点（1-4）：任何岗位角色都会使用网络，都会涉及终端违规网络访问风险问题，因此，该风险与内部人员相关：

a）高级管理岗位，如区域负责人等高层领导，风险不大。

b）地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，风险较大。

c）网络管理员，风险较大。

该风险与临时人员相关：辅助人员岗位，如食堂、车队、绿化等人员等，风险重大。

该风险与外来人员：外来厂家人员、外来维护人员风险重大。

风险点（5-8）：对于内部人员，特别是高级管理者，风险一旦导致不能及时正常审批业务势必造成严重影响；而对于关键业务和网络管理人员，他们可能面对的风险是不能及时开展业务，影响工作绩效；对于临时人员其风险不大。不过对于外来人员因为需要通过网络做一些维护和业务的操作，其风险程度与内部人员中的关键业务和网络管理人员的风险程度相当。

风险点（9）：对于内部人员，这个风险对于内部人员中的网络管理人员来说风险极大，可能导致安全策略不能有效贯彻，将导致内部网络运行失控的风险；对于外来人员特别是厂家维护人员同样需要涉及相同的风险；同样对于临时人来说也要涉及相同的风险。

风险点（10-11）：对于内部人员，特别内部人员中的网络管理人员来说如果不能及时知晓他们的行为，并对可能出现的恶意网络行为做及时告警和阻止，势必对网络的正常运行带来较大风险；对于外部人员，特别是厂家维护人员同样存在相同的风险；对于临时人来说也存在相同的风险。

（d）合规性要求

合规性要求见表 B-6。

表 B-6

序号	安全类	等级保护（三级）要求	符合程度
1	网络安全	7.1.2.2 访问控制（G3） 安全审计 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录	符合

2．风险管控

每类风险在管控过程中，需要针对风险的事前、事中和事后 3 种状态进行监控，做到事前预防、事中控制、事后审计追查。下面风险管控处理流程，尽量从事前、事中和事后 3 方面对风险进行管控。

（1）风险点（1-4）：终端网络访问缺失访问策略的风险

事前处置：首先能够了解当前的网络态势，做出足够详细的不同网络业务的访问基线，那么在后续的实际操作中就可以逐步完善这些策略。这就是网络访问的“规矩”。

把收集到的防火墙日志数据按照用户关心的业务及相关资产来分类，然后按照一定的步长（小时、分钟）来统计，找出每小时的连接，确定内部终端的网络访问特征，即它一般每天访问哪些 IP，它是否会被其他终端访问等。

对于每一个需要关注的终端对象，需要按照一定的时间步长（1h）进行以下持续的统计：

- ✓ 作为源地址访问的所有目的地址列表 （Fan Out）
- ✓ 作为源地址的所有目的端口（协议）列表
- ✓ 作为目的地址的所有源地址列表（Fan In）
- ✓ 作为目的地址的所有源端口列表
- ✓ 相互通信列表（a 与 b 的交集）

将上面的统计结果按照资产排序，找出不同的 TOPN，将本期的 TOPN 与前一期的 TOPN 记录比较发现变化。

通过这个过程，一台机器的网络行为模型就基本建立，这样就可以回答用户关心的如下问题：

- ✓ 某一天访问了哪些地址，与每天访问的地址列表中的地址（白名单）相似度是多少，这些不同的地址是否属于恶意地址（黑名单）
- ✓ 这些地址是否属于整个内部大的白名单？是否确定需要更新名单（黑白）
- ✓ 通过整理内部所有机器的访问目的地址列表，找出交集，形成了内部大的目的地址白名单
- ✓ 通过整理所有的不同地址的目的端口列表，来确定内部目的端口（服务）白名单

事中处置：对终端上内嵌防火墙组件，结合前面制定的访问控制策略，加载内嵌防火墙策略，防火墙策略应该有以下的全局内容：

- ✓ 防火墙应该是绿灯模式（白名单），即只有策略明确允许的通信才可以放行，默认策略是禁止
- ✓ 防火墙上应该有本终端允许访问的服务器地址列表
- ✓ 防火墙上应该有本终端允许访问的服务器协议和端口列表
- ✓ 防火墙上应该有允许访问本终端的的其他终端地址列表
- ✓ 防火墙上应该有访问时间段定义，如工作时间、特殊业务时间
- ✓ 防火墙所有策略应该可以记录日志。这些日志如果正常联网就发送给管理中心，如果漫游日志信息要记录在本地特殊的文件夹中
- ✓ 这个防火墙服务终端用户不能卸载
- ✓ （可选）还应该有允许的带宽策略，其他应用策略

事后处置：管理平台上可以得到详细的管理日志，通过分析日志，可以了解到当前的策略是否有效，是否对业务有影响，然后根据这些日志分析的结果去完善更新策略。

- ✓ 对于关键业务人员，需要对其访问的对象地址、访问时间以及协议做细致的控制，做行为审计记录
- ✓ 对于网络管理人员，由于其实际权限极大，一旦被利用，对整个网络环境的风险极高，因此必须通过管理手段加以管理，并做行为审计记录
- ✓ 对于临时人员入网，由于其安全状态不合规而安全防护措施不足，造成被攻击并作为系统薄弱点成为攻击跳板，因此需要对其网络行为做细致的审计
- ✓ 对于外来人员入网，特别是需要进入业务系统的外来厂商运维人员，应该严格执行有关管理制度，杜绝自带移动 PC 设备入网，只能使用业务终端入网。在该终端上临时开启访问策略，严格限制其访问的对象地址、访问时间以及协议，并进行严格的

行为审计

控制流程见图 B-9。

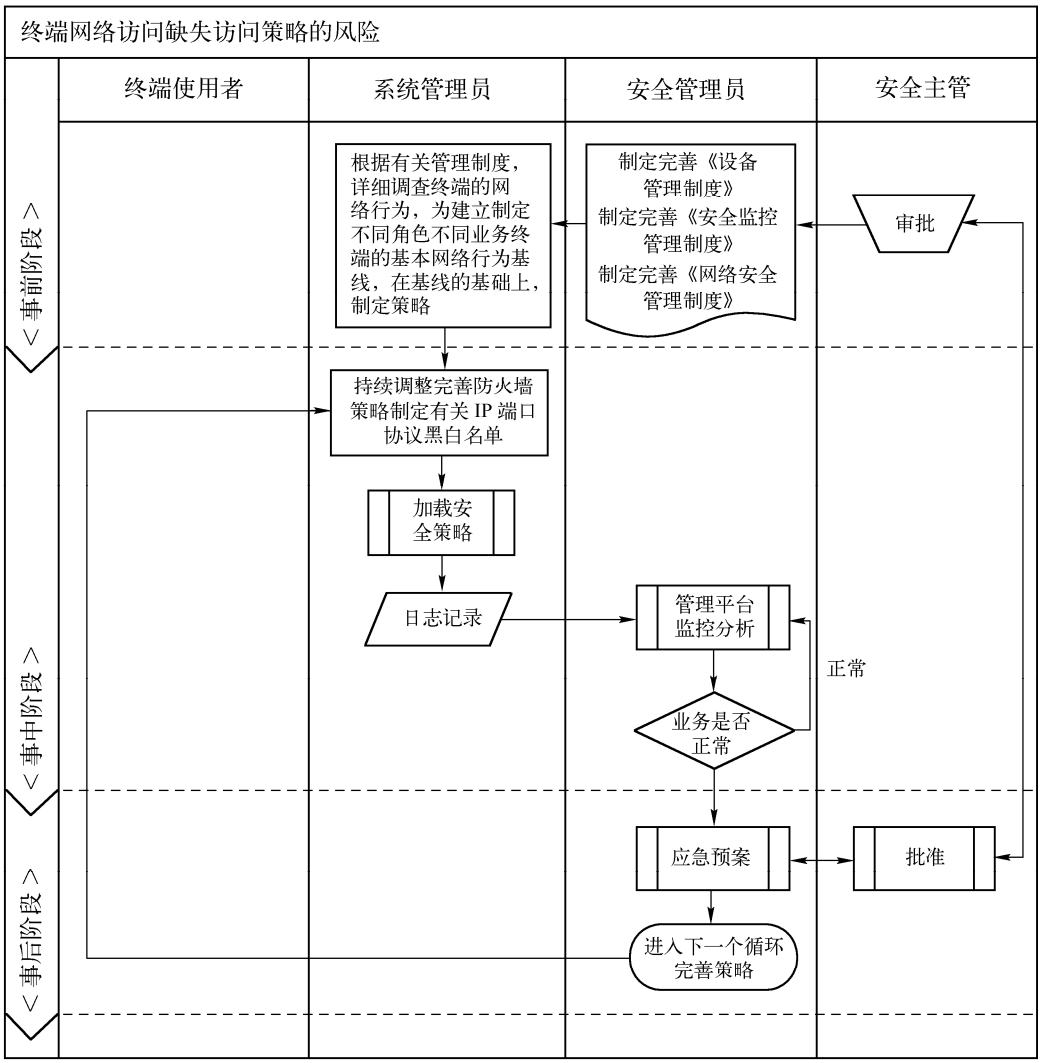

图 B-9

（2）风险点（5-8）：终端网络访问策略没有及时更新的风险

事前处置：定义与业务相关的网络访问策略，并且根据实际情况实时更新和维护。需要制定有关的应急响应预案，一旦策略不能及时更新而技术手段无法实现时就需要启动。

事中处置：通过分析实时的通信日志，来确认策略是否已经得到更新。需要有一种技术机制能够定期更新策略，如果在规定的时间内得不到反馈信息，则需要启动应急预案。

事后处置：一旦前面的技术手段都失效，就需要在安全主管的认可下启动应急预案。首先在确保业务顺利进行的前提下，人工在本地更新策略，在此基础上再考虑其他问题，如策略不能更新的故障原因、涉及的部门和人员，造成问题的是平台本身的性能原因还是其他问题，这些问题是否在管理制度中做出了相关规定，是否需要完善或补充等。

控制流程见图 B-10。

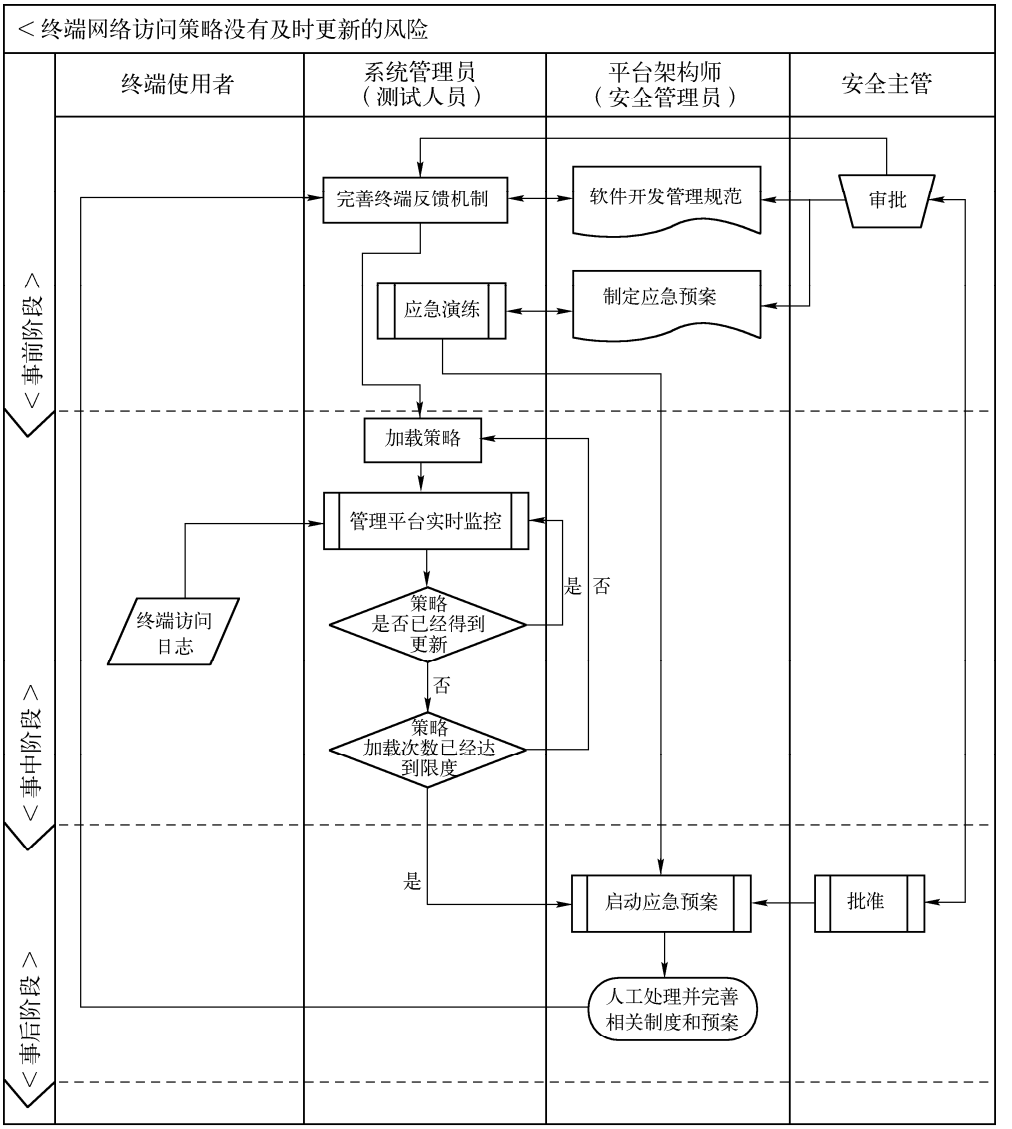

图 B-10

（3）风险点（9）终端网络访问策略失效禁用或被卸载的风险

事前处置：完善技术机制，尽可能确保从终端上不能卸载访问策略；同时终端跟平台之间也要有一个定期的通信机制，来确认终端的网络访问策略存在并生效。

事中处置：管理平台定期轮询客户端的有关软件是否正常运行，一旦发现异常，需要采取系列手段来应对：

1）通过客户端发送通知信息。

2）给该客户端所有人（用户）发送通知邮件。

3）如果在规定的时间内没有得到回应，则管理员需要通过电话再跟该该客户端所有人联系，了解具体情况。

4）直至通过管理平台采取断网措施。

事后处置：一旦前面的技术手段都失效，就需要在安全主管的认可下启动应急预案。首先确保业务本身的安全。在此基础上再考虑其他问题，如故障现象、可能的故障原因、涉及的部门和人员，造成问题的是平台本身的性能原因还是其他问题，这些问题是否在管理制度中做出了相关规定，是否需要完善或补充等。

控制流程见图 B-11。

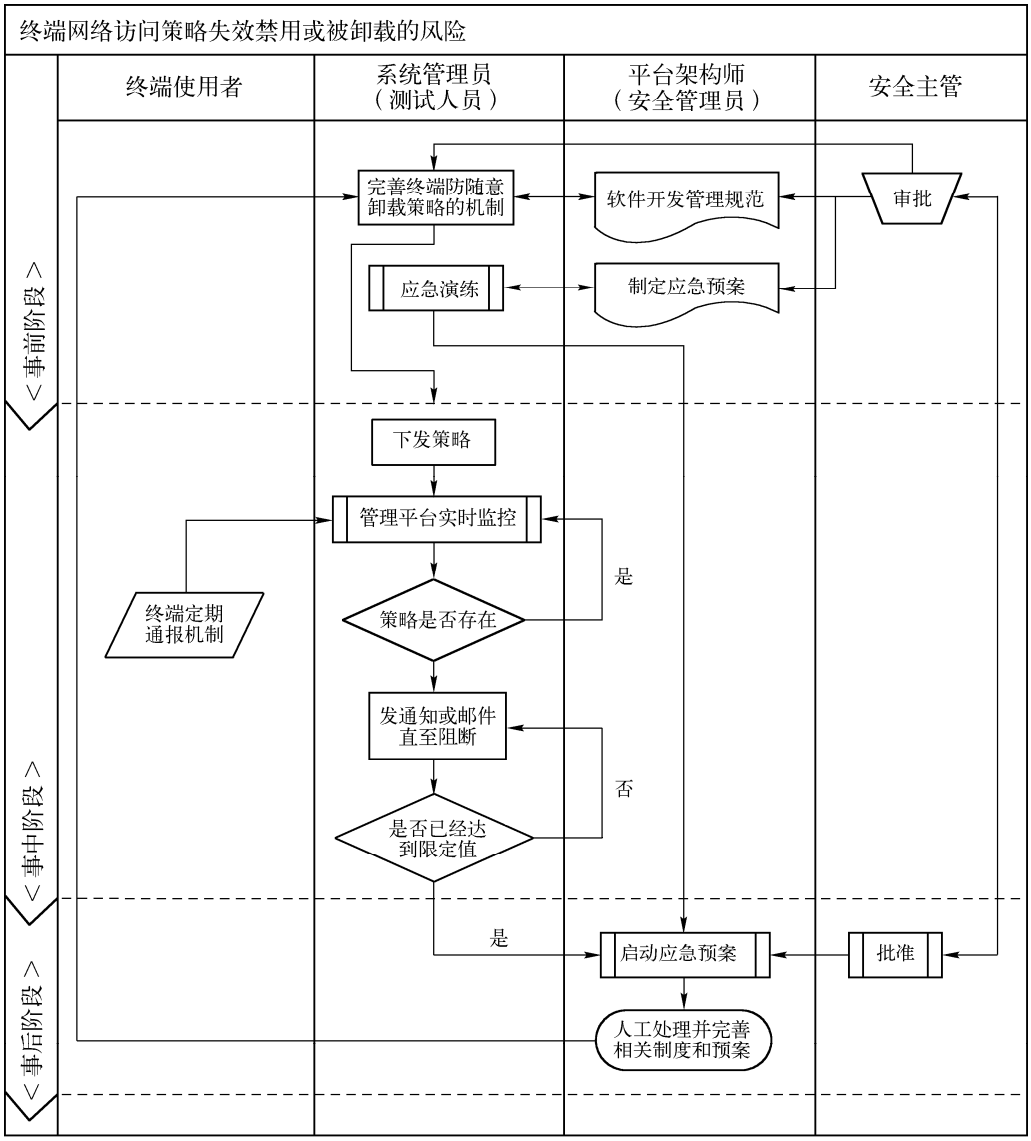

图 B-11

（4）风险点（10-11）：终端网络设备运行监控平台自身风险

事前处置：严格执行软件开发管理规范，明确功能需求，严格审核测试方案和测试用例，并且确保软件能够解决现有工作中的问题。充分预见可能的失效场景，拟定对应的应急预案，明确一旦由于平台的性能出现瓶颈，导致出现业务停止的情况时，需要采取的应急措

施。有关人员需要按照应急措施定期去演练，以达到熟悉的程度。

事中处置：平台的健康自诊断系统需要及时检测平台的资源使用情况，如果超出预先规定的阈值，则需要及时向管理员报警，要求管理员必须及时反馈；通过分级部署的方式来规避集中部署的性能瓶颈。

事后处置：一旦平台出现问题导致严重影响业务，则安全主管必须及时启动应急预案，确保业务本身的安全。在此基础上再考虑其他问题，如故障现象、可能的故障原因、涉及的部门和人员，造成问题的是平台本身的性能原因还是其他问题，这些问题是否在管理制度中做出了相关规定，是否需要完善或补充等。

控制流程见图 B-12。

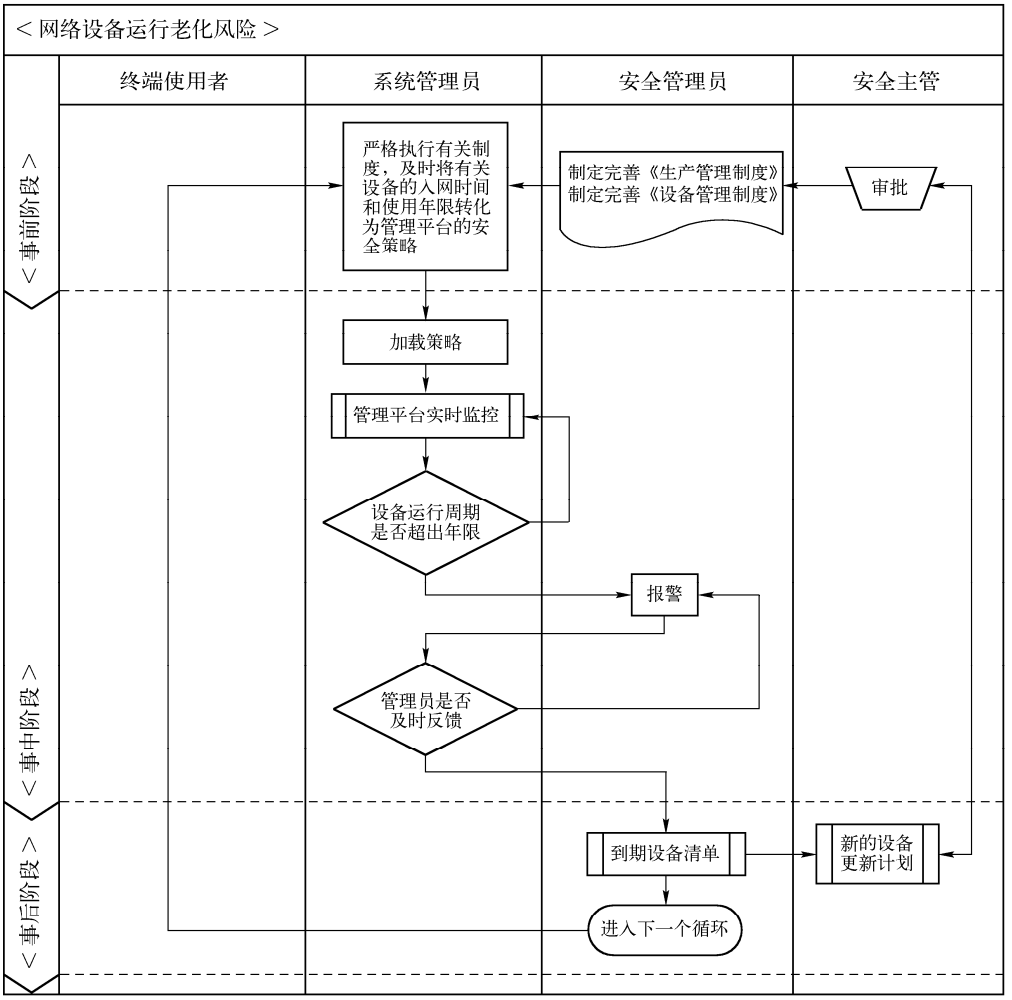

图 B-12

3．风险控制效果

对于此类风险涉及的终端违规访问风险，通过采取管理、规范、流程、技术不同的措施，分别从事前、事中、事后 3 个方面来加以控制，可以基本达到风险管控的目的。

通过事前对终端的需要访问的目的地址、协议、端口和时间详细了解，逐步建立标准网

络访问基线，建立正常访问基线，事中根据这个基线进行监控和事后效果的分析和改善，实现了 PDCA 的最佳实践，为有效控制网络流量异常风险达到了效果。事后通过日志审计，可以查找风险源，追溯到终端责任人，这可以给后续的考评管理提供依据。

由于控制平台本身的性能可能会造成风险事件在采集、汇集、分析、展示等不同阶段的遗漏和误判，这一点还需要按照残余风险的处理办法去加以处理。

B.1.4 IP/MAC 地址篡改风险（9 个风险点）

1．风险分析

（1）风险描述

一般的访问控制都是通过 IP 过滤功能来控制局域网内不同 IP 地址的上网权限来实现的。例如限定某个 IP 地址或某一段 IP 地址只能访问 Web 和收发邮件，规定一些地址可以访问权限更高的资源，如数据库、人事资料库等。但是 IP 地址的修改是非常容易的，局域网用户可以通过更改自己的 IP 地址（例如盗用权限更高人员的 IP 地址）以获得更多访问权限。如果对 IP/MAC 地址篡改信息不及时监控、上报和采取有效措施的话，会严重威胁到业务的持续有效的运行。

该类风险主要表现在：

1）私自篡改 IP 地址会造成 IP 地址冲突，导致网络中断，使正常工作的主机无法使用网络办公的风险。

2）因为事前没有对所有终端网卡的 MAC 地址和对应的 IP 地址进行登记，致使盗用 IP 地址不能及时发现、或者发现后不能及时采取有效措施的风险。

3）IP/MAC 绑定策略被停止或被删除的风险，而不能采取技术手段及时恢复 IP 地址的初始状态并通报管理员。

4）IP/MAC 绑定模块与某些业务冲突，造成业务连续性风险。

下面对 IP/MAC 地址篡改风险进行详细的分解：

（2）相关风险点

IP/MAC 地址篡改风险点详见表 B-7。

表 B-7

	序号	风 险 点	风险属性	隐患/风险
IP/MAC 地址篡改风险	1	没有记录所有网卡的 MAC 地址和对应的 IP 地址	原生风险	隐患
	2	终端的 IP/MAC 地址绑定可以随意修改	原生风险	风险
	3	不对终端的多网卡状态进行监控	原生风险	隐患
	4	不能及时发现终端的多网卡状态	原生风险	隐患
	5	不能及时发现终端的 IP/MAC 地址绑定随意修改状况	原生风险	隐患
	6	不能发现终端的 IP/MAC 地址绑定模块被随意停止或删除	原生风险	隐患
	7	发现终端的 IP/MAC 地址绑定模块随意修改后，不能采取技术手段及时恢复 IP 地址的初始状态	原生风险	隐患
	8	发现终端的 IP/MAC 地址绑定模块随意修改后不能对终端进行提示违规行为记录并上报管理员，警告直至人工现场处理	原生风险	隐患
	9	终端的 IP/MAC 地址绑定模块加载后与某些程序和应用冲突	原生风险	风险

以下将分别从资产使用生命周期、相关信息安全、资产使用人员和合规性 4 个方面对以上 9 个风险点进行详细描述：

（a）基于资产使用生命周期分析

资产使用生命周期包含入网前、运行阶段、维修阶段、报废阶段，网络设备运行风险按照资产使用生命周期的分析如下：

风险点（1-3）：涉及入网前、运行阶段。由于基本管理措施的缺失，没有所有网卡的 MAC 地址和对应的 IP 地址的记录，一旦出现 IP 地址随意设置，就会造成 IP 地址冲突，导致网络冲突，查找故障点非常困难，导致正常工作的主机无法使用网络办公，业务停滞的风险。

风险点（4-6）：涉及运行阶段。由于终端管理模块的 IP/MAC 模块没有设置或没有正常设置或因种种原因，导致不能及时有效而全面地监控 IP 修改状态，甚至 IP/MAC 模块本身被删除的严重情形，最后可能出现网络运行失控的状态，给业务带来极大的风险。

风险点（7-9）：涉及运行阶段。由于技术控制措施不到位，不能对全部的 IP/MAC 违规现象进行纠正，如发现终端的 IP/MAC 地址绑定模块随意修改后，不能采取技术手段及时恢复 IP 地址的初始状态，也不能对终端进行提示违规行为记录并上报管理员，告警，直至人工现场处理的一系列措施，也会出现网络运行失控的状态，给业务带来极大的风险。

（b）基于相关信息安全关系分析

相关信息安全分为在线信息风险和存储信息风险，IP/MAC 篡改风险按照相关信息安全关系的分析如下：

风险点（1-3）：如果缺失有关的 IP/MAC 异常的监控措施，一旦网络出现任意修改 IP 地址，造成 IP 地址冲突，必将造成业务运行中的在线信息风险和存储信息风险。

风险点（4-6）：虽然建立了 IP/MAC 异常的监控措施，但是如果不能及时有效地起到监控作用，出现网络运行失控的状态，造成业务运行中的在线信息风险和存储信息风险。

风险点（7-9）：如果管理平台的技术能力不够，不能及时发现所有的 IP/MAC 异常违规，或者不能对所有的 IP/MAC 异常违规及时告警或处理，将造成安全策略执行不到位。将会给业务带来在线信息风险和存储信息风险。

（c）基于资产使用人分析

资产（终端）使用人包括内部人员、临时人员和外部人员 3 大类，而内部人员可以再细分为高级管理者，关键业务人员和网络管理人 3 种角色，临时人员主要是辅助人员岗位（如食堂、车队、绿化等人员），而外部人员包括外来厂商运维人员和系统内外来人员。终端的使用者因为不同的角色和不同的操作意图，一个相同的风险点对应不同身份的终端使用人风险级别也不同。以下将 IP/MAC 异常违规风险按照终端使用人角色分析如下：

风险点（1-3）：任何岗位角色都会使用网络，都会涉及终端违规网络访问风险问题，因此，该风险与内部人员相关：

a）高级管理岗位，如区域负责人等高层领导，他们不太会修改 IP，但是他们的 IP 地址具有极高的权限，极有可能会被仿冒。

b）地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，他们不太会修改 IP，但是他们的 IP 地址具有较高的权限，较有可能会被仿冒。

该风险也与临时人员相关：辅助人员岗位（如食堂、车队、绿化等人员等），可能会假

冒其他人员的 IP，访问与其身份不符的资源，其风险重大。

该风险与外来人员相关：外来厂家人员、特别是外来维护人员其网络知识丰富，也有可能进行 IP/MAC 假冒，其风险重大。

风险点（4-6）：内部人员在网络使用时，必须有在用终端的 IP/MAC 对应关系，否则一旦出现问题，不能做有效查找；重点需要了解高级管理岗位，如区域负责人等高层领导在用终端的 IP/MAC 对应关系和地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员的在用终端的 IP/MAC 对应关系；而对于临时人员和外部人员的，因无法事先对其在用终端的 IP/MAC 作出基线，风险较大。

风险点（7-8）：对于高级管理岗位，如区域负责人等高层领导的在用终端的 IP/MAC 策略需要重点保证，一旦策略不能及时有效下发，或不能了解当前策略是否有效，造成重要业务不能及时审批，给业务的有效性造成风险。对于地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，一旦策略不能生效或与业务冲突，势必对业务造成风险。

风险点（9）：该风险对于高级管理岗位较大，一旦在用终端的 IP/MAC 绑定监控模块与领导的业务冲突，导致不能上网，必然给业务带来严重风险；当然这个风险也会给内部管理人员如地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员的业务带来威胁；这个风险与临时人员和外来人员的风险级别不大。

（d）合规性要求

合规性要求见表 B-8。

表 B-8

序号	安全类	等级保护（三级）要求	符合程度
1	网络安全	7.1.2.2 访问控制（G3） 重要网段应采取技术手段防止地址欺骗	符合
2	网络安全	7.1.2.3 安全审计（G3） 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录	符合

2．风险管控

每类风险在管控过程中，针对风险的事前、事中和事后 3 种状态进行监控，做到事前预防、事中控制、事后审计追查。下面的风险管控处理流程，尽量从事前、事中和事后 3 方面对风险管控进行描述。

（1）风险点（1-5）：IP/MAC 地址篡改监控缺失风险

事前处置：需要在终端机器入网前，调查记录内部网络配置，做好 IP 地址，MAC 地址，接入区域，接入交换机对应端口，涉及员工等信息登记在 IP/MAC 绑定表，将这些信息导入分别倒入管理中心，接入交换机对应端口，内置防火墙上。

事中处置：如果发现终端上修改了 IP/MAC 对应信息，即给终端发出提示信息，提示信息包含有关的警告信息；如果发现终端上修改了 IP/MAC 对应信息，而且发现有利用修改后的 IP 地址从事违规的网络活动，管理员有权发送阻断策略，强制将违规终端断网；对于需要进行 IP/MAC 信息修改的工作要求，可以提交主管领导和信息安全管理人员审批，经过核准之后，才能由管理员进行修改；以上的处置措施都必须作出完整的日志记录，及时上报管理

中心。

事后处置：对于该类风险，保留日志记录，如果出现安全事件，可以追溯责任人进行批评和责罚。同时，通过日志审计，对 IP/MAC 对应表做一些梳理，确定是否需要改进。

控制流程见图 B-13。

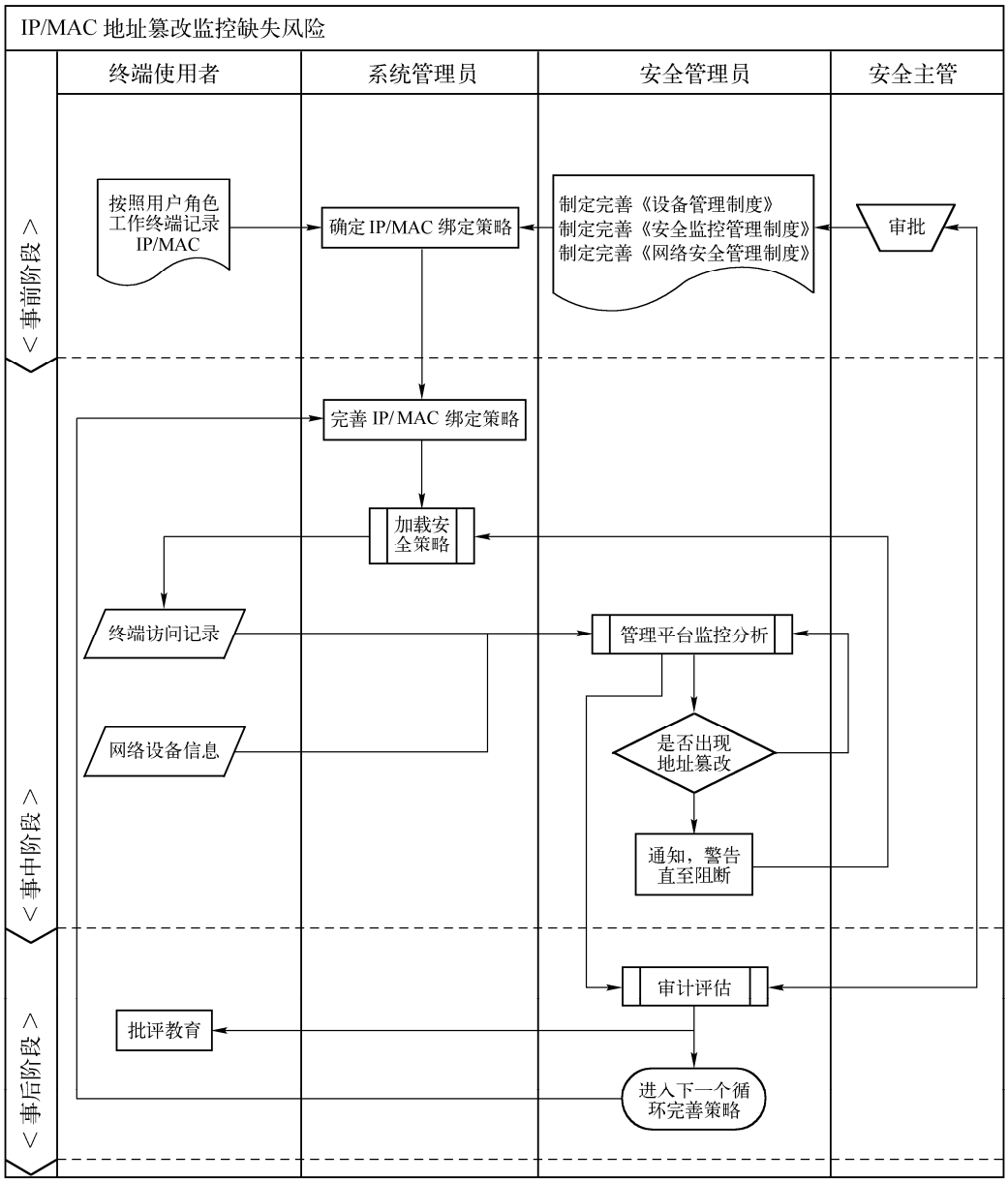

图 B-13

（2）风险点（6-9）：IP/MAC 地址篡改技术控制措施失效风险

事前处置：使用技术手段对终端的 IP/MAC 等网络配置进行监测和保护，对于违规情况可以及时发现并在适当的情况下进行修复和保护。需要制定有关的应急响应预案，一旦出现策略不能及时更新而技术手段无法实现时需要启动；一旦出现 IP/MAC 篡改盗用，导致业务

遭到影响时需要启动。

事中处置：通过分析实时的终端通信日志、实时的网络设备通信日志了解 IP/MAC 地址对应是否正常，或者及时发现 IP/MAC 地址绑定模块被停止和被删除，或者了解 IP/MAC 地址绑定模块与某些业务是否冲突；如果在规定的时间内得不到反馈信息，需要启动应急预案；一旦出现策略与业务的兼容性问题，需要有逃生机制，即通过人工卸载策略，确保业务的顺利进行。

事后处置：一旦前面的技术手段都失效，需要在安全主管的认可下启动应急预案。首先在确保业务顺利进行的前提下，人工在本地更新或卸载策略。在此基础上再考虑其他问题，如策略不能更新的故障原因、涉及的部门和人员，造成问题的是平台本身的性能原因还是其他因素，这些问题是否在管理制度中作出了相关规定，是否需要完善或补充等。

控制流程见图 B-14。

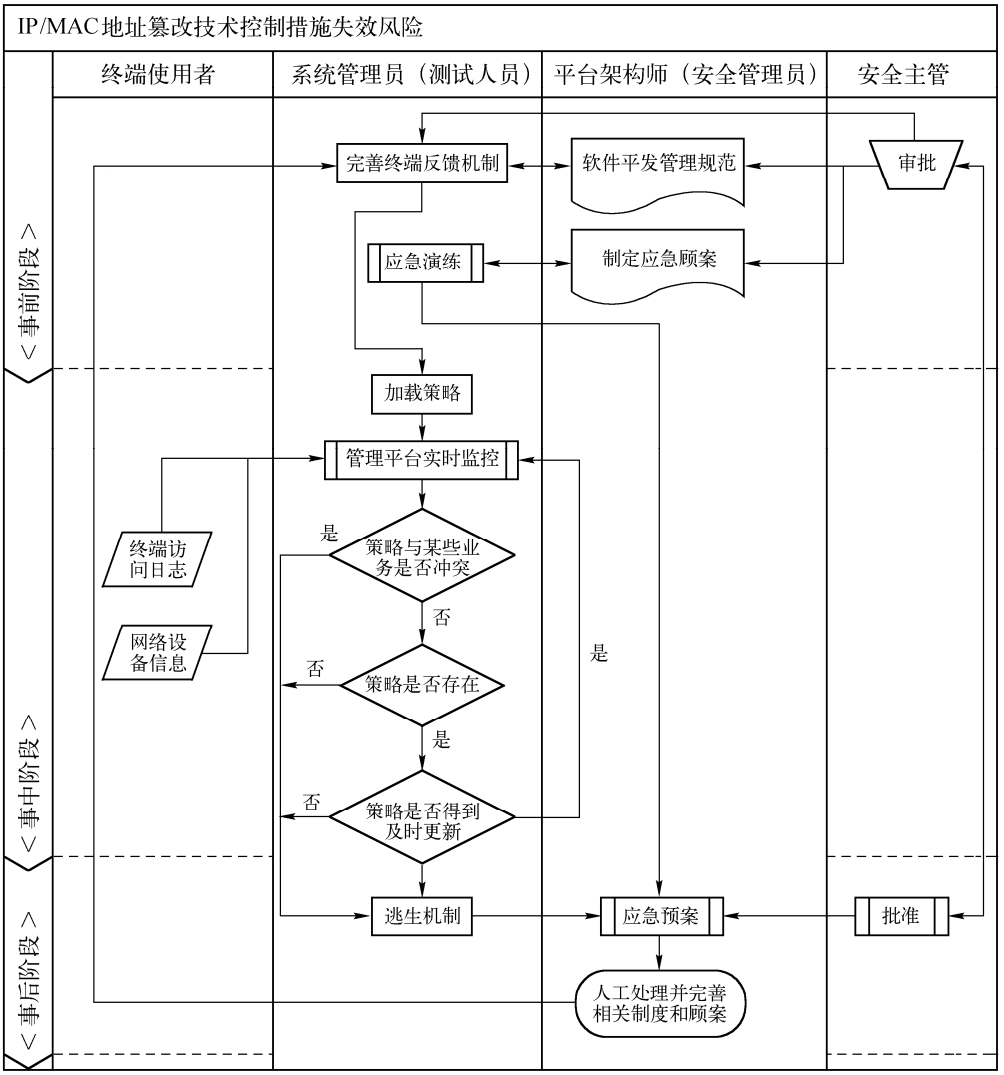

图 B-14

3．风险控制效果

对于此类风险涉及的 IP/MAC 篡改风险，通过采取管理、规范、流程、技术不同的措施，分别从事前、事中、事后 3 个方面来加以控制，可以基本达到风险管控的目的。

通过事前对不同角色的用户，逐步建立 IP/MAC 基线，事中根据这个基线进行监控和事后效果的分析和改善，实现了 PDCA 的最佳实践，为有效地控制网络流量异常风险达到了效果。事后通过日志审计，可以查找风险源，追溯到终端责任人，这可以给后续的考评管理提供依据。

由于控制平台本身的性能可能会造成风险事件在采集、汇集、分析、展示等不同阶段的遗漏和误判，可能给业务带来风险，因此需要根据可能出现的场景，如策略与业务冲突，定制的技术处理手段失灵等，制定应急预案并做定期演练，努力确保业务的连续性和可靠性。

B.2 终端运行安全（RR1.2）

B.2.1 进程/服务运行的风险（20 个风险点）

1．风险分析

（1）风险描述

该类风险主要表现为一些终端客户在没有管控的情况下，会私自安装一些与正常工作无关的软件，并在客户端上运行这些软件的进程/服务。这些进程/服务，通常被称为黑名单进程/服务。这些黑名单进程/服务的运行，可能会大量占用终端的 CPU、内存和硬盘资源，更有甚者，一些病毒或者木马进程会造成信息泄漏或者病毒传播，进而影响全网安全。与此同时，为了支撑正常业务运转，需要在终端上启用一些必要的进程/服务，这些进程/服务通常被称为白名单进程/服务。只有白名单上的进程/服务都启用，才能支撑正常业务运转。

黑名单进程/服务：不允许在终端上运行的进程/服务，运行会给终端带来风险，比如对系统存在威胁的病毒木马进程/服务等；下面是几个常见的对系统存在威胁的的病毒木马进程。

- ✓ mario.exe：Trojan.Mario 木马的部分进程，植入者会远程访问计算机，并窃取用户信息和密码等资料。
- ✓ win32ssr.exe：是 Backdoor.Win32.Rbot.aob 木马的进程。
- ✓ wincomm.exe：通常这个木马启动之后会同时运行 winlock.exe，两者互相监控是否运行。一旦发现对方不在内存中，就立即使对方运行。会捆绑其他的病毒，在 DOS 下可清除。
- ✓ Scvhost.exe ：臭名昭彰的安哥病毒进程了，变种达几十个之多。跟冲击波病毒（Worm.Msblast）一样，利用系统 RPC 漏洞传播。

黑名单进程/服务还可以是一些占用大量带宽的下载程序，也可以是一些聊天、视频等工具，应明确规定不允许在终端上进行这些进程/服务。对不同的体系，会维护一个黑名单进程/服务列表。

白名单进程/服务：终端主机上必须要求运行的进程和服务。不同主机要求的进程/服务不尽相同。对不同的体系，需要维护一个白名单进程/服务列表。

备注：需要结合终端的使用分类，对不同的终端维护一份黑白名单进程/服务列表，且该列表的内容需要及时调整和更新。

（2）相关风险点

进程/服务运行的风险点详见表 B-9。

表 B-9

	序号	风 险 点	风险属性	隐患/风险
进程/服务运行的风险	1	黑名单进程/服务运行	原生风险	隐患
	2	黑名单进程/服务运行，没有提示终端用户	原生风险	隐患
	3	黑名单进程/服务运行，审计信息没有上报管理员	原生风险	风险
	4	黑名单进程/服务运行，没有产生告警	原生风险	隐患
	5	黑名单进程/服务运行，没有通过策略阻止	原生风险	风险
	6	黑名单进程/服务运行，提示用户禁止进程/服务，但用户又重启该进程/服务	次生风险	风险
	7	黑名单机制不完整	原生风险	隐患
	8	黑名单机制不完整，相应的策略内容不完整	次生风险	隐患
	9	黑名单进程/服务运行，不能用已有的黑名单机制来检测，导致黑名单进程/服务不能检测	残余风险	风险
	10	白名单进程/服务运行不完整	原生风险	隐患
	11	白名单进程/服务运行不完整，没有提示终端用户	原生风险	隐患
	12	白名单进程/服务运行不完整，审计信息没有上报管理员	原生风险	风险
	13	白名单进程/服务运行不完整，没有产生告警	原生风险	隐患
	14	白名单进程/服务运行不完整，没有通过策略启用进程/服务	原生风险	隐患
	15	白名单进程/服务运行不完整，提示用户启用进程/服务，但用户又禁止该进程/服务	次生风险	风险
	16	白名单机制不完整	原生风险	隐患
	17	白名单机制不完整，相应的策略内容不完整	次生风险	隐患
	18	白名单进程/服务运行，不能用已有的白名单机制来检测，导致白名单进程/服务不能检测	残余风险	风险
	19	黑名单进程/服务运行，导致 CPU 占用率持续高	次生风险	风险
	20	黑名单进程/服务运行，导致内存占用率持续高	次生风险	风险

（a）基于资产使用生命周期分析

该类风险涉及入网前、运行阶段。入网前由于终端资产不包含敏感信息和数据，风险较低；入网后，由于运行过程中涉及敏感信息和生产数据，如果不加以控制，将会导致损失较大，风险较高。进程/服务运行的风险对终端的影响在资产使用生命周期的体现如下：

风险点（1-9）：黑名单进程/服务在终端上运行，这些风险主要涉及入网前和运行阶段。

维修和报废阶段，终端不运行，不存在该类风险。

入网前，终端运行黑名单/进程服务，会对终端本身的安全带来一些风险，如果是病毒进程，会造成终端感染的风险；如果是与工作无关的进程，会影响工作效率。但影响的范围在终端本身，不会对整体系统造成大的风险，风险一般。

终端入网处于运行阶段后，如果黑名单进程是与病毒有关的，会将病毒扩散到整个系统，风险极高；如果该黑名单进程占用大量 CPU 资源时，会造成正常业务进程运行所需要的 CPU 资源得不到满足，从而影响业务使用；如果该黑名单进程占用大量内存资源时，会造成正常业务进程运行所需要的内存资源得不到满足，从而影响业务使用；如果该黑名单进程是与工作无关的进程，会影响正常工作的开展，降低工作效率。如果该黑名单进程是下载类的进程/服务，会占用大量的带宽，从而影响正常的业务通信，影响业务使用。

风险点（10-18）：白名单进程/服务在终端上运行不完整，这些风险主要涉及入网前和运行阶段。维修和报废阶段，终端不运行，不存在该类风险。在入网前阶段，此时终端未接入网络，不涉及数据传输，白名单进程/服务运行不完整导致的风险比较低；终端入网运行后，如果不进行白名单检测，导致本应该运行的进程/服务，却没有运行，如果该进程是与业务相关的，则影响业务开展。

风险点（19-20）：黑名单进程/服务，导致终端的 CPU、内存资源占用率持续高。该风险主要涉及入网前和运行阶段。维修和报废阶段，终端不运行，不存在这些风险。入网前，这些风险只会对终端本身有影响，风险较低。入网后处于运行阶段时，高资源占用会导致终端不能维持正常业务运转，风险较高。

（b）与信息安全关系

进程/服务运行的风险涉及在线信息安全风险和存储信息风险。

风险点（1-9）：黑名单进程/服务的运行，如果是病毒程序，会导致在线信息被篡改或者丢失；同时，因为黑名单进程/服务的运行，会开放一些端口，进而造成终端上的一些在线信息被窃取或者修改；黑名单进程/服务运行，如果是病毒程序，会导致终端上的存储信息被篡改或者丢失；同时，因为违规进程/服务的运行，会开放一些端口，进而造成终端上的一些存储信息被窃取或者修改。

风险点（10-18）：白名单运行不完整的风险，如果必须运行的防病毒软件没有运行，会导致终端得不到应有的保护（具体风险可参考终端防病毒类别的风险）。会对在线信息和存储信息造成信息篡改和丢失的风险。如果只是业务处理软件，不运行不会对在线信息和存储信息造成风险。

风险点（19-20）：黑名单进程/服务导致的终端异常资源占用，会对在线信息的存储和处理带来风险；对已存储信息不会影响，风险较低。

（c）基于资产使用人分析

风险点（1-18）：任何岗位角色都涉及进程/服务的不按规定使用问题。因此，该风险与内部人员相关：高级管理岗位，如区域负责人等高层领导；地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员；开发人员、研发人员等，考虑根据业务和工作需要执行相关的黑白名单进程/服务运行的权限。

临时人员：辅助人员岗位，如食堂、车队、绿化等人员，该类人员在使用终端的过程中，如果随意启动黑名单之列的进程/服务，会导致终端上运行不允许运行的进程/服务，进

而影响终端的使用。

外来人员：外来厂家人员、外来维护人员一般情况下，是不赋予对进程/服务的操作权限的，如果因为工作需要，应先将需要运行的进程报批，在黑白名单进程中备案后，再根据相关的策略运行相关的进程。

风险点（19-20）：任何岗位角色都可能存在违规进程/服务导致的终端资源异常占用的问题。因此，需要严格控制各类人员对进程/服务的启动/禁用权限。同时，要执行严格的黑白名单检测机制，避免出现黑名单进程的异常资源占用，从而导致终端不可用的风险。

（d）合规性要求

合规性要求见表 B-10。

表 B-10

序号	安全类	等级保护（三级）要求	符合程度
1		等级保护中没有明确对进程/服务运行的要求	

该风险属于运行时风险，一般来说，运行的进程和服务，对于不同类型的终端来说，要求的进程和服务不尽相同，与实际运维环境密切相关。等级保护方面在这块没有明确的要求。

相关技术和管理的风险管控措施参见以下小节阐述。

2．风险管控

（1）风险点（1-9）：黑名单进程/服务运行管理控制流程

事前处置：定义具体的黑名单/服务的范围，哪些是明确不允许在内网终端上运行的进程/服务。这个黑名单/服务列表是随着运维过程变化而变化的，不同类型的终端上，运行的黑名单进程/服务不尽相同。

事中处置：

- ✓ 定时检测终端运行的进程/服务列表
- ✓ 将获取的进程/服务列表与事前定义的黑名单列表进行比较
- ✓ 如果有黑名单上的进程和服务，提示终端用户运行了黑名单进程/服务（通知终端用户，消息的方式）
- ✓ 根据黑名单运行策略执行操作，提示终端使用者，并且发送防护平台
- ✓ 记录违规运行黑名单进程/服务的行为及终端使用者的操作，发送至防护平台服务器
- ✓ 发现黑名单进程/服务运行违规行为时，记录黑名单违规运行的审计记录，保存至防护平台服务器
- ✓ 对黑名单进程/服务违规运行的行为进行取证（黑名单违规运行的进程名称、进程运行的终端使用者、终端 IP 等原始记录信息），保存至防护平台服务器

事后处置：根据整体安全态势分析，调整安全策略，针对终端下发新的黑名单进程/服务运行安全策略。管理员通过黑名单违规运行的记录对违规黑名单进程/服务行为进行追溯，并通过管理流程进行相应的处罚，处罚时以防护平台保存的访问原始记录作为处罚依据。

处置流程见图 B-15。

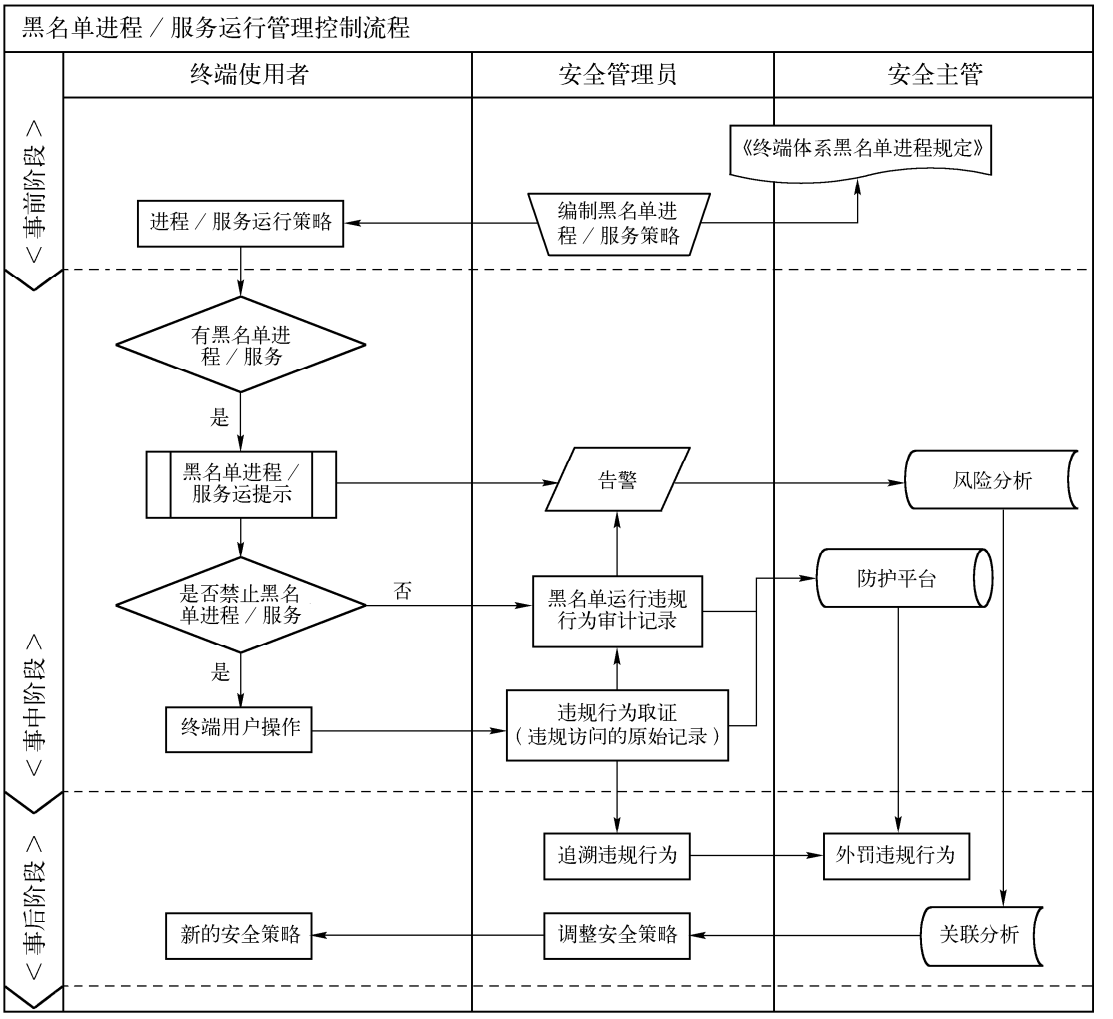

图 B-15

（2）风险点（10-18）：白名单进程/服务运行管理控制流程

事前处置：定义具体的白名单/服务的范围，哪些是为了保证正常的工作和业务开展，必须在终端上运行的进程/服务；白名单进程/服务列表是随着运维过程变化而变化的，不同类型的终端上，运行的白名单进程/服务不尽相同。

事中处置：

- ✓ 定时检测终端运行的进程/服务列表
- ✓ 将获取的进程/服务列表与事前定义的白名单列表进行比较
- ✓ 如果终端上运行的进程/服务与白名单相比较，白名单规定的进程/服务在终端上没有运行或者运行不完整，提示终端用户哪些进程/服务需要在终端上开启运行（通知终端用户，消息的方式）
- ✓ 根据白名单运行策略执行操作，提示终端使用者，并且发送防护平台
- ✓ 记录违规运行白名单进程/服务的行为及终端使用者的操作，发送至防护平台服务器

- ✓ 发现白名单运行违规行为时，记录白名单违规运行的审计记录，保存至防护平台服务器
- ✓ 对白名单进程/服务违规运行的行为进行取证（白名单违规运行的进程名称、进程运行的终端使用者、终端 IP 等原始记录信息），保存至防护平台服务器

事后处置：

根据整体安全态势分析，调整安全策略，针对终端下发新的白名单进程/服务运行安全策略。管理员通过白名单违规运行的记录对违规白名单进程/服务行为进行追溯，并通过管理流程进行相应的处罚，处罚时以防护平台保存的访问原始记录作为处罚依据。

处置流程见图 B-16。

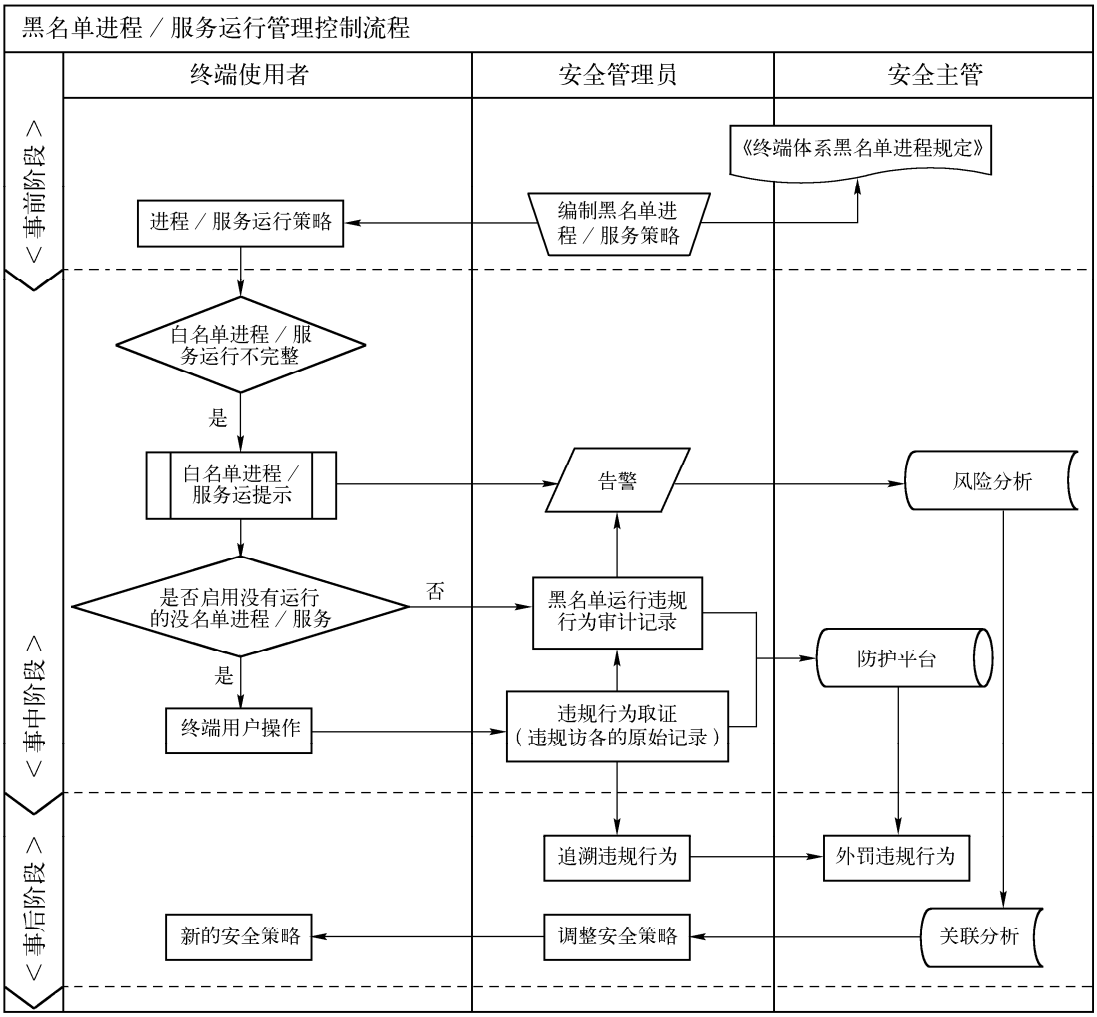

图 B-16

（3）风险点（19）：黑名单进程/服务运行导致 CPU 占用率持续高的管理控制流程

事前处置：定义具体的黑名单/服务的范围，哪些是明确不允许在内网终端上运行的进程/服务。这个黑名单/服务列表是随着运维过程变化而变化的，不同类型的终端上，运行的

黑名单进程/服务不尽相同。定义一个进程 CPU 使用率异常的范围，根据实际运维的经验，当 CPU 使用率持续异常时，检测其是否为黑名单进程（如果是正常的进程，CPU 使用率应该是在一个合理的范围内）。

事中处置：

- ✓ 检测终端上 CPU 使用率异常的进程
- ✓ 将使用率异常的进程/服务与黑名单进行/服务进行比较
- ✓ 如果有黑名单上的进程和服务，提示终端用户运行了 CPU 使用率异常的黑名单进程/服务（通知终端用户，消息的方式）
- ✓ 根据黑名单运行策略执行操作，提示终端使用者，并且发送防护平台
- ✓ 记录违规运行黑名单进程/服务的行为及终端使用者的操作，发送至防护平台服务器

事后处置：根据整体安全态势分析，调整安全策略，针对终端下发新的黑名单进程/服务运行安全策略。

处置流程见图 B-17。

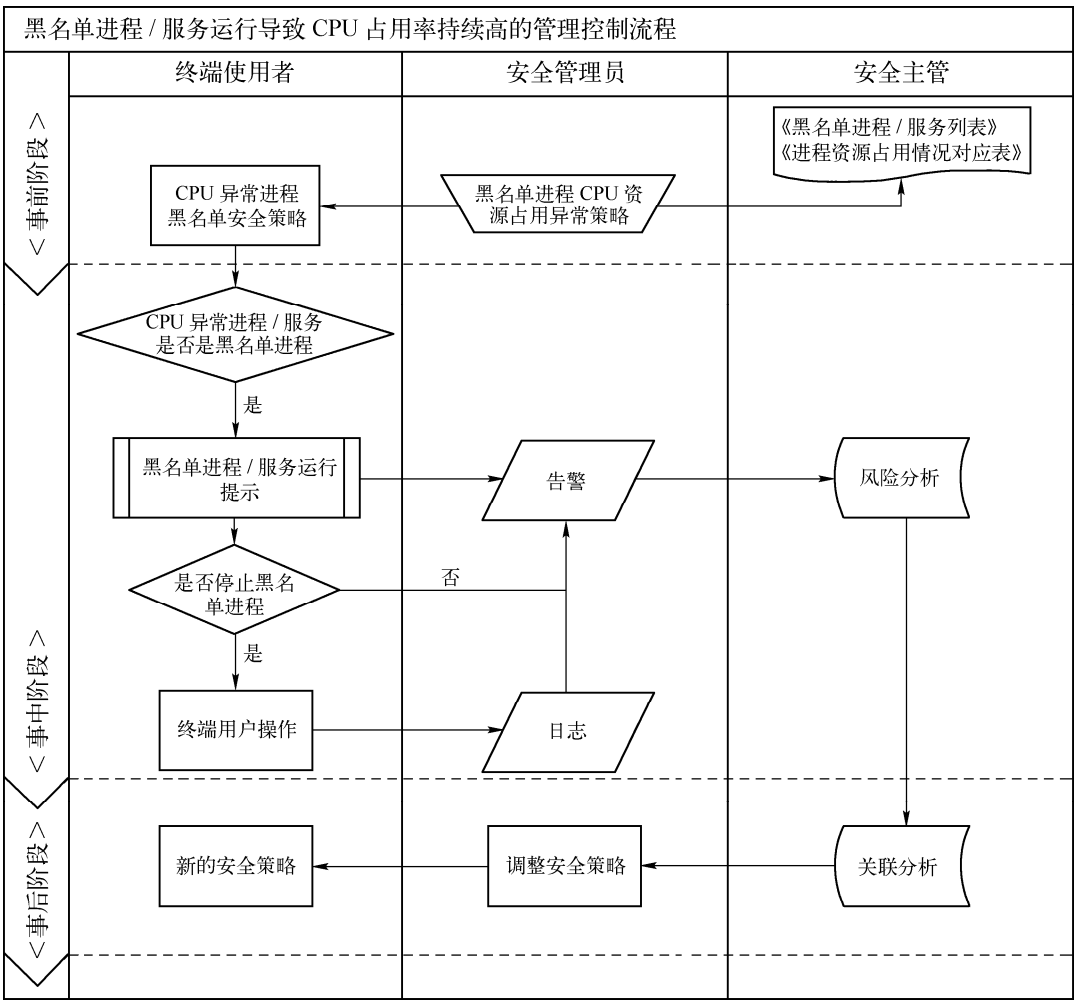

图 B-17

（4）风险点（20）：黑名单进程/服务运行导致内存占用率持续高的管理控制流程

事前处置：定义具体的黑名单/服务的范围，哪些是明确不允许在内网终端上运行的进程/服务。这个黑名单/服务列表是随着运维过程变化而变化的，不同类型的终端上，运行的黑名单进程/服务不尽相同。定义一个进程内存使用率异常的范围，根据实际运维的经验，当进程内存使用率持续异常时，检测其是否为黑名单进程（如果是正常的进程，内存使用率应该在一个合理的范围内）。

事中处置：

- ✓ 检测终端上内存使用率异常的进程
- ✓ 将使用率异常的进程/服务与黑名单进行/服务进行比较
- ✓ 如果有黑名单上的进程和服务，提示终端用户运行了内存使用率异常的黑名单进程/服务（通知终端用户，消息的方式）
- ✓ 根据黑名单运行策略执行操作，提示终端使用者，并且发送防护平台
- ✓ 记录违规运行黑名单进程/服务的行为及终端使用者的操作，发送至防护平台服务器

事后处置：根据整体安全态势分析，调整安全策略，针对终端下发新的黑名单进程/服务运行安全策略。

处置流程：处置流程与 CPU 资源持续过高的流程类似。

（5）残余风险处理

进程/服务的黑白名单是需要根据实际情况调整的。在对进程/服务运行进行风险管理工作中存在这样的情况：

- ✓ 具体的黑白名单需要在运维中确定；实施初期，黑白名单机制内容不完整
- ✓ 在黑白名单机制还不完整时，一些违规的进程/服务在终端上运行，如果是病毒进程，会造成终端感染，如果病毒继续传播，将感染其他终端，风险较高
- ✓ 在黑白名单机制还不完整时，一些违规的进程/服务在终端上运行，如果运行的进程开放一些端口，会造成终端上的重要信息泄漏等风险，风险较高

因此，尽管部署了完备的检测和管理技术手段，但黑白名单机制是需要根据运维情况随时改进的，如果这个黑白名单机制不及时更新，违规进程/服务运行的风险继续存在。

针对该问题，建议增加以下几方面工作：

- ✓ 加强安全意识培训和教育，加强黑白名单机制的建设工作
- ✓ 注意黑白名单内容的更新工作，及时根据运维情况，调整黑白名单的详细内容
- ✓ 提供制度保障，要求定期对黑白名单的内容进行检查和更新
- ✓ 建立定期检查和整改制度，定期对组织内黑白名单的更新情况进行检查，并督促其整改
- ✓ 设立针对进程/服务运行的考核管理措施，将该项工作作为终端使用人、终端所有单位安全工作考评中的考核指标

3．技术管控中存在的问题和对策

如果终端操作系统有错误，其进程/服务信息可能无法获取，会造成无法控制，需要先修复操作系统，保证其进程/服务信息可获取。

4．风险控制效果

通过终端运行进程/服务的检测，可以监控终端进程/服务的运行情况。同时结合监控资源使用率，可以有效地发现运行中的异常进程，对黑名单中的非法进程/服务严格禁止运行，并对私自运行黑名单的责任人给予考评扣分管理处罚。同时，通过对白名单进程/服务的检测，保证终端上必须运行的进程和服务都得以运行，从而保证业务和工作的正常开展。

B.2.2 违规软件安装的风险（20 个风险点）

1．风险分析

（1）风险描述

违规软件安装的风险主要表现为一些终端客户端在没有管控的情况下，出现个人私自安装与客户端工作无关的非必要软件，这些私自下载安装的应用程序，有些是非授权的软件，也有些是占用资源很大的游戏软件、电影、P2P 下载类软件等，还有些甚至是隐藏了后门的黑客软件，这些软件轻则分散工作时的注意力，重则引起带宽消耗、网络风暴、病毒、黑客攻击等。如果是核心的业务所在终端上运行了这些违规软件，还有可能造成敏感信息泄漏的高风险。如果不对软件的安装情况进行管控，由用户随意安装、卸载、使用，存在下面的风险：

- ✓ 如果用户日常工作需要的软件没有安装，会导致用户无法正常进行工作
- ✓ 如果用户日常工作需要的软件被卸载，同样会导致用户无法正常进行工作
- ✓ 如果用户安装了与工作无关的某些软件并使用，可能会在工作时间做与工作无关的事情，影响工作效率
- ✓ 如果用户安装了某些大量占用带宽的下载软件，在使用时会对网络带宽造成严重影响，使得网络的可用性下降

违规软件的定义：结合一般业务系统的特点，按不同的终端类型对违规软件做如下定义：

核心业务主机：此类主机，上面运行的就是核心业务，不应该允许一些个人化的软件，比如聊天软件、游戏软件、下载软件、播放软件等。

个人正常办公终端：如果是正常办公终端，只允许安装与工作处理相关的软件，一些游戏软件、下载软件等是不允许安装的。

备注：违规软件的定义需要结合实际情况进行，上面只是一部分可以参考的内容，软件种类比较多，违规与否需要与实际结合。建议项目实施时，对该部分内容进行详细调研，确定不同类型终端上对应的违规软件。

（2）相关风险点

违规软件安装的风险点详见表 B-11。

表 B-11

	序号	风险点	风险属性	隐患/风险
程/服务运行的风险	1	违规软件安装	原生风险	隐患
	2	违规软件安装，没有提示终端用户	原生风险	隐患
	3	违规软件安装，审计信息没有上报管理员	原生风险	风险
	4	违规软件安装，没有产生告警	原生风险	隐患
	5	违规软件安装，没有通过策略卸载	原生风险	隐患
	6	违规软件安装，提示用户卸载软件，但用户重新安装了该软件	次生风险	风险
	7	违规软件列表不完整	原生风险	隐患
	8	违规软件列表不完整，相应的策略内容不完整	次生风险	风险
	9	违规软件安装，不能用已有的违规软件检查机制来检测，导致违规软件安装不能检测	残余风险	风险
	10	必须安装软件安装不完整	原生风险	隐患
	11	必须安装软件安装不完整，没有提示终端用户	原生风险	隐患
	12	必须安装软件安装不完整，审计信息没有上报管理员	原生风险	风险
	13	必须安装软件安装不完整，没有产生告警	原生风险	隐患
	14	必须安装软件安装不完整，没有通过策略进行软件分发	原生风险	隐患
	15	必须安装软件安装不完整，提示用户安装软件，但用户不安装软件	次生风险	风险
	16	必须安装软件列表不完整	原生风险	隐患
	17	必须安装软件列表不完整，相应的策略内容不完整	次生风险	隐患
	18	必须安装软件的检测，不能用已有的必须安装软件列表来检测，导致必须安装的软件检测无法进行	残余风险	风险
	19	对终端软件安装信息变化不记录，不产生告警	次生风险	风险
	20	对终端软件安装信息变化不记录，不审计	次生风险	风险

（a）基于资产使用生命周期分析

该类风险涉及入网前、运行阶段。入网前由于终端资产不包含敏感信息和数据，风险较低。入网后，由于运行过程中涉及敏感信息和生产数据，如果不加以控制，导致的损失较大，风险较高。违规软件安装的风险对终端的影响在资产使用生命周期的体现如下：

风险点（1-9）：违规软件在终端上安装，这些风险主要涉及入网前和运行阶段。维修和报废阶段，终端不运行，不存在该类风险。

入网前，终端安装了违规软件，只会对终端本身的安全带来一些风险，如果是病毒软件，会造成终端感染的风险；如果是与工作无关的软件，会影响工作效率。但影响的范围在终端本身，不会对整体系统造成大的风险，风险一般。

终端入网处于运行阶段后，如果核心业务主机上安装了下载软件，因为下载，会占用大量带宽，进而影响业务运行的正常通信，风险较高；如果核心业务主机上安装了下载软件，如果下载到了病毒程序，会导致业务主机中毒，不能运行，影响业务运行，风险较高；如果核心业务主机上安装了下载软件，如果下载到了病毒程序，导致业务主机中毒，同时通过网

络，还会将病毒传播到整个网络，风险较高；如果核心业务主机上安装了游戏软件，会占用业务主机的磁盘空间，同时，因为游戏软件的运行，会消耗主机上的 CPU 和内存资源，从而影响主机业务的运行，风险较高；如果核心业务主机上安装了播放软件，会占用业务主机的磁盘空间，同时，因为播放软件的运行，会消耗主机上的 CPU 和内存资源，从而影响主机业务的运行，风险较高；如果个人办公终端安装了下载软件，如果下载到了病毒程序，导致个人办公终端中毒，同时通过网络，还会将病毒传播到整个网络，风险较高；如果个人办公终端安装了下载软件，如果下载到了病毒程序，导致个人终端中毒，影响个人日常工作的正常开展，风险较高；如果个人终端安装了下载了软件，占用了带宽资源，影响其他用户的正常网络使用，风险较高；如果个人终端安装了游戏软件，因为游戏软件的安装，影响正常的办公工作，同时，因为终端上运行游戏，会降低工作效率，风险较高；如果个人终端安装了电影播放软件，会影响工作效率，同时电影播放软件的资源会占用大量硬盘空间，因而影响工作开展，风险较高。

风险点（10-17）：必须安装的软件在终端上没有安装，这些风险主要涉及入网前和运行阶段。维修和报废阶段，终端不运行，不存在该类风险。

在入网前阶段，此时终端未接入网络，不涉及数据传输，必须安装的软件安装不完全，只会影响终端本身的使用，不会影响体系内其他机器，风险比较低。

终端入网运行后，如果是核心业务主机，如果必须安装的软件安装不完整，会造成核心业务不能运行，正常业务无法开展；如果是个人终端，会导致一些特定的工作无法进行，影响正常工作的开展。

风险点（18）：该风险主要是必须安装软件列表制定方面的风险，与资产生命周期无关。

风险点（19-20）：这两个风险与资产入网运行后阶段相关。资产入网前，无法对终端上的安装软件进行检测，与该阶段无关。在资产入网运行后，如果不对终端软件安装的变化情况记录和告警，会出现终端用户随意变更终端上安装的软件的情况，风险较高。维护和报废阶段，终端不运行，无法检测终端软件的安装情况，不存在这两个风险。

（b）与信息安全关系

风险点（1-9）：终端上安装了违规软件，违规软件的运行，会导致正常的业务进程因为得不到运行所需要的硬盘、CPU、内存等资源而无法运行，进而造成正常业务的不可用。对在线信息而言，可能会因为缺少必要的资源造成在线信息得不到及时的处理和存储；同时，由于违规软件的安装运行，会开放一些端口，进而造成终端上的一些在线信息被窃取或者修改；如果违规软件的运行，导致业务主机感染病毒或木马，会造成在线信息被篡改，风险非常高。违规软件的安装和运行，会开放一些端口，进而造成终端上的一些存储信息被窃取或者修改；违规软件如果是病毒程序，安装和运行后，主机感染病毒或木马，会造成存储信息感染病毒或被篡改，风险非常高。

风险点（10-17）：必须安装的软件如果没有安装，取决于软件的类型，如果是防病毒软件没有安装，会导致在线信息和存储信息感染的风险，风险较高；如果只是应用类软件，不安装仅仅是影响正常工作使用，不会对在线信息和存储信息造成风险。

风险点（18）：与信息安全无关。

风险点（19-20）：这两个风险对信息安全的影响，同样取决于软件的类型，如果用

户违规安装了软件或者卸载了不允许卸载的软件，会对在线信息和存储信息带来泄漏和篡改的风险。

（c）基于资产使用人分析（外来人员、临时工、内部人员）

风险点（1-9）：任何岗位角色都可能存在在终端上进行违规软件安装的问题。因此，该风险与内部人员相关：高级管理岗位，如区域负责人等高层领导，地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员，开发人员、研发人员等，考虑根据业务和工作需要执行相关的软件安装权限。临时人员：辅助人员岗位，如食堂、车队、绿化等人员，该类人员在使用终端的过程中，一般不应允许在终端上安装软件。外来人员：外来厂家人员、外来维护人员一般情况下，是不赋予软件安装权限的，如果因为工作需要，需要先将要安装的软件的相关情况报批，在软件安装允许列表中备案后，再进行软件安装。

风险点（10-17）：只有那些在终端上进行软件安装的人员才有软件安装的控制管理权，必须安装的软件安装不完整的风险与人员无关，与终端的类型相关。

风险点（18）：管理制度相关，与内部人员相关：高级管理岗位，如区域负责人等高层领导；地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员相关。

风险点（19-20）：同风险点（1-9）。

（d）合规性要求

合规性要求见表 B−12。

表　B−12

序号	安全类	等级保护（三级）要求	符合程度
1		等级保护中没有明确对违规软件安装的要求	

该风险属于运行时风险，一般来说，一个终端上所需要安装的软件，对于不同类型的终端来说，要求安装的软件和对违规软件的定义不尽相同，与实际运维环境密切相关。等级保护方面在这块没有明确的要求。

相关技术和管理的风险管控措施参见以下小节阐述。

2．风险管控

（1）风险点（1-9）：违规软件安装检测管理流程

事前处置：定义违规软件的范围，哪些是明确不允许在终端上安装的软件。这个违规软件列表是随着运维过程变化而变化的，不同类型的终端上，违规软件的定义不尽相同。

事中处置：

- ✓ 定时检测终端上安装的软件列表
- ✓ 将获取的软件列表与事前定义的违规软件列表进行比较
- ✓ 如果有违规软件之列的软件安装，提示用户安装了违规软件（通知终端用户，消息的方式）
- ✓ 根据违规软件策略执行操作，提示终端使用者，并且发送防护平台
- ✓ 记录违规软件安装的行为及终端使用者的操作，发送至防护平台服务器

事后处置：根据整体安全态势分析，调整安全策略，针对终端下发新的违规软件安装运

行安全策略。

处置流程见图 B-18。

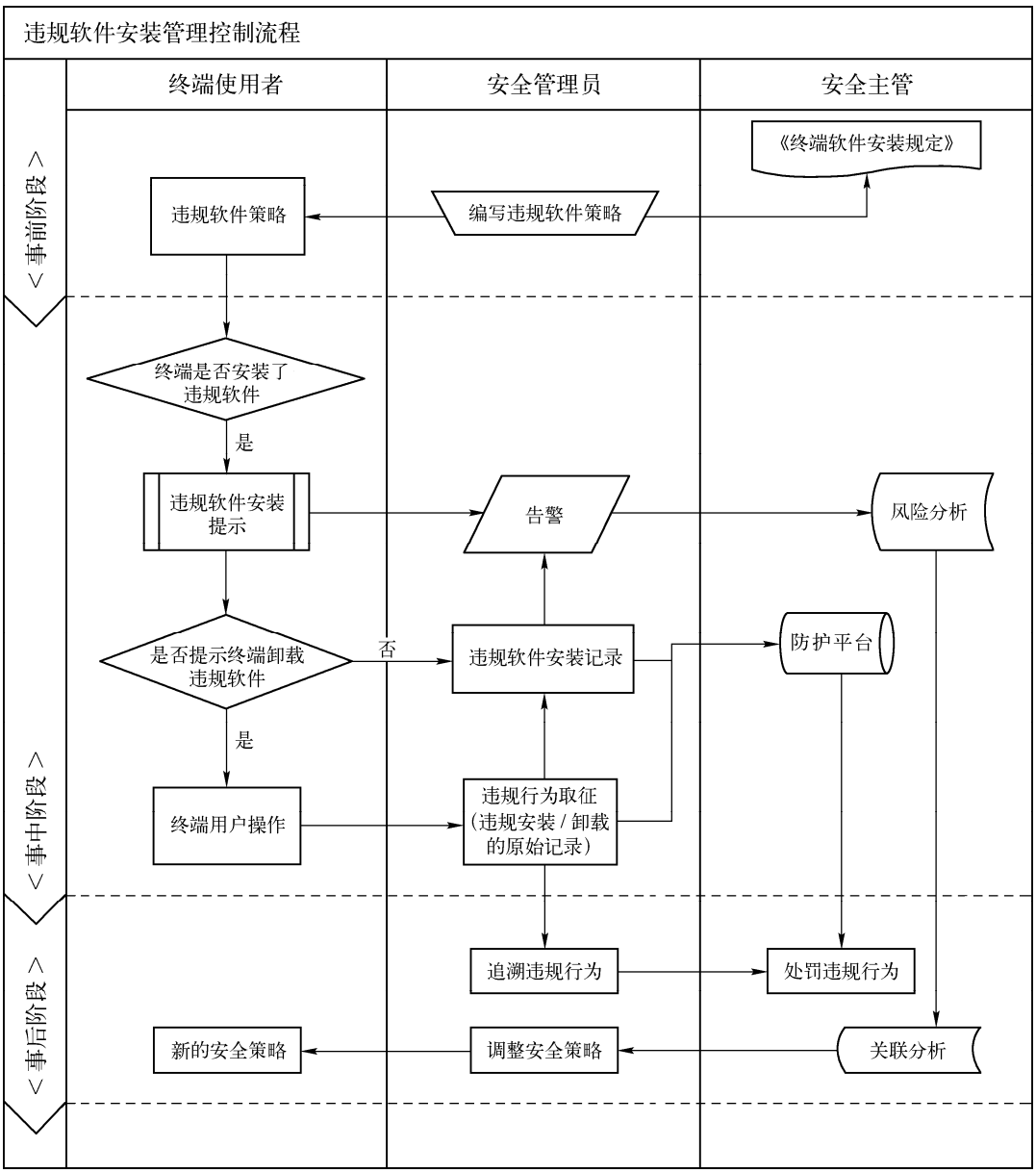

图 B-18

（2）风险点（10-17）：必须安装软件检测管理流程

事前处置：定义必须安装的软件列表，不同类型的终端上，必须安装的软件不尽相同，必须安装的软件列表是随着运维过程变化而变化的。

事中处置：

✓ 定时检测终端上安装的软件列表

- ✓ 将获取的软件列表与事前定义的必须安装的软件列表进行比较
- ✓ 如果有必须安装的软件没安装，提示用户软件安装不完整（通知终端用户，消息的方式）
- ✓ 根据软件分发策略执行操作，提示终端使用安装必装软件，并且发送防护平台
- ✓ 记录软件安装不完整的终端及软件信息，发送至防护平台服务器

事后处置：根据整体安全态势分析，调整安全策略，针对终端下发新的软件分发安全策略。

处置流程见图 B-19。

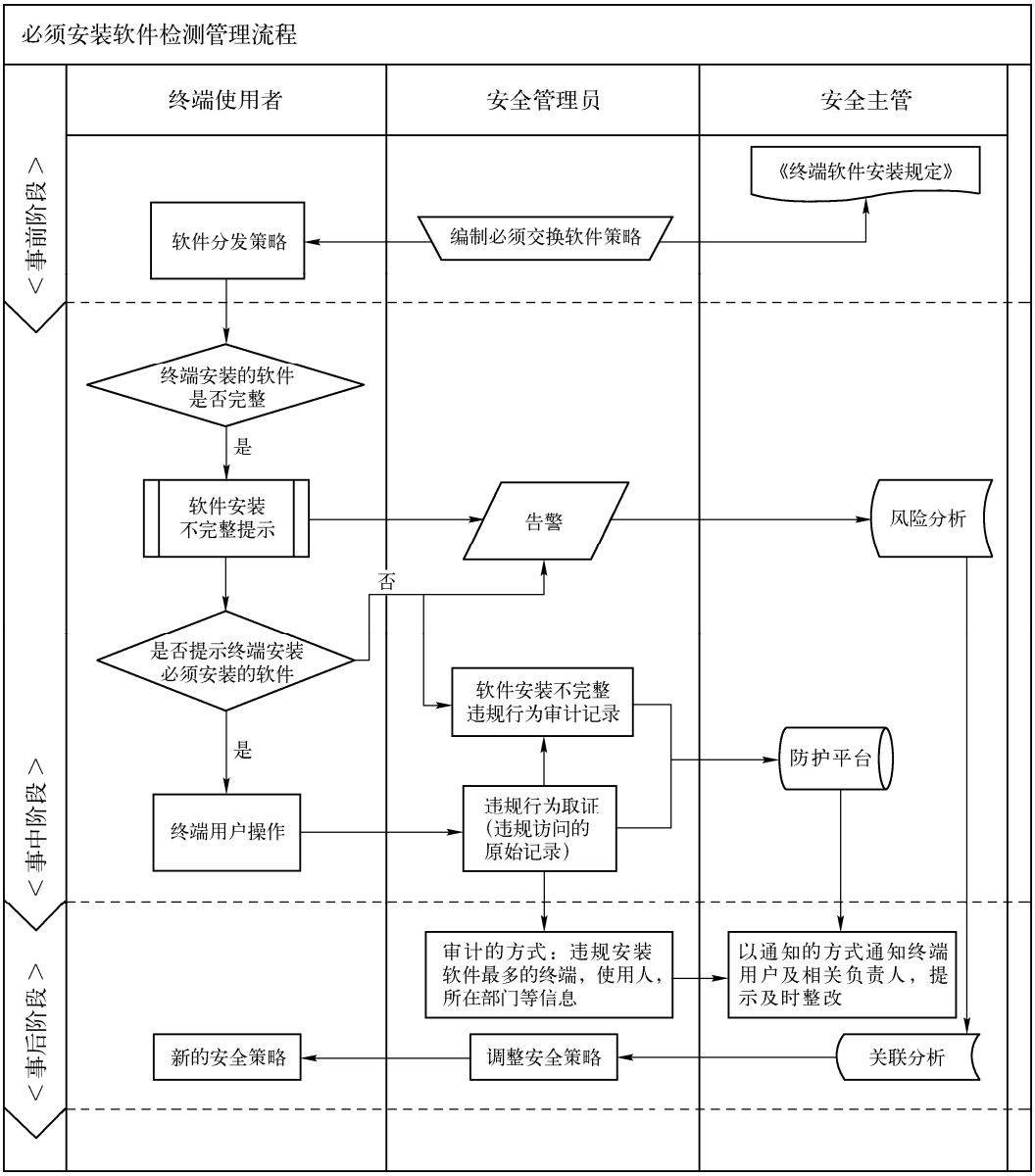

图 B-19

（3）风险点（19-20）：终端软件安装变化审计和告警管理流程

事中处置：

- ✓ 发现终端软件安装情况有变化时，记录软件变化的审计记录，保存至防护平台服务器。同时以告警的方式通知安全管理员和终端使用者
- ✓ 对安装违规软件的行为进行取证（违规软件的名称、违规软件安装的终端、终端使用者、终端 IP 等原始记录信息），保存至防护平台服务器
- ✓ 对违规卸载软件的行为进行取证（卸载的是必须安装软件列表中的软件，被卸载的必须安装的软件的名称、终端使用者、终端 IP 等原始记录信息），保存至防护平台服务器

事后处置：管理员通过违规软件安装和必须安装软件的卸载记录对随意改变终端软件安装的情况进行追溯，并通过管理流程进行相应的处罚，处罚时以防护平台保存的访问原始记录作为处罚依据。

（4）风险点（18）：必须安装软件的检测，不能用已有的必须安装软件列表来检测，导致必须安装的软件检测无法进行；属于残余风险处理的内容。

安装软件的黑白名单是需要根据实际情况调整的，具体的黑白名单需要在运维中确定；实施初期，可能出现一些违规软件的安装。

- ✓ 具体的违规软件名单需要在运维中确定；实施初期，违规软件的内容可能不完整
- ✓ 在违规软件内容还不完整时，一些违规软件会在终端上被安装但不能检测出来。一些违规软件如果是病毒软件，会造成终端感染，如果病毒继续传播，将感染其他终端，风险较高
- ✓ 在违规软件内容还不完整时，一些违规软件会在终端上被安装但不能检测出来。一些违规软件如果是开机就自动运行的软件，会占用大量资源，导致正常工作软件所需要的资源使用得不到保证，从而影响正常的工作开展，风险较高

因此，尽管部署了完备的检测和管理技术手段，但违规软件名单是需要根据运维情况随时改进的，如果这个软件违规名单不及时更新，违规软件安装的风险继续存在。

针对该问题，建议增加以下几方面工作：

- ✓ 加强安全意识培训和教育，加强违规软件名单的建设工作
- ✓ 注意违规软件名单内容的与时俱进工作，及时根据运维情况，调整违规软件的详细内容
- ✓ 提供制度保障，要求定期对违规软件的内容进行检查和更新
- ✓ 建立定期检查和整改制度，定期对组织内违规软件的更新情况进行检查，并督促其整改
- ✓ 设立针对违规软件安装的考核管理措施，将该项工作作为终端使用人、终端所有单位安全工作考评中的考核指标

3．技术管控中存在的问题和对策

如果终端操作系统有错误，其安装的软件信息可能无法获取，会造成无法控制，需要先修复操作系统，保证其安装的软件信息可获取；一些违规软件，如果安装信息不写入注册表

或其他配置文件，可能无法获取其安装信息，也不能将其与违规软件比对。可能会存在软件安装信息遗漏的情况，目前暂无解决的方法，但是该类软件一旦在终端上运行，可以通过进程/服务监控手段监控到，具体管控措施参见 B.3.1 节。

4．风险控制效果

通过软件安装信息检测，可以监控终端违规软件的安装情况。从而能够保证终端安装必需的软件，能够保证终端不安装禁止使用的软件，能够保证网络带宽不被下载软件占用，管理员可以设置查询条件对软件安装情况进行统计。同时，可以对违规安装软件的终端责任人进行记录，可以给后续的考评管理提供依据。

B.2.3 异常资源占用的风险（19 个风险点）

1．风险分析

（1）风险描述

终端本身资源包括 CPU、内存和磁盘存储空间等。终端正常运行时，各项资源的使用率会在一个正常范围内。安装运行的业务或应用软件过多、病毒感染或遭受攻击时，都可能会导致终端的某种资源占用率持续过高，影响正常的业务开展。

终端设备在运行一段过程后，常常由于运行软件过多，大量消耗内存和 CPU 资源，如果不能有效监控硬件资源使用情况，适时给用户提示告警，可能导致机器运行速度较慢，甚至业务服务无法运行。硬盘的剩余空间也需要随时监控，如果运行了关键业务的主机硬盘空间不够，导致数据不能存储，会有业务数据丢失和业务不能正常运行的风险。

CPU 使用率：表示系统资源的调用情况，如果利用率高就说明系统资源调取繁忙，会造成电脑运行反应缓慢。常见的引起 CPU 使用率高的因素有：

- ✓ 终端上的驱动没有经过认证，造成 CPU 资源占用 100%。大量测试版的驱动在网上泛滥，造成了难以发现的故障原因
- ✓ 防、杀毒软件造成故障。由于一些防、杀毒软件的运行，加入了对网页、插件、邮件的随机监控，增大了系统负担。可以根据情况有选择地开启服务
- ✓ 病毒、木马造成。大量的蠕虫病毒在系统内部迅速复制，造成 CPU 资源占用率居高不下

内存使用率：一般来说，内存使用率超过 85%，会认为内存使用率高。

磁盘剩余空间：终端上可用的磁盘空间大小。随着终端运行中的数据存储，以及所产生的垃圾文件，磁盘的可用空间会越来越小，如果磁盘空间过低，会造成操作系统运行速度的减慢，影响系统使用。安全的磁盘剩余空间大小需要根据实际情况确定，对于主要用于数据存储的终端设备，对磁盘剩余空间要求的值较大。对于普通终端设备，则对磁盘剩余空间要求的值没有那么高。

备注：各项资源具体的阈值需要结合实际情况确定。

（2）相关风险点

异常资源占用的风险点详见表 B–13。

表 B-13　异常资源占用风险的风险点列表（共 19 点，12 个原生风险、4 个次生风险、3 个残余风险）

	序号	风　险　点	风险属性	隐患/风险
进程/服务运行的风险	1	终端 CPU 使用率持续高	原生风险	隐患
	2	终端 CPU 使用率持续高，没有提示终端用户	原生风险	隐患
	3	终端 CPU 使用率持续高，审计信息没有上报管理员	原生风险	风险
	4	终端 CPU 使用率持续高，没有按照设定的阈值，以产生告警	原生风险	风险
	5	终端内存使用率持续高	原生风险	隐患
	6	终端内存使用率持续高，没有提示终端用户	原生风险	隐患
	7	终端内存使用率持续高，审计信息没有上报管理员	原生风险	风险
	8	终端内存使用率持续高，没有按照设定的阈值，以产生告警	原生风险	风险
	9	终端磁盘剩余空间不足	原生风险	隐患
	10	终端磁盘剩余空间不足，没有提示终端用户	原生风险	隐患
	11	终端磁盘剩余空间不足，审计信息没有上报管理员	原生风险	风险
	12	终端磁盘剩余空间不足，没有按照设定的阈值，以产生告警	原生风险	风险
	13	当终端 CPU 使用率持续过高时，将 CPU 占用率高的进程信息上报管理员，管理员禁止了该进程，但该进程不应禁止	次生风险	风险
	14	当终端内存使用率过高时，将内存占用率高的进程信息上报管理员，管理员禁用了该进程，但该进程不应禁止	次生风险	风险
	15	当终端磁盘剩余空间不足时，将磁盘空间不足的信息上报了管理员，管理员对磁盘空间进行了清理，删除了一些不能删除的文件	次生风险	风险
	16	当终端磁盘剩余空间不足时，将磁盘空间不足的信息上报了管理员，管理员对磁盘空间进行了清理，改变一些文件的存放路径	次生风险	风险
	17	对终端的 CPU 使用率进行了监控，但由于终端操作系统的问题，获取的 CPU 使用率信息不准确	残余风险	隐患
	18	对终端的内存用率进行了监控，但由于终端操作系统的问题，获取的内存使用率信息不准确	残余风险	隐患
	19	对终端的磁盘空间进行了监控，但由于操作系统的问题，获取的磁盘剩余空间信息不准确	残余风险	隐患

（a）基于资产使用生命周期分析

资产使用生命周期包含：入网前、运行阶段、维修阶段、报废阶段，异常资源占用的风险对终端的影响在资产使用生命周期的体现如下：

风险点（1-4）：终端 CPU 使用率持续高，这些风险主要涉及入网前和运行阶段。维修和报废阶段，终端不运行，不存在该类风险。入网前，终端 CPU 使用率持续高，只会影响终端本身的运行，对整体系统不会造成大的风险，此时风险较低。终端入网后，如果该终端的 CPU 使用率持续高，导致终端正常的工作不能开展，风险较高，如果终端运行了关键业务，则风险更高。

风险点（5-8）：终端内存使用率持续高，这些风险主要涉及入网前和运行阶段。维修和报废阶段，终端不运行，不存在该类风险。入网前，终端内存使用率持续高，只会影响终端本身的运行，对整体系统不会造成大的风险，此时风险较低。终端入网后，如果内存使用率持续过高，会导致一些进程和服务得不到必需的内存资源，不能正常运行，进而影响业务的

正常进行，风险较高。

风险点（9-12）：磁盘剩余空间持续不足，这些风险主要涉及入网前和运行阶段。维修和报废阶段，终端不运行，不存在该类风险。入网前，终端磁盘剩余空间不足，只会影响终端本身的磁盘存储，对整体系统不会造成大的风险，此时风险较低。终端入网进入运行阶段后，如果硬盘占用率持续过高，会导致一些进程和服务得不到必需的硬盘空间，运行数据得不到正常的存储，进而影响业务的正常进行，风险较高。

风险点（13-14）：这两个风险主要涉及运行阶段，对占用 CPU 和内存资源比较高的进程，管理员去禁止，但系统不允许禁止，进程占用的资源不能释放，进而影响终端其他进程/服务的运行，风险高。

风险点（15）：这个风险主要涉及入网前阶段和运行阶段，入网前对磁盘剩余空间不足的终端进行删除一些文件的操作，只会影响终端本身，风险较低。如果是运行阶段，且终端上存储的信息是关键信息，对终端进行文件删除、磁盘空间清理，会造成重要信息丢失的风险，风险高。

风险点（16）：这个风险主要涉及入网前阶段和运行阶段，入网前对磁盘剩余空间不足的终端进行改变文件路径的操作，只会影响终端本身，风险较低。如果是运行阶段，且终端上存储的信息是关键信息，对终端上的文件进行改变文件路径的操作，如果改变的路径在对应的系统中没有进行记录，会造成信息缺失的风险，风险较高。

风险点（17-19）：这些风险主要涉及运行阶段，在运行阶段过程中，如果这些资源占用信息不能准确获取，将不能进行对应的管控操作，风险较高。一般情况下，不会出现这些风险，但不排除系统不正常的时候这些风险出现。

（b）与信息安全的关系

异常资源占用风险涉及在线信息安全风险和存储信息风险。

风险点（1-4）：CPU 占用率过高，会导致正常的业务进程因为得不到运行所需要的 CPU 资源而无法运行，进而造成业务不可用。对在线信息而言，可能会因为缺少必要的资源造成在线信息得不到及时的处理和存储；对已经在终端上存储的信息而言，信息已经在存储状态，影响不大。

风险点（5-8）：内存占用率过高，会导致正常的业务进程因为得不到运行所需要的内存资源而无法运行，进而造成业务不可用。对在线信息而言，可能会因为缺少必要的资源造成在线信息得不到及时的处理和存储；对已经在终端上存储的信息而言，信息已经在存储状态，影响不大。

风险点（9-12）：磁盘剩余空间不够，会导致正常的业务进程因为得不到运行所需要的硬盘资源而无法运行，进而造成业务不可用。对在线信息而言，可能会因为缺少必要的资源造成在线信息得不到及时处理和存储；对已经在终端上存储的信息而言，信息已经在存储状态，影响不大。

风险点（13-14）：这两个风险主要是对占用资源高的进程处理，如果处理的进程与在线信息相关，比如进程涉及数据存储，对在线信息有影响，如果进程与信息存储无关，对在线信息影响不大。对已存储的信息无影响。

风险点（15）：对磁盘空间进行清理，删除不能删的文件时，如果删的文件是正在处理的在线文件，会不允许删除，不存在影响。如果是存储信息，则会造成文件误删的风险，风

险较高。

风险点（16）：对磁盘空间进行清理，改变一些文件的路径时，如果改变路径的是正在处理的在线文件，会不允许改变路径，不存在影响。如果是存储信息，对改变的路径需要记录在案，以便后续的文件再用，风险较低。

风险点（17-19）：不能获取资源的使用率情况，与后续的控制有关，与在线信息和存储信息无关。

（c）基于资产使用人分析

该类风险与人员分类没有明显的关系，主要取决于终端的使用目的，如果终端运行了关键业务，而关键业务所需要的资源又得不到满足，则会风险较高；对资源使用率持续过高的终端需要采取相应的预警机制，以保证终端资源的使用率始终控制在一个合理的范围内。

（d）合规性要求

合规性要求见表 B-14。

表 B-14

序号	安全类	等级保护（三级）要求	符合程度
1		等级保护中没有明确对异常资源占用的要求	

该风险属于运行时风险，对于异常资源占用的具体定义，等级保护方面在这块没有明确的要求。需要结合实际运维的情况不断修正异常占用率，从而及时解决终端中的异常资源占用问题。

相关技术和管理的风险管控措施参见以下小节阐述。

2．风险管控

每类风险在管控过程中，针对风险的事前、事中和事后 3 种状态进行监控，做到事前预防、事中控制、事后审计追查。下面的风险管控处理流程，尽量从事前、事中和事后 3 方面对风险进行管控。

（1）风险点（1-4）：终端 CPU 使用率异常检测管理流程

事前处置：定义 CPU 使用率异常的范围，不同的业务终端上，CPU 使用率异常的定义不尽相同；一般而言，CPU 使用率持续在 90%以上并且超过 10 s 可称为异常。

事中处置：

✓ 定时监测运行终端上 CPU 使用率的情况

✓ 设定 CPU 异常的使用率范围

✓ 如果终端 CPU 使用率超过设定的阈值，提示用户 CPU 使用率异常（通知终端用户，消息的方式）

✓ 根据 CPU 使用率异常策略执行操作，提示终端使用者，并且发送防护平台

✓ 记录 CPU 使用率异常的终端使用行为及终端使用者的操作，发送至防护平台服务器

事后处置：根据整体安全态势分析，调整安全策略，针对终端下发新 CPU 异常监控策略，查看持续高占用 CPU 资源的进程，采取禁用进程或者关闭不必要的任务的方式，降低 CPU 使用率。

流程图见图 B-20。

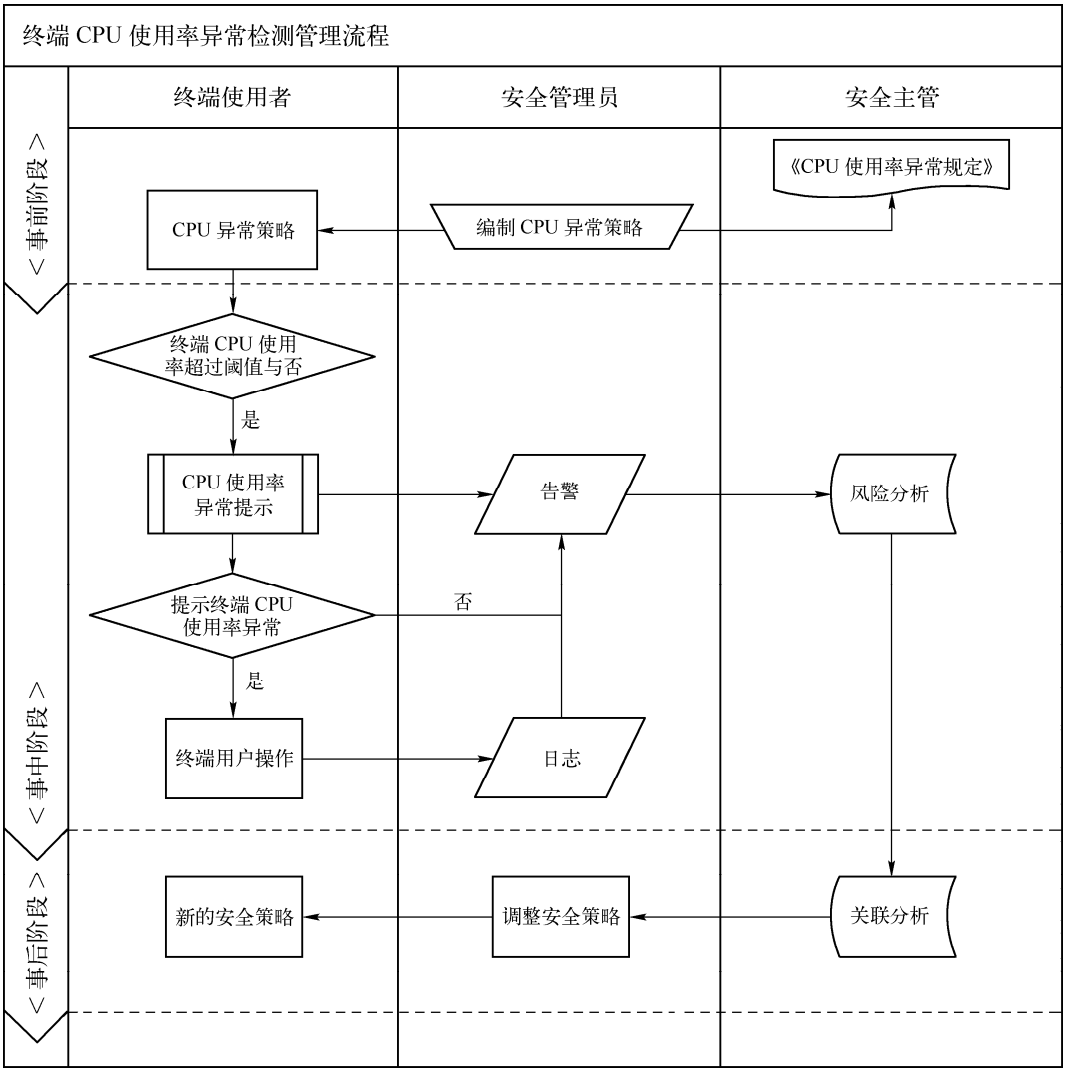

图 B-20

（2）风险点（5-8）：终端内存使用率异常检测管理流程

事前处置：定义内存使用率异常的范围，不同的业务终端上，内存使用率异常的定义不尽相同；一般而言，内存使用率持续 90%以上并且超过 10 s 可称为异常。

事中处置：

- ✓ 定时监测运行终端上内存使用率的情况
- ✓ 设定终端内存的使用率范围
- ✓ 如果终端内存使用率超过设定的阈值，提示用户内存使用率异常（通知终端用户，消息的方式）
- ✓ 根据内存使用率异常策略执行操作，提示终端使用者，并且发送防护平台
- ✓ 记录内存使用率异常的终端使用行为及终端使用者的操作，发送至防护平台服务器

事后处置：根据整体安全态势分析，调整内存监控策略，针对终端下发新的内存监控策

略，查看终端上持续高占用内存资源的服务或进程，采取禁用某些服务和进程的方式，降低终端上的内存占用情况，以保证关键业务的内存使用需要。

流程图见图 B-21。

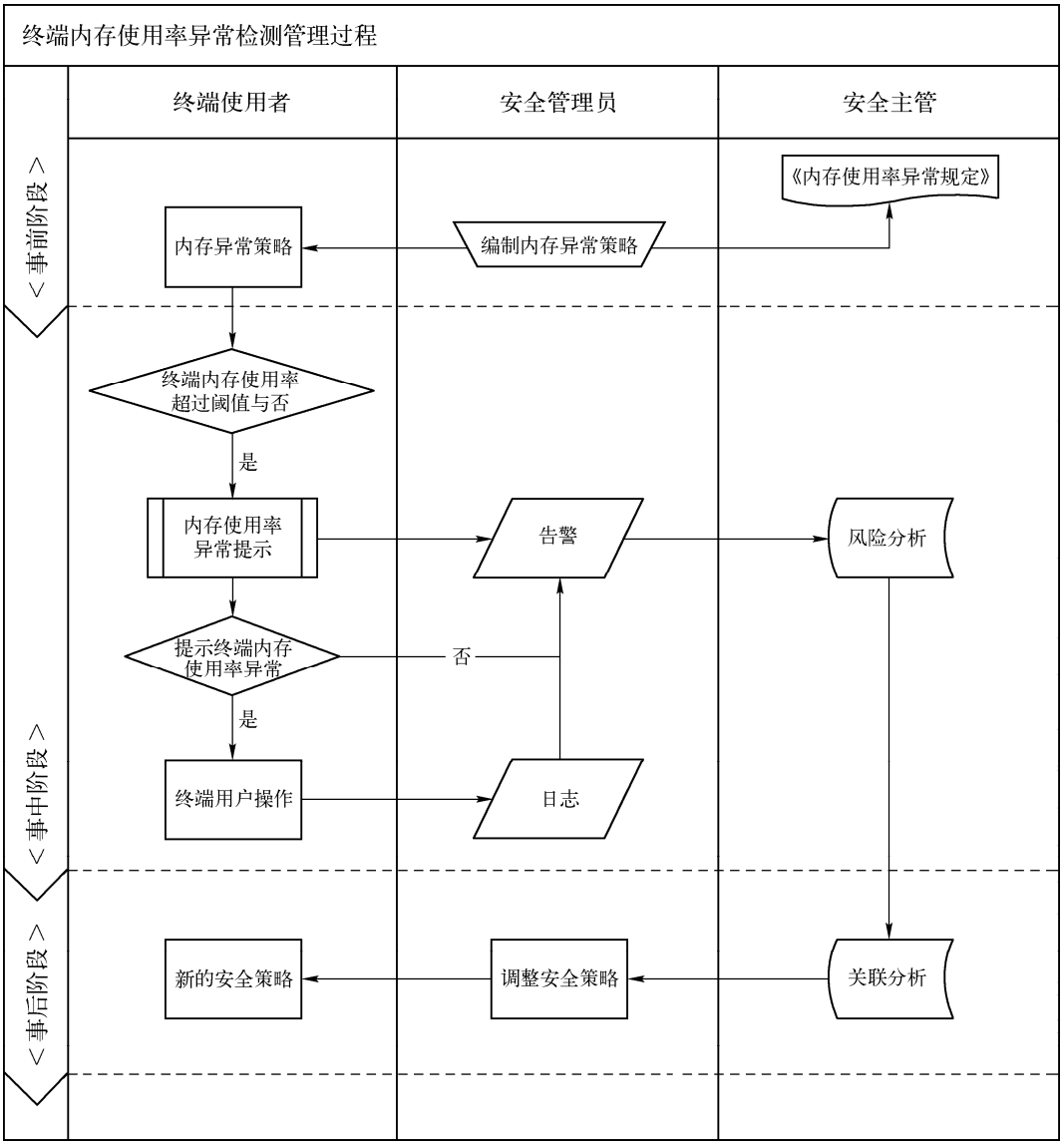

图 B-21

（3）风险点（9-12）：终端磁盘剩余空间不足检测管理流程

事前处置：定义硬盘剩余空间不足的最低值，不同的业务终端，不同的盘符下，对最低硬盘剩余空间的要求不尽相同。一般而言，对操作系统所在的盘符和应用数据所存储的盘符剩余空间要求不尽相同。还需要考虑终端用户数据增长的情况，对不同的终端制定不同的最低剩余硬盘空间值。

事中处置：

- ✓ 定时监测运行终端上硬盘各盘符的剩余空间的情况
- ✓ 设定终端剩余空间不足的最低阈值
- ✓ 如果终端硬盘剩余空间低于设定的的阈值，提示用户剩余硬盘空间不足（通知终端用户，消息的方式）
- ✓ 根据硬盘空间不足策略执行操作，提示终端使用者，并且发送防护平台
- ✓ 记录硬盘空间不足的终端使用行为及终端使用者的操作，发送至防护平台服务器

事后处置：根据整体安全态势分析，调整硬盘空间监控策略，针对终端下发新的硬盘监控策略，查看终端上硬盘空间不足的盘符，是否有垃圾数据，如果有垃圾数据，采取及时清除的方法；如果是运行数据保存所需，看是否可以做数据迁移，以保证有足够的空间供运行使用，或者采取追加磁盘空间的方式，以保证有足够的磁盘空间来保证终端正常运行。

流程图见图 B-22。

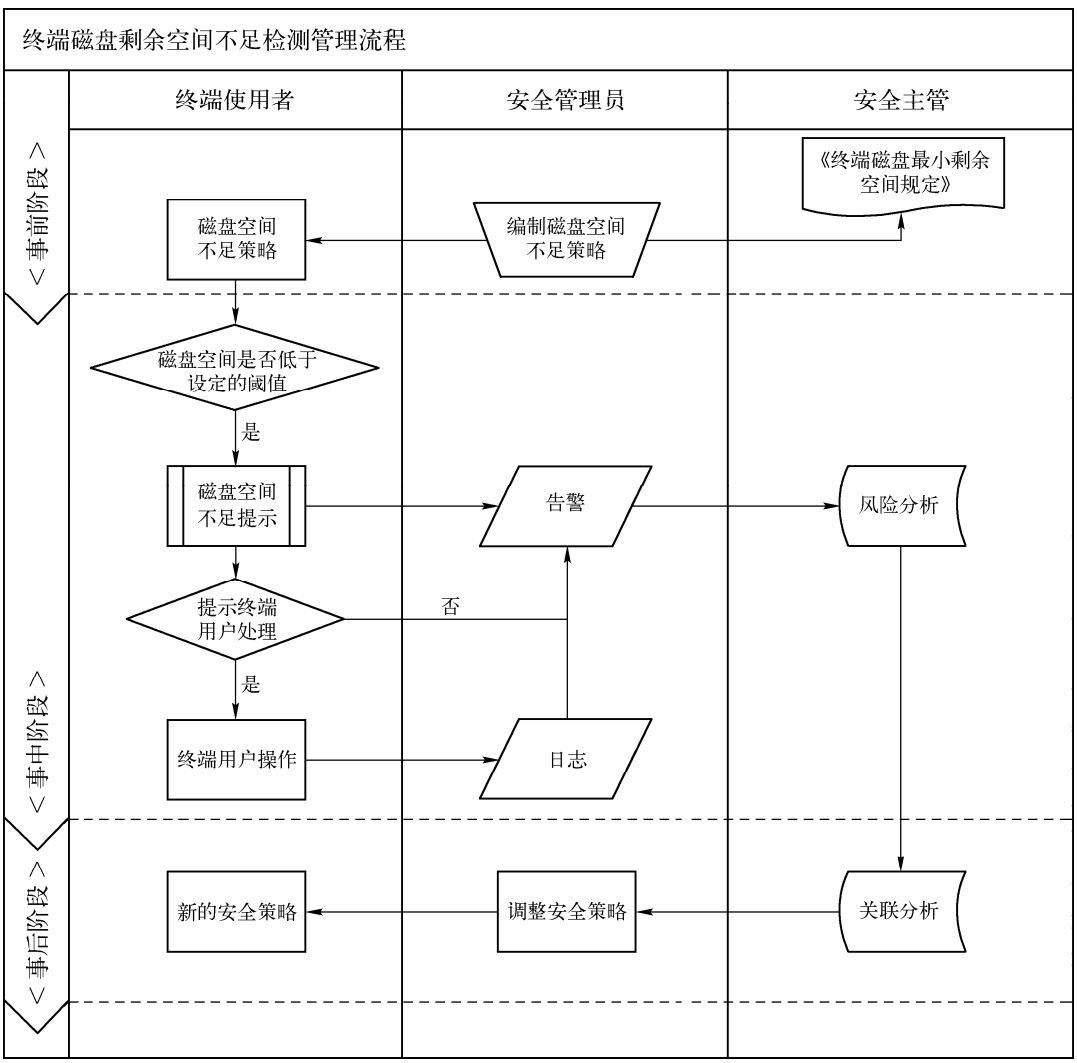

图 B-22

（4）风险点（13）：对 CPU 占用率异常的进程处理流程

事中处置：

- ✓ 发现终端 CPU 使用率持续过高时，记录终端 CPU 使用率的情况，保存至防护平台服务器
- ✓ 对持续占用 CPU 资源过高的进程和服务进行行为取证（占用高 CPU 使用率的进程、进程名称、CPU 使用率持续高的终端、终端使用者、终端 IP 等原始记录信息），保存至防护平台服务器

事后处置：管理员通过 CPU 持续过高的记录对终端上的 CPU 使用率情况追溯，发现持续占用 CPU 资源的终端上的进程或服务，并通过发送通知给终端用户，建议其停止占用过高 CPU 资源的进程的运行，如果该进程不允许停止运行（核心业务所需），定位 CPU 资源高占用的原因，排查问题，将 CPU 使用率降到一个合理的范围。

流程图见图 B-23。

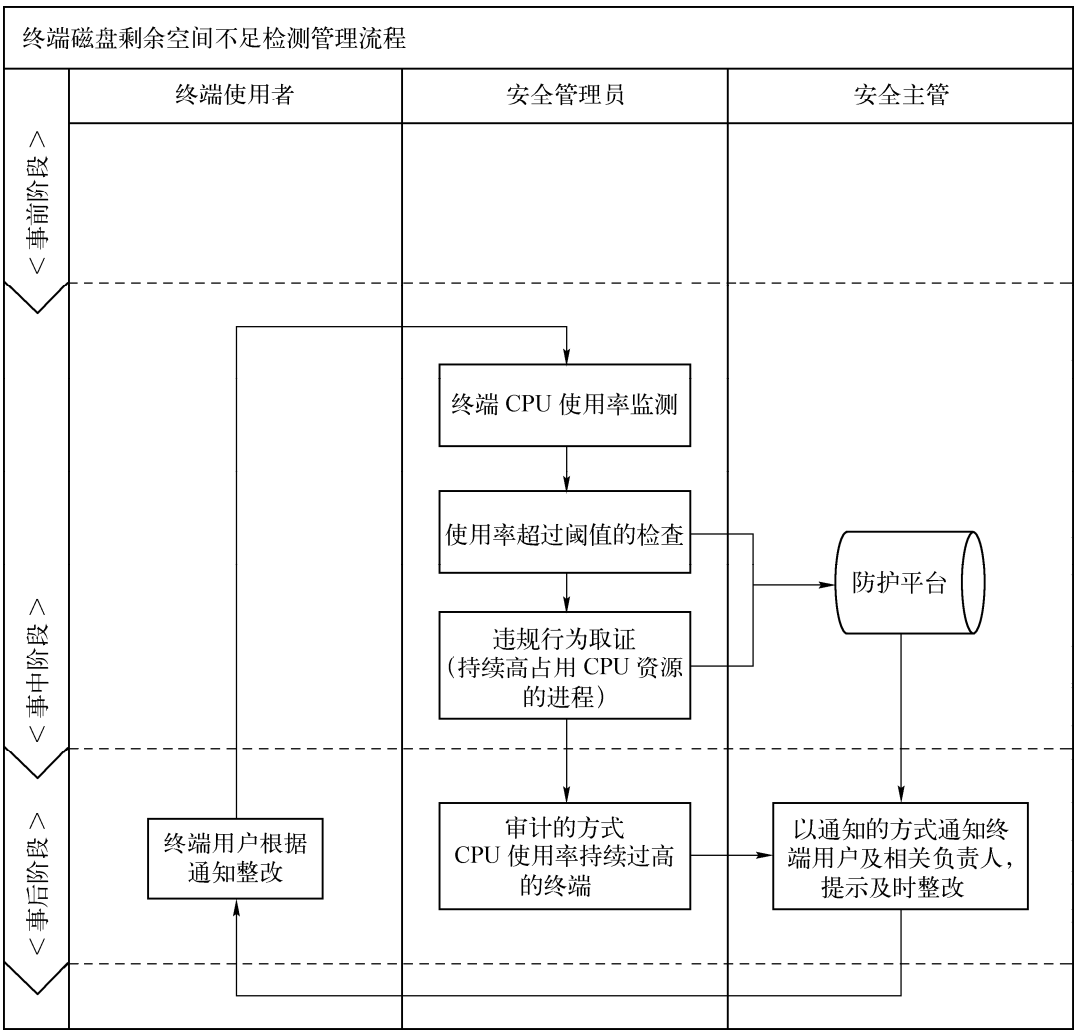

图 B-23

（5）风险点（14-16）：对内存使用率和磁盘剩余空间检测的流程与风险点 13 的流程图类似，此处不再赘述。

（6）风险点（17-19）

事前处置：目前主要通过获取 Windows 操作系统获取终端上各项资源的使用情况，如果终端操作系统有错误，其资源使用率信息可能无法获取，从而影响后续的资源控制策略和相关告警。

事中处置：需要先行修复操作系统，保证终端的资源使用率信息可正确获取。

事后处置：在获取的无误的终端资源使用率数据基础上，进行资源异常的检测和控制流程。

3．风险控制效果

通过对资源使用率的有效监控，也能够有效避免由于资源使用率过高而导致终端过慢，影响业务正常运行的情况发生。

资源占用率异常是一个动态的过程，实施前阈值的确定需要根据实际使用的需要来确定；在对终端资源使用率进行风险管理的时候存在这样的情况：

- ✓ 一些进程本身占用的资源就会更高，如果频繁对这些进程检测，会影响系统的工作效率和进程的使用
- ✓ 一些资源异常使用的信息报给管理员后，也未得到及时的关注和处理

因此，尽管部署了完备的检测和管理技术手段，却会因人的操作习惯和安全意识造成异常资源占用的风险继续存在。

针对该问题，建议增加以下几方面工作：

- ✓ 加强安全意识培训和教育，使终端用户意识到保持合理资源使用率的重要性，督促其定期关注终端的各项资源使用率的情况
- ✓ 提供制度保障，要求用户将终端各项资源的使用率控制在一个合理范围内
- ✓ 建立定期检查和整改制度，定期对组织内终端资源异常使用的状况进行集中检查，集中整改

B.2.4 操作系统用户管理的风险（20 个风险点）

1．风险分析

（1）风险描述

终端操作系统中，维护着一定数量的操作系统用户，Windows 系统作为一个多用户操作系统，允许多个用户共同使用一台计算机，而用户账号就是用户进入系统的出入证。用户账号一方面为每个用户设置相应的密码、隶属的组、保存个人文件夹及系统设置，另一方面将每个用户的程序、数据等相互隔离，这样在不关闭计算机的情况下，不同的用户可以相互访问资源。

在终端上，要执行某些任务，可能需要以 Administrators 组成员身份登录。“本地用户和组”用于管理计算机用户的用户和组。可以创建新用户和组、将用户添加到组、从组中删除

用户、禁用用户和组的账户以及重新设置密码。

终端用户账户类型：当多人共享计算机时，有时设置会被意外地更改，使用用户账户，可以防止其他人更改计算机设置。

当前一般的终端操作系统，有图 B-24 所示的两种账户类型。

	计算机管理员	受限用户
安装程序和硬件	√	
进行系统范围的更改	√	
访问和读取所有非私人的文件	√	
创建与删除用户账户	√	
更改其他人的用户账户	√	
更改自己的账户名或类型	√	
更改自己的图片	√	√
创建、更改或者删除自己的密码	√	√

图 B-24

必须对这些用户及用户组进行统一控制，如果不控制这些管理员的用户信息，会导致用户信息跨级别用，被不该使用的人员滥用，对终端造成信息泄漏或者信息丢失的风险。主要风险包括以下几个方面：

✓ 普通用户被违规加入管理员组，导致操作范围扩大带来的安全风险

✓ 非法用户通过越权修改用户权限，从而控制终端，执行非法操作

✓ 用户或用户组过多，导致管理复杂

✓ 大量闲置用户或用户组未及时删除，从而被非法利用

（2）相关风险点

操作系统用户管理的风险点详见表 B-15。

表 B-15

	序号	风 险 点	风险属性	隐患/风险
操作系统用户管理	1	操作系统受限用户权限被变更为管理员用户	原生风险	隐患
	2	操作系统受限用户权限被变更为管理员用户，审计信息不上报管理员	原生风险	风险
	3	操作系统受限用户权限被变更为管理员用户，不提示终端用户	原生风险	隐患
	4	操作系统受限用户权限被变更为管理员用户，不产生告警	原生风险	隐患
	5	操作系统受限用户权限被变更为管理员用户，用户使用变更后的权限登录终端，对终端进行操作	次生风险	风险
	6	操作系统管理员用户权限变更为受限用户	原生风险	隐患
	7	操作系统管理员用户权限变更为受限用户，审计信息不上报	原生风险	风险

（续）

	序号	风　险　点	风险属性	隐患/风险
操作系统用户管理	8	操作系统管理员用户权限变更为受限用户，不提示终端用户	原生风险	隐患
	9	操作系统管理员用户权限变更为受限用户，不产生告警	原生风险	隐患
	10	操作系统管理员用户权限变更为受限用户，用户使用变更后的权限登录终端，对终端进行操作	次生风险	风险
	11	增加/删除系统管理员权限的操作系统用户	原生风险	隐患
	12	增加/删除系统管理员权限的操作系统用户，审计信息不上报	原生风险	风险
	13	增加/删除受限用户权限的操作系统用户	原生风险	隐患
	14	增加/删除受限用户权限的操作系统用户，审计信息不上报	原生风险	风险
	15	操作系统用户组权限修改	原生风险	隐患
	16	操作系统用户组权限修改，不通知终端用户	原生风险	隐患
	17	操作系统用户组权限更改，审计信息不上报管理员	原生风险	风险
	18	增加/删除操作系统用户组	原生风险	隐患
	19	增加/删除操作系统用户组，审计信息不上报	原生风险	隐患
	20	对操作系统用户和用户组信息进行检测，由于操作系统的问题，获取的用户信息不准确，无法进行相应的用户控制	残余风险	隐患

（a）基于资产使用生命周期分析

该类风险涉及入网前、运行阶段。入网前由于终端资产不包含敏感信息和数据，风险较低；入网后，由于运行过程中涉及敏感信息和生产数据，如果不加以控制，导致的损失较大，风险较高。操作系统用户管理的风险对终端的影响在资产使用生命周期的体现如下：

风险点（1-5）：操作系统受限用户权限变更为管理员权限，用户权限提高。这些风险主要涉及入网前和运行阶段。维修和报废阶段，终端不运行，不存在该类风险。入网前，受限用户权限变更为管理员权限后，可以进行一些只有管理员才能进行的操作，会对其他用户的文件和终端的软硬件都进行一些更改，风险较高；入网后，如果受限用户变更为管理员，对终端进行操作，不仅对其他用户的文件和终端的软硬件都有一些更改，如果其在终端上进行进程停用等操作，会影响业务和正常工作的运行，风险极高。

风险点（6-10）：管理员权限用户变更为受限用户，用户权限降低。这些风险主要涉及入网前和运行阶段。维修和报废阶段，终端不运行，不存在该类风险。入网前，管理员权限用户变更为受限用户后，管理员本身可以进行的终端操作都不能运行，会造成一些工作不能正常开展，但不会对系统的信息造成风险，此时风险较低；入网后，管理员权限用户变更为受限用户，可能导致一些终端的操作无法进行，影响终端正常业务开展，风险较高。

风险点（11-12）：这些风险主要涉及入网前和运行阶段。维修和报废阶段，终端不运

行，不存在该类风险。入网前，增加/删除系统管理员权限的操作系统用户，只会影响对终端本身的操作，风险较低；入网运行后，如果新增加了系统管理员权限的用户，导致系统管理员权限用户增多，一些管理员的操作会冲突，进而影响终端正常业务的开展，风险较高；如果删除了系统管理员权限的系统用户，在需要该用户对终端操作时，却没有相应的管理员用户，导致工作不能正常开展，风险较高。

风险点（13-14）：增加/删除受限用户对终端影响不大。

风险点（15-17）：这些风险主要涉及入网前和运行阶段。维修和报废阶段，终端不运行，不存在该类风险。入网前，操作系统用户组权限修改，只会影响对终端本身的操作，风险较低；入网运行后，如果用户组权限提升，导致组下的用户可以操作的范围扩大，一些管理员的操作会冲突，进而影响终端正常业务的开展，风险较高；如果用户组权限降低，在需要该用户对终端操作时，却没有相应的管理员用户，导致工作不能正常开展，风险较高。

风险点（18-19）：这些风险主要涉及入网前和运行阶段。维修和报废阶段，终端不运行，不存在该类风险。入网前，增加/删除系统用户组，只会影响对终端本身的操作，风险较低；入网运行后，如果新增加了系统用户组，如果用户组分配的权限是系统管理员，会导致系统管理员权限用户增多，一些管理员的操作会冲突，进而影响终端正常业务的开展，风险较高；如果删除了系统用户组，在需要该用户组下的用户对终端操作时，却没有相应的用户，导致工作不能正常开展，风险较高。

风险点（20）：该风险与资产生命周期无关。

（b）与信息安全关系

操作系统用户管理的风险涉及在线信息安全风险和存储信息风险。

风险点（1-5）：操作系统受限用户变更为管理员用户后，一些只有管理员权限级别的管理员查看在线信息，会导致在线信息泄漏或被篡改；同时，这些用户还可以对原本没有操作权限的存储信息进行操作，会导致存储信息丢失、被篡改等风险。

风险点（6-10）：管理员用户变更为受限用户后，需要在线操作的管理员因为权限降低，无法进行相关操作，会导致在线信息不能及时存储。对存储的信息，不能查看和操作，不存在风险。

风险点（11-12）：增加管理员权限的用户，对在线信息可操作的管理员增加；会导致在线信息泄漏或被篡改。增加的管理员权限用户，可以对终端上的存储信息进行操作，会导致存储信息丢失、被篡改等风险；删除管理员权限用户，不会对存储信息有风险。对在线信息来说，如果需要管理员权限用户操作，但该用户被删除了，存在在线信息得不到及时处理的风险。

风险点（13-14）：增加/删除受限用户的权限对在线信息和存储信息没有风险。

风险点（15-17）：与风险点（1-5）类似。

风险点（18-19）：与风险点（1-5）类似。

风险点（20）：该风险与信息安全无关。

（c）基于资产使用人分析

风险点（1-20）：这些风险与人员类别密切相关，外来人员使用终端的操作系统，登录终端进行相应的操作，会造成信息泄漏或篡改；风险非常高；必须严禁外来人员使用内部终端，尤其是要闲置外部人员使用终端的管理员用户账号操作；临时人员有时候因为工作需要，必须使用内部终端，一定要控制其用户级别，避免出现跨权限的资源访问；内部人员在对操作系统用户管理时，必须做到及时删除多余的用户和用户组，同时一定要妥善保管好管理员账号，避免账号和密码泄漏，同时要做到权限控制，不要设置过多的具有管理员权限的账号。

（d）合规性要求

合规性要求见表 B-16。

表 B-16

序号	安全类	等级保护（三级）要求	符合程度
1		等级保护中没有明确对操作系统用户管理的要求	

基于以上风险点分析，如采取相关技术和管理手段管控 8 个风险点，则终端操作系统用户管理的风险符合等级保护相关要求。

相关技术和管理的风险管控措施参见以下小节阐述。

2．风险管控

（1）风险点（1-10）：操作系统用户权限变更管理流程。

事前处置：定义终端上每个用户对应的权限，检查用户的权限与事先指定的是否一致。制定制度，不允许随意变更用户的权限；对每一个终端，必须根据其使用的目的对终端的用户权限做统一规定。

事中处置：

- ✓ 定时检测终端操作系统用户的权限列表
- ✓ 将获取的用户权限列表与制度规定的用户权限列表相比较
- ✓ 如果用户的权限列表与制度规定的不符合，提示用户终端操作系统用户权限情况异常，有违反权限规定的用户存在，提示用户进行进一步处理（按规定修改用户权限等）
- ✓ 如果用户权限变化，及时根据规则产生报警，提醒管理员注意
- ✓ 如果用户的权限变化了，及时对变更进行记录（包括变更前权限、变更后权限、变更的时间、变更操作人员等信息），发送至防护平台服务器。

事后处置：根据权限变更的实际情况，进行相应的操作，如果是权限提升，产生报警，提醒终端用户及时按制度修改用户权限；如果权限降低，也需要通知用户权限过低，一些用户可能得不到必须的权限来使用终端资源。

操作系统用户权限变更管理流程如图 B-25 所示：

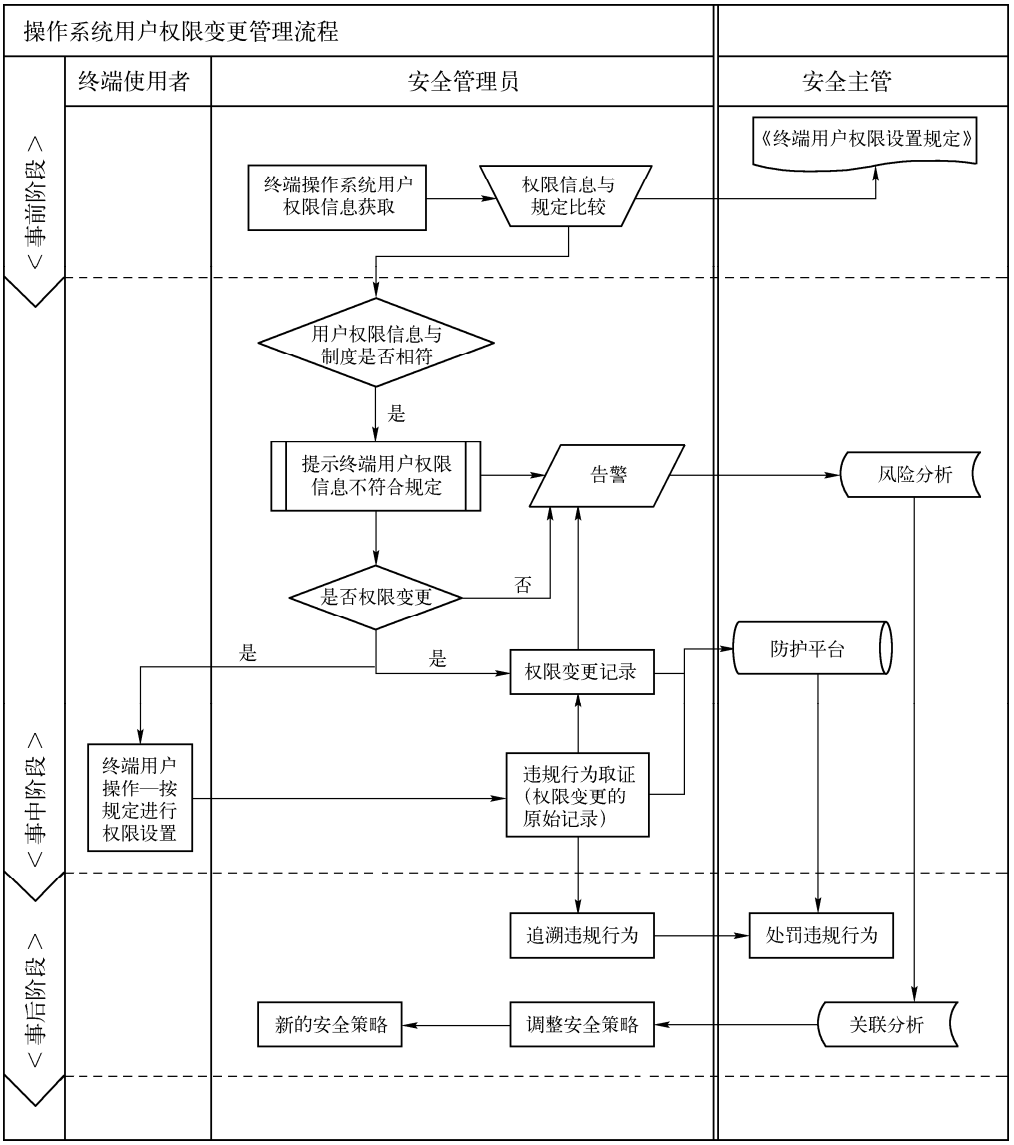

图 B-25

风险点（11-14）：操作系统用户增加/删除管理流程

事前处置：定义终端上可以有的用户数量、用户类别，规定不允许随意在终端上添加或删除用户；需要注意的是，不同的终端上可以有的操作系统用户是不尽相同的，比如个人办公终端，可能有管理员用户和一般个人用户就够了，但在一些业务服务器上，管理员用户可能只有一个，但一般用户可以允许有多个。具体的终端用户情况需要结合实际运维情况制定。

事中处置：

- ✓ 定时检测终端操作系统用户列表
- ✓ 将获取的列表与制度规定的用户数量和情况相比较
- ✓ 如果是随意增加了操作系统用户的情况，提示用户终端操作系统用户情况异常，有违反规定的用户存在，提示用户进行进一步处理（删除违规增加的用户等等）

- ✓ 如果是已有的用户被删除掉了，提示用户终端用户被异常删除，提示用户进行进一步处理（恢复被删除的用户）
- ✓ 记录用户变化的情况及终端使用者的操作，发送至防护平台服务器。

事后处置：

根据整体安全态势分析调整安全策略，针对终端下发新的用户管理策略，如果是违规增加了用户，提示终端删除用户，如果是违规删除了用户，提示终端恢复用户。对用户变化的情况进行记录，包括终端使用者、增加/删除的用户信息、更改的时间等信息。

操作系统用户增加/删除管理流程如图 B-26 所示：

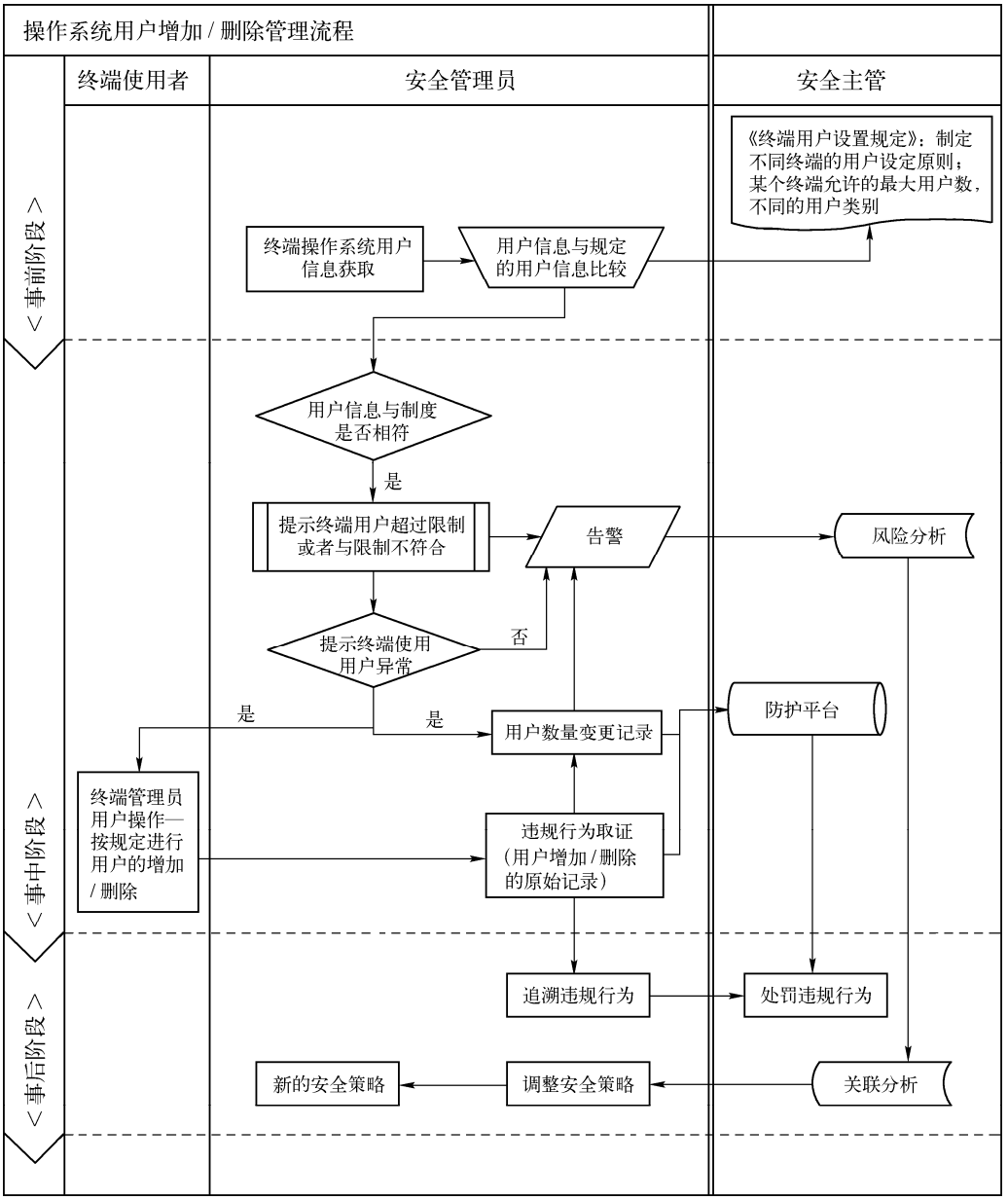

图 B-26

风险点（15-17）：操作系统用户组权限变更管理流程与用户权限变更管理流程类似。

风险点（17-19）：操作系统用户组增加/删除管理流程与操作系统用户增加/删除管理流程类似。

风险点（20）：由于操纵 Windows 系统的用户需要从操作系统获取，所以必须保证操作系统可用，且可以正确获取终端上的用户以及用户组信息，如果不能获取用户和用户组信息，后续的策略控制和报警都无从产生；

3．残余风险处理

在对终端的操纵系统用户进行管理时存在这样的情况：

- ✓ 对操作系统的用户权限没有严格按照要求分配
- ✓ 其审计信息报给管理员后，也未得到及时的关注和处理
- ✓ 系统因工作或维修需要增加了操作系统用户，事后未及时对这些用户进行删除操作
- ✓ 未按照规定进行操作系统用户组建设

因此，尽管部署了完备的检测和管理技术手段，却会因人的操作习惯和安全意识造成操作系统用户管理的风险继续存在。

针对该问题，建议增加以下几方面工作：

- ✓ 加强安全意识培训和教育，使终端用户意识到严格按照要求对操作系统的用户组和用户信心进行管理的重要性
- ✓ 需要在制度上规定不允许随意在终端上添加管理员用户，同时，提示用户，所有的用户权限修改都会有记录在案，不允许随意修改用户权限
- ✓ 闲置用户的定义也需要在制度上保证，必须有一个闲置用户的明确规定，才能根据这个判断哪些是限制用户
- ✓ 建立定期检查和整改制度，定期对组织内终端的操作系统用户情况进行集中检查，集中整改
- ✓ 设立针对操作系统用户相关的考核管理措施，将该项工作作为终端使用人、终端所有单位安全工作考评中的考核指标

4．风险控制效果

主要以监控为主，控制较弱，输出信息提示报警。

B.3 网络边界安全（RR1.3）

B.3.1 违规内联（30 个风险点）

1．风险分析

（1）风险描述

违规内联的风险主要体现在以下几个方面：

1）身份不合法的终端违规接入内网，包括终端未经过资产管理系统有效登记、终端与资产管理系统登记信息不符以及终端登录用户未经过有效登记等情况。身份不合法的终端违规接入内网可能存在非法终端盗用内网资源的情况，非法终端盗用内网资源有机会通过内网非法获取其他主机或应用系统中的信息，并可能对其他主机发起攻击。

2）健康状态不合规的终端违规接入内网，包括病毒检查不合规、木马检查不合规、应用软件检查不合规、外设检查不合规、操作系统补丁检查不合规等情况，违规终端接入内

网，因为健康检查未通过设定的健康检查规则，则可能存在病毒、木马、未被允许安装的应用程序、非经授权打开的外设端口、未安装最新操作系统补丁等情况，达不到内网的整体安全基准，成为内网信息系统的安全威胁。

3）非内网终端无相关入网审批流程，包括非内网终端没有合理的接入流程、没有合理的应急流程、没有相关审批流程等情况，可能造成有正常接入需求的非内网终端无法入网使用，造成工作不便。

4）身份合法状态合规的终端，非授权开启服务端服务（DHCP 等）或使用未经授权的 IP 地址躲避身份判断，非授权开启相关服务会影响到正常的服务应用，使用未经授权的 IP 地址可能造成 IP 地址冲突，影响原有合法终端正常使用网络。

（2）相关风险点

违规内联的风险点详见表 B-17。

表 B-17

	序号	风险点	风险属性	隐患/风险
违规内联	1	终端资产没有在资产管理系统登记的违规内联	原生风险	风险
	2	终端资产与资产管理系统登记信息不符的违规内联	原生风险	隐患
	3	登录终端用户没有合法登记的违规内联	原生风险	隐患
	4	终端身份标识符被篡改、冒用的风险	原生风险	风险
	5	终端身份标识符被冒用，在相应控制措施实施时可能导致的被冒用的合法终端无法上网	次生风险	风险
	6	终端病毒检查不合规的违规内联	原生风险	隐患
	7	终端操作系统补丁检查不合规的违规内联	原生风险	隐患
	8	终端应用软件检查不合规的违规内联	原生风险	隐患
	9	终端木马检查不合规的违规内联	原生风险	隐患
	10	终端外设控制检查不合规的违规内联	原生风险	隐患
	11	产生违规内联后，不能识别终端身份信息	原生风险	隐患
	12	产生违规内联后，没有上报审计信息	原生风险	风险
	13	不合规的违规内联终端，不被强制定位到隔离区	原生风险	隐患
	14	隔离区的终端，不进行有效验证就被允许入网	原生风险	隐患
	15	隔离区内的终端，用户未按流程进行合规化处理	残余风险	隐患
	16	手机违规连入内网	原生风险	隐患
	17	非内网终端连入内网，无流程化处理	原生风险	隐患
	18	非内网终端连入内网，无应急处理	原生风险	隐患
	19	非内网终端接入内网，无授权审批	原生风险	隐患
	20	非内网终端接入内网后，用户未按流程进行身份登记	残余风险	隐患
	21	非内网终端授权接入内网，不进行安全检测	原生风险	隐患
	22	非内网终端授权接入内网，不对其上传下载数据行为进行审计和记录	原生风险	隐患
	23	授权接入内网的终端，使用未经系统管理员分配的 IP 或 IP 段	原生风险	风险
	24	对非授权使用 IP 的终端不进行提示	原生风险	隐患
	25	对非授权使用 IP 的终端未进行审计上报	原生风险	隐患
	26	非授权使用 IP 的终端，用户未按提示修改 IP	残余风险	隐患
	27	授权终端，开启未经系统管理员允许的服务端服务（DHCP、代理）	原生风险	隐患
	28	对非授权开启服务器端服务的终端不进行提示	原生风险	隐患
	29	对非授权开启服务器端服务的终端未进行审计上报	原生风险	隐患
	30	非授权开启服务器端服务的终端，用户未按提示关闭服务	残余风险	隐患

（a）相关资产生命周期

资产生命周期包含入网阶段、运行阶段、维护阶段、废弃阶段，违规内联风险对终端的影响在资产生命周期的体现如下：

a）终端资产没有在资产管理系统登记的违规内联；终端资产与资产管理系统登记信息不符的违规内联；登录终端用户没有合法登记的违规内联；终端身份标识符被篡改/冒用的风险；终端身份标识符被冒用，在相应控制措施实施时可能导致的被冒用的合法终端无法上网风险存在于资产生命周期的入网阶段、运行阶段、维护阶段、废弃阶段，在上述 4 个阶段未对终端身份的合法性要求进行检测，则无法判断终端身份的有效性，可能产生非内网终端非法接入内网的情况，非内网终端非法接入内网可能导致对内网资源的攻击和窃取，主要危害内网其他资源，所以 4 个阶段终端自身的信息资源尽管不同，但对于其他内网资源的危害程度同样大，从 4 个阶段终端使用者的角度看，运行阶段是终端所有者使用，其他阶段使用者非终端所有者，从行政管理的角度更加难以控制，所以其他 3 个阶段从使用者的角度对产生此类风险的危害性更大。

b）终端病毒检查不合规的违规内联；终端操作系统补丁检查不合规的违规内联；终端应用软件检查不合规的违规内联；终端木马检查不合规的违规内联；终端外设控制检查不合规的违规内联的风险存在于资产生命周期的运行阶段。在运行阶段终端未进行病毒的合规性检查，则接入内网的终端可能感染病毒，导致病毒在内网中传播感染其他主机；没有对接入终端进行操作系统补丁的检查，则接入终端可能未安装最新的操作系统补丁，终端存在系统漏洞，不但自身容易遭受攻击，还可能成为内网安全的薄弱环节，成为攻击内网的跳板；没有对终端进行应用软件的检查，则接入终端可能存在非授权应用软件，导致影响内网正常运行，并可能存在安全漏洞；没有对终端进行木马检查，则接入终端可能存在木马，导致自身受到攻击，并可能成为别人的攻击跳板；没有对终端外设控制进行检查，则可能存在非授权的外设，存在输出类的外设（打印机等）可能带来信息的外泄，存在网络连接类的外设（无线网卡）则可能产生非法的外部连接。

c）不合规的违规内联终端，不被强制定位到隔离区；隔离区的终端，不进行有效验证就被允许入网；隔离区内的终端，用户未按流程进行合规化处理的风险存在于资产生命周期的运行阶段。在运行阶段没有将不合规终端定位到隔离区，则无法再限制使用内网资源的基础上对不合规终端进行强制合规处理；不进行有效验证就被允许接入内网以及隔离区内的终端，用户未按流程进行合规化处理造成不合规终端进入内网，产生不合规终端接入内网的危害。

d）手机违规连入内网的风险存在于资产生命周期的运行阶段，在运行阶段没有对手机违规接入内网终端进行检测与阻断，则可能通过手机获取终端或内网资源中的信息，并可能使该终端非法连接至外部网络。

e）非内网终端连入内网，无流程化处理；非内网终端连入内网，无应急处理；非内网终端接入内网，无授权审批；非内网终端接入内网后，用户未按流程进行身份登记；非内网终端授权接入内网，不进行安全检测；非内网终端授权接入内网，不对其上传下载数据行为进行审计和记录的风险存在于资产生命周期的运行阶段，在运行阶段没有对非内网终端接入内网进行流程化处理和应急处理，则非内网终端不具备合理的入网流程，导致非内网终端无法入网使用或入网使用，但没有被资产管理系统进行有效的管理；不具备非内网终端的接入

内网的授权审计，则可能导致非内网终端无法通过入网流程获得入网许可或非内网终端不经审批就接入内网；非内网终端授权接入内网如未经过安全检测，则非内网终端健康状态不合规，产生同不合规内网终端接入相同的风险；未对非内网终端进行上传下载数据的行为进行审计和记录，则无法掌握非内网终端的数据访问，在发生数据外泄时无法有效追查。

f）授权接入内网的终端，使用未经系统管理员分配的 IP 或 IP 段；对非授权使用 IP 的终端不进行提示；对非授权使用 IP 的终端未进行审计上报；非授权使用 IP 的终端，用户未按提示修改 IP；授权终端，开启未经系统管理员允许的服务端服务（DHCP、代理）；对非授权开启服务器端服务的终端不进行提示；对非授权开启服务器端服务的终端未进行审计上报；非授权开启服务器端服务的终端，用户未按提示关闭服务的风险存在于资产生命周期的运行阶段，在运行阶段使用非授权 IP 地址可能影响被冒用的合法用户对网络资源的使用，或者因为 IP 地址未登记，在产生违规行为时难以追查，非授权开启服务端服务可能造成对正常服务的影响（正常分配 IP 地址等），影响其他内网终端的服务使用。

g）产生违规内联后，不能识别终端身份信息；产生违规内联后，没有上报审计信息的风险存在于资产生命周期的运行阶段，在运行阶段未识别区分违规内联终端的身份信息就无法对违规内联的终端进行身份追查，无法在发生安全事件后根据违规内联终端的身份对威胁进行针对性的防护，并针对身份分析攻击目的进行针对性的补救措施；产生违规内联后，没有上报审计信息，就可能造成违规行为的不可知、不可控，由于不能进行针对性的取证，无法预防违规行为的再次发生，也不能提供对违规行为处罚的依据。

（b）相关信息风险

a）终端资产没有在资产管理系统登记的违规内联；终端资产与资产管理系统登记信息不符的违规内联；登录终端用户没有合法登记的违规内联的风险。

针对在线信息的影响在于非法终端连接内网，提供非法终端采用非法手段接入应用系统的途径，通过非法接入应用系统，非法删除、篡改和获取应用系统内的信息。

b）未进行终端病毒的合规性检查的风险：针对存储信息影响在于不合规终端可能在内网传播病毒，造成本机和其他终端存储信息不可用。

c）未进行终端最新操作系统补丁的合规性检查的风险：无最新系统补丁的终端易受攻击，并可能成为攻击其他业务终端的跳板，本终端和其他被攻击的终端存储信息可能被非法访问。当本终端和其他终端连接应用系统时，攻击者可借此对在线信息进行非法访问。

d）未进行终端木马的规性检查的风险：未进行木马检测的终端可能携带木马，被攻击者控制，并可能成为攻击其他业务终端的跳板。本终端和其他被攻击的终端存储信息可能被非法访问。当本终端和其他终端连接应用系统时，攻击者可借此对在线信息进行非法访问。

e）未进行终端外设控制的规性检查的风险：影响在于此类终端可能存在非授权开启的外设端口，造成本终端存储信息的泄漏，当终端连接应用系统时存在将在线业务信息扩散的风险。

f）未进行手机违规接入内网终端检测与阻断的风险：手机可能通过内网连接获取在线业务信息，并通过手机的数据连接向系统外扩散。

g）未对非内网终端授权接入内网进行安全检测的风险：存在非内网终端通过接入流程接入内网后，由于非内网终端健康状态不合规安全防护性能弱而被攻击，造成本机存储信息

被非法访问，当终端连接应用系统时在线业务信息被攻击者非法访问。

h）非内网终端按照流程审批通过接入内网后，未对其上传下载数据行为进行审计和记录的风险：对于在线信息来说，其危害在于非内网终端的临时性决定。非内网终端是数据外泄的易发生点，无响应审计和记录，就无法在业务数据外泄时判断其外泄途径。

i）未识别区分违规内联终端的身份信息的风险：针对在线信息影响主要在于违规内联的终端采用合法或非法权限连接应用系统，获取、修改应用系统内的信息，无法有效获取其终端身份，无法有效地进行追查。

针对存储信息影响主要在于，违规终端接入内网后由于健康状态不合规而形成的安全防护能力弱，被攻击，造成存储信息被非法获取时，无法获取其身份信息，就不能追溯存储信息外泄的途径，进行弥补和处罚。

j）未对违规内联的终端进行审计信息的上报的风险：针对在线和存储信息的影响主要在于，无法获知安全事件的发生，无法终止对信息有威胁的行为、防止再次发生和相应处罚。

（c）基于资产使用人分析

a）终端身份的合法性判断未按照要求进行终端违规内联检测，该风险主要涉及外部人员。外部人员非法接入系统可能造成不同目的人员非法获取网络资源，通过系统网络资源的获取可能造成对其他终端的攻击和应用系统的非法访问。

b）终端未进行合规性检查的风险，主要涉及内部人员、临时人员和经过入网审批流程的外部人员。无论上述哪一类人员均需要进行合规性检查，否则终端会因为安全状态不合规而安全防护措施不足，被攻击并被作为系统薄弱点成为攻击跳板。终端一旦被攻击，虽然终端的使用者：内部人员（特别是其中不同业务类别的终端）、临时人员和经过入网流程的外部人员，由于其存储信息重要程度和业务权限职责、权限不同，而造成不同的后果，但是作为攻击跳板对于其他主机发动攻击具有相同的风险。

c）不合规的终端未被系统自动强制定位到隔离区，进行合规修复的风险，主要涉及内部人员、临时人员和外部人员，在运行阶段没有将不合规终端定位到隔离区，则无法在限制使用内网资源的基础上对不合规终端进行强制合规处理。

d）非内网终端不具备接入内网的流程化处理和应急处理的风险，主要涉及外部人员，可导致外部人员的非内网终端无法入网使用或入网使用但没有有效的被资产管理系统有效管理。

e）非内网终端不具备接入内网的授权、审批的风险，主要涉及外部人员，可能导致外部人员的非内网终端无法通过入网流程获得入网许可或非内网终端不经审批就接入内网。

f）未对非内网终端授权接入内网进行安全检测的风险主要涉及外部人员，外部人员的非内网终端健康状态不合规，产生同不合规内网终端接入相同的风险。

g）非内网终端按照流程审批通过接入内网后，未对其上传下载数据行为进行审计和记录的风险主要涉及外部人员，外部人员作为行政管理手段的薄弱环节易产生数据外泄，未对其行为进行审计和记录，则在数据外泄产生时无法有效追查。

h）使用非授权 IP 的违规内联风险，主要涉及内部人员、临时人员和经过授权的外部人员，内部人员有固定分配的 IP 地址，威胁较小。临时人员和经过授权的外部人员可能在授权使用未完成的情况下使用非授权 IP 或为了获取内部人员的相应权限冒用 IP 地址，造成原

有合法用户无法使用网络资源，威胁更大。

i）开启非授权服务端服务的违规内联风险，主要涉及内部人员、临时人员和经过授权的外部人员，3 类人员同样可能因为误操作开启非授权服务端服务，影响正常服务。临时人员和经过授权的外部人员还有可能因为对网络环境不熟悉，启用相应服务，造成正常服务影响的可能性更大。

（d）风险场景

终端从准入的角度可以按照资产的属性划分成如下几类：内网终端、内网临时使用的终端、外网终端、本单位漫游终端、不明来源的终端。内网终端是进行了资产登记的专为内网使用的终端，内网临时终端是有在内网临时使用需求的终端，外网终端是进行了资产登记专门用于外网使用的终端，本单位漫游终端是本地位其他地区内网使用的终端由于工作需要漫游之本地内网的终端，不明来源的终端是所有不在内网登记使用，且无在本地内网使用的合理需求的终端。根据不同的终端种类，违规内联涉及以上终端入网、离网的场景。并根据入网需求的紧急程度不同，可以将入网离网的场景区分为一般场景和应急场景。

（e）合规性要求

合规性要求见表 B-18。

表 B-18

序号	安全类	等级保护（三级）要求	符合程度
1	网络安全	7.1.2.4 边界完整性检查（S3） a) 应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断	符合

基于以上风险点分析，如采取相关技术和管理手段管控 30 个风险点，则终端违规内联部分管理符合等级保护相关要求。

相关技术和管理的风险管控措施参见以下小节阐述。

2．风险管控

（1）终端身份合法性检测（终端资产没有在资产管理系统登记的违规内联；终端资产与资产管理系统登记信息不符的违规内联；登录终端用户没有合法登记的违规内联）

事前处置：终端入网登记，保存终端相关识别信息。

事中处置：

- ✓ 终端接入内网验证终端身份，检查终端是否在资产库中有合法登记。通过则进入下一流程，未通过则转入非内网终端入网流程
- ✓ 检查终端与资产库中登记的信息是否相符，通过则进入下一检查流程，未通过则进行告警，并进行审计记录
- ✓ 检查终端登录用户是否为登记用户，通过则正常使用网络资源，未通过则进行告警，并进行审计记录
- ✓ 安全管理员通过告警和日志记录进行风险分析

事后处置：安全管理员对违规内联的情况进行关联分析，由网络管理员调整安全策略。

处置流程见图 B-27。

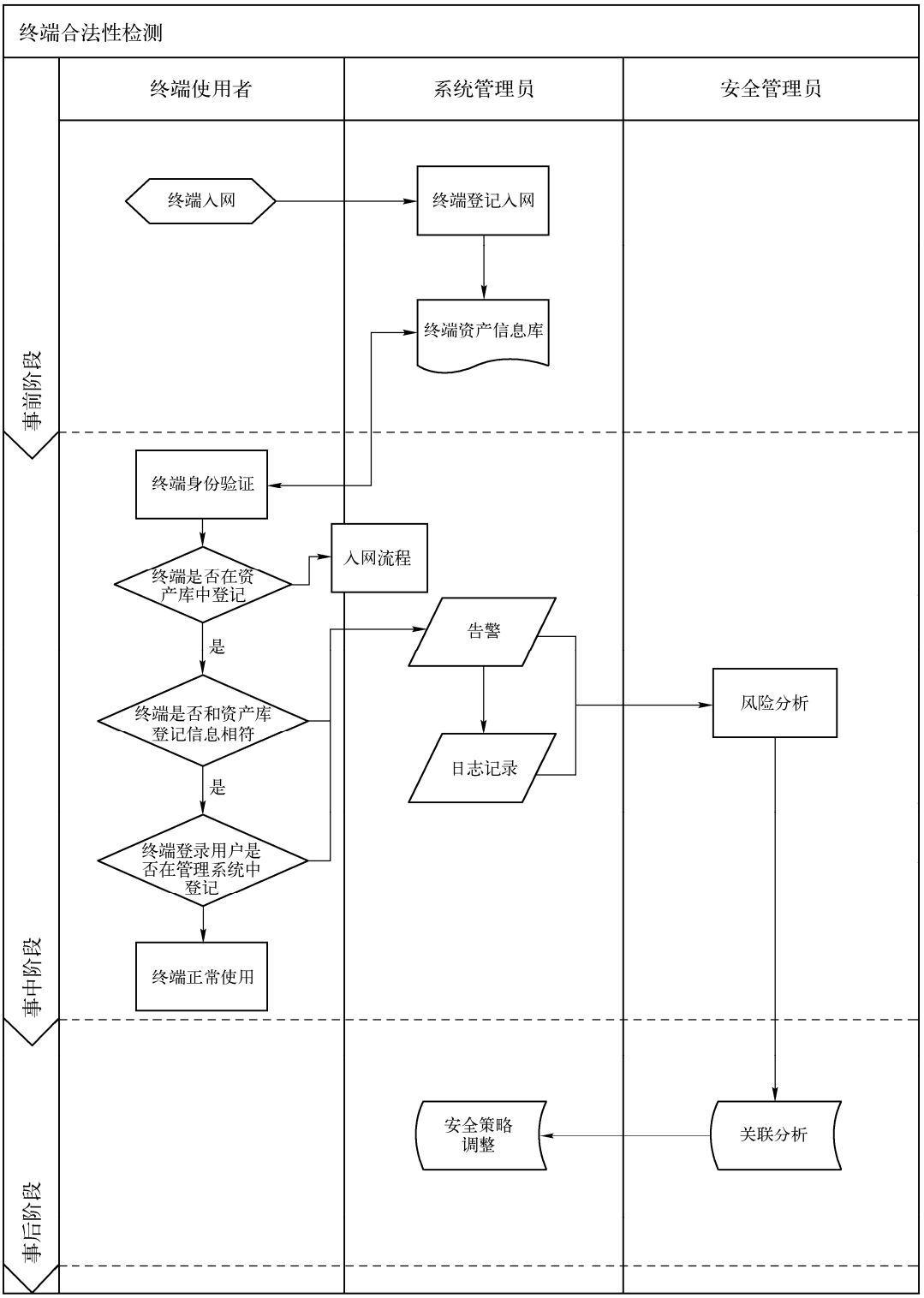
终端合法性检测
终端使用者
系统管理员
安全管理员
事前阶段
事中阶段
事后阶段
终端入网
终端登记入网
终端资产信息库
终端身份验证
终端是否在资产库中登记
入网流程
是
告警
终端是否和资产库登记信息相符
风险分析
是
日志记录
终端登录用户是否在管理系统中登记
终端正常使用
安全策略调整
关联分析

图 B-27

（2）终端身份标识冒用（终端身份标识符被篡改、冒用的风险；终端身份标识符被冒用，在相应控制措施实施时可能导致的被冒用的合法终端无法上网）

事中处置：

- ✓ 在产生安全日志时，记录终端多个特征信息，比对管理平台中身份标识符和终端特征信息的对应关系，发现身份标识符和终端特征信息不符则引发告警
- ✓ 检测终端标识符是否发现重复情况，发现身份标识符重复则说明有终端冒用身份标识符，首先阻断出现身份标识符重复情况终端的网络连接

事后处置：安全管理员根据终端标识符冒用和篡改的情况，进行相应处罚。

（3）终端身份合规性检测（终端病毒检查不合规的违规内联；终端操作系统补丁检查不合规的违规内联；终端应用软件检查不合规的违规内联；终端木马检查不合规的违规内联；终端外设控制检查不合规的违规内联；不合规的违规内联终端，不被强制定位到隔离区；隔离区的终端，不进行有效验证就被允许入网；隔离区内的终端，用户未按流程进行合规化处理）

事前处置：定义健康状态检查策略，例如病毒木马检测、操作系统补丁检测、应用软件安装情况检测、外设控制状态检测等。

事中处置：

- ✓ 进行终端病毒健康状态检查
- ✓ 进行终端操作系统补丁的健康状态检查
- ✓ 进行终端应用软件的健康状态检查
- ✓ 进行终端木马的健康状态检查
- ✓ 进行终端外设控制的健康状态检查。
- ✓ 未通过健康状态检查的终端进行用户提示（显示用户不合规的具体内容，及后续合规化处理的方式）
- ✓ 将不合规终端纳入隔离区进行强制合规处理
- ✓ 健康状态检查失败的终端身份信息进行日志记录

事后处置：根据整体安全态势分析，调整安全策略，针对终端下发新的安全策略。

处置流程见图 B-28。

（4）产生违规内联后，终端身份信息识别

事前处置：终端入网登记，保存终端相关识别信息。

事中处置：

- ✓ 进行违规内联的检查流程
- ✓ 对于违规内联的终端，判断其是否在资产库中有登记，如果有登记则直接从资产库中获取身份信息
- ✓ 如违规内联的终端不在资产库中登记则获取终端其他特征信息，根据特征信息判断其身份（机器名等）

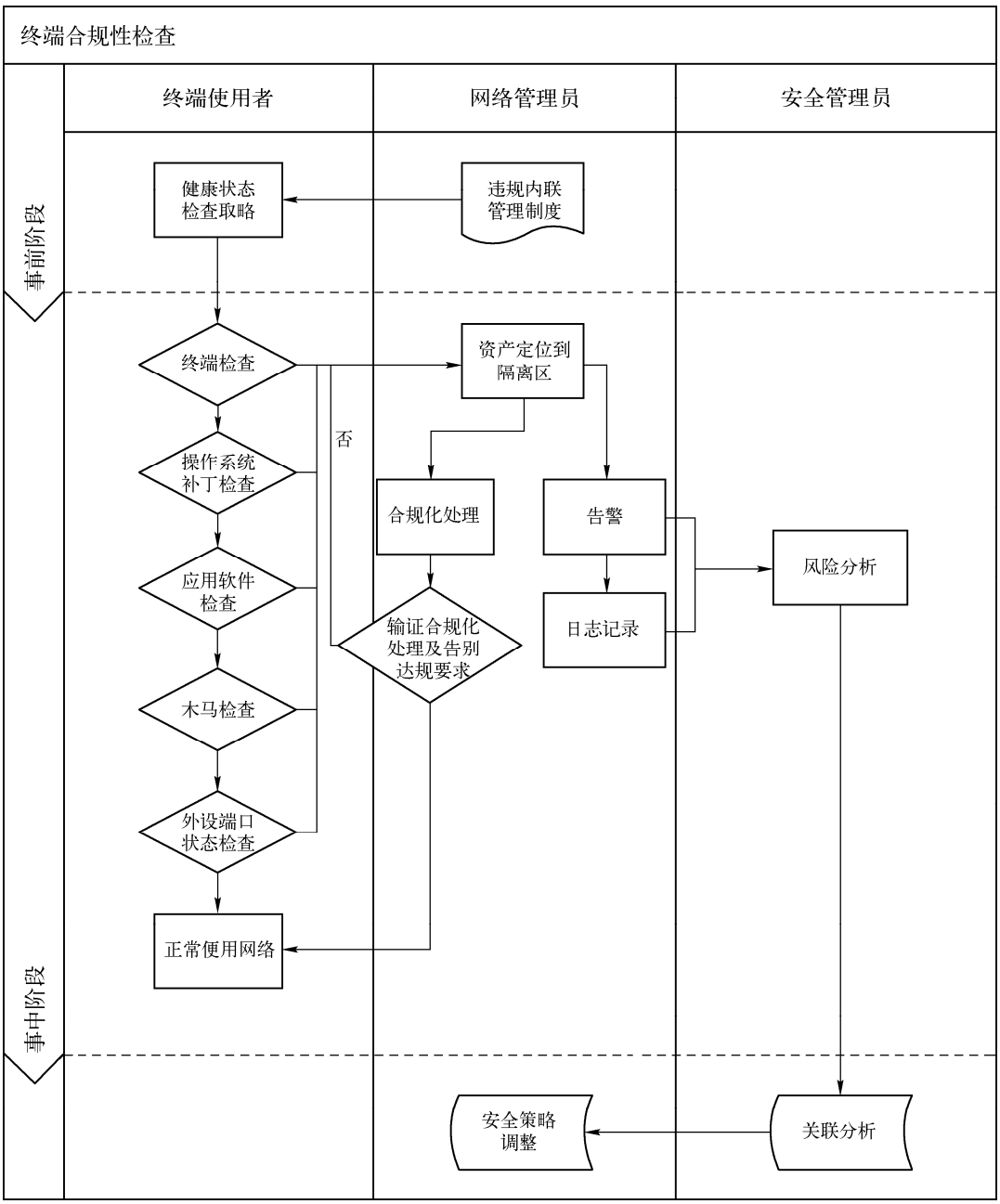

图 B-28

✓ 对违规外联的终端行为进行告警和日志记录

事后处置：根据整体安全态势分析，调整安全策略，针对终端下发新的安全策略。处置流程见图 B-29。

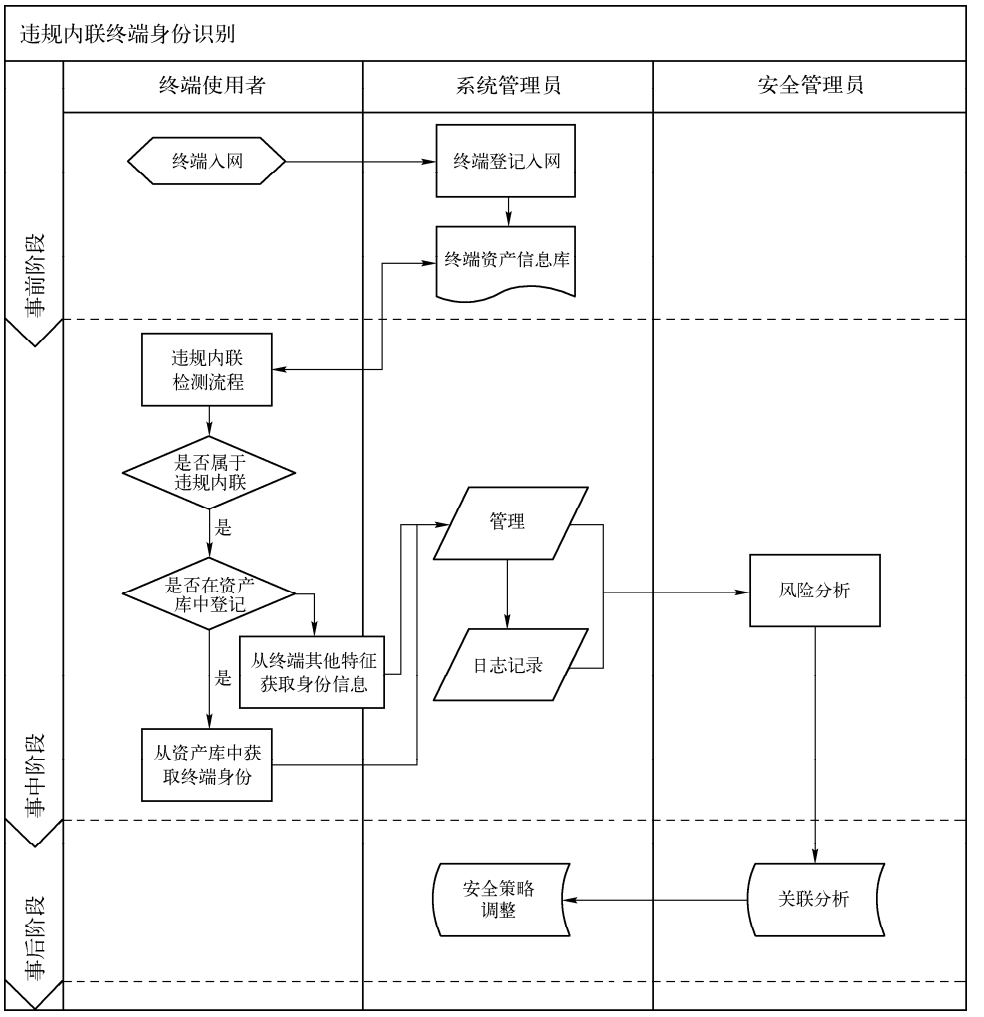

图 B-29

（5）非内网终端接入内网（非内网终端连入内网，无流程化处理；非内网终端连入内网，无应急处理；非内网终端接入内网，无授权审批；非内网终端接入内网后，用户未按流程进行身份登记；非内网终端授权接入内网，不进行安全检测；非内网终端授权接入内网，不对其上传下载数据行为进行审计和记录。）

事前处置：终端入网登记，保存终端相关识别信息。

事中处置：

- ✓ 终端接入内网验证终端身份，检查终端是否在资产库中有合法登记。通过则正常上网，未通过则进入临时入网流程
- ✓ 临时入网流程完成后进入审批流程，审批流程将相应临时资产信息保存到资产库中
- ✓ 审批流程完成后再次进行身份验证，通过身份验证则进入下一流程，未通过则再次进入临时入网流程修正临时入网流程中存在的问题
- ✓ 对临时入网的非内网主机进行安全性检查
- ✓ 对通过安全性检查的临时入网的非内网终端记录上传下载的审计信息

事后处置：安全管理员对违规内联的情况进行关联分析，由网络管理员调整安全策略。

处置流程见图 B-30。

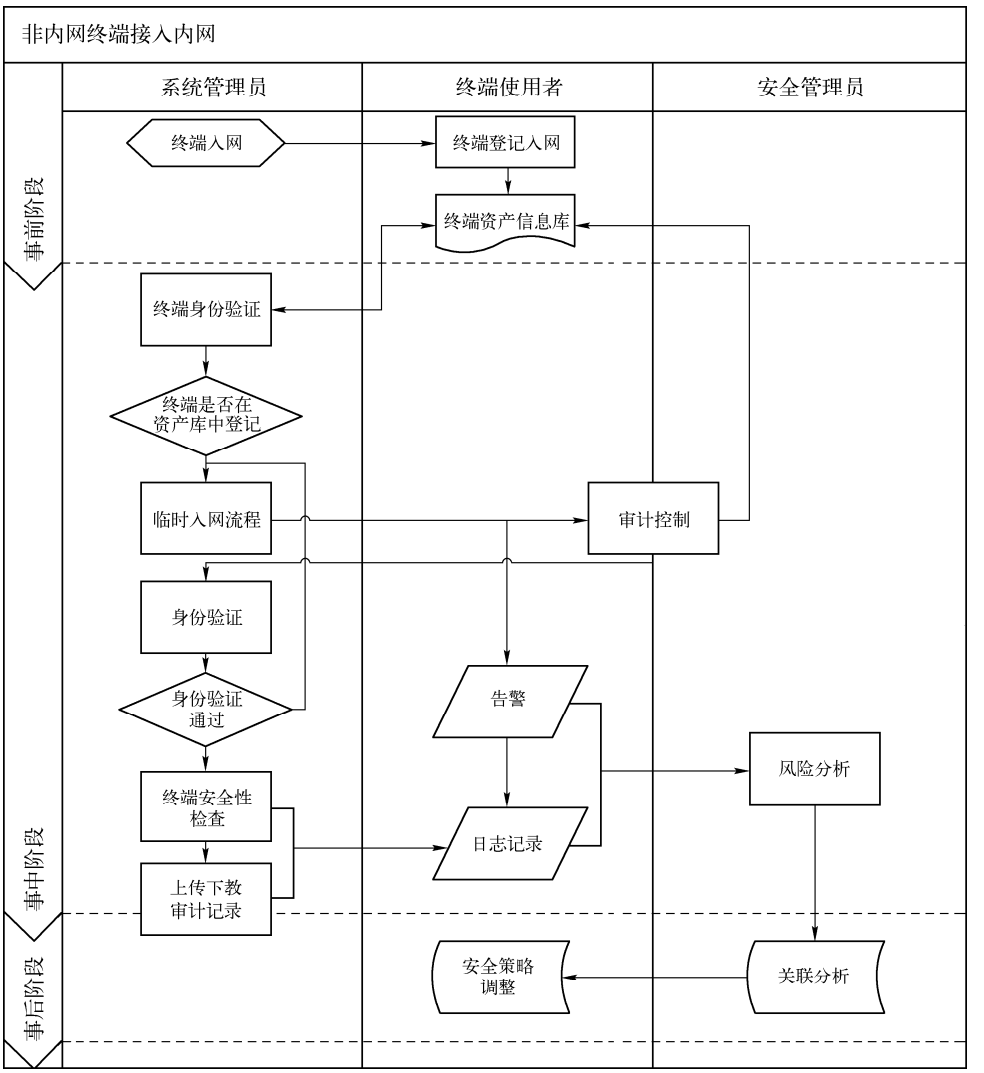

图 B-30

（6）非授权使用 IP 地址（授权接入内网的终端，使用未经系统管理员分配的 IP 或 IP 段；对非授权使用 IP 的终端不进行提示；对非授权使用 IP 的终端未进行审计上报；非授权使用 IP 的终端，用户未按提示修改 IP）

事前处理：指定 IP 地址分配方案，形成 IP 地址列表。

事中处置：

✓ 在终端入网检查过程中验证终端身份和 IP 地址的对应关系，如果验证通过则正常上网，验证未通过进入下一流程

✓ 对用户终端进行 IP 地址配置不正确的提示，提示用户修改

✓ 对用户终端违规使用 IP 地址的行为进行审计记录

✓ 阻断违规使用 IP 地址终端的网络连接，直至用户修改 IP 地址后重新验证入网

事后处置：安全管理员根据终端违规使用 IP 地址的情况，进行相应处罚。

（7）非授权开启服务器端服务（授权终端，开启未经系统管理员允许的服务端服务（DHCP、代理）；对非授权开启服务器端服务的终端不进行提示；对非授权开启服务器端服务的终端未进行审计上报；非授权开启服务器端服务的终端，用户未按提示关闭服务）

事前处理：统计内网中基础网络服务的服务器清单，形成服务与服务器的对应表。

事中处置：

- ✓ 在终端入网检查过程中验证其基础网络服务的服务开启情况，存在开启基础网络服务的终端则验证服务与服务器对应表，如果验证通过则正常上网，验证未通过进入下一流程
- ✓ 对用户终端进行非授权开启基础网络服务的提示，提示用户关闭
- ✓ 对用户终端违规开启基础网络服务的行为进行审计记录
- ✓ 阻断违规开启基础网络服务的服务端口

事后处置：安全管理员根据终端违规开启基础网络服务的情况，进行相应处罚。

（8）系统不能发现和解决的终端安全风险和对策

（a）隔离区内的终端，用户未按流程进行合规化处理

隔离区内的终端，用户会接到提示进行合规化处理的方法和内容，如果用户不按照提示进行相应合规化处理，则系统无法强制对终端进行合规化处理，需要从技术上限制未进行合规化处理的终端使用网络资源（包括隔离区网络资源），其次以相应审计记录为管理依据通过行政管理的手段强制用户进行合规化处理。

（b）非内网终端接入内网后，用户未按流程进行身份登记

非内网终端未通过身份验证的，可以按流程进行临时入网，如果用户没有合理入网需求或不按正常流程进行身份登记，则系统无法控制终端进行相应临时入网处理，首先需要从技术角度保证不进行临时入网处理就无法使用网络资源，其次以相应审计记录为管理依据通过行政管理的手段要求需要临时入网的终端通过临时入网流程进行身份登记。

（c）非授权使用 IP 的终端，用户未按提示修改 IP

非授权使用 IP 地址的终端，如果用户未按提示修改 IP，则系统无法控制终端的 IP 地址修改，需要首先从技术的角度保证非授权使用 IP 地址的终端无法使用网络资源，其次以相应审计记录为管理依据通过行政管理的手段要求需要非授权使用 IP 地址的终端修改 IP 地址。

（d）非授权开启服务器端服务的终端，用户未按提示关闭服务

非授权开启基础网络服务的终端，如果用户未按提示关闭相应基础网络服务，则系统无法控制终端的服务开启或关闭，需要首先从技术的角度保证非授权开启基础网络服务的终端不能使用相应业务端口，其次以相应审计记录为管理依据通过行政管理的手段要求需要非授权开启基础网络服务的终端关闭相应服务。

3．风险控制效果

对于内网中非法接入和违规使用的控制，保证访问内网的终端安全可控。

可以针对终端的合法性和合规性进行检测和阻断处理。能针对不合规的终端强制定位到隔离区进行合规处理。针对非内网终端接入内网进行流程化处理和和合理的授权管理，并对非内网终端的行为进行有效的审计和监控，针对终端数据外泄事件可以提供追查依据。

B.3.2 违规外联（12 个风险点）

1．风险分析

（1）风险描述

违规外联的风险体现在：

1）不能对违规外联的行为进行检测和阻断，终端的非法外联行为包括终端通过更换网线、通过其他数据接口或设备连接互联网或其他网络，如果不能对违规外联的行为进行检测和阻断，就会产生数据外泄无法管控、无法追踪，破坏系统安全边界，违背系统整体安全防护策略，系统面临严重安全隐患。

2）不能对终端离网状态下的违规外联进行检测和告警，终端在联网状态下由于不连接服务器，不能实现实时告警，但是终端本地可能保存重要信息，如果不能在离网状态下进行违规外联的检测和告警，就会导致信息外泄且无法获知外泄的行为。

3）不能对终端连入其他网络进行检测告警和阻断，终端违规连入其他网络（非互联）判断指标较难确定，但是违规连入其他网络可能造成内网和其他网络的联通，或造成终端本地信息向其他网络的外泄。

（2）相关风险点

违规外联风险点见表 B-19。

表 B-19

	序号	风险点	风险属性	隐患/风险
违规外联	1	终端在内网环境下的违规外联不能进行检测	原生风险	隐患
	2	终端在内网环境下的违规外联不能进行阻断	原生风险	隐患
	3	终端在内网环境下的违规外联进行阻断误报导致的正常使用终端断网	次生风险	风险
	4	不能检测终端在离网后的违规外联行为	原生风险	隐患
	5	不能对终端离网后的违规外联行为进行审计记录和告警	原生风险	风险
	6	终端离网状态下不能进行阻断，产生信息外泄	残余风险	风险
	7	发生违规外联事件时，不能发现并准确定位违规外联的途径	原生风险	隐患
	8	发现违规外联的状态时，无法界定内外网互联和离线上网的不同情况	原生风险	隐患
	9	不能对终端违规接入其他网络（非互联网）进行检测	原生风险	隐患
	10	不能对终端违规接入其他网络（非互联网）进行阻断	原生风险	隐患
	11	不能对终端违规接入其他网络（非互联网）进行审计记录和告警	原生风险	风险
	12	不能对违规外联的行为准确取证	原生风险	风险

（a）基于资产使用生命周期分析

资产使用生命周期包含入网前、运行阶段、维修阶段、报废阶段，违规外联风险对终端的影响在资产生命周期的体现如下：

a）终端在内网环境下，发生违规外联不能检测、阻断和报警的风险，存在于资产生命周期的运行、维修阶段。在运行阶段终端发生违规外联风险，可能是由于终端使用者不了解当前所处的网络环境，被外界利用终端现有的对外接口连通了终端，这可能导致网内数据外泄或引入病毒和木马等危害程序。因此面对外网的入侵和攻击等威胁，需要及时检测、阻断和报警，才可以有效防护和避免产生数据外泄或产生外部攻击的途径。在维修阶段产生违规外联，通常是由于维修阶段终端操作人员不是资产使用人员，一般可能是维修公司的人员，在使用终端时造成的。由于维修公司的人员不属于内部人员，人员管理和用户单位对资产使用人员的管理力度存在差距，产生恶意的泄漏信息、损害内网资产的可能性较大。维修阶段连接外网，使资产处于不安全的网络环境中，会直接面对外网的入侵和攻击等威胁，还可能引入病毒和木马等危害程序，如果不能检测到该种情况则无法分析该行为具体引发的影响，导致不能阻断连接

则无法有效防护资产，而不能报警则导致无法搜集和分析该资产发生的安全事件。

b）发生违规外联事件时，不能发现并准确定位违规外联的途径的风险存在于资产生命周期的运行、维修阶段。在运行阶段不能发现定位违规外联的途径，则无法针对该外联安全事件进行对应的管控行为，无法调整相关安全策略避免违规外联的再次发生，并且无法记录信息的流通情况。在维修阶段，不能发现并定位违规外联的途径，在信息发生外泄时就无法确定维修终端是如何产生信息外泄的，不能针对维修终端进行防护策略和维修管理制度进行针对性的调整防止外泄行为再次发生。

c）不能发现、阻断终端在离网后的违规外联行为的风险存在于资产生命周期的运行、维修阶段，在运行阶段终端不进行离网后的违规外联检测，可能产生终端离网后终端内信息外泄、病毒感染和木马入侵等威胁，终端再次接入内网之后，又可能将这些威胁带入内网，影响内网的安全环境，容易引发内网其他终端的同类安全事件，并且可能在离网状态下躲避防护系统对其状态和安全事件的监控；在维修阶段，终端离网意味着资产处于工作人员的监管范围之外，也离开了工作环境，本身已经处于危险的运行环境，如果不能发现违规外联行为，可能导致对于资产安全性的重新检测和识别。

d）发现违规外联的状态时，无法界定内外网互联和离线上网的不同情况的风险存在于资产生命周期的运行阶段，在运行阶段不能界定内外网互联和离线上网的违规外联行为，则无法根据终端是否在网对违规外联的行为进行区别处理（如在网状态首先要断开内网网络连接），可能因此而产生误判或基于误判结论分析的情况采取不适当的控制措施。

e）不能对终端违规接入其他网络（非互联网）进行监控管理的风险存在于资产生命周期的运行阶段和维修阶段，在运行阶段没有终端接入非互联网的其他网络进行检查，则违规外联的终端同样存在信息外泄和引入外部攻击的风险。在维修阶段，维修终端可能由于维修需要接入其他网络，维修终端接入其他网络就存在信息外泄和引入外部攻击的风险。

f）不能对违规外联的行为准确取证的风险存在于资产生命周期的运行阶段和维修阶段，在运行阶段没有对终端违规外联行为进行取证则无法对终端违规外联行为进行判断，不能评估违规外联过程产生的具体威胁和影响，进而本来应该采取的相关安全措施无法对应实施。在维修阶段不能对违规外联行为准确取证，就造成了发生安全事件时，无法明确安全事件是资产使用人还是维修人员的违规行为造成的，无法进行针对性的处罚。

（b）相关信息风险

a）终端在网状态下违规外联不能检测、阻断和报警的风险。对在线信息的影响主要在于违规外联的终端当连接至应用系统时可能造成在线业务信息的外泄。针对存储信息的影响在于违规外联可能造成本终端存储的信息通过违规外联外泄。

b）不能发现、阻断终端在离网后的违规外联行为的风险。针对存储信息的影响在于终端离网后产生违规外联，可能造成本终端存储信息的外泄。

c）发生违规外联事件时，不能发现并准确定位违规外联的途径。针对在线信息和离线信息，不能在发生违规外联时发现并定位违规外联的途径，则无法针对违规外联的途径进行相应控制（如断开外联途径），终止信息进一步外泄。

d）发现违规外联的状态时，无法界定内外网互联和离线上网的不同情况的风险。针对在线信息的影响在于，不能对内外网互联和离线上网区别处理（如断开内网连接等），导致不能断开违规外联终端的业务连接，造成在线业务信息的外泄。

e）不能对终端违规接入其他网络（非互联网）进行监控管理的风险。连接其他网络可

能造成在线业务信息和离线的存储信息向其他网络外泄。

（c）基于资产使用人分析

a）终端在网状态下违规外联不能检测、阻断和报警的风险涉及内部人员、临时人员、经过入网流程的外部人员，尤其是内部人员，因为内部人员可以接触到业务内网中的重要信息，这些信息包括生产信息、行业信息、个人信息等，在违规外联的情况下容易导致数据外泄；因为临时人员涉及的信息重要程度没有内部人员那么多，但是违规外联产生的系统安全边界破坏，带来的可能的外部攻击和内部人员相比危险是相同的，阻断的必要性是很高的；经过入网流程的外部人员是有机会接触部分重要信息的，而且由于工作需要，需要进行内外网交互，因此检测的重要性比较高，对于阻断的判断需要基于实际使用环境和状况。

b）发生违规外联事件时，不能发现并准确定位违规外联的途径时。如果是内部人员，可能是生产工作的需求，在不能确定是否正常工作需要的情况下，可能会需要对其采取放行避免影响生产工作，因而对违规外联的途径需要发现和准确定位，通过了解途径和外联的内容，才能明确该行为的风险；临时人员如果利用现有网络中的监控漏洞进行外联，不能确定违规外联的途径，就无法进行相应控制，阻止外泄的进一步发展，避免外部的入侵途径；经过入网流程的外部人员的外联如果属于例外开放，并且根据监控外联数据的内容不属于信息泄密，则对于网络的风险相对较小。

c）不能发现、阻断终端离网后的违规外联行为。对于内部人员而言，可能导致终端离网后终端内信息外泄；临时人员和经过入网流程的外部人员由于涉及的信息重要程度不高，而且使用的终端可能就是个人资产或者外来资产，离网属于正常使用，因此离网后的违规外联造成的数据外泄的严重程度与内部人员是不相同的。

d）发现违规外联的状态时，无法界定内外网互联和离线上网的不同情况的风险。对于内部人员而言，在离线上网的时候依然有机会发生信息泄密等安全事件，对于内部人员的终端应用来说，一旦暴露在外网就存在这种风险，因此对于界定两种情况的风险在内部人员终端上风险较小，因为两者具有同等的威胁；临时人员以及经过入网流程的外部人员由于使用的终端情况不同，不能界定内外网互联和离线上网的违规外联行为，则无法根据终端是否在网区别对违规外联的行为进行处理（如在网状态首先要断开内网网络连接），在无法界定两种情况时，威胁相对较大。

e）不能对终端违规接入其他网络（非互联网）进行监控管理的风险对内部人员而言较大，因为内部人员的终端进行的操作与业务相关的可能性非常大，如果接入其他网络一般需要提前进行申请和备案，否则该行为可能导致业务系统与外界相连，本地信息可能会泄漏；临时人员以及经过入网流程的外部人员所使用设备，如果没有接触重要信息，则终端接入非互联网的其他网络也需要进行检查，不能排除违规外联的终端同样存在信息外泄和引入外部攻击的风险。

f）不能对违规外联的行为准确取证的风险对于内部人员而言，由于涉及重要信息，所以在违规外联行为中传递的数据必须经过准确取证才能确保信息的安全；临时人员以及经过入网流程的外部人员如果无法对终端违规外联行为提供准确取证，将无执法依据，因此无论是内部人员、临时人员还是经过入网流程的外部人员，联入内网的前提都是遵守内网的管理要求。若违规均需要进行相应的处理。

（d）风险场景

a）终端内网在线状态下连接互联网，当终端连接内网时违规连入互联网，由于互联网用户成分复杂，容易引入互联网中恶意用户的攻击、及病毒和恶意代码；同时终端中存储的信息和终端

连接业务系统的在线信息如通过互联网外泄，无法对外泄信息的传播范围进行控制和传播目的无法确定，风险极大，需要通过技术手段严格禁止终端内网在线状态下的互联网违规连接。

b）终端内网离线状态下的互联网连接，终端在内网离线的状态下违规连入互联网，虽然不会通过终端造成互联网威胁对内网的直接攻击，但是也存在互联网中的病毒和恶意代码传播至终端本地，造成对于终端本身的侵害，另外当终端重新登录至内网时，会造成病毒及恶意代码向内网的传播。终端在离网状态下，业务信息不会直接通过互联网向外传播，但是终端本地保存的离线信息，可能通过互联网外泄，因此在信息外泄的方面也存在很大风险，需要通过技术手段严格禁止终端内网连线状态下的互联网违规连接。

c）终端内网在线的状态下连接非互联网的其他网络或终端，其他网络或其他终端均可能存在恶意的攻击，通过违规外联的终端直接攻击内网，通过传播病毒及恶意代码，终端在连接内网的状态下可能向连接的其他网络或其他终端传播业务信息和终端保存的本地信息，相对于互联网，通过其他网络或终端外泄的信息在一定程度上更容易进行事后的追查，但是外泄的风险依然很大。需要通过技术手段禁止或者严格进行数据传输监控审计。

d）终端在内网离线的状态下连接非互联网的其他网络或终端，其他网络或或其他终端不能通过违规外联的终端攻击内网，但是可能向违规终端传播病毒及恶意代码，当终端重新连接至内网时，还可能造成病毒及恶意代码向内网传播，终端在内网离网的状态下，在线的业务信息不会通过连接的其他网络或其他终端外泄，但是终端本地保存的信息可能通过连接的其他网络或其他终端外泄，因此终端在内网离线的状态下连接非互联网的其他网络或终端需要通过技术手段禁止或者严格进行数据传输监控审计。

（e）合规性要求

合规性要求见表 B-20。

表 B-20

序号	安全类	等级保护（三级）要求	符合程度
1	网络安全	7.1.2.4 边界完整性检查（S3） b) 应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断	符合

基于以上风险点分析，如采取相关技术和管理手段管控 8 个风险点，则终端违规外联部分管理符合等级保护相关要求。

相关技术和管理的风险管控措施参见以下小节阐述。

2．风险管控

（1）终端在网状态下违规外联检测、阻断和报警控制流程（终端在内网环境下的违规外联不能进行检测；终端在内网环境下的违规外联不能进行阻断；终端在内网环境下的违规外联进行阻断误报导致的正常使用终端断网）

事前处置：定义内网范围，定义外网连接，区分内外网的识别方式，定义违规外联的处理操作。

事中处置：

- ✓ 实时检测外网联通状态，没有联通外网继续正常上网
- ✓ 存在联通外网的情况进行用户终端违规外联行为的提示（屏幕显示，提示用户当前状态）

✓ 根据违规外联安全策略设定执行操作
✓ 记录违规外联行为及终端使用者的操作，发送至防护平台服务器
✓ 管理平台分析风险

事后处置：根据整体安全态势分析，调整安全策略，针对终端下发新的安全策略。处置流程见图 B-31。

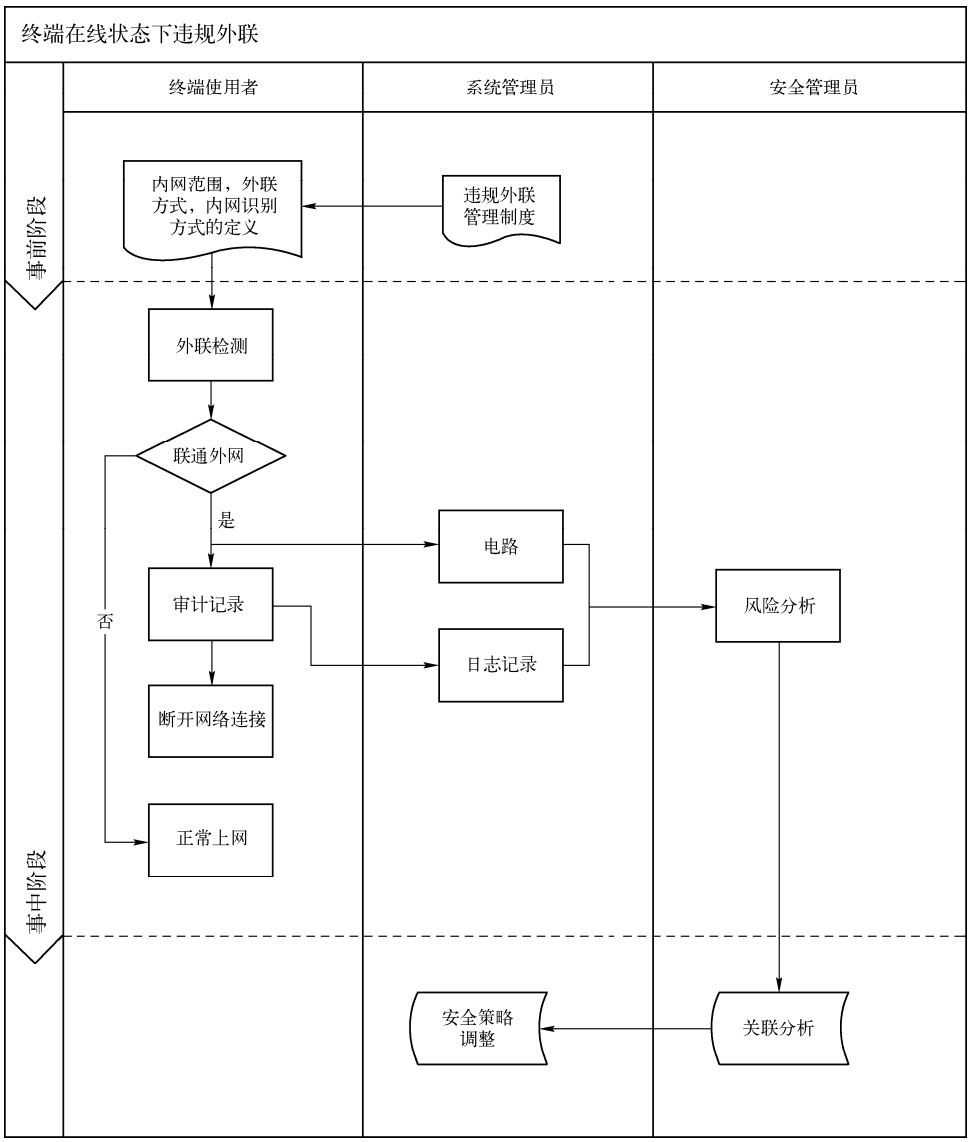

图 B-31

（2）终端在离网状态下违规外联检测、阻断和报警控制流程（不能检测终端在离网后的违规外联行为；不能对终端离网后的违规外联行为进行审计记录和告警；终端离网状态下不能进行阻断，产生信息外泄）

事前处置：定义内网范围，定义外网连接，区分内外网的识别方式，定义违规外联的处理操作，将策略保存至终端本地。

事中处置：

- ✓ 实时检测外网联通状态
- ✓ 存在联通外网的情况进行用户终端违规外联行为的提示（屏幕显示，提示用户当前状态）
- ✓ 记录违规外联行为及终端使用者的操作，在本地保存审计记录
- ✓ 终端再次入网后，上传审计信息并对终端离网状态的违规行为向系统管理员告警
- ✓ 管理平台分析风险

事后处置：根据整体安全态势分析，调整安全策略，针对终端下发新的安全策略。

处置流程见图 B-32。

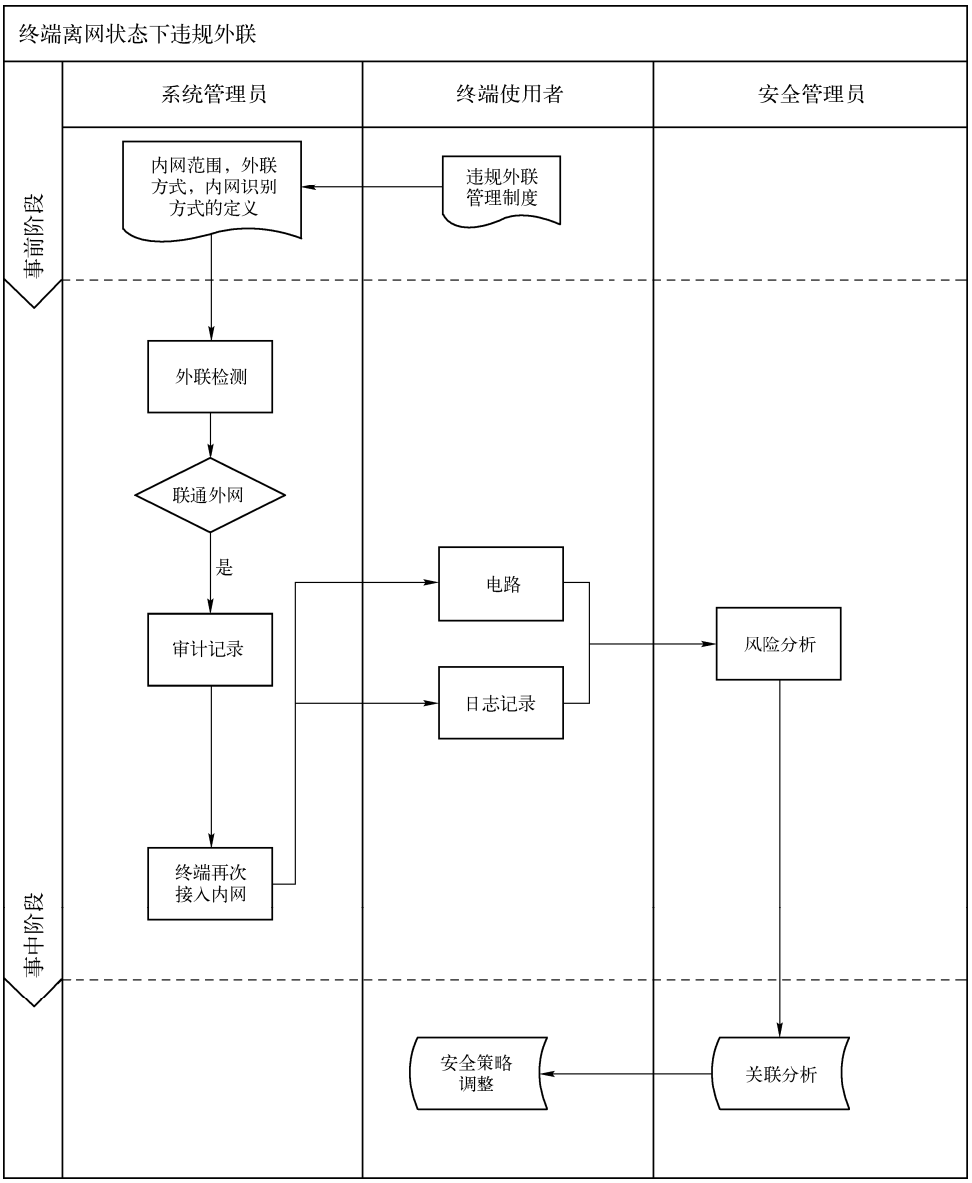

图 B-32

（3）发生违规外联事件时，不能发现并准确定位违规外联的途径

事中处置：

✓ 监控违规外联可能产生的方式，包括：

① 网络接口直接换用外网网线。

② 采用无线网卡外联。

③ 通过拨号外联。

④ 通过红外、蓝牙等数据接口外联。

⑤ 采用双网卡连接外网网线外联等。

✓ 针对不同违规外联的途径进行对应的控制

✓ 进行用户终端违规外联途径的提示（屏幕显示，要求用户确定）

✓ 记录违规外联行为及终端使用者的操作，发送至防护平台服务器

✓ 管理平台分析风险

事后处置：根据整体安全态势分析，调整安全策略，针对终端下发新的安全策略。

（4）发现违规外联的状态时，无法界定内外网互联和离线上网的不同情况

事前处置：指定内网终端数据端口/网络端口的管理策略，按照策略关闭非经授权的数据/网络端口，限制可能产生违规外联的途径。

事中处置：

✓ 发现违规外联行为产生时，判断终端是否连接至内网。对于连接至内网的违规终端首先断开内网连接（保持服务器的管理通道，便于服务器对终端的继续控制）

✓ 对于违规外联的途径进行控制，断开相应数据/网络接口

✓ 进行用户终端违规外联行为的提示（屏幕显示，要求用户确定）

✓ 审计记录违规外联行为，保存审计记录至防护平台服务器

事后处置：管理员通过违规外联的记录对违规外联行为进行追溯，并通过管理流程进行相应的处罚。

（5）终端违规连接其他网络（非互联网）违规外联检测、阻断和报警控制流程（不能对终端违规接入其他网络（非互联网）进行检测；不能对终端违规接入其他网络（非互联网）进行阻断；不能对终端违规接入其他网络（非互联网）进行审计记录和告警）

事前处置：定义内网范围，定义外网连接，区分内外网的识别方式，定义违规外联的处理操作。

事中处置：

✓ 实时检测外网联通状态（联通外网的检查标准和连接互联网的检测标准不同），没有联通外网继续正常上网

✓ 存在违规连接外网进行用户终端违规外联行为的提示（屏幕显示，提示用户当前状态）

✓ 判断终端是否连接内网，如连接内网则直接产生告警和审计记录，并根据违规外联安全策略设定执行操作

✓ 如非内网连接状态则将审计记录保存在本地，终端再次入网后上传审计记录并产生系统管理员告警

✓ 管理平台分析风险

事后处置：根据整体安全态势分析，调整安全策略，针对终端下发新的安全策略。处置流程见图 B-33。

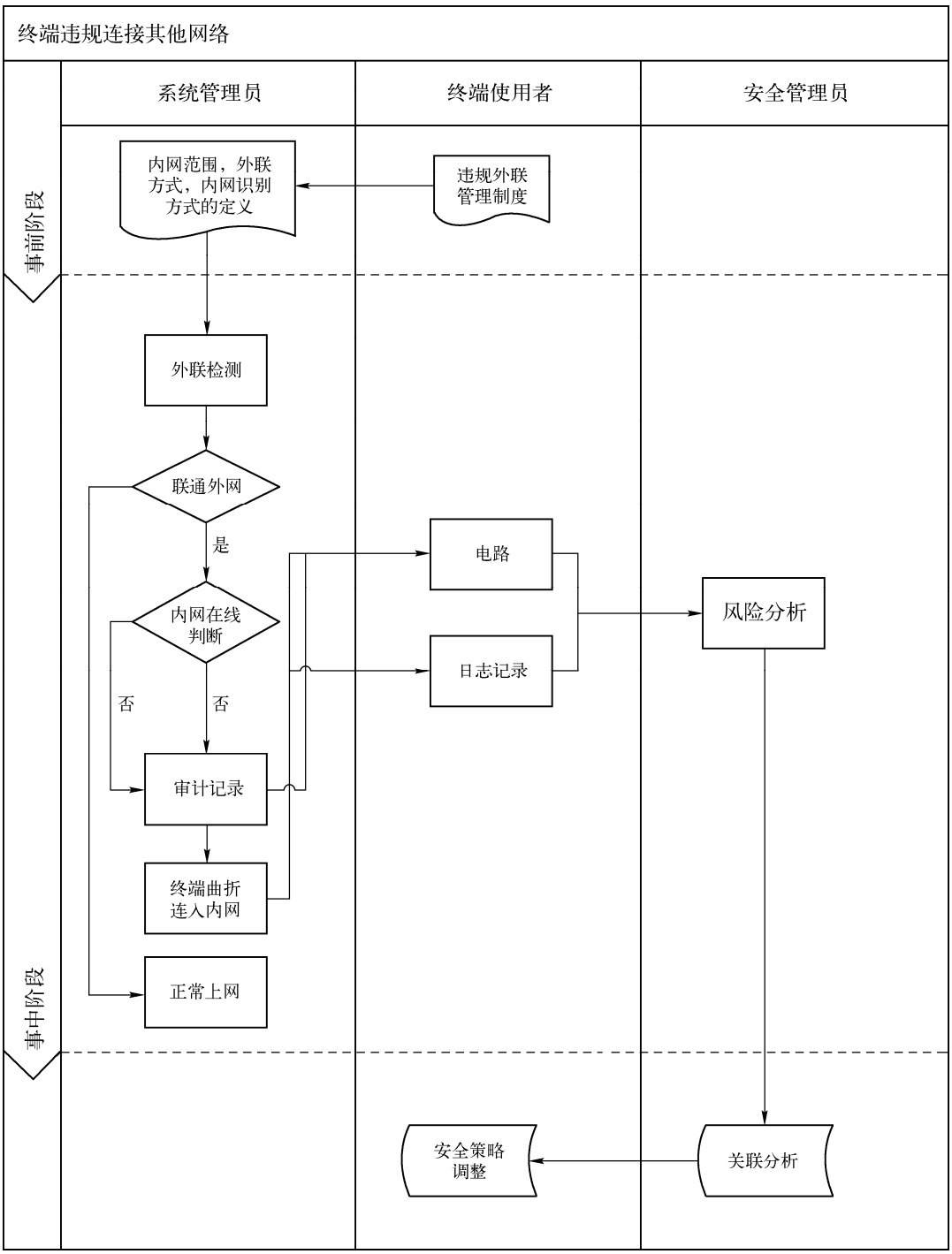

图 B-33

（注：处置流程和终端违规连接互联网的处置流程基本一致，主要的区别在于对违规外联的判断标准有区别，针对连接互联网和连接至非互联网络判断方式不同）

（6）不能对违规外联的行为准确取证

事中处置：

- ✓ 发现违规外联行为产生时，记录违规外联的审计记录，保存至防护平台服务器
- ✓ 对违规外联的行为进行取证（违规外联的访问记录、违规外联访问的访问关键字等原始记录信息），保存至防护平台服务器

事后处置：管理员通过违规外联的记录对违规外联行为进行追溯，并通过管理流程进行相应的处罚，处罚时以防护平台保存的访问原始记录作为处罚依据。

（7）系统不能发现和解决的终端安全风险和对策

终端离网状态下不能进行阻断，产生信息外泄。终端离网后，防护平台不能主动对终端断开网络连接，从而无法实施对离网终端的信息外泄行为进行阻断。需要加强终端外出携带的管理工作并限制在办公场所通过有线或无线手段的外网连接条件。

3．风险控制效果

对于终端违规外联的控制，实现了对于终端连接内网或断开内网时的违规外联行为，违规行为包括违规连接互联网和违规连接非互联网的其他网络，并可检测到终端的违规外联途径，可以判断离线上网和内外网互联的不同行为针对性的实施管控措施，并可以对违规行为进行取证以实现行政处罚的依据。

B.3.3 漫游管理（9 个风险点）

1．风险分析

（1）风险描述

漫游管理的风险体现在：

1）终端异地调拨或行业内工作人员携带终端异地办公时，终端在行业内部不同单位之间漫游时，目的地服务器不能发现，并自动接管漫游终端，导致终端在漫游过程中不能在异地网络中正常使用，漫游目的地服务器没有预定于漫游组并将漫游终端纳入漫游组中进行针对性管控，导致漫游终端不能被区别性的处理，由于漫游终端本身的流动性特点，带来的安全隐患。

2）漫游终端不能静默通过目的地网络中 802.1X 认证，导致漫游终端无法使用目的地网络资源。

3）源服务器无法获取漫游终端的漫游状态信息，源服务器不能掌握漫游终端的实际漫游情况，产生终端的随意漫游。漫游终端不将告警信息和审计记录上报给目的地服务器造成目的地服务器对漫游终端的使用情况不可获知，不能发现漫游终端产生的安全事件以及针对漫游终端的安全事件进行响应。漫游终端返回归属地时，不上报漫游期间的违规行为至源服务器，导致不能针对漫游终端的违规行为进行处罚，并根据漫游终端违规行为发生情况调整对漫游的管理。

（2）相关风险点

漫游管理的风险点见表 B-21。

表 B-21

	序号	风 险 点	风险属性	隐患/风险
漫游管理	1	终端在行业内部不同单位之间漫游时，目的地服务器不能发现，并自动接管漫游终端	原生风险	隐患
	2	目的地服务器不能预定义漫游组，并自动将漫游终端归入漫游组中	原生风险	隐患
	3	目的地服务器不能针对漫游组预定义各种安全策略	原生风险	隐患
	4	源服务器对终端漫游数据下发错误导致漫游终端无法在目的地入网	次生风险	风险
	5	漫游目的地服务器下发的漫游组安全策略弱于漫游终端在源网络中的安全策略	残余风险	隐患
	6	在所有服务器均启用 802.1X 认证的情况下，终端在漫游状态时，不能静默通过 802.1X 认证和接入网络	原生风险	隐患
	7	终端所属源服务器不能获取终端漫游状态信息	原生风险	隐患
	8	终端漫游时，不能自动将各种审计报警日志上报至目的地服务器	原生风险	风险
	9	回到注册源服务器后，不能及时上报终端的漫游期间的违规行为	原生风险	风险

（a）相关资产生命周期

资产生命周期包含入网前、运行阶段、维修阶段、报废阶段，违规内联风险对终端的影响在资产生命周期的体现如下：

a）终端在行业内部不同单位之间漫游时，目的地服务器不能发现，并自动接管漫游终端的风险存在于资产生命周期的运行阶段，在运行阶段目的地服务器不能发现并接管漫游终端，则漫游终端无法通过流程自动获得入网，需要手工干预，影响效率。

b）目的地服务器不能预定义漫游组，并自动将漫游终端归入漫游组中的风险存在于资产生命周期的运行阶段，在运行阶段不能预定义漫游组并自动将漫游终端归入漫游组中则无法实现漫游终端的针对性管理。

c）目的地服务器不能针对漫游组预定义各种安全策略的风险存在于资产生命周期的运行阶段，在运行阶段没有针对漫游组预定义各种安全策略则不能针对性对漫游终端实现安全部署，从技术上支撑对于漫游终端的针对性管理。

d）源服务器对终端漫游数据下发错误导致漫游终端无法在目的地入网的风险，存在于资产生命周期的运行阶段，在运行阶段源服务器下发终端漫游数据时如果存在错误，可能导致终端无法在目的地网络由于漫游参数不匹配而无法入网使用。

e）漫游目的地服务器下发的漫游组安全策略弱于漫游终端在源网络中的安全策略的风险，存在于资产生命周期的运行阶段，在运行阶段终端漫游至目的地网络，由于目的地网络需要对漫游组统一进行管理，所有漫游终端按统一的安全部署进行管控，则在源网络中如果是比较重要的终端会导致漫游目的网络的安全管控措施低于源网络中的措施，对重要终端资产产生风险。

f）在所有服务器均启用 802.1X 认证的情况下，终端在漫游状态时，不能静默通过 802.1X 认证和接入网络的风险存在于资产生命周期的运行阶段，在运行阶段不能使漫游终端静默通过 802.1X 认证，则合法漫游终端无法获取网络资源入网使用。

g）终端所属源服务器不能获取到终端漫游信息的风险存在于资产生命周期的运行阶段，在运行阶段源服务器不能获得终端漫游信息，源服务器无法验证终端漫游申请的和目的地是否相符，无法检测终端随意漫游的行为。

h）终端漫游时，不能自动将各种审计报警日志上报至目的地服务器的风险存在于资产生命周期的运行阶段，在运行阶段如果漫游终端不能将各种审计告警日志上报至目的地服务

器，则目的地服务器无法对漫游终端造成的安全事件进行统一管理。

i）处于漫游状态的终端在回到注册源服务器后，不能及时上报终端的漫游期间的违规行为的风险存在于资产生命周期的运行阶段，在运行阶段源服务器不能掌握终端漫游期间的安全事件，无法追查终端可能信息外泄，以及进行相应处罚。

（b）相关信息风险

a）漫游目的地服务器下发的漫游组安全策略弱于漫游终端在源网络中的安全策略。终端漫游目的地的安全控制策略如果弱于终端在源网络中的安全策略，就会对漫游终端本地保存的信息产生威胁。

b）目的地服务器不能预定义漫游组，并自动将漫游终端归入漫游组中的风险。漫游终端作为非本地终端，其设备和人员管理必然难以做到本地终端本地人员相同的力度，这就存在比本地终端更大的信息外泄风险。针对在线业务信息漫游终端如没有定义特定组，并归入该组管理，就不能弥补漫游终端相应的管理弱点，可能造成在线信息的外泄。

c）目的地服务器不能针对漫游组预定义各种安全策略的风险。漫游终端归入特定群组管理，但是没有手段进行针对性的安全策略部署，则还是无法保证对漫游终端针对性的安全部署，容易造成在线信息的外泄。

d）处于漫游状态的终端，在回到注册源服务器后，不能及时上报终端的漫游期间的违规行为的风险。针对存储信息，漫游终端的违规行为如不能回到注册服务器后及时上报，源服务器就无法掌握漫游终端漫游期间的违规行为，无法对漫游终端本地保存的信息的外泄行为进行追查和处罚。

（c）基于资产使用人分析

按照资产使用人的定义，外部人员包括厂商运维人员和系统内外来人员，因此漫游管理类的风险只涉及外部人员。

（d）合规性要求

合规性要求见表 B-22。

表 B-22

序号	安全类	等级保护（三级）要求	符合程度
1		等级保护中没有明确的对漫游管理的要求	

相关技术和管理的风险管控措施参见以下小节阐述。

2．风险管控

（1）漫游入网和管控（终端在行业内部不同单位之间漫游时，目的地服务器不能发现，并自动接管漫游终端；目的地服务器不能预定义漫游组，并自动将漫游终端归入漫游组中；目的地服务器不能针对漫游组预定义各种安全策略；源服务器对终端漫游数据下发错误导致漫游终端无法在目的地入网；漫游目的地服务器下发的漫游组安全策略弱于漫游终端在源网络中的安全策略）

事前处置：预定义漫游组，并定义漫游组的相关控制策略。

事中处置：

✓ 终端漫游前向归属地服务器提交漫游申请，归属地服务器下发相应的漫游数据

✓ 终端在漫游地入网时，会根据终端所携带的漫游数据调整相应准入策略

✓ 终端准入网络后，目的服务器按照预定义漫游组的安全规则，漫游终端按照漫游组

的安全规则进行防护

处置流程见图 B-34。

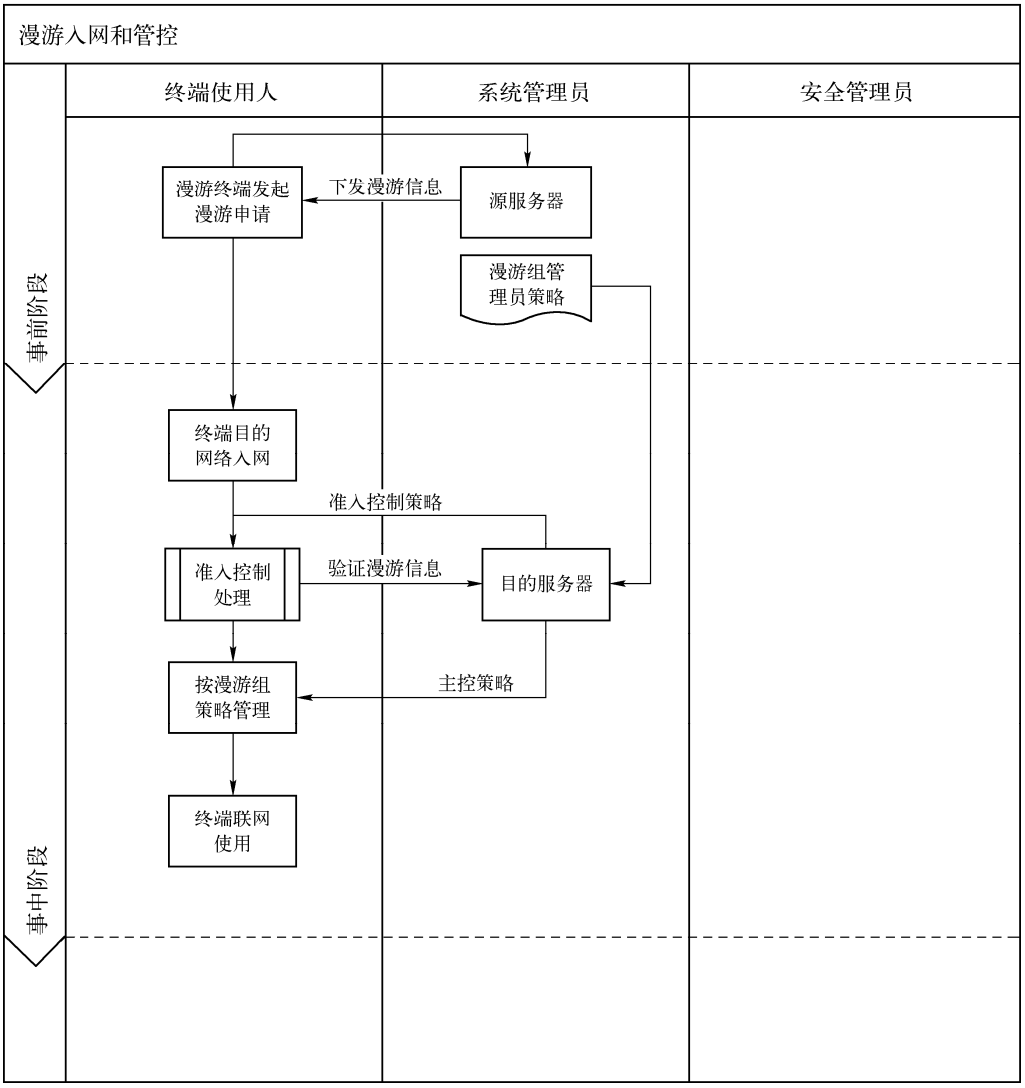

图 B-34

（2）在所有服务器均启用 802.1X 认证的情况下，终端在漫游状态时，不能静默通过 802.1X 认证和接入网络

事中处置：

✓ 漫游终端向目的地服务器上报漫游信息

✓ 目的地服务器和网管系统接口，由网管系统控制网络设备打开漫游终端的逻辑端口限制

✓ 漫游终端静默通过 802.1X 认证

（3）漫游信息上报（终端所属源服务器不能获取到终端漫游状态信息；终端漫游时，不能自动将各种审计报警日志上报至目的地服务器；回到注册源服务器后，不能及时上报终端

的漫游期间的违规行为）

事中处置：

✓ 漫游终端入网提交漫游信息，目的地服务器将漫游信息发送至源服务器

✓ 漫游终端联网使用后产生告警信息和审计日志上报至目的地服务器

✓ 终端返回归属地后将本地存储的告警信息和审计日志上报至源服务器

✓ 对漫游终端产生的告警和审计日志进行风险分析

事后处置：根据对漫游终端的风险分析，源服务器和目的服务器分别调整针对漫游管理的安全策略。根据源服务器接收的告警和审计日志对漫游终端在漫游期间的违规行为进行处罚。

处置流程见图 B-35。

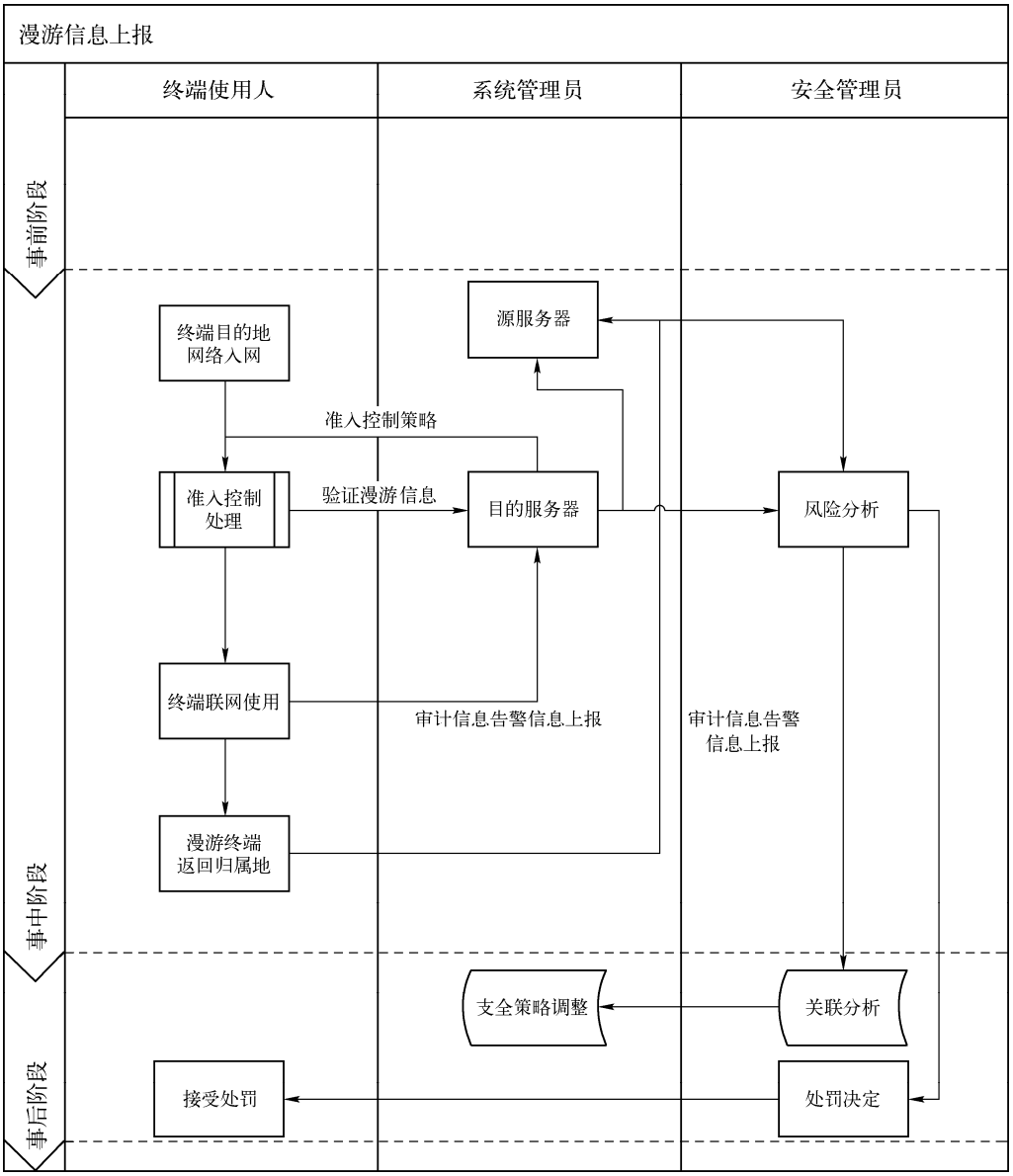

图 B-35

（4）系统不能发现和解决的终端安全风险和对策

漫游终端在漫游目的地的安全管控措施可能弱于漫游终端在归属网络中的管控措施。如果漫游终端在归属地属于重要终端资产，终端中保存了重要的信息，则漫游终端在归属地必然会依照严格的管控措施进行管控。当漫游终端在漫游目的地入网时，则需要接受漫游目的地对漫游组的统一策略管理。由于归属地对漫游目的地的管控平台没有控制权，所以可能造成归属地的重要终端资产没有按照原有的强度进行管控，给归属地的信息资产带来威胁。这就需要漫游归属地和目的地的系统管理员进行协调，针对重要的终端资产进行特别保护。

3．风险控制效果

通过漫游管理的管控实现终端有效的漫游入网管理，保证针对性地实施管理策略，保证对漫游终端的针对性管控部署，对漫游终端产生的告警和审计记录有效的分别向漫游目的地服务器和漫游归属地服务器上报，并由目的服务器和源服务器配合进行监管。

附录 C　终端安全信息风险

终端信息安全风险（IR：Information Risk）为终端中存储的信息，以及信息在传递过程中所面临的风险。该类风险包括传输过程风险、信息共享风险、介质存储风险以及加密使用风险，详见图 C-1。

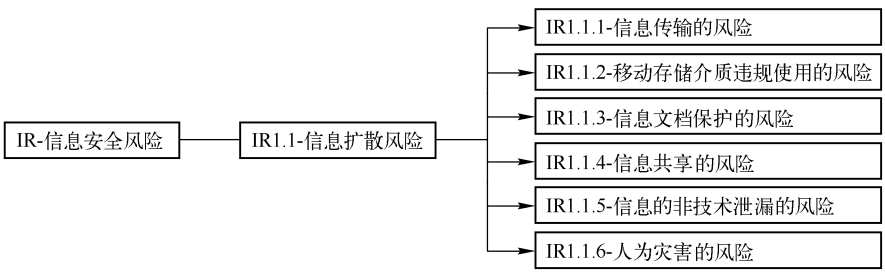

图 C-1**错误!**

C.1　信息扩散风险

C.1.1　信息传输（8 个风险点）

1．风险分析

（1）风险描述

信息传输的风险体现为内网终端由于需要处理生产办公任务，所以存在着大量的重要信息，而且根据业务需要，这些重要信息在内网中传输流转的方式也是各种各样，文件传输的不可控、不可审计引发一系列问题：

1）邮件发送的不可控、不可审计导致重要文件通过邮件方式不受控流转，产生扩散，且管理人员对扩散的情况不可知。

2）打印行为的不可控、不可审计，导致重要文件通过打印方式扩散或外泄，且管理人员对扩散和外泄的情况不能掌握。

3）内网终端中存在国家秘密信息，严重违反国家相应法律法规，由此可能产生泄密事件。

（2）相关风险点

信息传输的风险点详见表 C-1。

表 C-1

	序号	风险点	风险属性	隐患/风险
信息传输	1	不能对发送邮件行为进行控制	原生风险	隐患
	2	不能对发送邮件行为进行审计	原生风险	隐患
	3	邮件发送行为的控制导致某些内容不违规邮件无法发送	次生风险	风险
	4	不能对打印管理	原生风险	隐患
	5	不限定终端只能在指定的打印机上打印文件	原生风险	隐患
	6	不审计终端的打印行为（包括终端属性、打印时间、打印文件、份数、打印机等）	原生风险	隐患
	7	终端通过传输文件带来的安全风险	原生风险	隐患
	7	终端（包括移动存储设备）上存在国家秘密级或以上密级的文件的安全风险	原生风险	风险
	8	存在国家秘密文件的终端未按提示删除相应涉密文件	残余风险	风险

（a）相关资产生命周期

资产生命周期包含入网前、运行阶段、维修阶段、报废阶段，信息传输风险对终端的影响在资产生命周期的体现如下：

a）不具有发送邮件行为控制和审计的风险存在于资产生命周期的入网前、运行阶段、维修阶段和废弃阶段，在各阶段不能对终端发送邮件进行控制和审计，造成信息可能通过邮件方式外泄，且不具备审计记录无法对外泄行为进行追查。其中入网前和报废阶段由于终端尚未保存重要信息或重要信息按报废规定被删除，所以邮件发送造成的信息风险较低，运行阶段终端保存的重要信息较多导致的信息风险较高，维修阶段终端使用者非终端所有者终端储存的信息通过邮件发送外泄的信息风险最高。

b）不能对打印管理和审计的风险存在于资产生命周期的入网前、运行阶段、维修阶段和废弃阶段，在各阶段不能对打印进行管理，导致信息终端可能通过打印方式造成信息扩散和信息外泄且不能对通过打印输出造成的信息外泄进行追查。其中入网前和报废阶段由于终端尚未保存重要信息或重要信息按报废规定被删除，所以打印造成的信息风险较低，运行阶段终端保存的重要信息较多导致的信息风险较高，维修阶段，终端使用者或非终端使用者，都有可能把终端储存的信息通过邮件发送等方式外泄，这种情况的信息风险最高。

c）未经过授权的终端（包括移动存储设备)上存在国家秘密级或以上密级的文件的安全风险存在于资产生命周期的各个阶段，在各个阶段均严重违反国家法律法规，属于泄密事件。

（b）相关信息风险

a）不具有发送邮件行为控制和审计的风险。对于存储信息，不具有邮件行为控制和审计造成终端本地存储信息可能通过邮件的方式扩散，且无法对扩散行为进行追查。

b）不能对打印管理的风险对于业务的影响在于终端可能通过打印造成业务信息

外泄。针对存储信息，不能对打印进行管理和审计的风险，可能造成存储信息通过打印输出的方式外泄且无法对外泄行为进行追查。对在线业务信息的风险可以通过业务系统的打印功能进行控制。

（c）基于资产使用人分析

a）不具有发送邮件行为控制和审计的风险涉及内部人员、临时人员和经过入网处理的外部人员，内部人员、临时人员和外部人员由于其终端上存储的信息重要程度不同，需要在邮件控制和审计方面采用不同的部署策略。

b）不能对打印管理的风险。打印输出由于有独立的物理介质（打印纸）且易携带，不容易进行人工管理控制，因此需要严格进行打印管理，对内部人员、临时人员和外部人员需要采用不同策略，针对性管理，比如禁止临时人员、外部人员打印等。

c）不限定终端只能在指定的打印机上打印文件的风险。限定终端打印只能在指定打印机上打印文件涉及内部人员、临时人员和外部人员，针对不同人员采用不同策略，例如针对临时人员和外部人员要严格集中控制所使用的打印机，内部人员可在一定范围内选择。

d）不审计终端的打印行为（包括终端属性、打印时间、打印文件、份数、打印机等）的风险。对于打印行为的审计涉及内部人员、临时人员和外部人员，对所有人员的打印行为均需要进行审计，进行信息外泄后的追溯。

e）终端中存在国家秘密信息的风险。对于各类人员，使用的终端均属于非涉密终端，终端中存在国家秘密信息均属于泄密事件，所以对于各类人员均需要严格控制。

（d）合规性要求

合规性要求见表 C-2。

表 C-2

序号	安全类	等级保护（三级）要求	符合程度
1		等级保护中没有明确的对信息传输的要求	

相关技术和管理的风险管控措施参见以下小节阐述。

2．风险管控

（1）邮件发送控制（不能对发送邮件行为进行控制；不能对发送邮件行为进行审计；邮件发送行为的控制导致某些内容未违规邮件无法发送）

事前处置：制定邮件管理制度，定义邮件控制的关键字。

事中处置：

✓ 根据邮件管控策略对邮件进行关键字检查。通过关键字检查的允许邮件发送

✓ 未通过关键字检查的邮件被拦截，同时产生告警

✓ 拦截的邮件产生安全日志，并由管理员发送邮件被拦截的提示给发件人

✓ 成功发送的邮件进行审计记录

✓ 针对邮件拦截情况告警和日志进行风险分析

事后处置：对邮件管理的结果进行关联分析，调整邮件管理策略。

处置流程见图 C-2。

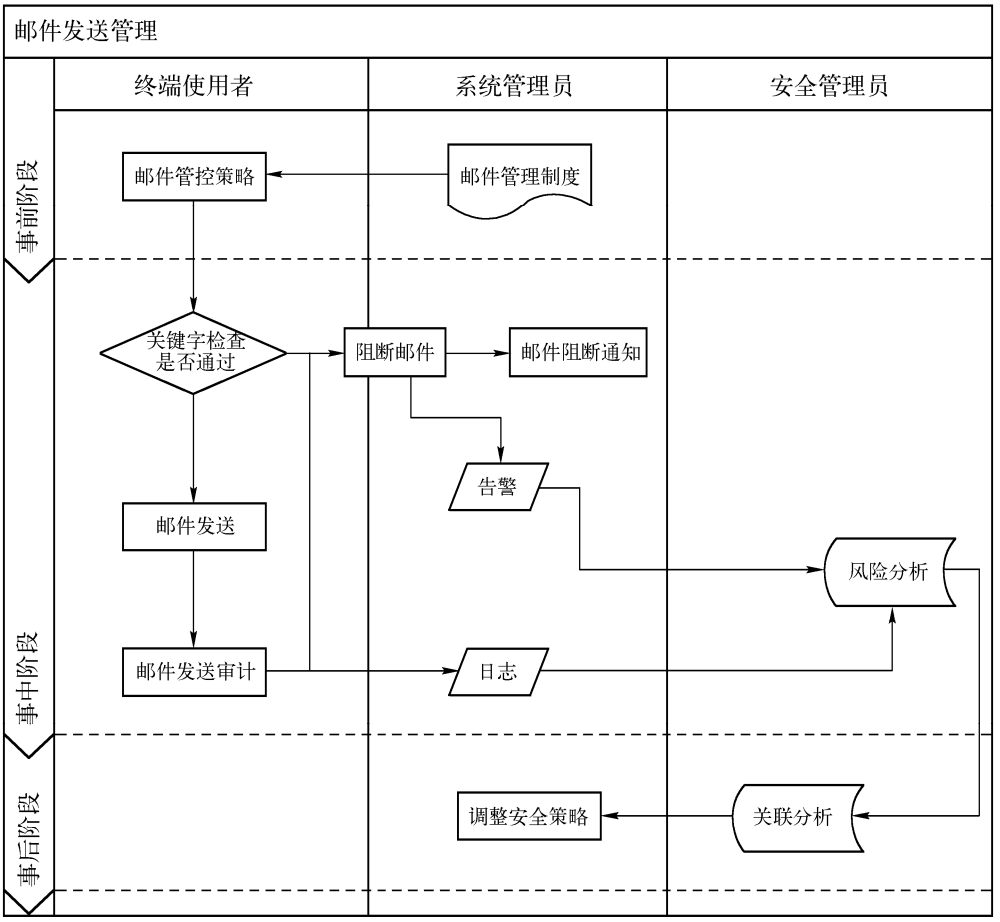

图 C-2

（2）打印管理（不能对打印管理；不限定终端只能在指定的打印机上打印文件；不审计终端的打印行为（包括终端属性、打印时间、打印文件、份数、打印机等））

事前处置：制定打印管理制度，规定人员的打印权限和对应的指定打印机。

事中处置：

✓ 检测用户是否具有打印权限

✓ 检测用户是否在指定打印时间打印

✓ 检测用户是否在指定打印机上打印

✓ 上述检测未通过则丢弃打印任务，并产生告警

✓ 逐项检测通过执行打印任务

✓ 对打印信息进行审计记录

✓ 根据打印告警和审计信息进行风险分析

事后处置：对打印管理的结果进行关联分析，调整打印管理策略。

处置流程见图 C-3。

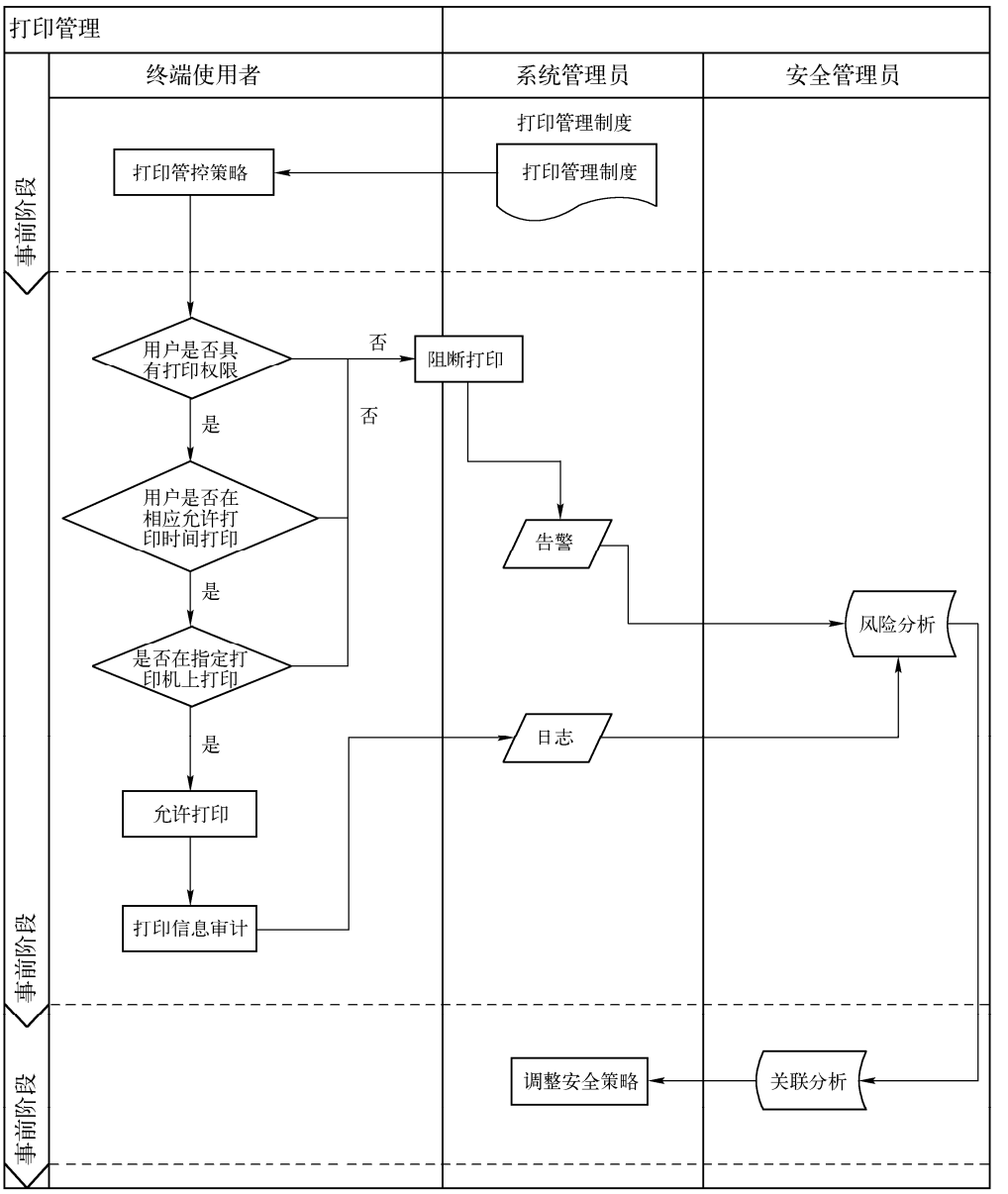

图 C-3

（3）涉密文件管理（终端上存在国家秘密级或以上密级的文件的安全风险；存在国家秘密文件的终端未按提示删除相应涉密文件）

事前处置：指定涉密信息管理制度，明确涉密信息范围和界定方式。

事中处置：

✓ 对终端进行周期性涉密信息的扫面检测

✓ 检查通过，则继续等待下一个周期的检查

✓ 检查未通过产生用户提示和告警

✓ 断开终端网络连接防止涉密信息进一步扩散

✓ 对涉密文件的使用记录进行审计记录

事后处置：根据涉密信息的告警情况对相应人员进行行政处罚，并且人工对涉及终端进行检查，检查终端中的涉密信息是否被清除，并对终端的存储介质进行相应处理。

处置流程见图 C-4。

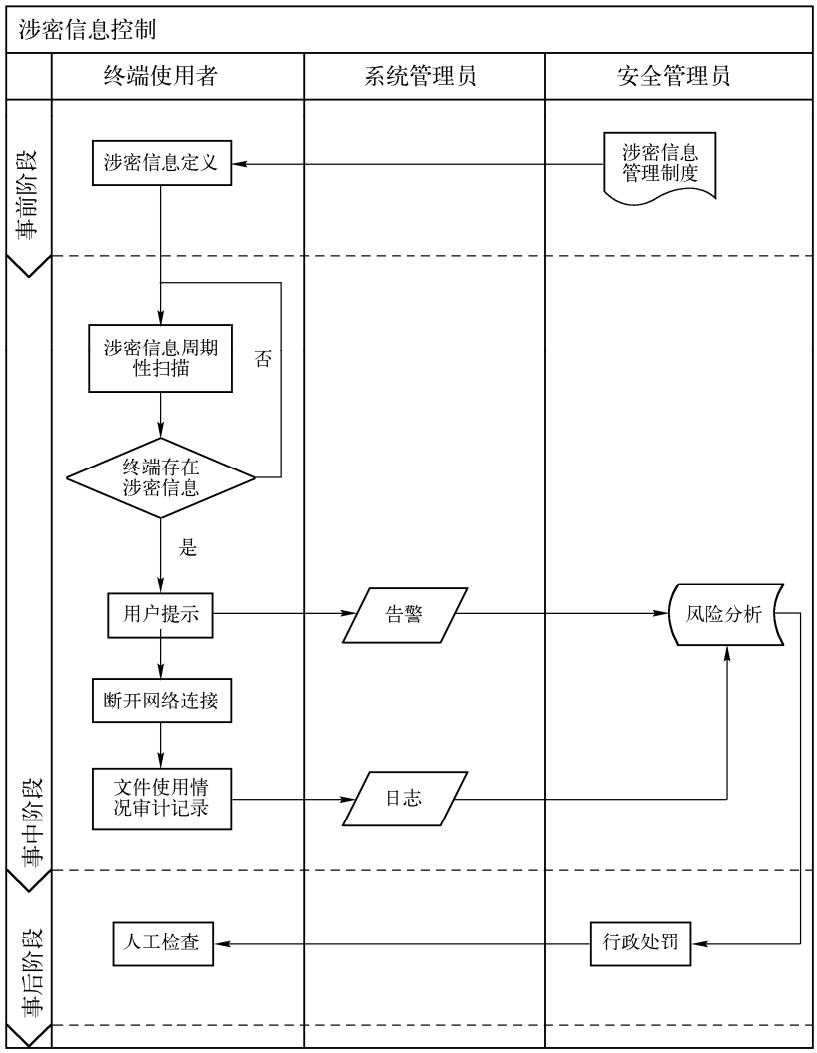

图 C-4

（4）系统不能发现和解决的终端安全风险和对策

对于终端上存在高密级文件的风险，如果高密级文件没有进行密级标示，从技术手段就无法进行检测，需要结合保密管理制度，通过技术手段为涉密文件添加不可篡改的密级标示，作为涉密文件的扫描检查依据。发现终端存在涉密信息后，对用户进行提示，但是控制平台无法直接对终端中的文件进行清楚，就需要借助人工手段验证文件是否被清除，并对涉及终端的存储介质进行进一步处理。

3．风险控制效果

根据对信息传输的管控实现了对人员的打印行为进行管理，实现对打印通过制定打印

机进行的控制，对邮件进行监控限制对于重要信息的邮件发送，对涉密文件进行扫描，监控内网终端/存储介质保存涉密文件的问题。并对上述行为均实现审计记录，实现对重要信息外泄和涉密信息泄密的追查。

C.1.2 移动存储介质违规使用（15 个风险点）

1．风险分析

（1）风险描述

该类风险主要表现为，因移动存储介质缺少申请、注册、审批、授权、报废等全生命周期的管理制度、流程和技术监控，造成移动存储介质的无序管理，由此将引发一系列问题：

1）外部移动存储进入内网使用，引发信息泄密、病毒感染等安全风险。

2）内部移动存储介质，虽然做到一定程度管理，但是无法从技术层面对其使用人员、范围、动作、内容和时间等信息进行监控，造成内部移动存储介质的违规使用，发生移动存储介质引发的安全事件无法定责。

3）如果发现有违规使用的移动存储介质，管理平台不提示告警，并采取如禁止等控制措施，那所谓的按规定使用移动存储介质的管理规定就形同虚设，不能起到任何安全防护效果。

移动存储介质是目前进行信息交换的重要方式，如果不对该部分的风险进行严格管理和控制，将会导致信息外泄、病毒感染，更有甚至将导致全网范围内的灾难性事件。下面将对其违规使用风险进行详细分解。

（2）相关风险点

移动存储介质违规使用详见表 C-3。

表 C-3

	序号	风险点	风险属性	隐患/风险
移动存储介质违规使用	1	移动存储介质没有进行资产登记管理对移动存储介质缺乏管理	原生风险	隐患
	2	U 盘没有进行单独注册和授权	原生风险	隐患
	3	移动存储介质没有进行安全等级划分	原生风险	隐患
	4	光盘介质使用没有进行禁止、限制范围的管理	原生风险	隐患
	5	移动存储介质格式化，授权信息被更改	原生风险	风险
	6	移动存储介质被重新分区，授权信息被更改	原生风险	风险
	7	移动存储介质授权信息被更改，没有报警提示和禁止	原生风险	风险
	8	外部移动存储，传输外部信息进内网的风险	原生风险	风险
	9	外部信息使用内部移动介质，没有进行安全检查	原生风险	隐患
	10	采用控制措施后，外部移动介质使用，没有报警、提示和禁止	残余风险	风险
	11	新增内网使用的移动存储介质，管理流程，无法确定其生命周期中的使用情况	原生风险	隐患
	12	新增申请流程不明确，造成移动介质滥用的潜在风险	次生风险	隐患
	13	新增设备，授权过程不明确，造成新设备无法识别	次生风险	风险
	14	缺少记录移动存储介质的申请-审批-授权的全过程。（包括授权人、授权使用范围、被授权人以及授权清除等记录）	原生风险	隐患
	15	有关移动存储介质申请-审批-授权审计信息，缺少安全措施，造成篡改和擦除	原生风险	隐患

（a）基于资产使用生命周期分析

资产使用生命周期包含入网前、运行阶段、维修阶段、报废阶段，移动存储介质风险对终端的影响在资产使用生命周期中的体现如下：

风险点（1-3）：移动存储介质属于组织重要的存储介质，从采购、使用、维修到报废都应该具有较为完善的流程管理，以确保移动存储介质的可控使用。因此，移动存储介质的管理风险将涉及终端使用生命周期：入网前、运行阶段、维修阶段、废弃阶段。在上述 4 个阶段中，移动介质的登记、配置初始化（安全等级划分、授权等）是移动存储介质实现可控管理的基础，因此在入网前阶段如果没有进行，将会带来很大的风险；在运行阶段，如果禁止使用非法移动介质的话，将不会带来更大的风险，如果没有做好控制措施，将会带来移动存储介质的滥用。

风险点（4）：光盘的使用发生在运行阶段。通过刻录光盘可以造成信息泄密，如果不对其进行禁止和监控，将会造成重要文件的泄密。如果全部禁止也会造成工作的不便，因此可根据用户环境，进行终端类型划分，确定禁止的范围，不禁止的也必须进行监控和记录，便于日后追踪。

风险点（5-7）：关于移动存储介质被格式化和分区，而导致的相关风险，主要发生在移动存储介质运行阶段和维修阶段。在使用阶段，移动存储介质违规进行格式化和分区的，技术上无提示和禁止措施，造成安全策略执行不到位，有可能造成注册、授权等工作重复进行；更有甚者如果格式化分区后还能够正常使用，将会造成更大安全风险。在维修阶段，必要的格式化和重新分区是不可避免的，为降低风险，维修之前应进行敏感信息处理，如果因故障无法做到，若存有重要信息，必须对维修过程进行全程的监控，避免造成信息泄漏。做到上述两点，在维修阶段所造成的安全风险将会大大降低。

风险点（8-10）：该风险主要出现在外部信息通过移动存储介质向内网导入的过程中。上述行为发生在运行阶段。外部移动存储介质为非注册授权类介质，健康状态不可控，存储内容不可知，如果私自接入内网，将会引起较大的安全风险。规定内部能够直接使用外部移动存储介质的区域，在使用之前要进行安全扫描，确保符合规定的安全状态，在使用时进行监控和记录；在其他区域，如果使用外部移动存储介质，技术平台必须做到提示、报警和禁止，否则将会给内网带来极大的安全隐患。

风险点（11-13）：新增移动存储介质，为组织的重要存储资产，其管理应符合组织的移动管理安全策略。因此与（1-3）设备管理内容一致，因此，涉及生命周期包括入网阶段、运行阶段、维修阶段、废弃阶段。

风险点（14-15）：该风险为全生命周期内移动存储介质管理审计轨迹风险，因此涉及移动存储介质的全生命周期：入网前、运行阶段、维修阶段、废弃阶段。在整个管理过程中，对各个环节进行记录和监控，并将信息进行集中存储，便于日后的审计和追查，否则，无法明确各流程是按规定进行，不能确保各岗位是否有渎职行为。

（b）与相关信息安全相关

风险点（1-4）：移动存储介质包括 U 盘、光盘等设备，属于当前最主流的移动存储设备，因其方便、廉价的优势受到广泛的应用，几乎任何从事与计算机操作相关工作的人员，均可能使用该类设备，该类设备可以存储任何形式的数据信息。

在线信息风险：由于在移动存储介质使用过程中，常常利用 USB 介质参与主机服务器

身份认证，信息移动存储设备向业务主机服务器上传下载数据等，典型应用如货运发票系统需对税控 U 盘进行读取和写入信息。档案管理系统也需要使用专用的 USBKey 等。因此必须根据业务系统的需要，考虑在线下载和上传数据的过程中可能带来的安全隐患。

存储信息风险：对于 U 盘中存储的信息，简而言之，根据信息管理，要有标签分类。涉密信息不应该出现在不受控制的 U 盘中，涉密信息应该指定专盘专用，设置指定到人保管。任何非授权下载、非授权拥有、非指定 U 盘出现涉密信息都是不应该的！要求被明令禁止。

风险点（5-7）：

在线信息风险：使用授权移动存储设备的终端，为重点终端设备，使用这类终端的业务系统应为重要业务系统。根据税务行业为例，其中税收管理信息系统、契税、耕地占用税管理软件、货运发票系统、公文处理系统、单位财务处理系统为重要的业务系统。因此，涉及上述业务系统的终端通过 U 盘在使用过程中要避免 U 盘被格式化、不受控制地下载信息导致不能审计、无法追溯的风险。

存储信息风险：如果 U 盘需要重新分配，在格式化和重新分区时要彻底，U 盘信息要保证不能被恢复，授权信息变更后要履行变更流程和重新入网登记。

风险点（8-10）：

在线信息风险：根据税务行业为例，信息传输路径分析，涉及外来数据信导入的系统主要包括：税收管理信息系统、契税、耕地占用税管理软件、货运发票系统。该类风险主要是 U 盘在导入导出信息过程中可能携带病毒、木马程序，可能将外部风险导入到内网中，造成业务主机感染病毒、木马，占用带宽等。另外接入内网的 U 盘同样存在利用该 U 盘上传下载非授权的涉密信息，比如下载个人税收信息、个人资料、企业秘密资料等。因此应采用严格的管理措施，例如禁止端口滥用，非指定 U 盘不能入网等，还可采用技术工具封闭端口的控制措施，达到预防该风险的目的。

存储信息风险：如果存储在移动存储介质中的信息涉密，保管人对信息要负责，严格按照涉密信息管理办法，不能随意将涉密信息复制到普通 U 盘，更不能将涉密信息复制到终端，和随意传播！对该信息要加密保存。

风险点（11-15）：

在线信息风险和存储信息风险同样适用于新增移动存储介质，和风险点（1）移动存储介质风险保持一致，涉及业务系统信息风险也相同。14 和 15 风险点主要针对移动存储介质管理的审计轨迹问题，是对资产使用信息审计追踪，主要涉及审计信息的存储风险，与移动存储介质的风险不相关。

（c）基于资产使用人分析

风险点（1-4）：任何岗位角色都涉及移动存储介质的使用问题，因此，该风险与内部人员相关：高级管理岗位，如区域负责人等高层领导；地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员；开发人员、研发人员等，考虑根据业务和工作需要授权开通端口和移动存储介质使用权限。

临时人员：辅助人员岗位，如食堂、车队、绿化等人员，该类人员在使用 U 盘过程中，可能会复制非涉及其岗位和授权文件的风险。

外来人员：外来厂家人员、外来维护人员不允许使用自带 U 盘，需要移动存储数据的必须有内部人员陪同，使用业务专用移动存储介质。同系统人员使用需使用系统内指定 U

盘，且必须经过登记检查，方可在服务器区域或者接入到业务中使用。

风险点（5-7）：

该风险涉及内部人员，使用授权终端的工作人员，具有两种特征：

a）具有一定行政职位，了解组织的重要信息。

b）具有业务职能，掌握和使用组织重要业务系统。

具备上述特点之一的工作人员均与该风险相关，包括高级管理岗位、地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员等。

严禁该类人员私自格式化移动存储设备。U 盘和人员挂钩，专盘专用，不得私自转借。U 盘归还入库重新分配要履行正常手续。

风险点（8-10）：

该风险涉及内部人员，必须严格要求，外部信息在通过移动存储介质接入到内网终端的时候，U 盘必须经过安全检测。

风险点（11-13）：与（1-4）移动存储介质相同

风险点（14-15）：根据资产管理的相关规定，资产的采购、使用和报废，会涉及管理层、工作人员、资产管理员角色等，因移动存储介质使用的广泛性，涉及的人员角色也非常广泛。必须根据工作需要、权限等分配领用，并要求执行有关移动存储介质使用规定。

（d）合规性要求

合规性要求见表 C-4。

表 C-4

序号	安全类	等级保护（三级）要求	符合程度
1	系统运维管理	7.2.5.3 介质管理（G3）： a) 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定 b) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理 c) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点 d) 应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁 e) 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同 f) 应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理	符合

2．风险管控

每类风险在管控过程中，针对风险的事前、事中和事后 3 种状态进行监控，做到事前预防、事中控制、事后审计追查。下面的风险管控处理流程，尽量从事前、事中和事后 3 方面对风险进行管控。

（1）风险点（1-4）移动存储介质管理控制流程

事前处置：根据组织的资产管理策略，制定相应的管理制度、流程、表单等相关文档，明确职责和分工，确定岗位责任。移动存储介质的申请、使用和报废将根据制定的流程进行

处理，并填写相应的表单以便责任追查。使用专门的工具标签化管理移动存储介质，区分不同的工作用途和使用者，限定不同标签的移动存储介质的使用范围，并且跟踪使用记录。

事中处置：参考相应文档指南，进行申请审批，不符合规定的审批将不予通过，并对处置事件进行记录，形成表单。

事后处置：根据资产管理规定进行资产管理介质管理的检查和抽查，或根据移动介质使用事实，对审批过程进行追溯。

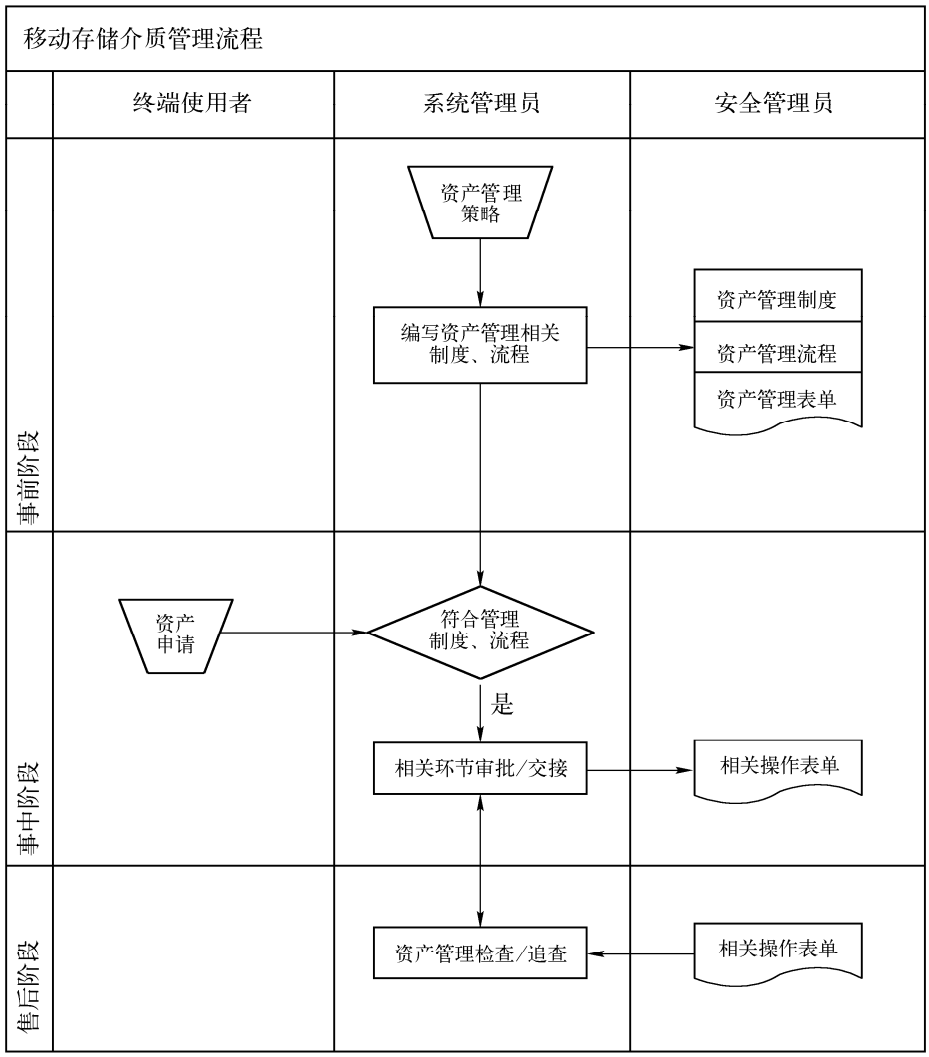

图 C-5

（2）风险点（5-7）格式化和重新分区时，授权信息被更改的风险

事前处置：可通过两种方式进行事前预防。

1）采购具有硬件保护的外设设备，授权信息保存在固定分区，该分区不能进行软件格式化。

2）通过注册设备对移动存储设备进行注册，并通过控制平台进行策略设置，不具有授

权信息的设备无法在系统内使用。

事中处置：

1）具有硬件保护的移动存储设备，将无法进行格式化。

2）通过注册方式的移动设备格式化后将无法在系统内使用。

同时，这两种格式化的企图和动作将记录在日志中，作为审计依据。

事后处置：根据监控平台的报警提示信息，对非授权的企图进行事件追查，其主要依据为系统日志信息。

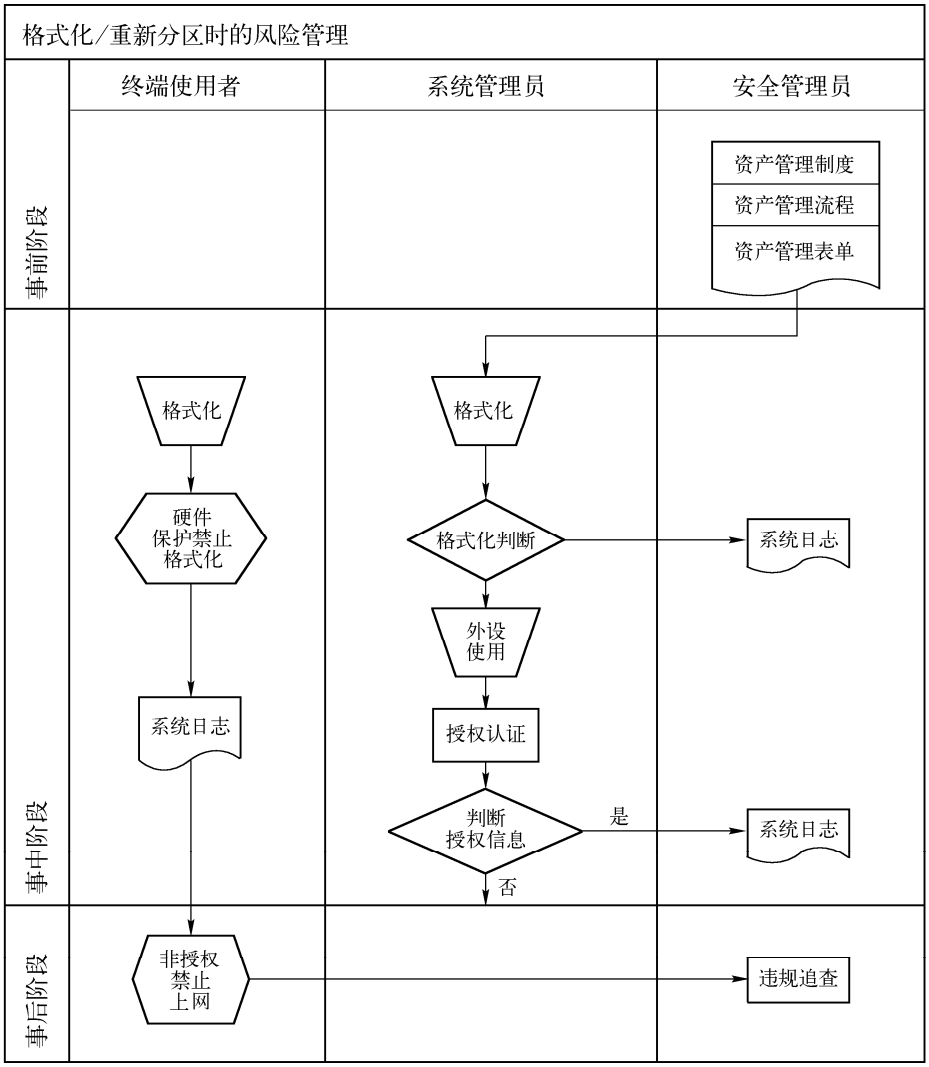

图　C-6

（3）风险点（8-10）外部信息通过移动存储传输进内网的风险

事前处置：根据组织的资产管理策略，制定相应的管理制度、流程对外部信息系统通过移动设备输入进行详细规定，并给出操作指南。对于未经授权的终端，禁止接入不知来源的移动存储介质。

事中处置：对外部信息复制严格遵守申请流程，对符合规定的在单机上进行安全扫描；入网时进行授权认证，并进行日志记录。如有工作需要，可以向部门主管和安全管理人员申请，获得批准之后，才能使用。

事后处置：根据监控平台的报警提示信息，对非授权的企图进行事件追查，其主要依据为系统日志信息。

管控流程见图 C-7。

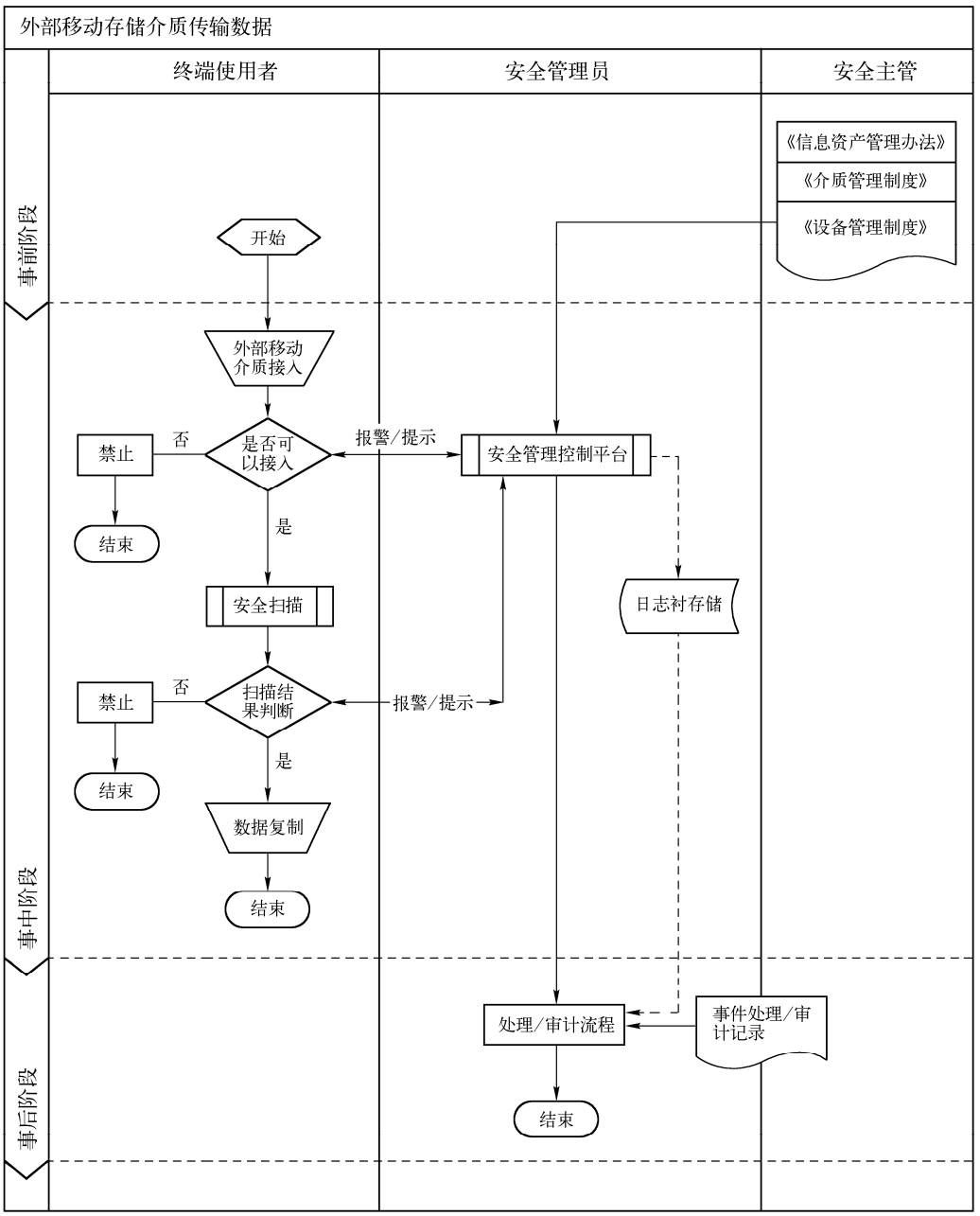

图 C-7

（4）风险点（11-13）与风险点（1-4）相同

同（1）管控流程。

风险点（14-15）：记录移动存储介质的申请–审批–授权的全过程

事前处置：根据组织的资产管理策略，制定相应的管理制度、流程对存储介质申请进行详细规定，并给出操作指南。

事中处置：事中根据制度、流程所制定的岗位职责进行审批，通过签名和数字签名确定岗位职责，并形成设备申请流程单。

事后处置：根据设备申请流程单，对使用的设备进行审批检查和追溯。

3．风险控制效果

实现移动存储介质的规范使用，注册移动存储介质只能在内网终端上使用，内网终端无法使用非注册移动存储介质，对注册移动存储介质可以设置口令访问，有数据交换需求的终端可以使用注册和非注册两种移动存储介质，但是对非注册的移动存储介质按照严格的读写权限控制使用。

对于移动存储介质所作的安全防护措施，仍不能避免违规使用，例如：

1）如果信息自身没有分级，则终端无法发现审核信息级别。

2）私自将终端存储设备带出，系统无法发现该违规行为。可以对重要信息加密，即使带出也可以保护重要文件无法打开。

残余风险处置措施如下：

1）需要对行业内信息分等级标识。

2）加强制度和意识培训。

3）移动存储介质分发需要根据业务需要和权限领用，需要人为参与判断。

移动存储介质的使用问题，除从技术角度进行监控外，更多的是管理问题，管理与组织的行政、资产管理等相关，因此，在技术实现上很难给出统一的实现，需要根据特定的管理环境和流程进行定制开发。

C.1.3 信息文档保护（5 个风险点）

1．风险分析

（1）风险描述

信息文档保护的相关风险表现为两类：

1）重要信息的存储风险。

2）重要信息的传输风险。

重要信息的存储风险主要表现为如果没有对使用的终端进行安全等级分类，重要文件存储在安全防护措施较低的终端上，将面信息泄漏的风险；对存储重要信息的终端没有制定相应的配置标准，造成安全防护等级不统一，同样也会使信息面临泄漏的风险。

重要信息的传输风险主要表现为信息存在两种形态存储和传输，传输有多种形式，比如从外网传输到内网，信息转换也可以看作传输的一种形态，在传输和使用过程中，如果没有适当的安全防护措施也将导致信息的外泄。

（2）相关风险点

信息文档保护风险点详见表 C–5。

表 C-5

	序号	风险描述	风险属性	隐患/风险
信息文档	1	重要文档没有加密存储	原生风险	隐患
	2	没有制定终端安全配置标准	原生风险	隐患
	3	存储重要文件的终端安全防护措施不达标，造成文件泄密	次生风险	风险
	4	重要文件的读、写、修改、传输等过程中出现信息泄漏的风险	原生风险	风险
	5	外来的重要文件进入内网，使其满足本地使用要求，过程中导致信息泄漏的风险	次生风险	风险

（a）基于资产使用生命周期

a）文档加密：终端在入网前不存储任何与业务有关的文档，在报废阶段也会进行存储设备的报废处理，因此与该风险相关的生命周期为运行阶段、维修阶段。

b）存有重要文件的终端进行模式化的管理：终端在入网前是不存储任何与业务有关的文档，在报废阶段也会进行存储设备的报废处理，因此与该风险相关的生命周期为运行阶段、维修阶段。

c）只允许在指定终端上存放重要文件，防止文件泄漏：该风险主要为管理控制类风险，涉及对指定终端的控制和文件的控制，主要存在于运行阶段，并涉及部分维修阶段，在重要设备转入到维护阶段时，必须进行事前的安全处理。所以，涉及的生命周期为运行阶段、维修阶段。

d）重要文件的读、写、修改、传输等过程中的信息泄漏风险：该风险主要存在于业务系统运行阶段，因此，针对于设备来讲与该风险相关的生命周期为运行阶段。

e）外来重要文件控制，使其满足本地使用要求，并防止信息泄漏：外来文件作为业务信息系统进行业务处理的一个重要信息来源，该过程仅发生在系统运行阶段，相对处理的终端设备也仅处于系统运行阶段。因此，与之相关的生命周期为运行阶段。

（b）与信息安全相关

a）文档加密：在线信息风险：在处理重要业务信息相关的文档时，会在终端进行解密，然后再进行处理，面临重要的文档信息在终端节点的明文泄漏的风险；存储信息风险：在终端内存储的敏感信息，因终端所处环境以及其灵活流动的特性，信息非法复制、信息非授权复原以及信息暴力破解等风险为信息的主要风险。

b）存有重要文件的终端进行模式化的管理：在线信息风险：在终端不进行模式化安全防护，造成重要业务在线处理信息没有统一的安全防护标准，造成各安全终端防护水平不均衡，容易造成安全防护弱点，面临终端攻击风险；存储信息风险：终端不进行模式化安全防护，使得终端存储信息环境复杂，管理困难，容易造成防护短板，无法在整体终端系统进行敏感信息的保护。

c）只能允许在指定终端上存放重要文件，防止文件泄漏：在线信息风险：在线敏感信息处理终端缺乏条件约束，造成敏感信息滥用，信息外泄风险加大；存储信息风险：存储敏感信息终端缺乏条件约束，造成敏感信息滥用，信息外泄风险加大。

d）重要文件的读、写、修改、传输等过程中的信息泄漏风险：在线信息风险：在线信息的读、写、修改等操作均在明文的基础上进行，容易造成信息的泄漏，传输过程不进行加

密传输容易造成信息被窃取、篡改等风险；存储信息风险：存储的重要文件的读、写、修改均在明文的基础上，通过终端监控软件及木马程序容易造成信息的泄漏。

e）外来重要文件控制，使其满足本地使用要求，并防止信息泄漏：在线信息风险：外来文件进入内网业务系统，不经过安全处理容易造成信息安全的破坏，如病毒带入、不符合加密规定，造成敏感信息的泄漏和篡改；存储信息风险：外来文件进入内网业务系统，不经过安全处理容易造成信息安全的破坏，如病毒带入、不符合加密规定，造成敏感信息的泄漏和篡改。

（c）基于资产使用人员

内部人员：当高级管理岗位（如高层领导）的终端资产存在以上风险，由于其终端含有企业核心信息和涉密信息，风险级别高；当部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员的终端存在以上风险，由于该类终端对业务支撑非常关键，且一般包含关键业务信息，风险级别较高；当生产人员、办公人员等终端存在该风险，尽管该类终端支持业务和对正常运营起保障作用，但因不涉及重要信息和关键业务，风险为中。

临时人员：如果该类风险发生在辅助人员岗位（如食堂、车队、绿化等人员），则该类终端一般不涉及业务、不包含敏感信息，风险为低。

外来人员：因外来人员不涉及组织内部信息和业务系统。此类人员终端发生该风险时，对于组织的影响很小，风险为低。

（d）合规性要求

合规性要求见表 C-6。

表 C-6

序号	安全类	等级保护（三级）要求	符合程度
1	数据安全及备份恢复	7.1.5.1 **数据完整性**（S3） a) 应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施 b) 应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施	符合

2. 风险管控

（1）文档加密

事前处置：根据组织的安全管理策略，制定信息安全分级分类标准，确定加密文档标准，制定文档加密配置指南，规定加密级别、加密算法，密钥管理规定等相关制度、流程和指南。

事中处置：针对符合政策标准的文档，进行加密处置，妥善保管密钥，并对文件处置过程进行日志、轨迹记录。

事后处置：根据处置日志和轨迹记录，对违规事件进行追查。

管控流程见图 C-8。

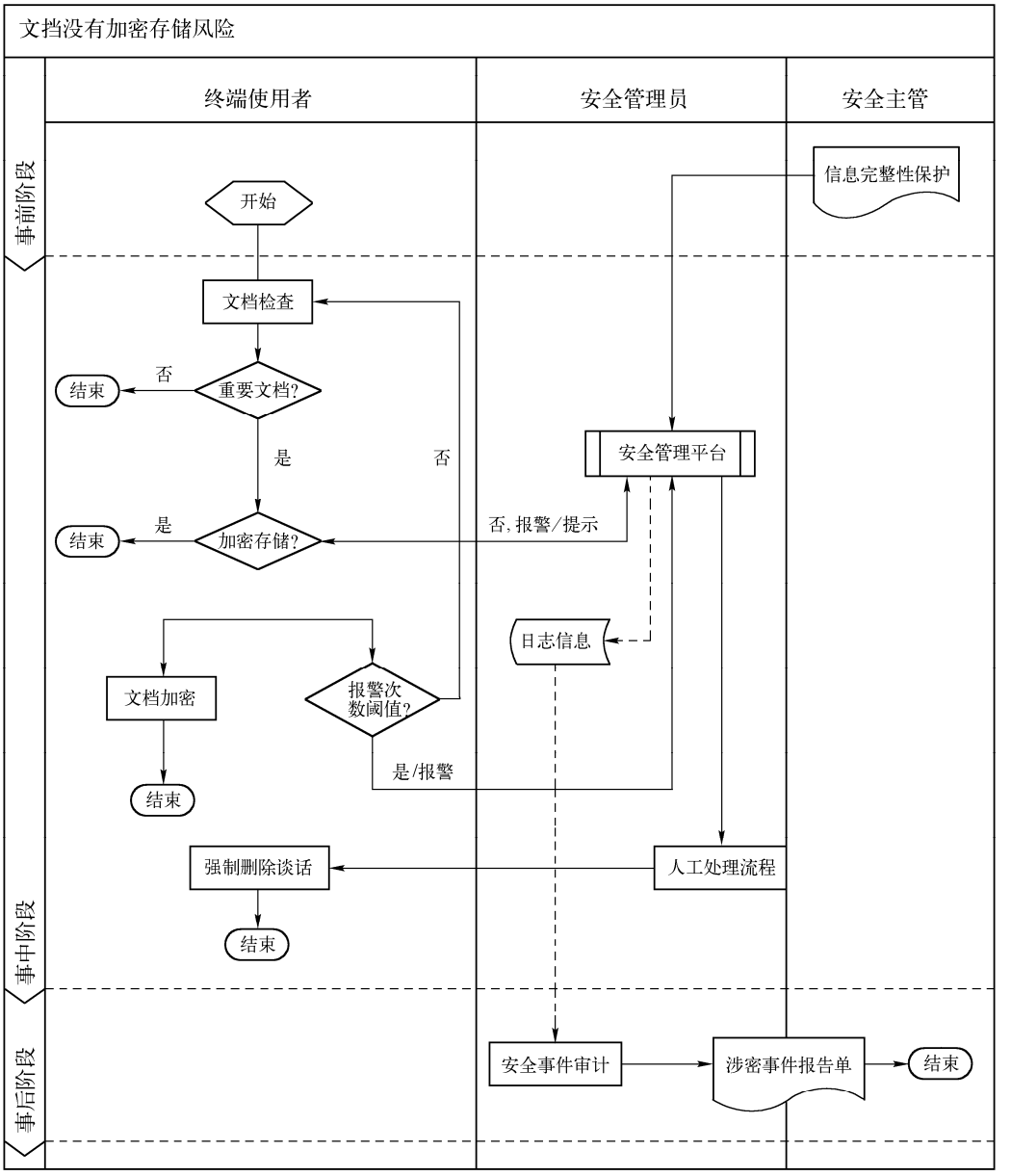

图 C-8

（2）存有重要文件的终端进行模式化的管理

事前处置：根据组织的安全管理策略，制定存有重要文件终端的安全防护标准，

确定技术控制措施、安全管理措施等内容。

事中处置：根据控制模型进行控制措施的实施，并对重要环节进行监控和记录，形成日志信息，以考证控制模式实现的符合度，确定各种控制措施的有效实施。

事后处置：根据处置日志和轨迹记录，对控制模型的有效性进行考察，并根据评价结果进行控制模式调整。

管控流程见图 C-9。

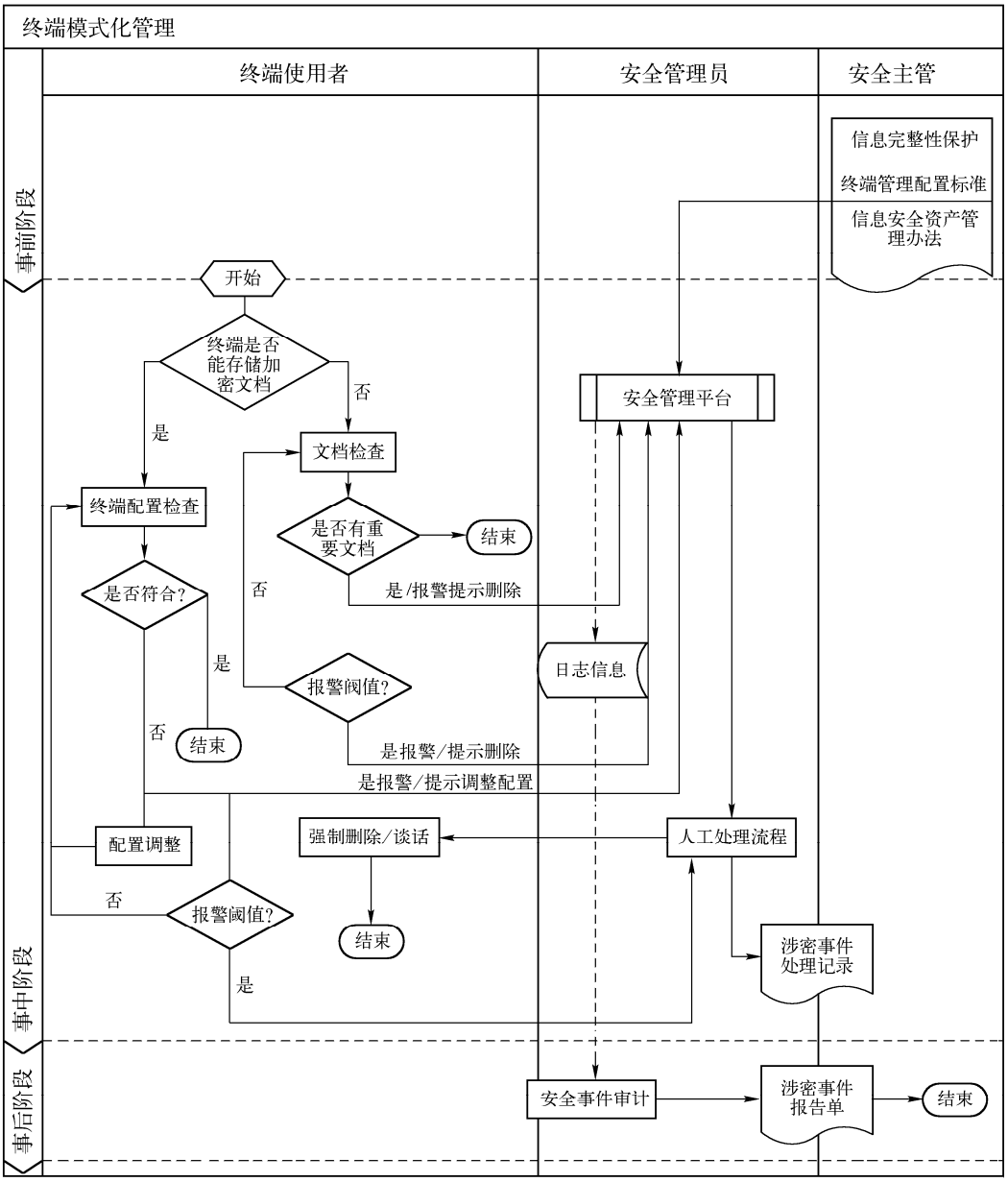

图 C-9

（3）只有允许在指定终端上放重要文件，防止文件泄漏

事前处置：根据组织的安全管理策略，制订存放重要文件的终端标准，可参考（2）中终端控制模式中的安全防护标准。

事中处置：对于重要文档的授权、监控和审计记录，在技术和管理双层进行控制；并根据重要文件存储记录单等相关记录信息，对所辖范围内定期实施技术扫描，防范重要文件的非正常存储。

事后处置：根据处置日志和轨迹记录，对重要文件的存储和访问进行审计和事件追踪。

控制流程图参见风险点 2 控制流程图。

（4）重要文件的读、写、修改、传输等过程中的信息泄漏风险

事前处置：根据组织的安全策略，制定文件分级分类标准，制定重要文件访问、处理安全标准和指南，确定文件访问授策略，根据授权策略进行访问授权。

事中处置：根据数据所有者或管理层批准的授权进行访问授权，如果文件传输，建议采用数据加密方式，为防止非授权的更改，需通过数字摘要签名的方式，确保传输文件的完整性。

事后处置：通过审批记录、日志记录、授权审批记录进行合规性审计和事后追查。

管控流程见图 C-10。

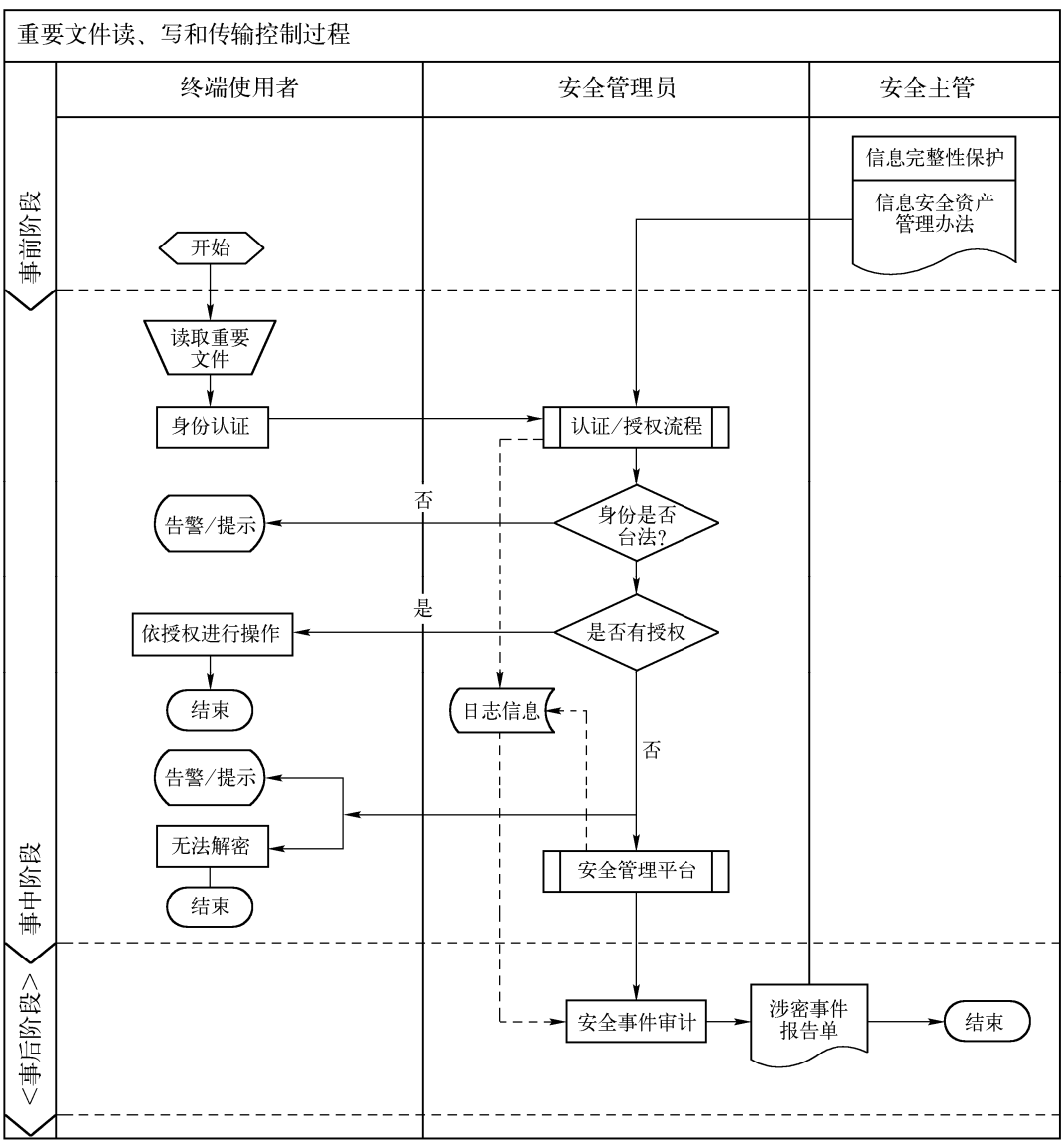

图 C-10

（5）外来重要文件控制，使其满足本地使用要求，并防止信息泄漏

事前处置：根据组织的安全策略，制订文件分级分类标准，制订外来重要文件访问、处理安全标准和指南，制订文件访问授权单，根据授权单进行访问授权。

事中处置：根据相关规定，由指定人员，指定方式进行外来重要文件接收和处置。外来重要文件以加密方式进行传输，根据正确密钥进行解密，确认数字签名，对比数字摘要，确保数据的机密性、完整性、可用性和抗抵赖性。接下来对文件进行安全扫描，排除安全隐患，根据重要文件存储规定进行文件入库。整个文件处理过程，需在重要节点进行审批和日志记录。

事后处置：通过处理流程记录、日志记录进行审计和事件追查。

管控流程见图 C-11。

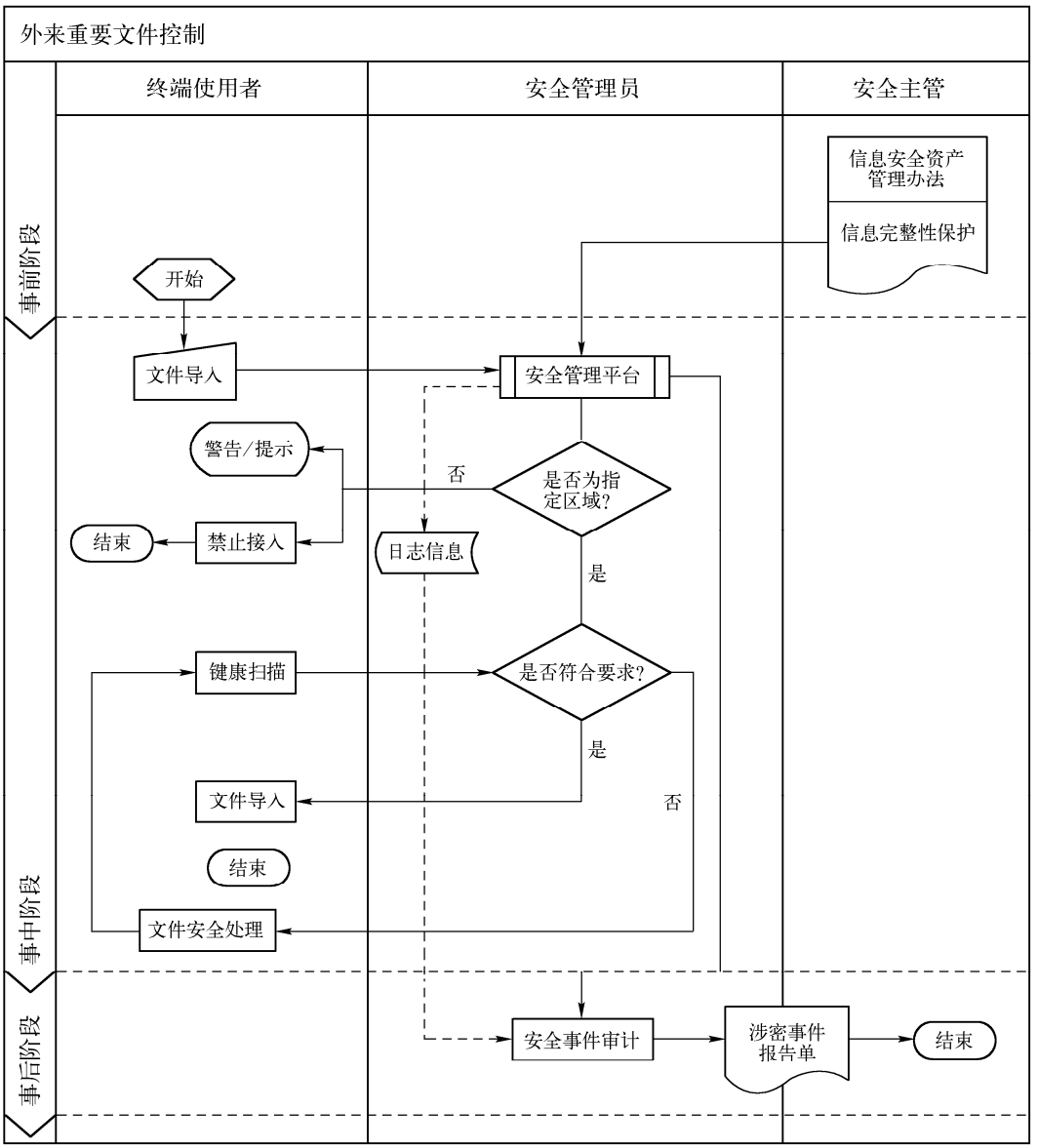

图 C-11

3．风险控制效果

实现对于重要文件的存储和传输进行加密，保证重要信息即使被非法获取也不能被解密读取，保证信息的保密性。

残余风险包括：如果信息自身没有分级，则终端无法发现审核信息级别，需要对行业内信息分等级标识。敏感信息接触者通过非技术类手段的泄漏，如拍照、摘抄、电话泄漏等，通过技术手段都无法做到监控。

处置对策：

1）长期的安全意识培训。

2）适当的人员监督机制。

3）严厉的惩罚措施。

4）保留事件调查、起诉的权利。

C.1.4 信息共享（3个风险点）

1．风险分析

（1）风险描述

信息共享风险在于系统共享的安全性较弱，不能有效地对信息共享实现监控，造成信息通过共享扩散风险。不能监控网络中的所有共享目录的情况，造成系统内共享行为不可控。不能监控审计终端通过共享目录复制文件的行为，造成通过共享可能发生的数据扩散情况不能有效监控。不能在发现网络中的共享目录后，关闭指定的共享，造成信息泛滥的风险。

（2）相关风险点

信息共享风险点见表C-7。

表 C-7

	序号	风险描述	风险属性	隐患/风险
信息共享	1	没有监控终端随意设置共享文件的情况	原生风险	隐患
	2	没有对终端共享情况进行审计	原生风险	隐患
	3	不能及时关闭共享	原生风险	隐患

（a）基于资产使用生命周期

上述 3 个风险为关联性风险，全部与共享有关。信息共享风险主要涉及资产的运行阶段，在运行阶段终端存在大量重要信息，系统共享的安全性较弱，没有有效共享控制，信息通过共享方式扩散，风险较大。

（b）与信息安全相关

在线信息风险：信息共享容易造成信息滥用，从而导致敏感信息外泄。

存储信息风险：信息共享容易造成信息滥用，从而导致敏感信息外泄。

（c）基于资产使用人员：

因该类风险相关的业务系统一致，推导出涉及的工作人员岗位和角色将会一致，涉及的工作人员包括：

a）高级管理岗位，如区域负责人等高层领导。

b）地市部门主管、网络管理员、配置管理员、系统管理员、财务部人员等关键岗位业务人员。

c）维护厂商、临时工作人员等。

上述相关人员根据级别和岗位职责，相关的安全风险级别不同。

（d）合规性要求

合规性要求见表 C-8。

表 C-8

序号	安全类	等级保护（三级）要求	符合程度
1	系统运维管理	7.2.5.9 密码管理（G3） 应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品	符合
2	系统运维管理	7.2.5.7 系统安全管理（G3） a) 应根据业务需求和系统安全分析确定系统的访问控制策略	符合

2．风险管控

上述 3 个风险，分别针对共享的整体风险进行了细化，因此，风险管控上存在极大的相关性，因此在这里建议采用统一管控措施，具体流程如下所示：

关于共享风险管控措施描述如下所示：

事前处置：制定相关管理制度，规定是否允许共享，允许共享的内容等。

事中处置：

1）通过对共享的扫描发现共享，设置共享策略，允许或禁用共享。

2）对共享目录的文件操作进行审计记录。

3）可以通过管理员手工关闭共享。

4）可以禁用系统共享功能。

事后处置：对于该类风险，主要保存扫描结果日志，在发生信息扩散事件之后，可以通过对日志的分析时追查责任人。

控制流程见图 C-12。

3．风险控制效果

有效监控共享行为，可以对共享的文件进行详细审计，并可实现管理员关闭指定共享和禁用系统共享功能，避免因共享造成的信息滥用。

如果信息自身没有分级，则终端无法发现审核信息级别，需要对行业内信息分等级标识。敏感信息接触者通过非技术类手段的泄漏，如拍照、摘抄、电话泄漏等，通过技术手段都无法做到监控。可通过管理手段进行管理和控制，处置对策如下所示：

1）长期的安全意识培训。

2）适当的人员监督机制。

3）严厉的惩罚措施。

4）保留事件调查、起诉的权利。

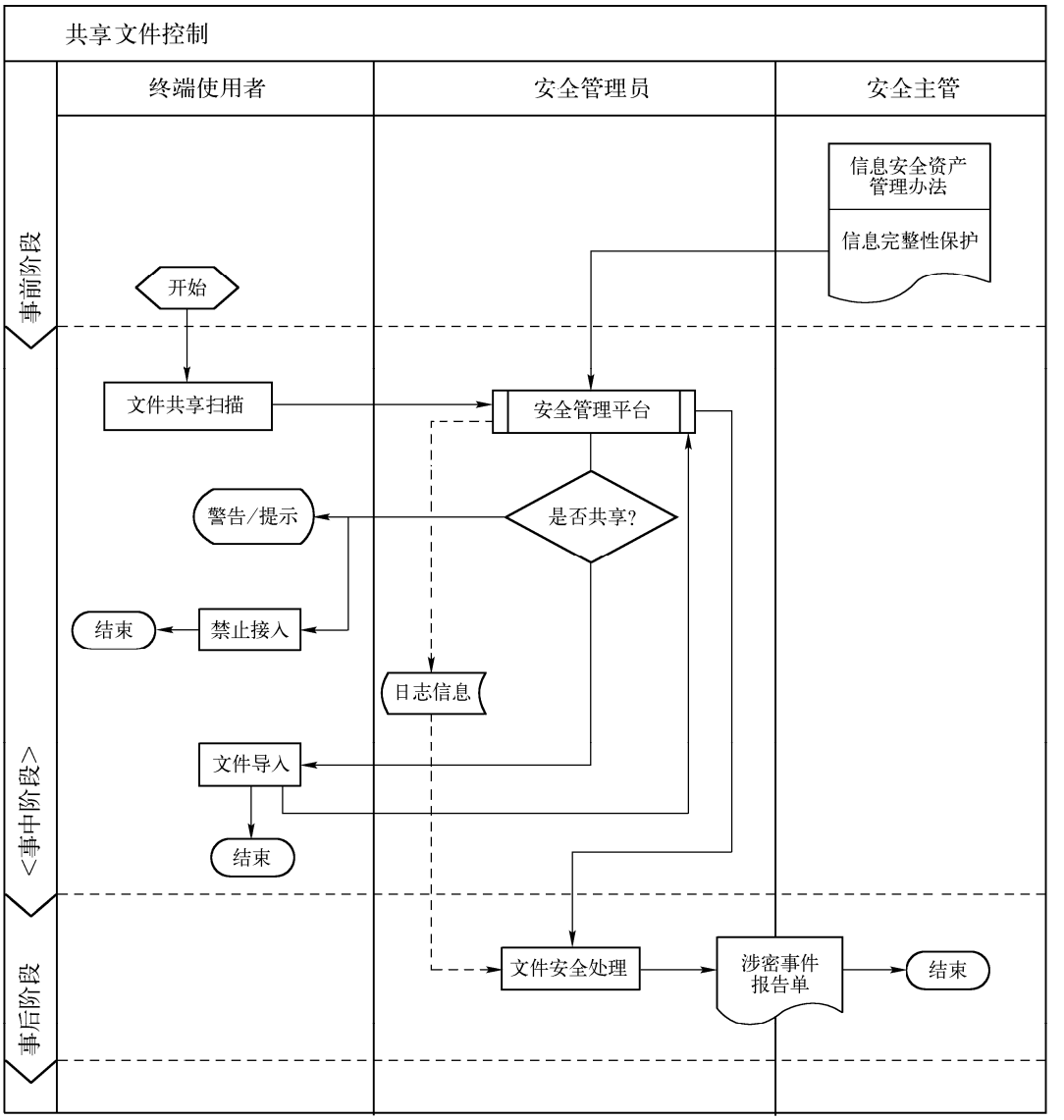

图 C-12

C.1.5 信息的非技术性泄漏（7 个风险点）

1. 风险分析

（1）风险描述

该类风险主要表现为社会工程类信息泄密，技术控制措施再严格，也不能抵御通过社会工程类的攻击，比如偷看、心理推测、搭线窃听等等。通过上述方式造成的信息窃取，难以发现和监控，造成安全事件很难追查，造成的安全损失也可能是不可挽回的，所以要引起组织的极大关注。

（2）相关风险点

信息的非技术性泄漏风险点详见表 C-9。

表 C-9

	序号	风险点	风险属性	隐患/风险
信息硬拷贝	1	不能禁止用户携带照相设备	原生风险	隐患
	2	不能禁止用户对终端显示信息进行记录	原生风险	隐患
	3	重要应用系统截屏，造成信息泄漏	原生风险	隐患
	4	屏幕电磁泄漏，造成信息泄漏	原生风险	隐患
	5	采用信号干扰措施，造成正常的无线通信故障	次生风险	风险
	6	物理线路上的电磁窃听，造成信息泄漏	原生风险	隐患
	7	采用视频监控，仍存在死角，不可避免非技术类的信息泄密	残余风险	隐患

（a）相关资产生命周期：

风险点（1-5）：

这 5 个风险点主要为通过使用终端设备，通过显示器显示的方式造成的信息泄漏。在资产生命周期 4 个阶段中，运行阶段、维修阶段和废弃阶段都有可能会涉及终端的使用，通过显示器都可能造成信息的泄漏，都会带来相应的安全风险。运行阶段，是资产生命周期中最为重要的阶段，该阶段用户存储和浏览的信息量很大，相关重要信息数量较多，因此所面临的风险级别较高。在维修和报废阶段，原则上应该进行脱密处理后，才能从运行阶段转入该阶段，这时面临的安全风险将会大幅下降；但在维修和废弃阶段，因信息处理不及时，造成的隐私、机密信息泄漏的案例比比皆是，造成很大的影响，因此，必须重视这两个阶段的安全防护问题。

风险点（6-7）：

这两个风险点主要是在终端使用过程中造成的信息泄漏，与用户的工作环境息息相关，因此，主要涉及运行阶段，该阶段的风险级别比其他阶段的风险级别高。

（b）相关信息风险

上述所涉及的信息，为屏幕显示信息和网络传输信息，均为使用中的信息，而非存储类信息，风险级别有所处理的信息类型而定。

（c）基于资产使用人分析

对于终端用户、内部人员、外部人员和临时人员都存在不同程度的风险。

（d）合规性要求

合规性要求见表 C-10。

表 C-10

序号	安全类	等级保护（三级）要求	符合程度
1	通信保密性	7.1.4.6 通信保密性 a）在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证； b）在对通信过程中整个报文或会话过程进行加密	符合
2	人员录用	7.2.3.1 人员录用 c）应签署保密协议 d）应对内部人员中选拔从事关键岗位的人员，并签署岗位安全协议	符合
3	外部人员访问管理	7.2.3.5 外部人员访问管理（G3） a）应确保在外部人员访问受控区域前提出书面申请，批准后由专人全程陪同或监督，并登记备案。 b）对外部人员允许访问的区域、系统、设备、信息等内容应进行书面规定，并按照规定执行。	符合

（续）

序号	安全类	等级保护（三级）要求	符合程度
4	环境管理	7.2.5.1 环境管理（G3） c）应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定 d）应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室立即交还该办公钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机推出登录状态和桌面上没有包含敏感信息的纸档文件等。	符合
5	电磁防护	7.1.1.10 电磁防护 c）应对关键设备和磁介质实施电磁屏蔽	符合

2．风险管控

上述风险因为其社会学的特点，因此很难通过信息技术去解决，具体的控制措施如下所示：

（1）事前处置

1）制定相关的管理制度，明确针对具有拍照、摄像、录音等功能的设备的使用规定，如相机、手机、摄像机、录音设备等。

2）对物理环境的安全监控进行明确规定，在重要区域进行视频监控。

3）制定人员的安全意识培训计划，提高全员安全防范意识。

4）制定参观来访规定，明确规定参观访问方式。

5）制定应用系统开发标准，明确规定重要应用系统不能通过截屏获得信息。

6）制定电磁辐射标准，明确使用电磁干扰的时间和场所。

（2）事中处置

1）通过门卫或设备严格检查带入办公区的设备，避免视频、照相设备带入，如有带入，及时劝阻。

2）对于截屏行为，在应用服务器端通过代码加以控制。

3）重要区域进行视频监控，确保抄写、照相等行为能够记录。

4）第三方参观人员参观时专人陪同，避免疏忽造成的信息泄漏。

（3）事后处置

如果仍然出现通过上述途径造成信息泄漏，可通过出入记录、视频记录进行事后追查。

3．风险控制效果

通过上述方式，在事前、事中和事后采取相应的安全管理控制措施，能够起到一定的防护效果。但是在实际工作中，还是存在很大的不确定性，尤其是使用人员的操作等方面，因此，在员工安全意识、职业素养培训上组织应该给予足够的重视。

C.1.6 人为灾害（3 个风险点）

1．风险分析

（1）风险描述

终端设备是信息系统中使用最为广泛和频繁的信息节点，具有使用灵活、人员众多、暴

露性较强等特点。因为与人接触较多，人的行为对设备的安全将会造成很大影响，因人为因素造成的设备损坏和丢失的情况极易发生。

（2）相关风险点

人为灾害风险点详见表 C-11。

表 C-11

	序号	风 险 点	风险属性	隐患/风险
人为灾害	1	关机状态下，拆除硬盘	原生风险	隐患
	2	人为造成的设备损坏，如淋水、明火、磕碰等	原生风险	隐患
	3	人为造成设备盗窃、丢失	原生风险	隐患

（a）相关资产生命周期

上述 3 个风险在资产生命周期的 4 个阶段都会有所涉及，只是其造成影响不同。在设备的使用阶段，如果人为的损坏和丢失，因其正处于服役期，内部存储和处理的信息相对较为重要，如果一旦损坏和丢失将会造成信息泄漏和工作中断等影响，因此风险级别较高。其他 3 阶段次之。

（b）相关信息风险

相关的信息主要为存储在设备中的信息。

（c）基于资产使用人分析

无论内部人员、外部人员还是第三方人员都可能面临上述问题，因此所处级别和岗位的不同，将面临不同级别的安全级别。

（d）合规性要求

合规性要求见表 C-12。

表 C-12

序号	安全类	等级保护（三级）要求	符合程度
1	物理访问控制	7.1.1.2 物理访问控制 a）机房出入口应安排专人值守，控制、鉴别和记录进入人员 b）需进入机房的来访人员经过申请和审批流程，并限制和监控其活动范围 c）应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域 d）重要区域应配置电子门禁系统，控制、鉴别和记录进入人员	符合
2	数据保密性	7.1.5.2 数据保密性（G3） b）应采用加密或其他保护措施实现系统管理数据、鉴别数据和重要业务数据存储保密性	符合
3	备份和恢复	7.1.5.3 备份和恢复（G3） a）应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份文件刻录光盘存放	符合

2．风险管控

（1）事前处置

对设备的使用编制使用指南，避免因水、火等原因造成意外损害，确定设备带出的规范，尽量防止设备的丢失，不过一切应以保证人员的生命安全为前提。

（2）事中处置

当有安全事件发生时，根据情况，采取控制措施。

1）如有淋水现象，及时切断电源，迅速提交给 IT 部门进行处理。

2）如遇丢失、盗窃等，及时上报和报警。

（3）事后处置

事后处理，及时总结经验，降低事件发生概率。

3．风险控制效果

不可预测的人为灾害而造成设备损害是不可避免的，因此，对信息事前的备份以及加密存储等措施必不可少。

ISBN 978-7-111-37390-2
策　　划：丁 诚
封面设计：子时文化 ZiShi Culture

在线互动交流平台
官方微博：http://weibo.com/cmpjsj
豆 瓣 网：http://site.douban.com/139085/
读者信箱：cmp_itbook@163.com

终端安全风险管理

尽管人们已经认识到终端是网络中大部分行为的源头和起点，也是最终的端点，并且认识到终端安全是网络与信息安全管理的重要内容，因此采用了大量产品和技术解决所面临的终端安全问题，但终端仍旧屡屡发生“问题”。其原因在于现有产品的技术工具色彩浓厚，单一功能性强，整体性不足。本书作者在多年实践经验的基础上，提出终端安全管理的实质就是终端安全风险管理，并系统地阐述了管理的关键是“管理自动化”的观点。本书从实际出发，基于信息安全风险评估理论,介绍可识别和分析的终端安全风险，构建结构性的终端安全风险体系，基于管理自动化的原则，构建终端安全管理体系的方法。本书有助于读者摆脱终端安全管理工作中面向威胁被动防护的局面，构建更为有效的面向能力的终端安全主动防御体系。

本书特别适合用作信息安全、计算机、通信、电子工程等领域的科技人员的技术参考书，或作为相关专业的教材。

地址：北京市百万庄大街22号　　邮政编码：100037
电话服务　　网络服务
社服中心：(010)88361066　　门户网：http:www.cmpbook.com
销售一部：(010)68326294　　教材网：http:www.cmpedu.com
销售二部：(010)88379649　　封面无防伪标均为盗版
读者购书热线：(010)88379203

定价：52.00元

ISBN 978-7-111-37390-2