Information Security Risk Assessments
Research and Practice

信息安全风险评估
探索与实践

张建军　孟亚平　主编

中国标准出版社

Information Security Risk Assessments
Research and Practice

信息安全风险评估
探索与实践

张建军　孟亚平　主编

中国标准出版社

图书在版编目(CIP)数据

信息安全风险评估:探索与实践/张建军等主编.
北京:中国标准出版社,2005
ISBN 7-5066-3791-X

Ⅰ.信… Ⅱ.张… Ⅲ.信息系统-安全管理-风险分析 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2005)第 050841 号

中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码:100045
网址 www.bzcbs.com
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 787×1092 1/16 印张 13.5 字数 290 千字
2005 年 6 月第一版 2005 年 6 月第一次印刷
*
定价 30.00 元

信息安全风险评估
探索与实践

编委会名单

序

信息化建设在我国国民经济和社会进步方面已经发挥了巨大的推动作用，特别是近几年电子政务蓬勃发展，通过信息化手段，更好地保证了政府职能的顺利执行。电子政务从信息化的角度来看主要是四个方面，公文处理、业务处理、信息发布与公众服务，也可以说其主要业务从这几个角度就可以概括出来。从系统结构来看，首先建立一个网络基础设施，然后建立应用支撑层，最后是应用层的建设，通过公众服务网向政府、企业、社团、公民提供服务。其中，不论是基础设施，还是应用支撑层，抑或应用层，都涉及到电子信息的安全。

实施有效的信息安全管理，组织或者某一个政府机关需要根据国家有关法律、法规、方针政策以及有关信息安全的技术标准，对系统资源进行分析，对所规划建设的项目或运行系统所面临的风险进行评估。为此，提出整体安全要求、进行可实施的技术控制以及所需要为安全付出的代价的领导决策，按照决策进行实施，包括设计、施工、运行和检测；在实施过程

中，可以要求信息评测机构对运行系统或对完成的系统进行信息安全测评，根据测评系统提出改进的意见，形成新的安全策略，最后采取相应的措施对系统进行进一步改造和安全的提升。信息安全风险评估是信息安全管理过程中的一个重要步骤，是进行科学决策、实施有效信息安全管理的基础。

信息安全风险评估活动涉及到很多的专业知识，并且与实践结合非常紧密，是一项既需要专业理论又需要实际操作的工作。目前国内外有大量风险评估的理论性论著，但很欠缺操作性强的指导性书籍。风险评估活动的意义更多地在于实践，很高兴看到有这么一群年轻人，能够编制这么一本理论与实践相结合并且偏重于实践的书。这是一项非常具有探索性的工作，是理论联系实践活动中的一项非常重要的工作，对于信息化主体组织了解风险评估的目的、意义，明了其中的具体内容，指导实施信息安全风险评估活动具有比较高的参考价值。特别是在操作的层面，用一个实际案例展开对风险评估所涉及的各项活动的阐述，更加符合实际环境，对需要了解如何做信息安全风险评估的组织来说尤为值得借鉴。

作为一名长期从事信息化工作的人员，我曾经有机会和这些年轻人一起合作，对他们的工作有一些了解。我很高兴和他们在一起，我欣赏他们直面问题、勇于创新的精神；欣赏他们不断努力、务实工作的态度。在这个高速发展的信息化社会，我们更多地需要创造性的工作：不仅需要原创性的努力，还需要在不断实践的基础上主动地“扬弃”，解决我国信息化建设中的实际问题。

姚世全

2005 年 5 月 25 日

前言

随着信息化的进一步深入，政府机构、企事业单位等组织对信息技术的依赖性日益增强，信息系统已经成为组织适应环境变化、提高竞争力的重要依托，信息和组织中的信息系统就此成为组织的重要资产。与此同时，一旦发生信息泄漏、病毒侵袭、系统中断、发布信息被非法篡改以及自然灾害等非期望的事件，将对组织造成重大的影响。这些潜在的非期望的信息安全事件的影响也就是组织所面临的风险。

当前国际上采用风险管理的方法实现组织的信息安全管理，通过一系列有计划的活动，标识与分析信息安全风险、制定风险管理计划、实施风险控制工程，监视风险、控制风险，全面实现对风险的管理。作为风险管理的第一步，标识与分析风险、制定风险控制计划的风险评估工作是实现风险管理的基础，在风险管理中具有重要的地位。

从专业角度来看，风险评估涉及到信息安全专业技能，包括对信息资产的分析、威胁与脆弱点的识别、安全控制措施评估等工作。从这个角度上来说，风险评估是一项专业性很强的工作。从组织的角度来看，风险评估是一个科学的决策过程，包括收集数据、分析数据、提出方案、制定计划。组织实施风险管理应当与组织本身的目标保持一致，风险

评估应当能够充分反映出组织目标因素。从这个角度上来说，风险评估本身具有很强的主观性。因此，有价值的风险评估需要认识到其中的主观性作用，才能够保持与组织的目标一致，对于风险评估的探索与实践也就是围绕着这条主线展开的。

在探索与实践的过程中，我们已经积累了一些经验、有了一些心得，但同时还有许多有待进一步开展的工作，需要有更多的不同领域的人员合作进行。本书无意成为一本理论性的读物，在全书的正文中，我们提供的是一些相对比较成熟的理论和方法介绍，这些内容是基于理论的探索与实践相结合的产物。

风险评估应当以组织为主体，研究组织的目标与信息安全之间的关系；以满足组织目标为出发点，开展信息安全风险评估目标、方法以及工程实施的研究，这成为贯穿本书信息安全风险评估的主要思路。在本书中主要表现在以下几个部分：

1. 理念层面(什么是风险评估)。赞同风险管理的概念，从控制的角度阐述了信息安全与组织以及信息系统之间的关系，说明了风险评估的目的与意义。

2. 方法层面(风险评估做什么)。从组织的角度以业务为主线识别关键资产；按业务系统、支撑性平台、安全设施的方式进行分类；各分类分解为具体可管理的组件。以业务流程为主线展开对信息安全的风险评估，提出了一种以组织参与的方式实施风险定性量化评估的方法，确保与目标的一致。

3. 操作层面(怎样做风险评估)。以组织为核心的风险评估方法还体现在评估团队的组成方面。以具有管理背景的人员为主组建风险评估团队，负责需求的确认以及风险事件的影响量化评估。围绕业务系统，针对不同层次人员展开相应的获取技术信息与管理控制信息的活动，以及一种考虑操作层、管理层、决策层的业务依赖性分析方法，组织中管理与专业技术人员共同参与的对项目的评审活动，以及最终组织充分参与的安全策略选择方法。

在本书的最后，说明了有关风险分析方法前期探索的实践活动，提出普遍适用的风险评估方法需要满足横向对比与纵向对比要求的问题以及对风险评估方法进行评判的因素(如效率、可观测性，可重复性)，供今后进一步探索与思考。

信息安全风险评估不仅是信息安全专业技术的问题，更是管理的问题。本书作为引玉之砖，期望有更多的人能够参与到其中来。

编　者

2005 年 5 月

信息安全风险评估
探索与实践

目录

什么是风险评估？

导读 在这个日新月异的时代，信息技术在组织中的角色已经越来越重要，随之而来的信息安全问题对组织的影响也越来越大，主要表现为信息的保密性、完整性、可用性的丧失，从而引起组织的利益、声誉受到损失。

对于组织来说，处理信息安全问题是一个综合管理的问题，是一项涉及整个组织范围的工作。针对信息安全问题的潜在性、不确定性的特点，借鉴传统质量管理 PDCA 循环的思想，国际上目前普遍采用风险管理的方法应对信息安全问题。从系统理论来看，风险管理蕴涵着丰富的控制论思想。

风险评估是风险管理的重要阶段，通过标识、分析风险，制定风险控制计划，为随后的风险管理活动提供方向。风险评估贯穿在信息系统生命周期的各个阶段，发挥着不同的作用。

在国际上风险评估已经经过了初级阶段、成熟阶段进入了全球合作的阶段。目前系统性评估模型与方法的研究一直是其中的热点。

风险评估可由不同的主体实施，对组织来说有着不同的优点与缺点。组织的风险评估还可以选择不同的范围，满足特定的要求。

从组织的角度来看，风险评估是实施风险管理中的计划阶段，是一个明确目标、科学决策的过程。

第1章 信息安全与风险管理

1.1 信息安全问题

我们正处于一个巨大的变革时代，环境的变化使各类组织，无论是商业组织，还是政府机构、社会团体都面临前所未有的新挑战——变化。面对外部环境的压力，组织必须采用现代管理模式和可行的管理手段，全面提升综合实力（商业组织的竞争力、政府的执政能力、社会团体的服务能力等）。而信息技术（IT，Information Technology）在推动流程改进、提高环境反应速度、降低成本和提高效率等方面的重要性，已获得广泛的认同。随着信息技术的广泛深入应用，对于组织来说，信息以及作为其支持过程的系统和网络已经成为组织生存与发展所依赖的重要资产。

与此同时，目前任何组织及其信息系统和网络都可能面临着包括欺诈、刺探、阴谋破坏、火灾、水灾等大范围的安全威胁。随着信息技术的日益发展和普及，计算机病毒、计算机盗窃、服务器的非法入侵破坏已变得日益普遍和复杂。这些威胁因素将可能产生诸如国家或商业秘密泄漏、业务中断、信誉受损等一系列的恶性后果。目前一些组织，特别是一些较大型组织的业务已经完全依赖信息系统进行业务管理，这意味着这些组织受到安全威胁的破坏影响更大。同时组织内网络的互连及信息资源的共享增大了实现事件控制的难度。在将信息系统作为重要资产的今天，信息安全已成为组织普遍面临的一个重要问题，需要认真对待。

从信息的角度来看，各类信息安全事件最终将导致信息的机密性丧失（信息被非授权访问的人访问）、完整性破坏（信息及处理方法的准确性和完备性丧失）或可用性丧失（已授权用户在需要时无法获取到信息）。对于组织来说，信息安全也就是应对与处置这些可能发生的信息的机密性、完整性、可用性丧失造成的对组织影响的问题。

1.2 信息安全管理

从组织的角度来看，信息安全问题是一个综合管理的问题，特别对于一些业务对信息技术依赖性强、信息技术应用范围大的组织。信息安

全问题涉及面广(法律法规、业务、软件、主机、网络、基础设施、环境、操作人员、开发人员……),专业技术性比较强(系统加固、系统备份、异常监控、日志分析、应急处理……)。信息安全问题需要协调组织内不同的层面(决策层、管理层、操作层),不同的业务部门(支持保障部门、IT 部门……),以及内外部的技术资源(专业技术人员、供应商、服务商),运用各种技术设施(防火墙、入侵检测、审计、备份),才能够进行有效的应对与处置。

1.2.1 风险管理的提出

对于组织来说,安全管理投入要求得到最大的回报,这些回报包括业务连续运行、组织的利益、声誉得到保护、符合国家的法律法规。由于环境、技术、人员中各类不确定因素的存在,不可避免对信息的安全使用产生影响,最终损害组织的利益。并且由于这些影响是潜在的并且有很大的不确定性,不恰当的管理方式将可能造成资源的过度投入,造成资源浪费,或保护不当使组织蒙受经济与声誉的损失。

借鉴传统行业风险控制的经验(保险、化工、电厂……),结合 Deming 的 PDCA(即 Plan(计划)、Do(实施)、Check(检查)和 Action(改进))循环改进思想,目前国际上普遍采取风险管理的方法来解决组织的信息安全问题。

如图 1-1 所示,信息安全风险管理是一个持续的过程,通过对信息安全潜在影响的标识、分析,制定针对性的规划(也就是风险评估),实施风险计划,监督检查风险,实施风险控制,再进行下一轮的循环。通过持续的循环活动对信息安全进行有计划、持续地控制,并且不断改进。

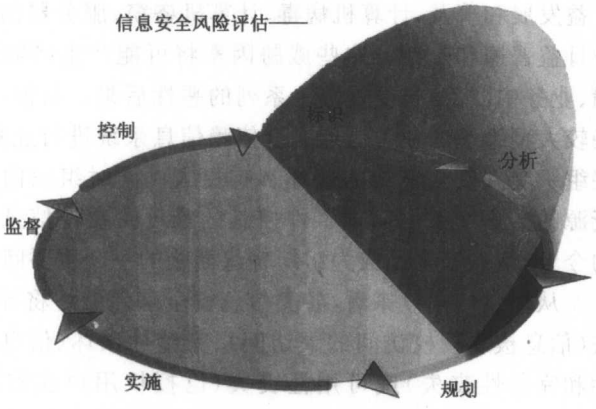


图 1-1 信息安全风险管理过程

1.2.2 风险管理中的控制论思想

控制理论是系统科学中的一个重要的理论分支,和系统论、信息论合称为“系统三论”。

按照控制理论大师维纳对控制理论的看法，控制理论是关于动物、机器和社会的控制和通信的科学。控制理论在我们的世界中无处不在，工程技术中对机器进行的调节、补偿、校正、操纵，社会过程中对组织或人的领导、指挥、支配、管理、经营、教育、批评、制裁，生命过程中的中枢神经活动，都是一定的控制行为。

信息系统是一种复杂的系统，涉及硬件、软件、人等多个子系统，保障信息系统的安全其实就是通过对风险的控制，使信息系统的风险保持在一个组织可接受的水平。可以这样说，缺乏控制的信息系统一定不是一个安全的信息系统，而一个保持在一个较高安全水平的信息系统一定是良好控制的。

站在控制理论的系统高度来理解信息安全和风险评估，可以让组织对风险管理有一个更加深入的理解，也有利于组织科学地开展风险管理活动。

1.2.2.1　控制理论简介

控制是一种有目的的活动，控制目的体现于受控对象的行为状态中。受控对象一定有多种可能的行为和状态，有些合乎目的，有些不合乎目的，由此规定了控制的必要性：追求和保持那些合乎目的的状态，避免和消除那些不合乎目的的状态。只有一种可能状态的对象没有控制的必要。控制是施控者的主动行为。施控者应有多种可供选择的手段作用于对象，不同的手段作用效果不同，由此规定了控制的可能性：选择有效的、效果强的手段作用于对象。只有一种作用手段的主体实际上没有施控的可能性。控制就是施控者选择适当的控制手段作用于受控者，以期引起受控者的行为状态发生合乎目的的变化，或者呈现有益的行为，或者抑制并消除不利的行为。所以，控制就是选择，没有选择就没有控制。

控制与信息是不可分的。在控制过程中，必须经常获得对象的运行状态、环境情况、控制作用的实际效果等信息，控制目标和手段都是以信息形态表现和发挥作用的。控制过程是一种不断获取、处理、选择、传送、利用信息的过程。

1. 控制系统分类

按照控制任务的不同，可以将控制系统分为以下几类：

1）定值控制

在有些控制问题中，控制任务是使受控量 y 稳定地保持在预定的常值 y_0 上，称为定值控制。实际存在的干扰因素使 y 偏离 y_0，控制任务就是抑制和克服干扰的破坏作用，使系统尽快恢复原状态，故又称为镇定控制。实际过程并不要求严格保持 $y=y_0$，只要求 y 对 y_0 的偏差 $\Delta y=y-y_0$ 不超过许可范围。

2）程序控制

在定值控制问题中，输入量或控制作用是常数，$u=c$。但多数控制过程中的控制作用随时间而变化，$u=u(t)$。如果 $u(t)$ 的变动规律能够预先精确确定，可以将 $u(t)$ 的变化规律作为一种程序表示出来，控制任务就是执行这个程序，因而称为程序控制。

3）随动控制

输入控制量 $u(t)$ 一般取决于外部过程，其变化规律往往不能预先确定，无法作为程序

固定在程序机构中，所以控制系统必须在工作过程中随时监测 $u(t)$ 的变化，并相应地改变输出量 $y(t)$，控制任务是使 $y(t)$ 随着 $u(t)$ 的变化而变动，因而称为随动控制。

4）最优控制

定值控制、程序控制和随动控制的控制任务可以统一表述为：保证系统的受控量和预定要求相符合。三者的区别在于这种预定要求是固定的还是变化的，变化规律是预先知道的还是只能在工作过程中随时监测的。但是，许多实际过程的控制任务不能作这种表述。在这类过程中，关于受控量的要求不仅不能作为固定值在系统中标定出来，或者作为已知规律引入系统作为程序，甚至无法在系统运行中实时获取。这类过程的控制任务应该表述为：使系统性能达到最优。

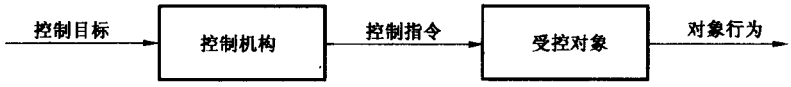
2. 控制方式分类

给定控制任务后，要用一定的控制方式来实现。实现同一控制目标可以有不同的控制方式，构成不同类型的控制系统。基本的控制方式可以分为三种：

1）简单控制

简单控制不考虑系统存在的外部干扰，也不管对象执行控制指令的效果如何，只根据控制目标的要求和关于对象在控制作用下的可能行为的认识来制定控制指令，让对象去执行。简单地说，就是只布置任务，不检查效果。

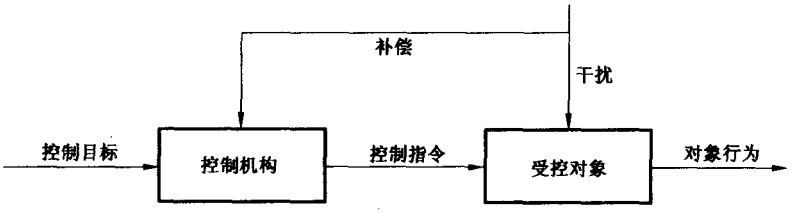
在外部干扰可以忽略不计、对受控对象的运行规律有确切的了解、能够制定出详尽可行的控制指令，且对象能忠实执行指令的情况下，简单控制策略是可行的。其优点是结构简单，使用方便，经济性好。简单环境中的简单系统都可能采取这种控制方式。简单控制可以用框图表示如下：



2）补偿控制

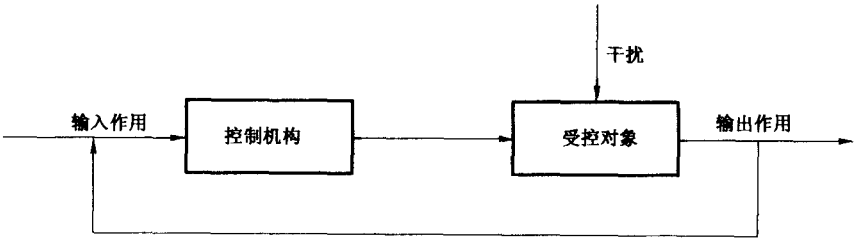
补偿控制的特点是，在依据控制目标制定控制指令的同时，实时地监测外部干扰，计算为抵消干扰可能造成的影响所需要的控制作用，并反映在控制指令中，通过控制把干扰的作用补偿掉。由于能够在干扰作用引起对象严重偏离目标之前就采取措施抵消干扰的影响，这种方式称为补偿控制。通俗地讲，就是“防患于未然”。

如果只有少量干扰作用且便于监测，又拥有抵消干扰的手段，这种控制方式是可行的。但如果干扰作用变量多、影响大，或者出现未曾料到的干扰作用，难以监测；或者虽然获得有关干扰的信息，但是没有足以抵消其影响的手段，则不宜采取补偿控制。补偿控制的框图如下：



3）反馈控制

反馈控制方式的特点是，不去监测干扰作用，不采取事先抵消干扰影响的补偿措施，只监测受控对象的实际运行情况，把输出变量的信息反向传送到输入端，与体现目标要求的控制变量进行比较，形成误差，根据误差的性质和大小决定控制指令，去改变对象的运行状况，逐步缩小并最后消除误差，达到控制目标。控制方案的着眼点是消除对象实际运行情况与预定情况之间的不一致，只有存在一定的误差，控制系统才能启动和工作。完全消除误差是不可能的，但要求通过控制把误差限制在许可的范围内，简单地说，反馈控制的特点是不但布置任务，而且检查执行效果，“赏罚分明”，根据对象的实际表现调整控制指令，直到达到控制目标。反馈控制的框图如下所示：



1.2.2.2　控制理论和信息安全

用控制理论的观点来看，信息安全活动就是对组织信息系统采取的一种控制任务，目的是使组织在信息安全上面临的风险维持在一个特定的水平。从执行的控制任务上来看，信息安全活动使用了多种控制方式，比如对信息系统整体风险的管理是一种随动控制，因为信息系统面临的风险是动态变化的，而应急响应中的应急预案则是一种程序控制方法。从控制方式上来看，基线控制方法是一种简单控制方式，因为基线控制方法并不考虑组织信息系统当前面临的风险状况，而只是根据对组织信息系统的一些了解布置安全控制措施；系统加固和病毒库定期升级则属于补偿控制方式，通过对信息系统脆弱点的弥补来抵消脆弱点对信息系统可能造成的影响；而风险评估则是一种反馈控制方式。

风险评估和控制活动是一种定值控制。在风险评估中，组织首先会通过访谈、调查表、讨论会等手段了解组织对信息安全的整体需求，即要把信息系统的安全风险控制在怎样的水平。接着，通过文档收集、人员调查、技术调查等手段收集组织在信息安全方面的相关信