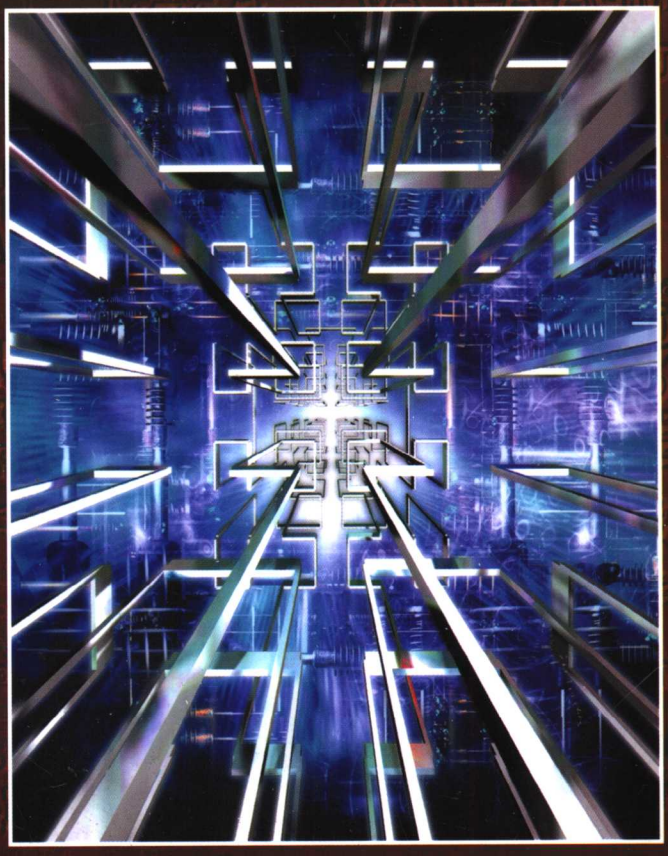
HZ BOOKS

信息安全技术丛书

完整涵盖CISSP考试范围

信息安全基础



The CISSP Prep Guide: Gold Edition

(美) Ronald L. Krutz
Russell Dean Vines 著

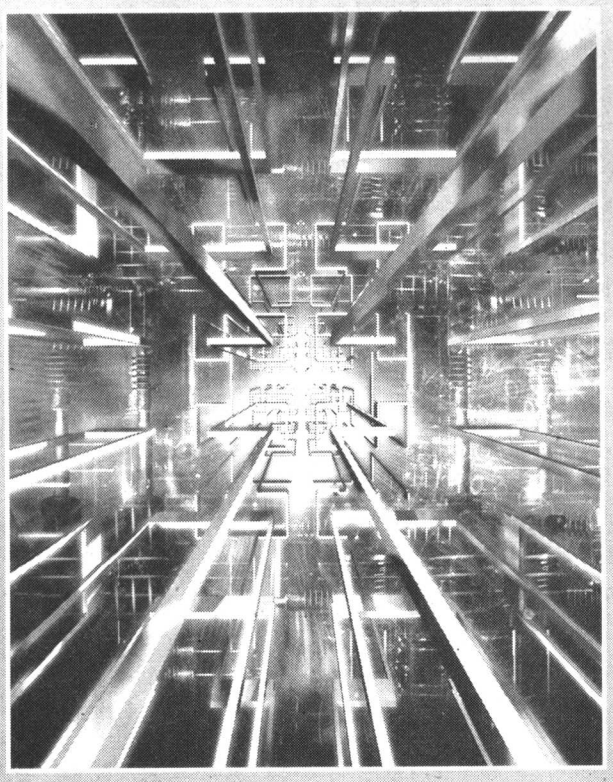
盛思源 成功 译

附赠CD-ROM

机械工业出版社
China Machine Press

信息安全技术丛书

信息安全基础



The CISSP Prep Guide: Gold Edition

(美) Ronald L. Krutz
Russell Dean Vines 著

盛思源 成功 译

机械工业出版社
China Machine Press

如果你准备开始进行CISSP（信息系统安全认证专业人员）认证，本书可为你提供一个框架，帮助你成为一名CISSP；如果你是一位受日益严重的安全问题困扰的IT经理，本书可为你提供一些基本的概念和原则，帮助你实现有效的安全控制；如果你已经是一名CISSP或是安全从业人员，本书将有助于你在安全领域取得成功。

本书除描述安全领域的各种问题外，还提供了大量习题，并在随书光盘中给出了习题答案，可供期望通过CISSP认证考试的读者自测、练习。

Ronald L. Krutz & Russell Dean Vines: The CISSP Prep Guide: Gold Edition (ISBN 0-471-26802-X).

Authorized translation from the English language edition published by John Wiley & Sons, Inc.

本书版权登记号：图字：01-2003-2622

图书在版编目（CIP）数据

信息安全基础 /（美）克鲁兹（Krutz, R. L.），（美）维恩丝（Vines, R. D.）著；盛思源等译. －北京：机械工业出版社，2005.2

（信息安全技术丛书）

书名原文：The CISSP Prep Guide: Gold Edition

ISBN 7-111-15946-2

Ⅰ. 信…　Ⅱ. ①克…　②维…　③. 盛…　Ⅲ. 信息系统－安全技术　Ⅳ. TP309

中国版本图书馆CIP数据核字（2004）第142908号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码　100037）

责任编辑：李　炎　　刘立卿

北京中兴印刷有限公司印刷 · 新华书店北京发行所发行

2005年2月第 1 版第 1 次印刷

787mm × 1092mm 1/16 · 22.5印张

印数：0 001-4 000册

定价：39.00元（附光盘）

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

本社购书热线：（010）68326294

作者简介

Ronald L. Krutz, 博士，职业工程师，通过了CISSP认证。Krutz博士是Corbett技术公司的一名高级信息安全顾问，还是该公司的能力成熟度模型的首席技术顾问，领导着Corbett的HIPAA-CMM评估技术的研究。他具有四十多年的分布式处理系统、计算机体系结构、实时系统、信息保障方法和信息安全训练等方面的工作经验。

他是REALTECH系统公司的信息安全顾问，卡内基－梅隆研究所（CMRI）的副董事长，卡内基-梅隆大学电子与计算机工程系的教授。Krutz博士创办了CMRI计算机安全中心，同时他也是CMRI计算机、自动化和机器人技术小组的创办人和主任。

Krutz博士领导和发起了计算机安全、人工智能、网络、建模和模拟、机器人技术及实时计算机应用等领域的应用研究和发展。他写了三本教科书，涉及微型计算机系统设计、计算机接口和计算机体系结构。他是数字系统领域七项专利的持有者。他是NEW HAVEN 大学计算机取证程序设计方面的著名访问学者，他还是Pittsburgh 大学计算机工程程序设计的兼职讲师，在那里他教授信息系统安全和计算机结构方面的课程。Krutz博士通过了CISSP认证，是一名注册职业工程师。

Russell Dean Vines通过了CISSP、CCNA、MCSE、MCNE认证。Vines先生目前是RDV Group公司（www.rdvgroup.com）——纽约的一家安全咨询服务公司的总裁和创办者，他的客户包括政府、金融界和新的媒体机构。多年来，Vines先生活跃在国际公司的安全脆弱性防护、检测和补救等领域，他在保密性、安全意识以及信息产业的最佳应用等方面经常发表意见。

Vines先生自个人计算机革命开始就已经在计算机工程领域工作了。他已经获得了Cisco、3Com、Ascend、Microsoft和Novell技术的高级认证，并且接受了国家安全局的ISSO信息评估方法的培训。他是计算机安全部门的负责人，同时管理全球信息系统网络的主要技术、运营和位于纽约的非盈利公司。以前他领导REALTECH系统公司的安全咨询服务小组，为CBS/Fox电视公司设计、实现和管理全球信息网络；他是纽约市儿童援助协会信息管理系统（MIS）的主任。

Vines先生早年职业生涯的辉煌并不是来自计算机行业，而是来自内华达州夜总会明亮的灯光。在获得了波士顿波克夏音乐大学Down Beat杂志的奖学金后，他为许多著名的演员，包括George Benson、John Denver、Sammy Davis Jr.和Dean Martin等伴奏。Vines先生创作和改编了上百首爵士乐和现代音乐，他以西方艺术家的身份创办和管理一个音乐出版公司。他还在纽约市演奏和教授音乐，并且是美国联邦音乐家协会的成员。

序

去年的一天，一个大媒体公司的首席执行官（CEO）收到了一封令人震惊的电子邮件。发件人说自己已经获得了进入该公司计算机系统的权限，如果CEO愿意支付一大笔钱，发件人说可以指出自己所发现的该公司计算机系统的缺陷。为了能够引起CEO的重视，邮件中附加了许多只能够从该公司网络上得到的重要文件（包括照片）。这件事可不是一次演习——这是真的。

正如你能想到的，这个问题立刻成为受害公司头号“必须解决”的问题。CEO需要很快得到一系列的答案和解决方法：电子邮件的真实来源，发件人声称内容的准确性，可能被他利用闯入系统的缺陷，为什么入侵检测系统没有检测出来，进一步的安全措施，可能采取的法律诉讼，以及对付敌人的最佳方法等。

此后几个月，许多人（包括计算机安全专家）都在收集信息和证据，保护系统的安全，追查攻击者的来源。最后，苏格兰场（伦敦警方）和美国联邦调查局（FBI）的便衣在伦敦的一个地方发现了“计算机勒索者”，并逮捕了他们。目前他们在监狱里，等待被引渡到美国。

对于任何一个有信息安全经验的人来说，这个案例使人们联想到这个行业的一些工具：日志，包嗅探器，防火墙和防火墙规则集，以及电子邮件通信的合法访问权限。这些内容本书都将讲述。而且，这个事件提出了问题：远程的敌人如何在不被检测出来的情况下进入计算机网络。

多年从事这个领域的人知道，应该智能地管理风险而不是消除风险来实现信息系统的安全。计算机信息安全专家认识到他们已经处于协作决策过程的核心。他们必须能够用正确的方法提供答案和解释。

日常事务中出现的安全问题并不都像这里所列举的案例那样严重，许多问题是相当小的。许多最优秀的技术人员开始更多地关注安全问题，大家逐渐达成共识，应该通过一个过程保证安全，而不是盲目信任软件或硬件。这个领域中的人都同意计算机安全专业人员必须经过训练，并且有丰富的经验。

阅读本书时，应该记住那些与公司商业运作密切相关的人员更容易发现异常。我经常向客户指出，可能只是那些非常了解网络特征和文件结构的人能够发现计算机被入侵。这一点不仅应该看到，更应该知道。

例如，如果你夜里回到家后发现放在卧室床头柜上的家庭照片散落四周，而房间内的其他物品没有被动过，你会立刻意识到有人进过你的房间。即使保安花时间检查你的床头柜，但不熟悉你家的保安能够注意到这个变化吗？很可能的回答是不能。同样，存在着许多除了熟悉系统的专家以外其他人不会注意到的、但可以被入侵者利用的计算机网络特征。

有时你必须向你的客户指出，信息系统安全的最大威胁是人，而不是机器。拥有计算机系统用户账号的内部人员有更大的优势可以攻击系统。计算机犯罪统计显示，与外部黑客相比，内部人员对系统的威胁更大。即使计算机罪犯很有才气，但选择他们作为计算机安全专业人员

也是一个糟糕的选择。

考虑一下：虽然电影《沉默的羔羊》中虚构的罪犯 Hannibal Lechter 博士在许多方面有才华，但我还是不能相信他。我尊重聪明人拥有的知识，但是当与其共事时，你将同时与其知识和道德观共处。

在学习本书中较深的材料时，你应该记住：今天的信息系统安全认证专业人员只是一个专业人员。专业人员必须遵守严格的标准，而有些标准是计算机不能提供的——这就是人的判断。因此，(ISC)²（国际信息系统安全认证联盟）在授予CISSP（信息系统安全认证专业人员）证书时，要求认证人员严格遵守其颁布的道德规范。

如果你准备开始进行CISSP认证，这本书可以提供一个框架，帮助你成为一名CISSP。如果你是一位被日益严重的安全问题所困扰的IT经理，为了实现有效的安全控制，这本书将给你提供一些基本的概念和可靠的基本原则。如果你已经是一名CISSP或者一位实际从业的安全专业人员，那么本书将有助于你在商业及国家安全等关键领域内取得成功。

Edward M.Stroz

Edward Stroz 是Stroz Associates公司（这是一家专门帮助客户检测计算机犯罪事件并对其进行响应的咨询公司）的董事长，他曾是美国联邦调查局的侦探，在纽约分局负责组织和管理计算机犯罪小组。可以通过下面的网站与他取得联系：www.strozassociates.com。

前　言

你掌握了一把钥匙，一把开启信息系统安全世界秘密的钥匙。这个世界将会给你带来许多新的挑战和回报，因为信息系统安全是人类不断探索有效通信的最后防线。通信已经经历了多种方式，因特网和电子通信只是人类近期的努力。但是为了维持和繁荣有效的通信，需要通信可靠、可信和安全。迫切需要能够为新的通信发展提供可靠基本原则的安全专业人员。需要像你一样的专家。

随着万维网越来越多地用于电子商务，必须保护交易信息不被泄漏。通常，对网络和信息系统的威胁来自公司内部和外部。这些威胁表现为偷盗知识财产、对消费者拒绝服务、对关键资源的未授权使用、破坏或修改重要数据的恶意代码。

保护信息资源的需要提出了对信息系统安全专业人员的需求。同时，还要求保证这些专业人员拥有执行所需任务的知识。

(ISC)²组织

CISSP认证是许多北美专家协会在1989年合作建立的国际信息系统安全认证联盟(ISC)²的产物。(ISC)²是一个非盈利的组织，它的惟一职责是建立和管理认证程序。该组织已经定义了一个知识共同体（CBK），CBK定义了这个领域中信息安全专业人员进行相互通信和建立会话的公共术语集。根据最新的CBK和技术（这些技术是(ISC)²为安全专业人员规定的）制定了指南。

- 访问控制系统和方法论
- 应用和系统开发安全
- 业务连续性计划和灾难恢复计划
- 加密技术
- 法律、调查和道德标准
- 操作安全
- 物理安全
- 安全体系结构和模型
- 安全管理实践
- 电信和网络安全

本书的结构

本书分成以下章节:

第1章——安全管理实践

第2章——访问控制系统

第3章——电信和网络安全

第4章——加密技术

第5章——安全体系结构和模型
第6章——操作安全
第7章——应用和系统开发
第8章——业务连续性计划和灾难恢复计划
第9章——法律，调查和道德标准
第10章——物理安全
附录A——NSA信息系统安全评估方法
附录B——公共标准
附录C——BS7799
附录D——进一步研究的参考资料
附录E——光盘上的内容
附录F——术语表和缩写
附录G至附录K没有出现在本书纸质印刷版中，收录在本书附带的光盘中。

附录包括了有用的参考资料和高级的主题。例如，附录A概述了美国安全局的信息安全评估方法（IAM）。附录B很好地介绍了公共标准，该公共标准取代了许多美国的和国际性的评估标准，包括可信计算机评估标准（TCSEC）。公共标准是多个标准相结合的产物，以建立一个能被国际组织所接受和使用的评估标准。

本书的读者

这本内容全面的指南面向三类读者:

1) 自己学习或参加CISSP复习研究班准备参加CISSP考试的人员将会发现这本书对他们准备考试非常有帮助。这个指南提供了一个获得所需信息的实际方法，而不需要从包含CBK各个领域的大量书籍中挑选资料，然后从中筛选出考试所需要的基本知识。书中所提供的样本问题可以使读者适应考试中出现的题型。答案可以巩固和补充参加考试人员的知识。

2) 许多主要的大学开设了信息系统安全认证培训，参加这些培训的学生会发现这本书是一本有用的参考书。同样，对于准备参加CISSP考试的人员来说，这本书是包括了基础的和最新的信息安全知识的惟一知识库。它给有经验的信息安全专业人员提供了信息，因此适合开设认证培训的大学的需要。

3) 这本书中所包含的材料对于信息安全专业人员来说，对他们的工作有实际的价值。通过认证或没有通过认证的专业人员，都可以把这本书作为信息安全基本知识的最新资料和应用新方法的指南。

目　录

第1章　安全管理实践

本章介绍安全管理。在本书中，许多信息系统安全（InfoSec）领域中的要素和概念是重复出现的。虽然在各个安全领域中都给出了清楚的定义，例如，本领域介绍的许多概念还将在第6章“操作安全”和第10章“物理安全”中做详尽的论述。书中将指出重复出现概念的章节。多个领域中出现的概念，读者需要明白它的重要性。

1.1　概述

国际信息系统安全认证协会[(ISC)²]规定，信息系统安全专业人员认证的目的是：

“希望参加考试的人员能够了解每个人在识别和保护机构信息资产中的计划、组织和作用；管理政策的发展和使用、在特定主题的地位、指导方针标准的使用和支持政策的手段；训练雇员的安全意识，使雇员意识到信息安全的重要性、重要意义和与他们的地位相关的具体安全需求；保密性、所有权和私有信息的重要性；雇佣合同；雇员的签约和解聘；以及识别、评估、减少特殊资源风险的风险管理实践和工具。”

一个专业人员应掌握以下内容：

- 安全管理概念的基本信息
- 政策、标准、指导方针和方法之间的区别
- 安全意识概念
- 风险管理（RM）实践
- 分类标准的基本信息

1.1.1　我们的目标

信息系统安全的安全管理领域将研究以下的内容：

- 信息安全管理的概念
- 信息分类过程
- 安全政策的实现
- 安全管理部门的作用和责任
- 风险管理评估工具（包括评估的基本理论）
- 安全意识培训

1.1.2　领域定义

信息数据资产与政策、标准、指导方针和方法的制定与执行相结合形成了信息系统安全的安全管理领域。它定义了数据分类和风险管理的管理原则。为了实现有效的安全控制，该领域

还通过威胁识别、机构的资产分类以及脆弱性评估等提出保密性、完整性和可用性的概念。

1.1.3 管理的概念

针对信息安全管理的概念，主要讨论以下内容：

- 大三角：保密性、完整性和可用性。
- 标识、认证、责任、授权和隐私的概念。
- 安全控制的目标——减少威胁的影响和威胁出现的可能性。

1. 大三角

本书论述了信息系统安全的三个基本原则：保密性、完整性和可用性（C.I.A.），如图1-1所示。这些基本概念体现了信息安全的三个基本原则。所有的信息安全控制、安全措施，以及所有的威胁、脆弱性和安全过程都满足C.I.A.标准。

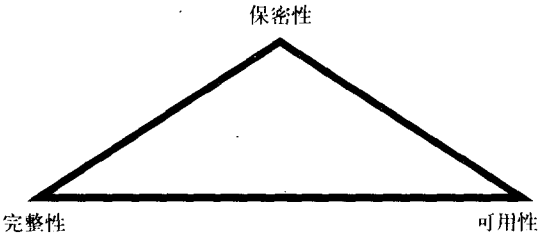


图1-1 C.I.A.三元组

保密性（Confidentiality） 保密性就是保护信息的内容免遭有意的或无意的、未授权的泄漏。有许多方法可以损害保密性，如有意泄漏公司的私有信息或滥用网络特权。

完整性（Integrity） 完整性就是确保：

- 未授权的人员或过程不能修改数据。
- 已授权的人员或过程未经授权不能修改数据。
- 数据的内部和外部相一致，也就是说，内部信息在所有的子实体中一致，内部信息与真实世界、外部场所相一致。

可用性（Availability） 可用性确保适当人员可靠地、及时地访问数据或计算资源。换句话说，可用性保证当需要系统时系统能启动和运行。另外，这个概念还保证安全从业人员所需要的安全服务处于正常的工作状态。

注意 D.A.D是C.I.A.的相反概念

保密性、完整性和可用性的相反概念是泄漏、改变和破坏（D.A.D）。

2. 其他重要的概念

还有其他的一些重要概念和术语是参加CISSP考试的人员必须完全了解的。这些概念包括标识、认证、责任、授权和保密。

标识（Identification） 用户向系统声明自己身份的方法。常用于访问控制，对于认证和授权来说标识是必须的。

认证（Authentication） 用户身份证据的测试和调整。它创建用户的标识符，确定用户是他所说的。

责任（Accountability） 确定系统中个人的行动和行为以及识别具体个人的系统能力。审计跟踪和日志支持责任功能。

授权（Authorization） 授予个人（或过程）权利和许可，使之能够访问计算机。一旦建立了用户标识和认证，授权的等级决定了操作者所拥有的系统权利范围。

隐私（Privacy） 系统提供给用户的保密性和保密防护的标准。它是安全控制的一个重要组成。隐私不仅保证操作者所使用公司数据保密性的基本原则，而且还保证隐私的数据等级。

3. 安全控制的目标

安全控制的主要目标是减少安全威胁的影响和一个机构所能承受的脆弱性。这需要确定威胁对一个机构的影响，以及威胁出现的可能性。分析威胁场景，提出一个评估潜在损失的典型值的过程被称为风险分析（RA）。

使用x-y图可以产生一个小矩阵，其中y轴表示实际威胁的程度，x轴表示威胁实现的可能性，都是从低到高设置。当矩阵产生后，就生成了如图1-2所示的图形。这里的目的是通过执行安全控制，减小影响的程度和威胁或灾难性事件发生的可能性。一个正确实现的控制应该将图形上的点从右上角（控制实现以前定义的威胁值）移到左下角（也就是0, 0），即控制实现后。在确定一个控制的成本效益比时，这个概念非常重要。

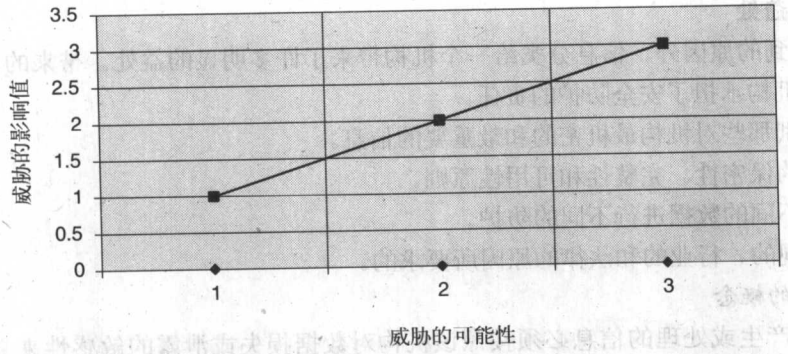


图1-2 威胁与可能性矩阵

因此，一个设计不正确或实现不正确的控制，在控制实现前后，图中点的位置没有多少移动。向（0,0）区域点的移动距离可能非常小（或者非常差的控制设计，则以相反的方向）以至于它不能保证实现的费用。另外，(0,0）点（不可能没有威胁）是不可能达到的，因为一个不可能的威胁仍然有0.000001的出现概率。因此，它仍然可能存在，可能产生适当的影响。例如，一个热的匹萨运输车与操作中心相互碰撞的概率几乎是没有的，然而，这个潜在的危险仍然可能出现并且对计算资源的可用性产生相当严重的影响。

多于四个部分的矩阵可以用于对威胁和影响进行更详细的分类。

1.1.4 信息分类过程

本章我们要研究的第一个主要信息系统安全过程是信息分类的概念。信息分类过程与业务连续性计划和灾难恢复计划有关，因为它们都关注业务风险和数据评估，然而，它仍然是一个

独立的基本概念——参加CISSP考试的人员必须了解的概念。

1. 信息分类的目标

对信息进行分类有多个原因。对于一个机构来说，并不是所有数据的价值都是一样的。有些数据对从事决策的人更加有用，因为它能帮助他们做出长期或短期的业务发展决策。有些数据（例如，商业秘密、规则及新的产品信息）是非常有价值的，这些数据的丢失会产生社会困扰，引起可信性缺乏，从而给商场中的企业造成重大的问题。

出于这些原因，信息分类具有较高的、企业级的益处。信息对业务产生全面的影响，不仅对业务单位，而且对生产线运作水平。它的主要作用是提高保密性、完整性和可用性，降低信息的风险。另外，通过加强防护机制和对信息领域的控制，可以达到更加有效的成本-效益比。

在政府部门，信息分类的历史最长。信息分类的价值已经被确定，当保护可信系统时，信息是一个必不可少的组成部分。在本节中，信息分类主要用于防止未授权泄露和保密性受到破坏。

信息分类还可以用于遵守保密规则或遵守规章制度。公司希望使用信息分类维持它在激烈的商场中的竞争地位。公司使用信息分类还有许多合理的法律原因，如减少债务或保护有价值的业务信息。

信息分类的益处

除了上面提到的原因外，信息分类给一个机构带来了许多明显的益处。带来的益处如下：

- 证实一个机构承担了安全防护的责任。
- 有助于识别那些对机构最机密的和最重要的信息。
- 支持数据的保密性、完整性和可用性原则。
- 有助于对不同的数据进行不同的防护。
- 可能是常规的、行业的和法律的原因所要求的。

2. 信息分类的概念

一个机构所产生或处理的信息必须按照该机构对数据损失或泄露的敏感性来划分。这些数据的拥有者负责定义数据敏感性等级。这个方法使得可以根据数据分类方案正确地实现安全控制。

分类术语

下面的定义描述了几个政府的数据分类等级，范围从敏感性的最低级到最高级：

1) 非密级的（Unclassified） 被指定为不敏感也不机密的信息。这类信息的公开不会破坏保密性。

2) 敏感但非密级的（Sensitive but Unclassified，缩写为SBU） 被指定为次秘密的信息，如果泄露这类信息不会产生严重的损失。对测试的回答属于这类信息。卫生保健信息是SBU数据的另一个例子。

3) 机密的（Confidential） 被指定为机密的信息。这类信息的未授权泄露可能会对国家安全造成一些损害。这个级别文件的敏感性介于SBU和秘密的之间。

4) 秘密的（Secret） 被指定为秘密的信息。这类信息的未授权泄露可能对国家安全造成严重的损害。

5) 绝密的（Top Secret） 信息分类的最高等级（实际上只有美国总统具有这个级别）。绝密信息的未授权泄露将会给国家安全造成非常严重的后果。

在所有这些分类中，除了具有访问信息的正确许可之外，个人或过程对信息的使用必须根据“按需知密”的原则。因此，被定为秘密或秘密以下级别的人不能访问秘密材料，因为对他来说，不需要执行这些材料所赋予的工作职能。

另外，在私有企业中还使用了以下的分类术语（见表1-1）：

1) 公开的（Public） 与非密级信息相类似的信息；不适合以下种类的任何公司信息都可以被认为是公开的。这类信息可能不会被泄露。然而，如果这类信息被泄露，也不会对公司产生严重的或不利的影响。

2) 敏感的（Sensitive） 比正常数据的分类级别高的信息。保护这类信息免受未授权的改变而降低保密性和完整性。

3) 私有的（Private） 私有信息，只供公司使用。这类信息的泄露可能对公司或雇员带来不利的影响。例如，工资水平和健康信息就是私有信息。

4) 机密的（Confidential） 非常敏感的信息，主要用于公司内部。根据信息自由法案，这类信息不能被泄露。这类信息的未授权泄露可能会对公司造成严重的、消极的影响。例如，关于新产品开发、商业秘密和合并谈判的信息就是机密信息。

表1-1 一个简单的私有的/商业的部门信息分类方案

定 义	描 述
公开使用	可以公布于众的信息
仅供内部使用	可以在公司内部公开，但不能泄露给公司外部的信息
公司机密	最敏感的按需知密信息

分类标准

我们使用几个标准来确定信息对象的等级：

价值（Value） 价值通常是私有企业内数据分类标准中最重要的一个。如果信息对一个机构是有价值的，那么就需要对它进行分类。

时效（Age） 随着时间过去，如果信息的价值降低，那么信息的等级就可能下降。在国防部，经过一段预定的时间后，有些等级的文件会自动解密。

有效期（Useful Life） 如果由于出现了新的信息，公司发生了实质性的变化或其他的原因导致信息过时了，那么常常可以将其解密。

个人相关（Personal Association） 如果信息与特定个体有关或是由保密规则提出的，那么这类信息需要被分类。例如，显示告密者姓名的调查信息就可能需要保密。

信息分类的步骤

建立一个分类系统需要多个步骤。以下是按照重要性次序排列的主要步骤：

1) 确定系统管理员/管理员。

2) 规定分类和标识信息的标准。

3) 数据的所有者对数据进行分类，并且接受管理员的检查。

4) 对分类政策的例外情况进行详细的说明并提供相应的文件。

5) 规定对每个类型等级的控制。

6) 规定解密信息或将信息的监护权转交给另一个实体的终止过程。

7) 建立关于分类控制的企业意识计划。

分类信息的发布

对外发布分类信息常常是需要的，并且需要指出内在的安全脆弱性。对外发布分类信息的一些必要场合是:

- 法院指令　遵照法院的指令，分类信息可能需要公开。
- 政府合同　根据与政府计划相关的协议，政府合同才可能需要公开分类信息。
- 高级获准　高层决策人可以批准向外部实体或机构公开分类信息。这种公开可能需要外部当事人签订一份保密协定。

3. 信息分类的作用

必须清楚地定义信息分类计划中所有参与者的作用和责任。分类方案的一个关键元素是与数据有关的用户、所有者或管理者的作用。描述信息分类中所有者、管理者和用户的作用，并牢记。

所有者

信息的所有者可能是公司的决策人或经理。他对必须保护的信息资产负有责任。所有者与管理员不同。所有者负有数据保护最终的法人责任，并且在正常管理下，所有者可能对由于疏忽而没有对数据进行保护负有责任。然而，保护数据的实际日常工作职责属于管理员。

信息所有者的责任包括:

- 根据对数据保护的业务需要，制定最初的信息分类等级。
- 定时地检查分类划分，按照业务的需要对分类划分做出改变。
- 将数据保护的责任交给管理员。

管理员

信息的所有者将保护信息的责任交给了管理员。这个角色常常由IT部门的职员来承担。管理员的职责是:

- 定时运行文件备份，定期地检查备份数据的有效性。
- 当需要时从备份文件中执行数据恢复。
- 根据已确定的信息分类政策维护那些保留的信息。

另外，管理员还有其他的职责，如作为分类方案的管理人。

用户

在信息分类方案中，最终用户（如操作员、雇员、外部人员）将信息作为他们日常工作的一部分。这类人员也被认为是数据的消费者（他们每天需要访问信息完成任务）。下面是有关最终用户的几条重要职责:

- 用户必须遵循公司安全政策中规定的操作步骤，而且他们必须遵守为使用安全政策而公布的指导方针。