◆王光远◆时　现／主编

【内部审计前沿报告书系】

Global Technology Audit Guide

全球信息系统审计指南

（下）

●时　现●李庭燎／等译

中国时代经济出版社
China Modern Economic Publishing House

◆王光远◆时　现／主编

【内部审计前沿报告书系】

Global Technology Audit Guide

全球信息系统审计指南

（下）

●时　现●李庭燎／等译

中国时代经济出版社
China Modern Economic Publishing House

图书在版编目(CIP)数据

全球信息系统审计指南(下册)/时现,李庭燎等译.
—北京:中国时代经济出版社,2010.1
(内部审计前沿报告书系)
ISBN 978-7-5119-0077-7
Ⅰ.①全… Ⅱ.①时…②李… Ⅲ.①信息系统-审计-指南 Ⅳ.①F239.6-62
中国版本图书馆 CIP 数据核字(2009)第 232974 号

书　　名:全球信息系统审计指南(下册)
出 版 人:宋灵恩
作　　者:时现,李庭燎等
出版发行:中国时代经济出版社
社　　址:北京市西城区车公庄大街乙 5 号鸿儒大厦 B 座
邮政编码:100044
发行热线:(010)68320825　68320484
传　　真:(010)68320634
邮购热线:(010)88361317
网　　址:www.cmepub.com.cn
电子邮箱:zgsdjj@hotmail.com
经　　销:各地新华书店
印　　刷:北京市鑫海达印刷有限公司
开　　本:787×1092　1/16
字　　数:300 千字
印　　张:18
版　　次:2010 年 1 月第 1 版
印　　次:2010 年 1 月第 1 次印刷
书　　号:ISBN 978-7-5119-0077-7
定　　价:78.00 元(上、下册)

目　录

6

IT 薄弱点的管理与审计

作者
Sasha Romanosky，卡内基梅隆大学，公共行政管理学院
Gene Kim，Tripwire Inc. and IT Process Institute
Bridget Kravchenko，通用公司
2006 年 10 月

6.1 执行摘要

从责任的角度来看，信息技术管理和信息技术安全的责任是确保技术风险能被合理地掌控。这些风险在很多情况下来自于IT资产的发展和对IT资产的使用，例如配置系统的不正确或对受限制的软件进行访问。然而，人们是能够通过监测薄弱点或评估这些风险的潜在影响来识别和减轻它们的，且在必要时可以通过实施相应的措施来修正。

薄弱点管理是指一个被组织用来识别、评估并补救可能导致商业风险[①]或安全风险[②]的IT薄弱点（在IT资产或程序中的薄弱点）的过程和技术。从美国国家薄弱点数据库[③]来看，每年会有大约5000个新的薄弱点被发现，其中的40%有“很高的严重程度”（例如，他们会给组织造成重大破坏）。

也许读者会考虑为什么自己应该阅读一个薄弱点管理的指南？毕竟，自己不能够完全代表坐在组织的IT审计人员，不是吗？通常而言，IT相关风险的潜在影响会难以界定或容易被忽视，直到碰上某个蠕虫病毒，例如SQL Slammer病毒，将运行着的交易自动中止才引起人们的关注。在薄弱点管理的重要性层面上，如果能掌握有效的教育和告知高级管理层的方式和方法，将有助于推动支持措施的建立和并有助于采取行动。高级管理层必须理解有效的薄弱点管理程序，他们必须设计一套程序来检查、评估和减少薄弱点，并通过将这些任务不断地整合到一个完整的IT流程体系中来减少漏洞。

这些与薄弱点管理有关的问题本质上并不都是技术问题，事实上，这些困难中大多数都与激发员工个人和推动有效的流程有关。

本指南的制定是为了帮助首席审计执行官（CAE）在评估IT安全人员在薄弱点管理中的有效性时，提供一个正确的参考评判标准。它通过给出具体的管理做法来帮助组织实现并维持一个较高的有效性水平，并说明了高效和低效的薄弱点管理结果的不同之处。

在读过这个指南后，人们可以：

- 对薄弱点管理过程有一个全面的了解。

---

① 譬如说，由于财务报告的不完整以及生产经营的损失带来的风险。

② 譬如说，数据的机密性、完整性以及有用性遭受侵害的风险。

③ http://nvd.nist.gov.

- 有能力分辨高效和低效的薄弱点管理组织的区别。
- 熟悉典型的演化模式——从基于技术的方法到基于风险的方法，再到基于IT流程的方法。
- 针对薄弱点管理的最佳实践为IT管理提供有效的指南。
- 能够向所在组织的CIO、CISO、CEO、CFO提出更有效的建议。

IT薄弱点已经成为一种组织中非常常见的症状，它把网络完全暴露给黑客、病毒和蠕虫。事实上，在硬件和软件产品[①]中每天都能至少发现12个以上新的薄弱点。而其他类型的IT薄弱点还包括不够充分的密码管理、不适当的文件访问、弱密码以及应用程序的错误配置。因此，对于IT经理和IT安全专业人员来说，保持及时更新和为系统打上最新补丁程序已经成为一项不可间断的工作。然而，有一些方法则比这些方法更加有效。

6.2 介绍

6.2.1 如何识别脆弱的薄弱点管理

脆弱的薄弱点管理过程的六大特征如下：

- 在给定的一段时间内所发生的安全事件的数量高过了可接受数量[②]的水平。
- 无法系统地识别IT薄薄弱点，导致关键资产暴露。
- 无法根据每个薄薄弱点来评估风险，也不能采取薄弱点分级的行动。
- 由于IT管理层和IT安全部门之间工作关系不够融洽，导致无法控制和标识计算机资产的变化。
- 缺乏资产管理系统。
- 缺乏与减少薄弱点的工作相结合的配置管理过程。

6.2.2 改进薄弱点管理

能改进薄弱点管理流程的六个步骤：

- 根据组织对风险的承受能力来确认并纠正IT薄弱点，并获得高级管理层的支持。

---

① 来源：美国国家薄弱点数据库。

② 这个可接受的事件的数量可以通过将可容忍的损失和过去的损失相比较来衡量。然后，人们可以通过衡量控制工具的成本以及修补所有薄弱点的成本来考虑薄弱点管理。

- 获取所有 IT 资产及其薄弱点的完整清单。
- 根据业务风险来为纠正措施分级。
- 通过对 IT 管理提供计划的项目来纠正薄弱点。
- 不断对新的资产进行更新[①]、薄弱点测试和纠正过程。
- 尽可能在最大的范围内使用自动化的补丁管理和薄弱点发现技术。

6.2.3 内部审计师的作用

薄弱点管理已经成为一个高度优先的工作，因为 IT 控制已被认为是高于财务报告之上的内部控制结构的一部分，并要求遵守相关的法规，如美国 2002 年出台的萨班斯法案，美国联邦金融机构检查委员会（FFIEC）[②] 以及加拿大和日本的萨班斯法案的版本。因此，人们越来越需要 IT 管理为企业提供关键控制的服务。IT 管理和 IT 安全性对组织是否具有足够的安全控制且该安全控制能否有效运行而负责，从而满足内部控制和监管的需求。

内部审计人员对业务的很多方面提供指导。根据内部审计协会（The IIA）：

“内部审计人员应当评估针对过去攻击行为的各项预防、检查和缓解措施的有效性，从而合理估计未来的企图或者事件发生的可能性。内部审计人员也应当确定董事会（或董事）是否已经被告知了相关威胁，意外和对薄弱点被利用的情况，以及相应的补救措施。”

内部审计人员还应当为管理层遵守国内监管法规要求提供建议，以此来提高他们对于薄弱点可能产生影响的认识和关注。只有通过这种方式，内部审计师才能协助高级管理层确定企业可能的风险来源，从而避免因违反规章而引发的安全意外。特别值得一提的是，内部审计人员能够识别 IT 安全无法有效实施薄弱点管理的环节，并证实现有的薄弱点纠正措施的效果。

审计师通常会考虑这样一个问题：一个薄弱点审计的范围看起来应该是怎样的？表 1 就为审计师可考虑的活动范围提供了一个简要介绍。而下文对于各部分将进行更具体的介绍。

6.2.4 漏弱点管理如何驱动 IT 基础设施的变化

扫描和发现薄弱点而引发的风险评估过程，可能要求改变 IT 资产。随着薄弱点的不断扩散，成功执行从发现薄弱点到迅速修复薄弱点的这一过程，对于尽可能减少影响的范围来说是至关重要的。这就意味着对于薄弱点的管理必须结合组织的变化和补丁管理活动。

---

① 这将在 6.3 部分做讨论。

② http://www.ffiec.gov.

就如我们所讨论的，将IT资产进行重要性分级并执行变更通常是一项非常重大的挑战，但同时也有可行的方法，可用来判断是否已经具备了一套完全融入组织变更管理实践的有效的薄弱点管理过程。在GTAG2中我们充分讨论了管理流程的变更：变更和补丁管理控制。

表1 薄弱点管理审计范围

识别和确认	风险评估及风险分级	修复	维护和改进
资产清单 确保具有当前应用的所有IT系统的资产清单。 确保设别的IT系统已根据相应的业务风险进行了分组和优先级划分。 确保配置管理和变更管理的进程之间存在依赖关系。	**风险评估** 确定根据发现的薄弱点进行风险分配的标准。 确保该标准被整个组织使用。	**监控** 识别自动和手动进程的薄弱点。 一旦确定薄弱点未能及时修补则应制订应急计划。	**配置管理** 确保IT资产均保持在一种标准化的格式下，以协助追踪IT资产的逻辑因素和物理因素，如模型、应用程序的安装和补丁等。 确保变更管理和事件管理能与配置管理相结合。
薄弱点检查 确保使用自动化工具来扫描和检测网络及主机设备。 确保对IT资产实行定期扫描。 识别及时应用于薄弱点信息的资源。（例如，第三方，软件供应商，CERT）	**薄弱点分级** 根据系统的关键性和影响对分析重要性如何被量化。 确保业务影响也作为衡量优先权的因素之一。	**事件管理** 修复程序应贯穿于整个组织。 事件的影响和情况的紧急程度应和资产的业务风险相关联。 事件的指标，例如恢复原状的平均时间等应被明确界定或跟踪，以确保满足操作级别协议（OLAs）。	**操作级别协议** 查明操作级别协议是否就位，以确保薄弱点管理的及时性和进程的推进能被合理测量。
确认发现 确保某一程序能够查明误报及检查中的疏忽。 确保在本地环境中能够恰当地分析各薄弱点。	**变更管理** 分析某些变化是否能反映已确认的薄弱点。在实施补丁之前应该首先进行计划和测试。 由薄弱点引起的变化应该能尽可能地减少对业务引起的破坏。	**政策和要求** 确保各角色和其职责在识别、沟通和补救过程中能发挥作用。 确保各项政策和程序有助于各项战略和决策的制定。	**补丁测试** 明确如何有效地部署集中补丁来确保效率，即消除对同一个薄弱点所做的重复修补。 确保补丁通过病毒的测试和检查。 确保补丁在预生产环境下通过测试，以确保补丁不会生成意外风险或影响服务的问题。 识别自动和人工的补丁程序，以确保部署效率。

本节旨在为了说明：对于一项有效的薄弱点管理程序而言，只有关键的组成部分才是必需的。而我们可以在补丁和薄弱点管理程序中建立一个更具综合性的讨论。

表1显示了相关IT安全和IT操作功能之间的依存关系。而我们给出这份文件的目的更多考虑的是一个正在实施ITIL框架的组织的功能。

在这里，薄弱点管理的生命周期是从识别IT资产开始的，随后扫描并监控IT薄弱点。接下来通过验证薄弱点有关的数据来证实这些薄弱点是否确实存在。最后根据组织的风险程度将薄弱点分级。

关键的薄弱点通过事件管理程序来处理，它与使用应急管理程序的变更管理相协调。而非关键的薄弱点则能通过标准的变更管理程序审核。一旦获得批准，发布管理就会进行准备、测试并促进变化。接下来，变更管理会再次复查这些变化以确保变更满足了所有要求。最后，配置管理数据库会升级并反映这些改进后（例如，更安全）的修改。

需要注意的是，无论修补工作是否紧急，所有的变化都是由变更管理安排好的。它们扮演着通过IT机制推动变更并使变更成功完成的重要角色。

6.3 薄弱点管理的生命周期

6.3.1 识别与确认

划分系统范围

为了恰当地划分系统范围，审计人员应该获得一份在组织中运行的所有网络设备的清单，例如公司的有线和无线网络、生产网络、备份或管理网络、传输网络、实验室和测试网络以及移动办公软件。这其中的每一个网络都必须经过确认并记录在案。

这些网络同样应该包括在一个网络结构图中，这个图能像周边安全设备那样显示网络间的相互关联关系，例如路由器、防火墙和网络入侵检测系统。同时，这个结构图也能使管理者了解在一个网络中被发现的薄弱点是如何影响其他网络的资产的安全性的。

检查薄弱点

一旦得到了一个网络资产清单，那就应当对连接到每一个网络的IT资产都实施扫描或者定期监控薄弱点。这些资产设备包括商务应用服务器（例如数据库、电子邮件、网络和客户关系管理服务器）、安全设备、电信和网络设备以及打印机。