CISSP 认证考试指南
(第 6 版)

[美] Shon Harris 著

张胜生 张博 付业辉 译

清华大学出版社

北 京

Shon Harris
CISSP All-in-One Exam Guide, Sixth Edition
EISBN: 978-0-07-178174-9

图书在版编目(CIP)数据

CISSP 认证考试指南(第 6 版) / (美) 哈里斯(Harris, S.) 著；张胜生，张博，付业辉 译. —北京：清华大学出版社，2014

书名原文：CISSP All-in-One Exam Guide, Sixth Edition

ISBN 978-7-302-34440-7

Ⅰ. C… Ⅱ. ①哈… ②张… ③张… ④付… Ⅲ. ①信息系统—安全技术—资格考试—指南 Ⅳ. ①TP309-62

中国版本图书馆 CIP 数据核字(2013)第 270024 号

责任编辑：王　军　于　平
装帧设计：牛艳敏
责任校对：邱晓玉
责任印制：

出版发行：清华大学出版社
　　网　　址：http://www.tup.com.cn，http://www.wqbook.com
　　地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
　　社 总 机：010-62770175　　邮　　购：010-62786544
　　投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
　　质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：64.75　　**字　　数**：1784 千字
版　　次：2014 年 1 月第 1 版　　**印　　次**：2014 年 1 月第 1 次印刷
印　　数：1～4000
定　　价：128.00 元

产品编号：

译 者 序

随着我国信息化技术的蓬勃发展，信息安全问题也越发严重，但信息安全工作还存在很多误区，比如：重技术，轻管理；重解决单个问题，轻规划方案；重计划，轻考核；重 IT 人员，轻业务人员教育；重建设，轻运维保障。这些问题困扰着信息安全从业人员，如何从信息安全原理上分析信息安全各个层面的问题，如何全面地审视信息安全威胁，如何将风险控制到可以接受的程度，《CISSP 认证考试指南(第 6 版)》给出了深入浅出的讲解。同时书中还强调了信息安全要从管理和业务层面入手，设计出信息安全策略，并根据策略进一步落实实施。作者的循序引导将给读者耳目一新的感觉，能够让读者快速建立起自己的信息安全知识体系，不愧是一本经典权威之作。

我从事信息安全工作 13 年，开展大中型企业的信息安全教学工作也已有 8 年，在与数万名学员的交流过程中，我学到了很多知识，我与我的师资团队一起开发了 15 门演练实战课和多门考试认证精讲类课程，在这其中我感受最深的是《CISSP 认证考试指南》中的知识精华给我带来的巨大帮助。

本书全面而细致地讲解了信息安全涵盖的 10 个领域，在每个领域中都贯穿了信息安全风险管理的精髓，作者通过大量案例不断帮助读者拓宽视野，了解行业中的管理和防御实践，本书是参加 CISSP 考试和提高信息安全水平的一本好书！

由于本书知识量大、涵盖面广，在阅读这本书的时候建议大家采用树型图软件梳理，当然关于知识汇总和大家的疑惑交流，也可以访问我的博客 http://blog.sina.com.cn/anquan1000。

本书的翻译过程很艰辛，在此我要特别感谢我的两位搭档：

张博：2005 年开始从事网络与信息安全工作，在一流的网络信息安全公司从事过大量安全项目的实施，并且曾经供职中国移动多年，有深厚的理论知识和丰富的实践经验，在书中的语言描述深入浅出。

付业辉：2002 年起，进入大型跨国企业并一直从事信息安全领域至今，拥有非常丰富的信息安全架构设计和大型安全项目的实施管理经验，对信息安全管理有着国际化的视野。

在翻译过程中，许多人给了我很多帮助，其中包括中国移动集团及各省公司的安全朋友们，向你们积极进取的精神致敬！最后还要感谢我的家人和我的学生们给予的支持和帮助。

本书博大精深，但在实际翻译过程中由于时间和能力所限，肯定存有各种不足之处，恳请读者理解和体谅，也欢迎读者对其中的问题给出批评指正，有关技术问题的交流信箱是 390890513@qq.com。

张胜生

CISSP/CISP/CISA/ISO27001 资深讲师

“红黑演义”云端攻防演练平台总设计师

从业人员对本书的赞誉

我和张胜生老师认识是在教育部 2009 年“第三届中国信息安全学科建设与人才培养研讨会”上，当时张老师在会上做了“大中型企业人才培养”专题发言，那时张老师已经是国内知名的 CISSP 讲师了。《CISSP 认证考试指南》作为行业认可的国际化 CISSP 教材，所涉及的知识领域十分广泛，既适合于行业人士深造所用，同时在高校研究生和本科生教学过程中也可以作为选定教材和参考资料。

朱建明
中央财经大学信息学院院长/教授、博导

IT 和互联网技术已经渗透我们工作和生活的方方面面，互联网金融、手机支付、信息家电、智慧城市、物联网等新兴技术已经逐步由概念变为现实，IT 和互联网技术将与我们的身体健康、财产管理、日常工作、社交活动、 休闲娱乐、个人消费等发生更多更加紧密的联系。因此，IT 和互联网是否安全可靠，将会成为决定我们工作和生活品质的重要因素，网络与信息安全问题已经被提升到了前所未有的高度，而且其重要性还在不断增加。现在很多从业人员、学生和爱好者们都在学习网络与信息安全技术，以实现自己在个人发展、工作需要或者兴趣爱好上的目标。而《CISSP 认证考试指南(第 6 版)》能够满足从业人员、学生和爱好者们的需要，可以在 CISSP 备考时起到极其重要的作用，也可以作为工具书和兴趣读物来使用。

孙晶
首都五一劳动奖章获得者
2010 年北京职工职业技能大赛信息安全比赛冠军

有幸认识张胜生老师是在 7 年前，他那时就已经在 CISSP 教学的第一线奋战多年，CISSP 的理念和知识已经深深融入张老师的血液中。虽然本书是一本国外教材的翻译版，但张老师在翻译本书的过程中，倾注了大量的心血，将自己对 CISSP 教学的丰富经验融入其中，使读者能够更加容易地理解本书原作者要表达的 CISSP 全部内容。

一本好书可以改变一个人的命运和前程，我认为《CISSP 认证考试指南(第 6 版)》就是一本这样的好书。作为 CISSP 认证考试的权威教材，本书以海一样广阔的胸怀容纳了安全行业的方方面面，从不同的角度，不同的主题系统化地阐述了建设和管控企业安全的方法和知识。

如果你是一个安全从业者，我认为这是一本温故而知新，每看一遍都有不一样体会的书。

如果你是一名安全初学者，我认为这是一本指导你走向安全岗位，并获得从业资格的宝典。

聂万泉
阿里巴巴高级安全专家

我是在 5 年前的 CISSP 培训课上认识张胜生老师的，他对信息安全深邃而独到的见解以及丰富的 CISSP 经验，给我留下了深刻的印象。《CISSP 认证考试指南》可以说是 CISSP 考试的宝典，而张老师翻译的《CISSP 认证考试指南(第 6 版)》和他更是相得益彰。

张健
完美世界信息安全总监

作 者 简 介

Shon Harris 是 Shon Harris 安全有限责任公司和逻辑安全有限责任公司的创始人兼首席执行官，她是一名安全顾问，是美国空军信息作战部门的前任工程师，也是教师和作家。自 2001 年以来，Shon 拥有并经营着自己的培训和咨询公司，她为财富 100 强公司和政府机构广泛的安全问题提供咨询服务。她撰写了 3 本最畅销的 CISSP 图书，同时还是 *Gray Hat Hacking：The Ethical Hacker's Handbook* 和 *Security Information and Event Management*(*SIEM*) *Implementation* 的特约作者，*Information Security Magazine* 的技术编辑。她还为 Pearson 出版公司开发了许多数字化安防产品。

技术编辑简介

Polisetty Veera Subrahmanya Kumar 拥有 CISSP、CISA、PMP、PMI-RMP、MCPM、ITIL 认证证书，在信息技术领域拥有 20 多年的经验。他的专业领域包括信息安全、业务连续性、项目管理和风险管理。他最近担任项目管理协会 PMI-RMP(PMI-Risk Management Professional，风险管理专业)资格认证委员会的主席，曾是 ISACA 印度 Growth Task Force 团队成员。过去他还曾担任各种 PMI 标准开发项目的内容开发团队负责人。他还是 PMI(美国项目管理协会) PMBOK(项目管理知识体系)培训的首席讲师。

致　　谢

我要感谢所有在信息安全领域富有激情、具有奉献精神的行业开拓者。信息安全行业的精英就是那些追求道德成果的人。

我要感谢那么多的圈内人愿意花时间联系我，并让我知道我的工作直接影响着他们的生活。我感激人们花时间和精力反馈给我这些信息。

我也要感谢下列人士，在我撰写第 6 版时给我的帮助：

David Miller，他的工作热情、忠诚和友谊一直激励着我。能够与 David 共事，我觉得非常荣幸。没有他，我永远无法尝到龙舌兰酒的醇香。

Clement Dipuis，他待人热情，乐于助人，是一位不可多得的导师和朋友。

我公司的团队成员：Susan Young 和 Teresa Griffin，我无法表达对你们每个人深深的感激之情。

Greg Andelor，他是位图形艺术家，我这本书和我的其他项目很多图表都是出自他手，不幸的是他如此年轻就离我们远去了，我将永远怀念他。

Tom Modden 和 Randy Vickers，感谢他们为这本书写的精彩前言。

我的编辑 Tim Green 和我的出版合伙人 Stephanie Evans，他们在和我一起处理这些项目时总能耐心工作。

我最好的朋友和母亲 Kathy Conlon，即使她身体有时不太好，但总是陪伴在我身边。

特别是，我想要感谢我的丈夫 David Harris，谢谢他一直以来的支持与爱。没有他对我的坚定信心，我根本无法取得目前的成就。

前　言

我已经从事安全业务 39 年了，其中 26 年专注于信息安全。这些年我们已经看到了这个行业前所未有的变化：原来的计算机有一间屋子那么大，而且必须用水冷。到现在手机的计算能力已经超过了美国宇航局用于登陆月球所用的计算机。

我们敬畏地看着这一切，技术在发展，我们的生活质量也在不断提升。例如，我们可以通过手机来支付，我们的汽车也是计算机控制的，计算机控制带来了性能的优化和燃料的经济性，我们可以在酒店的房间办理登记手续并且得到登机牌。

但遗憾的是，一些人却通过技术和自己的优势找到漏洞，把这些进步变成了他们个人或其组织谋取政治利益和经济利益的工具。

为了应对这些对手，信息安全专业出现了。第一个认识到信息安全专业的组织是$(ISC)^2$，它成立于 1988 年。1994 年$(ISC)^2$创建了注册信息系统安全专家(Certified Information System Security Professional，CISSP)认证并举行了第一次考试。这样就可以给经理和雇主(和潜在的雇主)一个保证，证实证书持有人对组成公共知识体(Common Body of Knowledge，CBK)中的 10 个领域都有基本的理解。

Shon Harris 撰著的《CISSP 认证考试指南》(*CISSP All-in-One Exam Guide*)是为应考者准备 CISSP 考试的指导书籍。我看到过许多类似的考试指南，Shon 的书和别人的区别是她的书并不教人们如何通过考试，而是教你要通过考试所需的知识和材料。这意味着，虽然可能已经通过考试并获得证书，但是 Shon 的书仍然会在你的书架上(或平板电脑中)作为一个有价值的参考指南。

我认识 Shon 已经将近 15 年了，感动我的是她的奉献精神、道德和荣誉。她是我们这个行业里我遇到的最专业的人。她不断工作来改进她的书以便所有水平的读者都能理解各个主题。她开发了一种学习模式，帮助确保一个组织从底层到最高管理层的每个人都知道对他们负责的数据尽职尽责是明智的选择。

很荣幸有机会帮助介绍 CISSP。我是 Shon 的忠实读者，我认为学习完这本书之后，你也会成为 Shon 的忠实读者。享受这段学习经历，为了这个证书而付出努力将物有所值。

Tom Madden, MPA, CISSP, CISM
疾病控制中心首席信息安全官

当今，网络安全环境不断变化，我们在很多正常活动时，比如收发电子邮件、上网冲浪等，都会遭受攻击。敌人可能会一直通过手机应用、电子邮件(钓鱼、垃圾邮件)、网站(重定向)或者其他工具对我们的日常活动发起攻击，来获得知识产权、个人信息或其他敏感数据。黑客行动主义者、罪犯和恐怖分子通过使用上述信息实现未经授权地访问系统和敏感数据。

黑客行动主义者通常使用攻击期间收集的信息来传递他们的消息，达到他们的目标。据赛门铁克的报告，在 2010 年，发现 163 个与移动计算相关联的新漏洞，286 亿个恶意软件变种，网络攻击数量增加了 93%，260 000 个身份信息泄漏。据迈克菲的报告，在 2011 年的前两个季度出现了 16 200 个恶意网站，平均每天有 2600 个钓鱼网站出现。

我们也看到了在我们的日常活动中新技术在不断发展。新的智能手机和平板电脑已经成为常见的家用电脑。但是新工具往往意味着新的漏洞，网络安全专家必须处理。信息技术实施人员需要快速设计和实施。其中关于新技术讨论最多的很可能对整个系统或组织造成风险。CSO/ CISO 会与技术部门一起寻找运用新技术的最佳方法，但物理安全和网络安全是部署策略中非常重要的部分。

培训是非常重要的，可以帮助最终用户、网络安全从业者，高级管理层明白他们的行为对组织内部有什么影响。甚至技术人员在家远程办公，连接到企业网络或将数据带回家都可能产生严重的后果。安全策略的推行将帮助建立一个更强的安全基线。组织已经意识到这个问题，很多组织已经开始编写可实现可接受的网络使用策略。这些策略如果执行得当，将有助于减少网络安全事件的发生。

一个解决方案是不可能解决网络安全问题的。深度防御、最佳业务实践、培训和意识教育、及时的信息共享等技术可以使网络攻击的影响降到最低。网络安全专家们需要使领导层及时了解最新的威胁和减少这些威胁影响的方法。由首席财务官、首席执行官、首席运营官做出的许多日常行为和决定，将会对任务实现产生影响；安全决策也应该成为这个流程的一部分。

在我获得证书后，《CISSP 认证考试指南》一直是我的一本重要参考资料。Shon Harris 创作并继续完善着这本全面的学习指南。组织机构各个层面的人，特别是网络安全人员，应该努力获得 CISSP 认证。这本学习指南是成功获得这个认证的关键，是网络专家准备和获得 CISSP 的工具包。CISSP 的 10 个相关领域将协助个人从许多角度来认识信息安全。我们不再仅仅关注信息安全领域的一个方面，它为我们提供了多个视角，提供了专业的、总体的网络安全。从策略领域到技术领域，CISSP 和这个学习指南涉及了网络安全的方方面面。即使这不属于你目前的培训计划，这本书将帮助任何人成为一个更好的安全从业者并且改善他们的组织安全状况。

Randy Vickers
Alexa Strategies, Inc.
网络安全分析师和顾问
CERT 美国的前总裁，国防部 CERT(JTF-GNO)前首席

目　录

第 1 章

成为一名 CISSP

本章主要内容:

- CISSP 的定义
- 成为 CISSP 的理由
- 参加 CISSP 考试所需条件
- 公共知识体系(Common Body of Knowledge，CBK)及其包含的内容
- $(ISC)^2$ 和 CISSP 考试的发展历史
- 估判读者当前安全知识水平的评估测试

本书不仅提供了通过 CISSP 认证所需的信息，而且能够引领你进入令人兴奋和充满挑战的安全领域。

CISSP(Certified Information Systems Security Professional，信息系统安全专家认证)考试涵盖了 10 个不同的主题，这些主题通常也称为“领域”。其中，每一个领域都有自己的研究重点，在很多情况下，某些专家只从事个别领域内的工作。面对众多的主题，要想成为某个领域中的专家，你就必须查阅和参考大量的资料。因此，人们常常误认为通过 CISSP 考试的唯一途径是学习大量的文献资料。幸运的是，目前还存在一种更容易的方法。借助于这本《CISSP 认证考试指南(第 6 版)》，你就能够成功地通过 CISSP 考试并获得 CISSP 认证资格。本书旨在把通过 CISSP 考试所需的全部信息内容组合在一起，帮助了解各个领域之间的相互依存关系，从而掌握一整套涉及安全领域的实践做法。此外，在你获得 CISSP 认证资格后相当长的一段时间里，本书对于你仍然具有很大的参考价值。

1.1 成为 CISSP 的理由

随着世界不断改变，人们对于增强安全、改进技术的需求越加迫切。过去，“安全”仅仅是技术领域的热门话题；但是，现在它已经逐渐成为我们日常生活的一部分。每个组织、政府机构、企业和军事单位都已开始关注安全问题。10 年前，计算机和信息安全是一个只有少数人关心的模糊领域。因为当时安全风险相对较低，所以很少有人对安全专业知识感兴趣。

然而，这种状况已经发生了显著变化。如今，几乎所有的公司和组织机构都在积极寻求才华横溢、经验丰富的安全专业人员，因为只有这些专家才能保护它们赖以生存和保持竞争的宝贵资

源。而 CISSP 认证能够证明你已经成为一名拥有一定知识和经验的安全专业人员。当然，这些知识和经验是认证体系预先规定的，并且得到了整个安全行业的理解和认可。如果获得了 CISSP 认证资格，那么就表明你已经掌握了与维护信息安全相关的最新知识和技能。

下面列出了一些获取 CISSP 认证资格的理由：

- 满足不断增长的要求，在一个突飞猛进的领域中寻求发展。
- 充实现有的关于安全概念和实际应用的知识。
- 把安全专业知识引入当前的工作。
- 让自己在这个竞争激烈的劳动力市场中占据优势。
- 表明对安全规则的关注和贡献。
- 增加收入，并且能够得到更多的工作机会。

CISSP 认证能够帮助公司确认某人是否具有相应的技术能力、知识和经验，从而能够从事具体的安全工作，执行风险分析，谋划必要的对策，并且可以帮助整个组织机构保护其设施、网络、系统和信息。CISSP 认证还能担保通过认证的人员具备安全行业所需的熟练程度、专业技能和知识水平。安全对于成功企业的重要性在未来只可能不断增长，从而导致对技术熟练的安全专业人员的更大需求。CISSP 认证表明，可以由被公众认可的第三方机构负责确定个人在技术和理论方面的安全专业知识，并且将其与缺乏这种专业知识的普通人员区分开来。

对于优秀的网络管理员、编程人员或工程师来说，理解和实现安全应用是一项至关重要的内容。在大量并非针对安全专业人员的职位描述中，往往仍然要求应聘人员正确理解安全概念及其实现方式。虽然许多组织机构由于职位和预算的限制而无法聘请单独的网络和安全人员，但是它们都相信安全对于组织机构自身来说至关重要。因此，这些组织机构总是尝试将安全知识和其他技术知识合并在一个角色内。在这个问题上，如果具有 CISSP 资格，那么你就会比其他应聘人员更有优势。

1.2 CISSP 考试

因为 CISSP 考试涵盖了构成公共知识体系的 10 个领域，所以常常被描述为“尽管内容不深，然而包罗万象”。这意味着，考试中出现的问题实质上不一定非常详细，并且不要求你在所有主题上都是专家。但是，这些问题却要求你熟悉许多不同的安全主题。

CISSP 考试由 250 道选择题构成，并且要求在 6 个小时内完成。这些题目均来自一个庞大的试题库，从而能够尽量做到考题因人而异。此外，为了更准确地反映最新的安全趋势，试题库会不断变化和更新，考题则根据需要在库中经常循环和替换。每个问题都有 4 个选项，其中只有一个选项是正确答案。考试中计入成绩的只有 225 道题，其余 25 道题仅供出题人员研究之用。但是，这 25 道题与计分的题目毫无区别，因此应试人员并不知道哪些题目是计入总分的。通过 CISSP 考试的最低分数是 700 分(总分是 1000 分)，每道题都会根据难度设定权重，而且并非每道题的分值都是一样的。此项考试不面向特定的产品或供应商，这意味着没有任何问题会针对特定的产品或供应商(例如 Windows 2000、UNIX 或 Cisco)，而是涉及测试这些系统所使用的安全模型和方法。

$(ISC)^2$(International Information Systems Security Certification Consortium，国际信息系统安全认

证协会)还在 CISSP 考试中增加了基于场景的问题。每个问题都向应试人员展示了一个简短的场景，而不是要求他们区分术语和/或概念。增加基于场景的问题，其目的是确保应试人员不仅知道和理解 CBK 中的概念，而且能够将这些知识应用到现实生活场景中。这种做法更为实用，其原因在于现实生活中不可能有人询问你："共谋(collusion)的定义是什么？"此时，除了需要知道"共谋"的定义外，还需要知道如何检测并阻止共谋的发生。

通过考试后，你会被要求提供由担保人认可的证明文件，以证明你确实具有相关类型的工作经验。担保人必须签署一份文件，从而为你提交的安全工作经验提供担保。因此，在注册并支付考试费用之前一定要与担保人取得联系。你肯定不愿意看到这样的局面：在支付费用并通过考试后，却发现无法找到担保人帮助你完成获得认证所需的最后步骤。

之所以要求提供担保，是为了确保获得认证的应试人员拥有为公司服务的实际工作经验。虽然书本知识对于理解理论、概念、标准和规章极其重要，但是决不能替代亲身经历。因此，请你一定要证明拥有支持认证实用性的实践经验。

$(ISC)^2$ 将从通过考试的候选人中随机挑选少数应试人员进行审查。在审查过程中，$(ISC)^2$ 工作人员将向候选人选定的担保人和联系人核实应试人员相关工作经验的真实性。

这项考试的挑战性在于：虽然大多数认证候选人都从事安全领域内的工作，但是不一定通晓 CBK 包含的全部 10 个领域。虽然某人被视为脆弱性测试或应用程序安全方面的专家，但是她可能不擅长于物理安全、密码学或安全实践。因此，为这项考试而学习将极大地拓宽你在安全领域的知识。

考题涉及构成 CBK 的 10 个安全领域，如表 1-1 所示。

表 1-1　构成 CISSP CBK 的 10 个安全领域

安 全 领 域	描　　述
访问控制	这个领域研究管理员和经营者控制访问的机制和方法。管理员和经营者需要控制被访问的内容、经过授权和身份验证后的用户权限、对访问活动的审计和监控。 该领域的部分主题包括： ● 访问控制威胁 ● 标识和身份验证技术与技巧 ● 访问控制管理 ● 单点登录技术 ● 攻击方法
通信与网络安全	这个领域研究内部的、外部的、公共的和私有的通信系统、互联结构、设备、协议以及远程访问和管理。 该领域的部分主题包括： ● OSI 模型和分层 ● 局域网(Local Area Network，LAN)、城域网(Metropolitan Area Network，MAN)和广域网(Wide Area Network，WAN)技术 ● 互联网、内联网和外联网问题 ● 虚拟专用网(Virtual Private Network，VPN)、防火墙、路由器、网桥和中继器 ● 网络拓扑和布线 ● 攻击方法

(续表)

安 全 领 域	描　　述
信息安全治理与风险管理	这个领域研究公司资产的标识，确定必要的安全保护级别的正确方式，用于降低风险和减少资金损失的安全实现应当采用何种类型的预算。 该领域的部分主题包括： ● 数据分类 ● 策略、措施、标准和指南 ● 风险评估和管理 ● 人事安全、培训和意识
软件开发安全	这个领域研究安全的软件开发方法，应用程序安全和软件缺陷。 该领域的部分主题包括： ● 数据仓库和数据挖掘 ● 不同的开发方法及其风险 ● 软件组件和脆弱性 ● 恶意代码
密码学	这个领域研究密码学中的技巧、方法和技术。 该领域的部分主题包括： ● 对称与非对称算法及其使用 ● 公钥基础设施(Public Key Infrastructure，PKI)与散列函数 ● 加密协议及其实现 ● 攻击方法
安全架构与设计	这个领域研究安全设计软件所应该使用的方式方法。也包括国际安全衡量标准以及这些标准对于不同平台的具体含义。 该领域的部分主题包括： ● 操作状态、内核功能与内存映射 ● 安全模型、架构和评估 ● 评估准则：可信计算机安全评估标准(Trusted Computer Security Evaluation Criteria TCSEC)、信息技术安全评估标准(Information Technology Security Evaluation Criteria，ITSEC)和通用准则 ● 应用程序与系统的常见缺陷 ● 认证与认可
操作安全	这个领域研究对人事、硬件、系统以及审计和监控技术的控制，此外还涉及可能的滥用途径及其识别和应对措施。 该领域的部分主题包括： ● 与人事和职位相关的行政管理责任 ● 防病毒、培训、审计和资源保护活动中的维护概念 ● 预防性、检测性、纠正性和恢复性控制 ● 标准、遵从与适当关注的概念 ● 安全与容错技术
业务连续性计划(Business Continuity Planning，BCP)与灾难恢复计划(Disaster Recovery Planning，DRP)	这个领域研究发生干扰或灾难时对业务活动的保存，它涉及对具体风险的标识、适当的风险评估以及对策的实现。 该领域的部分主题包括： ● 业务资源的标识和价值分配 ● 业务影响分析与可能损失预测 ● 业务单元的优先顺序与危机管理 ● 计划的开发、实现与维护

(续表)

安 全 领 域	描　　述
法律、合规、调查与遵从	这个领域研究计算机犯罪、法律和法规。它不仅包括犯罪调查、证据搜集和处置步骤所使用的技巧，而且涉及如何开发和实现事故处理程序。 该领域的部分主题包括： ● 法律、法规和犯罪的类型 ● 许可证发放和软件盗版 ● 进出口法律和事宜 ● 证据的类型以及获得法庭的接纳 ● 事故处理 ● 取证
物理(环境)安全	这个领域研究威胁、风险以及针对保护设施、硬件、数据、介质和人事的措施。它包括设施的选择、授权进入的方法以及环境和安全步骤。 该领域的部分主题包括： ● 受限区域、授权方法和控制 ● 运动探测器、传感器和告警 ● 入侵检测 ● 火灾的探测、预防和灭火 ● 栅栏、防护措施和安全证件的类型

为了紧跟安全领域的新技术和新方法，$(ISC)^2$ 每年都要在试题库中加入大量的新试题。这些试题都基于最新的技术、运用、方法和标准。例如，1998 年的 CISSP 认证考试没有出现关于无线安全、跨站点脚本攻击或 IPv6 的问题。

以前的考试中还未涉及的主题有：安全监管、即时通信、网络钓鱼、僵尸网络、VoIP 和垃圾邮件。虽然这些主题在过去不属于考试内容，但如今的考试会对它们进行考查。

CISSP 考试基于国际上普遍接受的信息安全标准和运用。例如，如果登录$(ISC)^2$ 的网站查询考试时间和地点，你就会发现，也许这个星期二在美国加利福尼亚有一场考试，而下个星期三在沙特阿拉伯也有一次同样的考试。

如果没有通过考试，那么你可以选择在任何时间重新参加考试。$(ISC)^2$ 曾经规定重考和前一次考试之间必须间隔一定的时间，然而目前该规定已被取消。$(ISC)^2$ 会记录你在初次考试时使用的试卷版本，从而确保在重考时采用不同版本的试卷。$(ISC)^2$ 还会向未通过考试的 CISSP 候选人提供报告，其中详细说明了该候选人最薄弱的知识领域。虽然现在可以立即参加随后的考试，但是你最好花一些时间复习这些薄弱环节，以便提高重考的成绩。

1.3　CISSP 认证的发展简史

长期以来，计算机和信息安全领域并不是一个结构化的和严格规范的行业。这个领域缺乏很多定义明确的专业目标，因此常常被人误解。

在 20 世纪 80 年代中期，计算机安全专业人员开始认识到需要通过某种资格认证体系来规范计算机安全行业，并证明从业人员的能力和资格。建立这样的资格认证体系将从整体上提高计算机安全行业及其从业人员的可信度。

1988 年 11 月，数据处理管理协会(Data Processing Management Association，DPMA)下属的计算机安全特别兴趣小组(Special Interest Group for Computer Security，SIG-CS)将几个对组建安全资格认证体系感兴趣的组织召集在一起，这些组织包括信息系统安全协会(Information Systems Security Association，ISSA)、加拿大信息处理协会(Canadian Information Processing Society，CIPS)、计算机安全研究所(Computer Security Institute，CSI)、爱达荷州立大学(Idaho State University)以及其他一些美国和加拿大的政府机构。正是由于这些组织的义务行动，才有了今天全面而系统的安全资格认证体系。$(ISC)^2$ 是在 1989 年年中成立的，作为一个非营利性机构，它负责为信息系统安全从业人员建立一套安全资格认证体系。这项认证旨在衡量专业能力，并帮助公司挑选安全专业人员。尽管$(ISC)^2$ 成立于北美洲，但它很快在国际上得到认可，如今已在全球范围内发挥着测试功能。

因为安全的范围很广，形式多样，并且涵盖了技术和业务的许多领域，所以最初的联盟决定采用一个信息系统安全的公共知识体系(CBK)。CBK 由 10 个子领域构成，涉及计算机、网络、业务和信息安全的各个方面。此外，由于技术的迅猛发展，因此紧跟安全趋势、技术和业务发展是维持 CISSP 认证的必然要求。除了考试本身，联盟还推出了道德规范、考试细则以及简明学习指南。

1.4 如何注册考试

要成为一名 CISSP，首先必须登录 www.isc2.org 报名参加考试。在该网站上，你会找到一个考试注册表单，填写表单后将其提交给$(ISC)^2$。你需要提供自己的安全行业工作经历以及必要的教育背景材料。你还必须阅读$(ISC)^2$ 的道德规范，并且签订一份文件，表示你理解这些规定并承诺照此执行。提交报名表的同时要支付考试费用，并告诉组织者你希望在何时何地参加考试。www.isc2.org 上会列出许多考试地点和日期。

1.5 本书概要

如果你想成为一名经过$(ISC)^2$ 认证的 CISSP，那么在这本书里能够找到需要了解的所有内容。本书讲述企业如何制定和实现策略、措施、指导原则和标准及其原因；介绍网络、应用程序和系统的脆弱性，脆弱性的被利用情况以及如何应对这些威胁；解释物理安全、操作安全以及不同系统会采用不同安全机制的原因。此外，本书还回顾美国与国际上用于测试系统安全性的安全准则和评估体系，诠释这些准则的含义及其使用原因。最后，本书还将阐明与计算机系统及其数据相关的各种法律责任问题，例如计算机犯罪、法庭证物以及如何为出庭准备计算机证据。

尽管本书主要是为 CISSP 考试编写的学习指南，但是在你通过认证之后，它仍不失为一本不可替代的重要参考用书。

1.6 CISSP 应试小贴士

如果你参加的是涂卡测试，则由 CISSP 考官监场。你带进考场的任何食物和饮料都不得放在自己的考桌上，要统一存放在考场后面的桌子上。考官会检查你带入考场的所有物品。此外，考生在考试中会有去洗手间的固定时段，但是通常每次只允许一人前往。因此，最好不要为了保持精力而

在考试前饮用过多的咖啡。

注意：

(ISC)^2 仍然使用机读卡，需要在考卷上涂黑选项。考试机构正考虑通过 PearsonVue 中心提供数字形式的考试。

在考试过程中禁止使用手机和移动设备。你可以把它们放置在考场前面，考试结束时再拿走。以往的考试中很多人使用手机或者移动设备作弊，所以现在采取了这样的防范措施。

许多人考试时会感觉题目比较绕弯。所以一定要仔细阅读问题和所有备选答案，而不是看了几个单词就断定自己已知道问题的答案。某些答案选项的差别不明显，这就需要你花一些时间耐心地将问题再阅读领会几遍。

与大多数考试一样，你最好先解答自己知道的问题，然后再解答较为困难的问题。CISSP 认证考试还没有计算机化(但(ISC)^2 正逐渐向计算机化转型)，所以会发放成册的试卷与一张答题卡。如果你在答题卡上涂黑的范围超出了规定的边框，那么阅卷机就会将答对的考题视为答错。因此，我建议你第一遍答题时在试卷上标注正确答案，直至全部问题解答完毕。随后，再次检查答案并填写答题卡，这样就不会有过多的涂抹，从而避免阅卷机可能造成的错误。试卷可以任意涂写。考试结束后，考生必须同时上交试卷和答题卡，但是只有答题卡上的答案有效。因此，务必确保在答题卡上填写了所有答案。

在同一考场内可能会同时进行(ISC)^2 的其他认证考试，如 SSCP(Systems Security Certified Professional，系统安全认证专家)、ISSAP 或 ISSMP(信息系统安全架构专家或信息系统安全管理专家，分别涉及架构和管理)以及 ISSEP(信息系统安全工程专家，关注于工程)。这些认证考试的时间长短各不相同。因此，如果看到其他人离开考场，那么千万不要着急，因为他们参加的可能是时间较短的其他考试。

做完试题后，不要立即交卷。你有 6 个小时的时间，因此不要因为觉得厌倦或感到焦虑就浪费考试时间。一定要充分利用这 6 个小时。在交卷前，最好再花点时间检查一下是否回答了所有的问题，尤其是要留意在回答一个问题时是否粗心地填涂了两个答案。

遗憾的是，你无法在考试刚结束时就知道结果。(ISC)^2 规定最多等待 6 个星期就可以知道结果，不过应试人员平均只需 4 天～两个星期就会收到邮件和/或电子邮件通知。

如果通过了考试，那么通知单上就不会出现你的分数，你只知道自己通过考试了。如果不幸没有通过考试，那么通知单上会列出你各项的成绩，这样应试人员就能知道自己的强项和弱项，从而在准备下次考试时有针对性地重点学习自己较弱的领域。如果没有通过考试，那么不要气馁，要知道某些十分聪明且有天分的安全专家也并非第一次就通过了考试，毕竟这项考试涵盖的主题实在太广泛了。

关于这项资格认证较为常见的抱怨之一是考试本身。与 Microsoft 的许多考试相同，CISSP 考试的题目并不绕弯子，但是偶尔也会出现两个难以区分的答案。虽然(ISC)^2 已经不再使用诸如“不”、“除……之外”之类的否定词，但是它们在试卷中有时仍会出现。基于场景的问题需要应试人员理解多个领域的概念才能给出正确答案。

此外，还有人抱怨 CISSP 考试略带主观色彩。例如，有这样两个问题。第一个是技术问题，考查的是防止中间人攻击的 SSL(Secure Socket Layer，安全套接字层)所采用的具体机制；第二个问题则询问周长为 8 英尺的栅栏提供的是低级、中级还是高级的安全防护。你会发现，前一个问题比后一个问题更容易回答。许多问题要求应试人员选择最佳方法，而一些人会认为很难说哪一

个是最佳方法，因为这都带有主观色彩。此处给出这样的示例并非是批评(ISC)^2 和出题人员，而是为了帮助你更好地准备这项考试。本书涵盖了所有的考试范围和需要掌握的内容，同时也提供了大量问题和自测试卷。大部分问题的格式都采用了实际试题的形式，从而使你能够更好地准备应对真实的考试。因此，你一定要阅读本书的全部内容，同时特别注意问题及其格式。有些时候，即使对某个主题十分了解，你也可能答错问题。因此，我们需要学会如何应试。

尽量让自己熟悉行业标准，并且了解自己工作之外的技术知识和方法。再次强调一下，即使你在某个领域是专家，仍然可能不熟悉考试所涉及的全部领域。你可以利用本章的评估测试题测试一下自己的知识水平，并做好准备学习自己尚未接触或并不熟悉的内容。

1.7 本书使用指南

本书的作者尽了很大努力才将所有重要的信息汇编成书；现在，轮到读者尽力从本书中汲取这些信息了。要想从本书受益最大，你可以采用以下学习方法：

(1) 认真学习每个章节，真正理解其中介绍的每一个概念。许多概念都必须完全理解，如果对一些概念似懂非懂，那么对你来说将是非常不利的。CISSP CBK 包含数以千计的不同主题，因此需要花时间掌握这些内容。

(2) 确认学习和解答每章末尾以及本书附带光盘中的所有问题。如果不能正确解答其中的问题，那么需要再次阅读相关的章节。需要记住的是，真实考试中的某些问题含糊其辞，看上去比较难回答，为此本书作者特意设计了一些这样的问题。因此，不要误以为作者不会设计问题而忽视了这些含糊其辞的问题。相反，它们的存在具有明确的目的性，对此读者要特别注意。

(3) 如果对某些具体的主题(如防火墙、法律、物理安全或协议功能)不熟悉，那么需要通过其他信息源(书籍和文章等)以达到对这些主题更深入的理解程度，而不是局限于自认为通过资格考试所需的范围。

(4) 阅读本书之后，你需要学习所有问题和答案，并进行自测。接着，查看(ISC)^2 的学习指南，确信对列出的每条内容都十分了解。如果对某些内容还觉得困惑，那么请重新复习相关的章节。

(5) 如果参加过其他资格认证考试(如 Cisco、Novell 和 Microsoft 的认证考试)，那么你可能习惯于记忆一些细节和配置参数。但是请记住，CISSP 考试强调的是广度而非深度，因此在记忆具体细节之前一定要先掌握每个主题中的各种概念。

(6) 记住该考试是需要找出最佳答案，所以，对于有些问题应试人员可能会对全部或部分答案持不同意见。记住要在所给的 4 个答案中找出最佳的那一个。

1.7.1 问题

为了更好地测试自己的专业水平，了解自己与通过 CISSP 考试之间的差距，你可以尝试解答下面的问题：

1. Which of the following provides an incorrect characteristic of a memory leak?

A. Common programming error

B. Common when languages that have no built-in automatic garbage collection are used

C. Common in applications written in Java

D. Common in applications written in C++

2. Which of the following is the best description pertaining to the "Trusted Computing Base"?

A. The term originated from the Orange Book and pertains to firmware

B. The term originated from the Orange Book and addresses the security mechanisms that are only implemented by the operating system

C. The term originated from the Orange Book and contains the protection mechanisms within a system

D. The term originated from the Rainbow Series and addressed the level of significance each mechanism of a system portrays in a secure environment

3. Which of the following is the best description of the security kernel and the reference monitor?

A. The reference monitor is a piece of software that runs on top of the security kernel. The reference monitor is accessed by every security call of the security kernel. The security kernel is too large to test and verify

B. The reference monitor concept is a small program that is not related to the security kernel. It will enforce access rules upon subjects who attempt to access specific objects. This program is regularly used with modern operating systems

C. The reference monitor concept is used strictly for database access control and is one of the key components in maintaining referential integrity within the system. It is impossible for the user to circumvent the reference monitor

D. The reference monitor and security kernel are core components of modern operating systems. They work together to mediate all access between subjects and objects. They should not be able to be circumvented and must be called upon for every access attempt

4. Which of the following models incorporates the idea of separation of duties and requires that all modifications to data and objects be done through programs?

A. State machine model

B. Bell-LaPadula model

C. Clark-Wilson model

D. Biba model

5. Which of the following best describes the hierarchical levels of privilege within the architecture of a computer system?

A. Computer system ring structure

B. Microcode abstraction levels of security

C. Operating system user mode

D. Operating system kernel mode

6. Which of the following is an untrue statement?

i. Virtual machines can be used to provide secure, isolated sandboxes for running untrusted applications.

ii. Virtual machines can be used to create execution environments with resource limits and, given the right schedulers, resource guarantees.

iii. Virtualization can be used to simulate networks of independent computers.

iv. Virtual machines can be used to run multiple operating systems simultaneously: different versions, or even entirely different systems, which can be on hot standby.

A. All of them
B. None of them
C. i, ii
D. ii, iii

7. Which of the following is the best means of transferring information when parties do not have a shared secret and large quantities of sensitive information must be transmitted?
A. Use of public key encryption to secure a secret key, and message encryption using the secret key
B. Use of the recipient's public key for encryption, and decryption based on the recipient's private key
C. Use of software encryption assisted by a hardware encryption accelerator
D. Use of elliptic curve encryption

8. Which algorithm did NIST choose to become the Advanced Encryption Standard (AES) replacing the Data Encryption Standard (DES)?
A. DEA
B. Rijndael
C. Twofish
D. IDEA

Use the following scenario to answer questions 9–11. John is the security administrator for company X. He has been asked to oversee the installation of a fire suppression sprinkler system, as recent unusually dry weather has increased the likelihood of fire. Fire could potentially cause a great amount of damage to the organization's assets. The sprinkler system is designed to reduce the impact of fire on the company.

9. In this scenario, fire is considered which of the following?
A. Vulnerability
B. Threat
C. Risk
D. Countermeasure

10. In this scenario, the sprinkler system is considered which of the following?
A. Vulnerability
B. Threat
C. Risk
D. Countermeasure

11. In this scenario, the likelihood and damage potential of a fire is considered which of the following?
A. Vulnerability
B. Threat
C. Risk
D. Countermeasure

Use the following scenario to answer questions 12–14. A small remote facility for a company is valued at $800,000. It is estimated, based on historical data and other predictors, that a fire is likely to

occur once every ten years at a facility in this area. It is estimated that such a fire would destroy 60 percent of the facility under the current circumstances and with the current detective and preventative controls in place.

12. What is the single loss expectancy (SLE) for the facility suffering from a fire?

A. $80,000

B. $480,000

C. $320,000

D. 60 percent

13. What is the annualized rate of occurrence (ARO)?

A. 1

B. 10

C. .1

D. .01

14. What is the annualized loss expectancy (ALE)?

A. $480,000

B. $32,000

C. $48,000

D. .6

15. Which of the following is not a characteristic of Protected Extensible Authentication Protocol?

A. Authentication protocol used in wireless networks and point-to-point connections

B. Designed to provide improved secure authentication for 802.11 WLANs

C. Designed to support 802.1x port access control and Transport Layer Security

D. Designed to support password-protected connections

16. Which of the following best describes the Temporal Key Integrity Protocol's(TKIP) role in the 802.11i standard?

A. It provides 802.1x and EAP to increase the authentication strength

B. It requires the access point and the wireless device to authenticate to each other

C. It sends the SSID and MAC value in ciphertext

D. It adds more keying material for the RC4 algorithm

17. Vendors have implemented various solutions to overcome the vulnerabilities of the wired equivalent protocol (WEP). Which of the following provides an incorrect mapping between these solutions and their characteristics?

A. LEAP requires a PKI

B. PEAP only requires the server to authenticate using a digital certificate

C. EAP-TLS requires both the wireless device and server to authenticate using digital certificates

D. PEAP allows the user to provide a password

18. Encapsulating Security Payload (ESP), which is one protocol within the IPSec protocol suite, is primarily designed to provide which of the following?

A. Confidentiality

B. Cryptography

C. Digital signatures

D. Access control

19. Which of the following redundant array of independent disks implementations uses interleave parity?

A. Level 1

B. Level 2

C. Level 4

D. Level 5

20. Which of the following is not one of the stages of the dynamic host configuration protocol (DHCP) lease process?

i. Discover

ii. Offer

iii. Request

iv. Acknowledgment

A. All of them

B. None of them

C. i

D. ii

21. Which of the following has been deemed by the Internet Architecture Board as unethical behavior for Internet users?

A. Creating computer viruses

B. Monitoring data traffic

C. Wasting computer resources

D. Concealing unauthorized accesses

22. Most computer-related documents are categorized as which of the following types of evidence?

A. Hearsay evidence

B. Direct evidence

C. Corroborative evidence

D. Circumstantial evidence

23. During the examination and analysis process of a forensics investigation, it is critical that the investigator works from an image that contains all of the data from the original disk. The image must have all but which of the following characteristics?

A. Byte-level copy

B. Captured slack spaces

C. Captured deleted files

D. Captured unallocated clusters

24. _____ is a process of interactively producing more detailed versions of objects by populating variables with different values. It is often used to prevent inference attacks.

A. Polyinstantiation

B. Polymorphism

C. Polyabsorbtion

D. Polyobject

25. Tim is a software developer for a financial institution. He develops middleware software code that carries out his company's business logic functions. One of the applications he works with is written in the C programming language and seems to be taking up too much memory as it runs over a period of time. Which of the following best describes what Tim needs to look at implementing to rid this software of this type of problem?

A. Bounds checking

B. Garbage collection

C. Parameter checking

D. Compiling

26. _____ is a software testing technique that provides invalid, unexpected, or random data to the inputs of a program.

A. Agile testing

B. Structured testing

C. Fuzzing

D. EICAR

27. Which type of malware can change its own code, making it harder to detect with antivirus software?

A. Stealth virus

B. Polymorphic virus

C. Trojan horse

D. Logic bomb

28. What is derived from a passphrase?

A. A personal password

B. A virtual password

C. A user ID

D. A valid password

29. Which access control model is user-directed?

A. Nondiscretionary

B. Mandatory

C. Identity-based

D. Discretionary

30. Which item is not part of a Kerberos authentication implementation?

A. A message authentication code

B. A ticket-granting ticket

C. Authentication service

D. Users, programs, and services

31. If a company has a high turnover rate, which access control structure is best?

A. Role-based

B. Decentralized

C. Rule-based

D. Discretionary

32. In discretionary access control, who/what has delegation authority to grant access to data?

A. A user

B. A security officer

C. A security policy

D. An owner

33. Remote access security using a token one-time password generation is an example of which of the following?

A. Something you have

B. Something you know

C. Something you are

D. Two-factor authentication

34. What is a crossover error rate (CER)?

A. A rating used as a performance metric for a biometric system

B. The number of Type I errors

C. The number of Type II errors

D. The number reached when Type I errors exceed the number of Type II errors

35. What does a retina scan biometric system do?

A. Examines the pattern, color, and shading of the area around the cornea

B. Examines the patterns and records the similarities between an individual's eyes

C. Examines the pattern of blood vessels at the back of the eye

D. Examines the geometry of the eyeball

36. If you are using a synchronous token device, what does this mean?

A. The device synchronizes with the authentication service by using internal time or events

B. The device synchronizes with the user's workstation to ensure the credentials it sends to the authentication service are correct

C. The device synchronizes with the token to ensure the timestamp is valid and correct

D. The device synchronizes by using a challenge-response method with the authentication service

37. What is a clipping level?

A. The threshold for an activity

B. The size of a control zone

C. Explicit rules of authorization

D. A physical security mechanism

38. Which intrusion detection system would monitor user and network behavior?

A. Statistical/anomaly-based

B. Signature-based

C. Static

D. Host-based

39. When should a Class C fire extinguisher be used instead of a Class A?

A. When electrical equipment is on fire

B. When wood and paper are on fire

C. When a combustible liquid is on fire

D. When the fire is in an open area

40. How does halon suppress fires?

A. It reduces the fire's fuel intake

B. It reduces the temperature of the area

C. It disrupts the chemical reactions of a fire

D. It reduces the oxygen in the area

41. What is the problem with high humidity in a data processing environment?

A. Corrosion

B. Fault tolerance

C. Static electricity

D. Contaminants

42. What is the definition of a power fault?

A. Prolonged loss of power

B. Momentary low voltage

C. Prolonged high voltage

D. Momentary power outage

43. Who has the primary responsibility of determining the classification level for information?

A. The functional manager

B. Middle management

C. The owner

D. The user

44. Which best describes the purpose of the ALE calculation?

A. It quantifies the security level of the environment

B. It estimates the loss potential from a threat

C. It quantifies the cost/benefit result

D. It estimates the loss potential from a threat in a one-year time span

45. How do you calculate residual risk?

A. Threats × risks × asset value

B. (Threats × asset value × vulnerability) × risks

C. SLE × frequency

D. (Threats × vulnerability × asset value) × control gap

46. What is the Delphi method?

A. A way of calculating the cost/benefit ratio for safeguards

B. A way of allowing individuals to express their opinions anonymously

C. A way of allowing groups to discuss and collaborate on the best security approaches

D. A way of performing a quantitative risk analysis

47. What are the necessary components of a smurf attack?

A. Web server, attacker, and fragment offset

B. Fragment offset, amplifying network, and victim

C. Victim, amplifying network, and attacker

D. DNS server, attacker, and web server

48. What do the reference monitor and security kernel do in an operating system?

A. Intercept and mediate a subject attempting to access objects

B. Point virtual memory addresses to real memory addresses

C. House and protect the security kernel

D. Monitor privileged memory usage by applications

1.7.2 答案

1. C	**2. C**	**3. D**	**4. C**	**5. A**	**6. B**	**7. A**	**8. B**	**9. B**	**10. D**
11. C	**12. B**	**13. C**	**14. C**	**15. D**	**16. D**	**17. A**	**18. A**	**19. D**	**20. B**
21. C	**22. A**	**23. A**	**24. A**	**25. B**	**26. C**	**27. B**	**28. B**	**29. D**	**30. A**
31. A	**32. D**	**33. A**	**34. A**	**35. C**	**36. A**	**37. A**	**38. A**	**39. A**	**40. C**
41. A	**42. D**	**43. C**	**44. D**	**45. D**	**46. B**	**47. C**	**48. A**		

第 2 章

信息安全治理与风险管理

本章主要内容:

- 安全术语和原则
- 保护控制类型
- 安全框架、模型、标准和最佳实践
- 安全企业架构
- 风险管理
- 安全文档
- 信息分类和保护
- 安全意识培训
- 安全治理

其实， 除安全实践外，组织机构还有很多其他事情可做。毕竟，企业存在的目的是赚钱。只有大部分非营利组织如慈善机构、教育中心和宗教实体等，其存在的目的是提供某种类型的服务。而多数组织机构存在的目的都不是要专门部署和维护防火墙、入侵检测系统、身份管理技术和加密设备。没有企业真正愿意开发成百上千的安全策略，部署反恶意软件，维护脆弱性管理系统，不断更新事件响应能力，以及不得不遵循各种令人眼花缭乱的安全法规(SOX、GLBA、PCI-DSS、HIPAA)和联邦与州的法律。企业主只愿意制造他们的产品，销售他们的产品，然后回家。但是，这样简单的日子一去不复返了。现在组织机构面临着挑战：有人想要偷取企业顾客数据，从而可以窃取身份以进行银行欺诈。公司机密不断被来自内部和外部的实体窃取，用于从事经济间谍活动。系统被劫持和用于僵尸网络，以攻击其他组织或者传播垃圾邮件。公司资金被来自不同国家的有组织的犯罪团伙通过复杂的、难以确认的数字方法秘密抽走。那些发现自己已经成为攻击者目标的组织机构正在不断地遭受攻击，他们的系统和网站可能数小时或者数日都不能运作。当今的企业需要践行大量安全规则才能维护他们的市场份额、保护他们的顾客和底线，远离牢狱之灾，以及销售产品。

本章将讨论组织为整体践行安全而必须遵循的诸多原则。每个组织机构都必须开发企业安全计划，该计划中所包含的技术、措施和进程将贯穿整本书。在从事安全工作的整个职业生涯中，你会发现，多数企业只践行了“企业安全计划”的一部分，而不是全部。几乎每个组织都在处心积虑地考虑如何评估公司所面临的风险以及如何分配资金和资源来遏制那些风险。可以说，当今企业所制定的安全计划中有很多只是片面的和残缺的。团队熟悉的领域，其安全计划也优越，而

不熟悉的领域，安全计划就匮乏。因此，你有责任尽可能全面地了解整个安全领域，只有这样，才能识别安全计划中的不足之处，然后改进它们。这也是 CISSP 考试覆盖技术、方法和进程等诸多领域的原因所在。如果要帮助一个组织执行整体的安全任务，就必须从整体的角度理解并掌握它们。

首先，我们会从安全的基本内容入手，然后在此基础上展开本章甚至整本书的内容。构建知识基础就好比盖房子：没有坚实的基础，房子就不坚固，后果就不可预料，不知什么时候就会倒塌。我们的目标是确保你拥有扎实和牢固的根基，这样才能保护自己免受诸多威胁的伤害，保护那些依赖你和你的技术的商业组织和政府组织免受伤害。

2.1 安全基本原则

我们需要知道，安全的核心目标是为关键资产提供可用性、完整性和机密性(AIC 三元组，如图 2-1 所示)保护。每项资产所需的保护级别不相同，具体将在下面讨论。所有安全控制、机制和防护措施的实现都是为了提供这些原则中的一个或多个，并且要为潜在的能力衡量所有风险、威胁和脆弱性，以平衡一个或全部 AIC 原则。

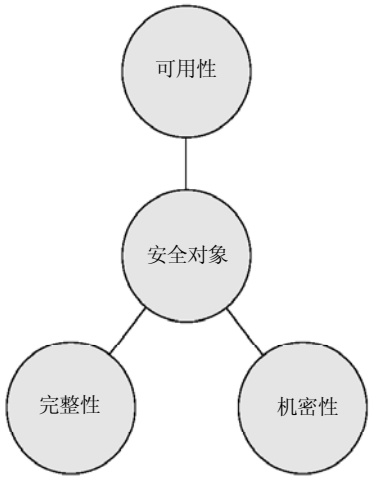

图 2-1 AIC 三元组

注意：

在某些文档中，三元组用 CIA 表示，分别代表机密性(confidentiality)、完整性(integrity)和可用性(availability)。

2.1.1 可用性

——紧急情况！我访问不了我的数据！

——打开计算机！

可用性(availability)保护确保授权的用户能够对数据和资源进行及时的和可靠的访问。网络设备、计算机和应用程序应当提供充分的功能，从而能够在可以接受的性能级别以可预计的方式运行。它们应该能够以一种安全而快速的方式从崩溃中恢复，这样生产活动就不会受到负面影响。

应该采取必要的保护措施消除来自内部或外部的威胁，这些威胁会影响所有业务处理组件的可用性及工作效率。

和生活中的许多其他事情一样，确保组织内部必要资源的可用性听起来容易，实际做起来却很难。网络由众多必须在深夜持续运行的组件构成(路由器、交换器、DNS 服务器、DHCP 服务器、代理和防火墙)。软件也由众多必须健康运行的组件构成(操作系统、应用程序和反病毒软件)。此外还有很多能够影响到组织运营的环境因素(如大火、洪水、HVAC 问题、电子问题)、潜在的自然灾害和物理偷窃或攻击。组织必须完全了解它的运营环境和它在可用性方面的缺陷，才能采取正确的对策。

2.1.2　完整性

完整性(integrity)指的是保证信息和系统的准确性和可靠性，并禁止对数据的非授权更改。硬件、软件和通信机制必须协同工作，以便正确地维护和处理数据，并且能够在不被意外更改的情况下将数据移动至预期的目的地。应当保护系统和网络免受外界的干扰和污染。

实施和提供这种安全属性的系统环境能够确保攻击者或用户错误不会对系统或数据的完整性造成损害。当攻击者在系统中加入病毒、逻辑炸弹或后门时，系统的完整性就被破坏了。随后，它将破坏系统上保存的信息的完整性，如使数据出错、恶意修改数据或替换为不正确的数据。严格的访问控制、入侵检测和散列运算可以抗击这些威胁。

用户也会经常错误地影响系统或数据的完整性。当然，内部用户也可能故意做坏事。例如，用户可能在不经意间删除了配置文件，因为硬盘已满，而用户又不记得使用过文件 boot.ini。或者，用户也可能在数据处理应用程序中输入了错误值，使得本应交纳 300 美元的客户交纳了 3000 美元。在数据库中存储的被错误修改的数据是用户偶尔使数据出错的一种常见方式，这种错误会造成持久的影响。

应当精简用户的能力，只向其提供少数几个选择和功能，这样错误就会减少，而且也不会那么严重。应当限制用户对系统关键文件的查看和访问。应用程序应当提供检查输入值是否有效且合理的机制。数据库应当只允许授权用户修改数据，而传输数据则应当通过加密或其他机制进行保护。

2.1.3　机密性

——我保护了我最机密的秘密。

——没人想知道它。

机密性(confidentiality)确保在数据处理的每一个交叉点上都实施了必要级别的安全保护并阻止未经授权的信息披露。在数据存储到网络内部的系统和设备上时、数据传输时以及数据到达目的地之后，这种级别的机密性都应该发挥作用。

攻击者能够通过网络监控、肩窥、盗取密码文件以及社会工程来威胁机密性机制。这些内容将在后面的章节中进行更深入的讨论。简单地说，肩窥(shoulder surfing)指的是某人越过其他人的肩膀观察其按键动作或偷看计算机屏幕上显示的数据。社会工程(social engineering)指的是欺骗其他人共享机密信息，例如装扮成已被授权的人以访问机密信息。社会工程还可以采用其他许多形式。事实上，任何一对一的通信介质都能够用于执行社会工程攻击。

当用户在向其他人发送信息而没有加密的时候，在成为社会工程攻击的牺牲品的时候，在共享公司商业秘密的时候，或者是在处理机密信息而没有采取额外保护措施的时候，他们都会有意或无意泄露了某些敏感信息。

通过以下途径可以提供机密性：在存储和传输数据时进行加密；使用严格的访问控制和数据分类；以及对职员进行适当的数据保护措施培训。

可用性、完整性和机密性是安全问题的关键原则。我们应当理解这 3 个原则的含义、各种机制如何提供这些原则以及缺少这些原则会对系统环境造成怎样的负面影响。

2.1.4 平衡安全

实际上，在涉及信息安全问题时，往往只针对机密信息保密(机密性)。而完整性和可用性威胁可以被忽略，除非它们遭到破坏。某些资产严格要求机密性(如公司商业秘密)，某些资产严格要求完整性(如金融交易数值)，某些资产严格要求可用性(电子商务网络服务器)。很多人知道 AIC 三元组的概念，但却可能并不完全理解实施必要的控制措施以为所有这些概念所覆盖的领域提供保护的复杂性。下面提供了一些控制措施及它们所对应的 AIC 三元组的原则。

- 可用性
  - 廉价磁盘冗余阵列(RAID)
  - 群集
  - 负载平衡
  - 冗余数据和电源线
  - 软件和数据备份
  - 磁盘映像
  - co-location 和异地备用设施
  - 回滚功能
  - 故障切换配置
- 完整性
  - 散列(数据完整性)
  - 配置管理(系统完整性)
  - 变更控制(进程完整性)
  - 访问控制(物理的和技术的)
  - 软件数字签名
  - 传输 CRC 功能
- 机密性
  - 加密休息中的数据(整个磁盘、数据库加密)
  - 加密传输中的数据(IPSec、SSL、PPTP、SSH)
  - 访问控制(物理的和技术的)

本书将会对所有上述控制措施一一赘述。重要的是此处要了解 AIC 三元组的概念看似简单，而实际满足它的要求是非常具有挑战性的。

关键术语

- **可用性** 确保授权的用户能够及时、可靠地访问数据和资源。
- **完整性** 保证信息和系统的准确性和可靠性，并禁止对数据的非授权更改。
- **机密性** 强制实施了必要的保密级别，防止未经授权的信息披露。
- **肩窥** 越过别人肩膀浏览未授权浏览的信息。
- **社会工程** 欺骗他人共享敏感信息以获取未经授权的访问。

2.2　安全定义

——我很脆弱，觉得你是个威胁。

——好。

我们常常使用术语“脆弱性”、“威胁”、“风险”和“暴露”来表示同样的事情，然而，它们实际上有不同的含义，相互之间也有不同的关系。理解每一个术语的定义是非常重要的，但更重要的是应当理解它们彼此之间的关系。

脆弱性(vulnerability)是指缺少安全措施或者说采用的安全措施有缺陷。它是一种软件、硬件、过程或人为缺陷。这种脆弱性可能是在服务器上运行的某个服务、未安装补丁的应用程序或操作系统、没有限制的无线访问点、防火墙上的某个开放端口、任何人都能够进入服务器机房的松懈安防或者服务器和工作站上未实施的密码管理。

威胁(threat)是指利用脆弱性而带来的潜在危险。威胁就是某人或某个软件识别出特定的脆弱性，并利用其来危害公司或个人。利用脆弱性的实体就称为威胁主体。威胁主体可能是通过防火墙上的某个端口访问网络的入侵者、违反安全策略进行数据访问的过程或者毁坏设施的龙卷风，也可能是某位雇员犯下的、可能泄露机密信息或破坏文件完整性的意外错误。

风险(risk)是威胁主体利用脆弱性的可能性以及相应的业务影响。如果某个防火墙有几个开放端口，那么入侵者利用其中一个端口对网络进行未授权访问的可能性就会较大。如果没有对用户进行过程和措施的相关教育，那么雇员由于故意或无意犯错而破坏数据的可能性就会较大。如果网络没有安装入侵检测系统，那么在不引人注意的情况下进行攻击且很晚才被发现的可能性就会较大。风险将脆弱性、威胁和利用可能性与造成的业务影响联系在一起。

暴露(exposure)是造成损失的实例。脆弱性能够导致组织机构遭受破坏。如果密码管理极为松懈，也没有实施相关的密码规则，那么公司的用户密码就有可能会被盗取并在未授权状况下使用。如果没有人监管公司的规章制度，不预先采取预防火灾的措施，公司就可能遭受毁灭性的火灾。

控制(control)或对策(countermeasure)能够消除(或降低)潜在的风险。对策可以是软件配置、硬件设备或措施，它能够消除脆弱性或者降低威胁主体利用脆弱性的可能性。对策的示例包括强密码管理、防火墙、保安、访问控制机制、加密和安全意识培训。

注意：

术语控制(control)、对策(countermeasure)和防护措施(safeguard)交替使用，都是指降低风险的机制。

如果某个公司只是在服务器上安装防病毒软件，但是不能及时更新病毒特征库，那么这就是一种脆弱性。该公司很容易遭受病毒攻击。威胁是指病毒将出现在系统环境中在系统环境中并破坏系统的工作能力。病毒出现在系统环境中并形成危害的可能性就是风险。如果病毒渗透入公司的系统环境，那么脆弱性就被利用，公司也将遭受损失。这种情况下的对策就是更新病毒特征库，并在所有计算机上都安装防病毒软件。图 2-2 说明了风险、脆弱性、威胁和对策之间的关系。

应用正确的对策可以消除脆弱性和暴露，从而能够降低风险。这个公司并不能消除威胁主体，但是可以保护自己，以及防止威胁主体利用系统环境中的脆弱性。

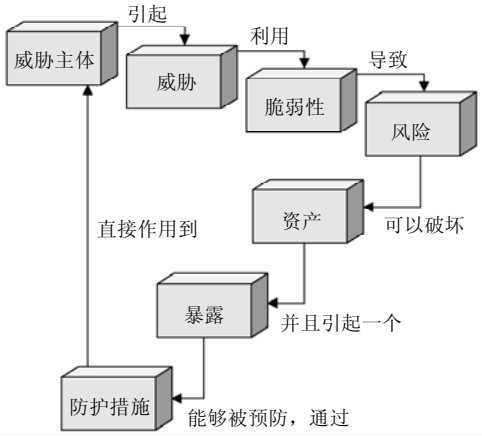

图 2-2　各种安全组件之间的关系

许多人忽视这些基本术语，认为在信息安全界它们并非那么重要。但是，你将发现如果安全团队没有就此达成共同意见，混乱很快就会出现。这些术语代表着安全领域的核心理念，如果混淆这些理念，据此所做的加强安全的任何活动也往往会被混淆。

关键术语

- **脆弱性**　缺陷或者缺少措施。
- **威胁实体**　能够利用脆弱性的实体。
- **威胁**　利用脆弱性的威胁实体所带来的危险。
- **风险**　威胁实体利用脆弱性的可能性及其相关影响。
- **控制**　为降低风险而采用的防护措施，也叫对策。
- **暴露**　显示脆弱性，把组织暴露于威胁之下。

2.3　控制类型

到本节为止，已经讲述了安全目标(可用性、完整性、机密性)和安全行业的术语(脆弱性、威胁、风险和控制)。如果组织要想很好地开展安全工作，必须要理解这些基础知识。要解决的下一个基本问题是可以实现的控制类型及其相关的功能。

正确运用控制措施能降低组织面临的风险，控制包含 3 种类型：管理控制、技术控制和物理控制。管理控制(administrative control)因为通常是面向管理的，所以经常被称为“软控制”。安全文档、风险管理、人员安全和培训都属于管理控制。技术控制(technical control)也称为逻辑控制由软件或硬件组成，如防火墙、入侵检测系统、加密、身份识别和认证机制。物理控制(physical control)用来保护设备、人员和资源，保安、锁、围墙和照明都属于物理控制。

正确运用这些控制措施才能为企业提供深度防御，深度防御是指以分层的方法综合使用多个安全控制类型，如图 2-3 所示。由于入侵者在获得访问关键资产前将不得不穿越多个不同的保护机制，因此多层防御能够将渗透成功率和威胁降低到最小。例如，A 公司按照分层模型采用了以下物理控制措施：

- 围墙
- 外部上锁的门
- 闭路监控
- 保安
- 内部上锁的门
- 上锁的服务器房间
- 物理防护的计算机(线缆锁)

技术控制措施通常会采用以下分层方法部署应用：

- 防火墙
- 入侵检测系统
- 入侵防御系统
- 恶意代码防御
- 访问控制
- 加密

实际采用的控制类型必须与公司面临的威胁相对应，保护的层数必须与资产的敏感程度相对应。“拇指型规则”描述了资产越敏感，部署的保护层数越多。

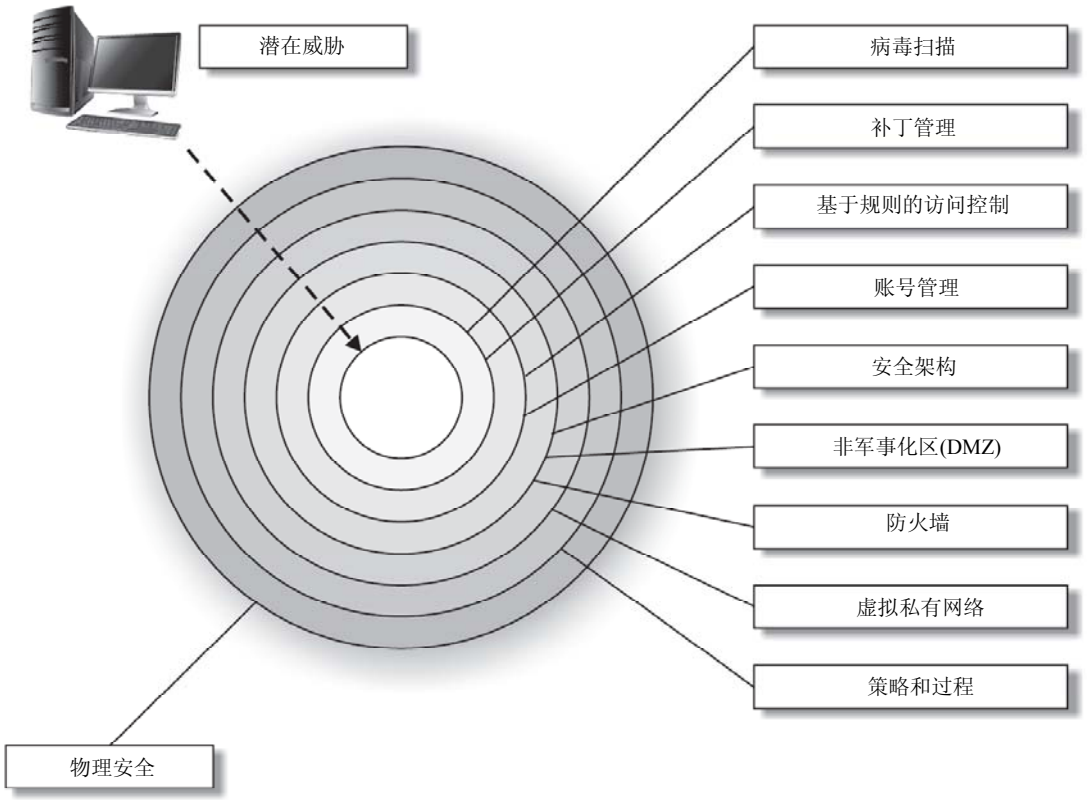

图 2-3　深度防御

可以运用不同的控制类型——管理控制、技术控制、物理控制，这些控制措施是如何发挥作用的呢？在我们寻求措施保护我们的环境时，需要理解每个控制措施的不同功能。

安全控制措施的不同功能有：预防性、检测性、纠正性、威慑性、恢复性和补偿性。更好地

理解安全控制措施的不同功能后，在特定条件下就能做出明智的决定，选择出最合适的控制措施。下面是 6 种不同的安全控制功能。

- 威慑性：威慑潜在的攻击者。
- 预防性：避免意外事件的发生。
- 纠正性：意外事件发生后修补组件或系统。
- 恢复性：使环境恢复到正常的操作状态。
- 检测性：帮助识别意外活动和潜在入侵者。
- 补偿性：能提供可替代的控制方法。

一旦完全理解了不同控制措施的作用，在应对特定风险时，就能正确运用它们或把它们运用在最适合的地方。

当查看一个环境的安全结构时，效率最高的方法是使用预防性的安全模型，然后使用检测、恢复和纠正机制支撑这个模型。最初，是想在麻烦开始前预防它们，但必须能够在麻烦发现你时快速行动并应对它们。因为预防一切是不可行的，所以如果不能预防麻烦，就必须能够快速检测它们。这就是为什么预防性和检测性控制措施必须一起实施且应该相互补充的原因。深入分析一下：不能够预防的则必须能够检测到，同时，如果能检测到，意味着你不能预防。因此，应该采取纠正性措施，确保下一次发生时能够预防。综上所述，预防性措施、检测性措施和纠正性措施应该一起使用。

下面描述的控制模型(管理的、物理的、技术的)从本质上讲都是预防性的。在开发企业范围的安全程序时，理解这一点很重要。

- 预防—管理性措施
  - 策略和规程
  - 高效的雇用实践
  - 聘用前的背景调查
  - 受控解聘流程
  - 数据分类和标签
  - 安全意识
- 预防—物理性措施
  - 证件、磁卡
  - 警卫、警犬
  - 围墙、锁、双重门
- 预防—技术性措施
  - 密码、生物识别、智能卡
  - 加密、安全协议、回拨系统、数据库视图、受约束的用户界面
  - 杀病毒软件、访问控制列表、防火墙、入侵防御系统

表 2-1 展示了这些安全控制机制是如何实现这些不同的安全功能。很多学生在理解哪种控制可以提供哪些功能这个问题上十分困惑。通常存在这种认识：“防火墙是一个预防控制措施，但如果攻击者知道有防火墙的部署，那它将成为一种威慑。”先让我们停在这里，不让问题更加复杂化。在试图根据功能需求选择控制措施时，控制措施的部署位置将成为主要考虑因素。防火墙的作用是试图防止恶意事情的发生，这是因为它是一种预防性控制。日志审计是在事件发生后开展的，所以它是检测性的。数据备份系统的开发目的是为了数据能够恢复，因此它是一种恢复性控制。生成计算机映像的目的是在软件损坏后，它们依旧可加载，因此这是一种纠正性控制。

表 2-1　安全控制提供的服务

	控 制 类 型				
	预防 (避免意外事件发生)	检测 (识别意外事件的发生)	纠正 (纠正已发生的意外事件)	威摄 (挫败安全违规)	恢复 (恢复资源和能力)
控制类别					
物理性控制措施					
围墙				×	
锁	×				
徽章系统	×				
警卫	×				
生物识别系统	×				
双重控制门	×				
照明				×	
移动检测器		×			
闭路监控系统		×			
异地设施					×
管理性控制措施					
安全策略	×				
监视和监督		×			
职责分离	×				
岗位轮换		×			
信息分类	×				
人员流程	×				
调查		×			
测试	×				
安全意识培训	×				
技术性控制措施					
访问控制列表(ACL)	×				
路由器	×				
加密	×				
日志审计		×			
入侵检测系统(IDS)		×			
杀毒软件	×				
服务器映像			×		
智能卡	×				
回拨系统	×				
数据备份					×

另外一种常被人们努力争取的控制措施是补偿性控制。来看一些补偿性控制的案例，以更好地解释它们的功能。如果公司需要实现强大的物理安全防护，你可能建议管理层去雇佣保安，但在计算完雇佣保安的全部成本后，公司可能采取补偿性(替代性)的控制措施，这种控制措施提供类似的保护，而它的成本却容易被承受，比如使用围墙。再如，假设你是安全管理员，负责维护公司的防火墙。管理人员告诉你有一个协议出于业务原因必须通过防火墙，而你知道该协议存在一个可以加以利用的漏洞。针对这个协议，网络就需要一种补偿性控制加以防护，比如建立一个针对特定通讯类型的代理服务器，以便于对这个协议进行适当的监视和控制。因此，补偿性控制是一种备选控制措施，它能提供类似原控制措施的功能，但因为它容易被承受或能满足特殊的业务功能而不得不使用。

几种安全控制类型并存需要协同工作，控制和它们所处环境的复杂性会引发控制之间冲突或留下安全空缺。这在公司保护方面将引发不可预见的漏洞，实施者对此却不能完全理解。一个公司部署有十分严格的技术访问控制和所有必要的管理控制，但如果任何人被允许物理访问设施内的任何系统，那么环境中就存在明显的安全风险了。总之，这些控制措施应该一起工作，配合默契，才能提供健康、安全和高效的环境。

控制类型和功能

- 控制类型：管理控制、技术控制和物理控制
- 控制功能：
  - 威慑——挫败潜在攻击者。
  - 预防——防止意外事件发生。
  - 纠正——事件发生后修复。
  - 恢复——恢复必要的组件到正常的操作状态。
  - 检测——事件发生后识别其行为。
  - 补偿——向原来的控制措施那样提供类似保护。
- 深度防御：

为使成功渗透和威胁更难实现而采用多种控制措施。

2.4 安全框架

在后面每一部分将深入探讨这章中的一些提纲挈领的话题。讲到这里我们已经清楚地了解需要实现的目标(可用性、完整性和机密性)，所能使用的工具(管理控制措施、技术控制措施和物理控制措施)，当然我们也学会了如何讨论这个问题(弱点、威胁、风险和控制)。在讲述如何开展组织范围的安全规划前，首先要掌握不能做什么，这个问题经常被称为通过隐匿实现安全。通过隐匿实现安全的前提是假想你的敌人没有你聪明，同时他们也猜测不出你的计策。一个通过隐匿实现安全的非技术例子是为了避免把你自己锁在房子外边之前，把备用钥匙放在门前台阶下这种传统做法。假想前提是没有人知道这个备用钥匙，只要他们不知道，就被认为是安全的。这样做的弱点在于如果能找到这个备用钥匙，任何人都可以轻易进入这栋房子，而对于有经验的攻击者(如

夜贼)，他们知道这种弱点存在并采取相应步骤就能找出这把钥匙。

在技术领域里，很多厂商认为经过编译后的产品能比基于开源代码的产品安全，他们推出自己的产品就建立在这种假设前提下，因为他们以为编译后将没有人能查看他们最初的编程指令。但是攻击者有大量的逆向工程软件可用，用这些工具就可以重构产品源代码，当然也有很多其他方法不用逆向工程就可以知道如何攻击软件，如模糊测试、数据输入校验等(这些软件安全专题将在第 10 章深入讲解)。实现安全的正确方法是确保最初的软件不包含缺陷，同时不要假设源代码编译后的格式就能提供必要的保护级别。

另外一个常见的隐匿安全例子是开发私有的加密算法替代行业通用的加密算法。一些组织机构假设，如果攻击者不熟悉其私有算法的逻辑功能和数学方法，那么他们在这个方面的知识欠缺就提升了必要的安全水平。但事实上，攻击者往往聪明伶俐且有想法。如果这些算法中有缺陷，它们极有可能被识别并加以利用。最好的方法是使用行业认可的算法，其原因是他们被证明足够强大，而且不依赖于算法私有的特性。鉴于此，可以认为这样是安全的。

有些网络管理员会在自己的防火墙上重新映射协议，以使 HTTP 不使用众所周知的端口 80，而使用 8080 端口进入环境。管理员认为攻击者猜不到这种重映射，但事实上，基本的端口扫描器和协议分析软件就可很容易地检测到端口被重映射。因此不要尝试在耍花招方面胜过这些坏家伙，反之，更需要以成熟的、务实的方法实现安全。不要试图隐藏可能被利用的缺陷，而是要去除这些缺陷并同时采用已经被证实的安全实践。

用混乱情况下的信任证明安全显然十分危险。虽然每个人都需要相信自己的同事天生善良，但事实上如果真是那样，所有安全专家即将失业。在安全方面，好的实践正像谚语所说的那样“世界上，我只相信两个人——你和我，不过我对你也不是绝对相信”。其原因在于安全实际上能被任何人在任何时间所威胁，因此这就是我们需要持有的最好态度。

我们不想组织机构的安全建立在虚无缥缈之上，也深知我们最不可能成功欺骗敌人，那么该怎么做呢？建立一个堡垒，又称之为安全计划。数百年前你的敌人不可能通过网络使用数据包攻击你，在当时可能骑马拿着大棒攻击你。当一个派系与其他派系进行斗争保护自我时，一般不会仅在自己的领地高处杂乱堆积石块来防御(当然，可能一些派系也是这么做的，但他们很快灭亡了，他们也没有认识到这个问题)。而有些派系建立了可以抵御进攻结构的堡垒，墙壁和房顶由很难穿透的坚固材料构成，建筑的结构提供了分层保护。建筑配备了防御和攻击性的工具，并且一些建筑有护城河环绕保护。这就是我们的目标，其中包含组织自身部分但不包含外围设施。

一个安全规划是有很多实体构成的框架：逻辑、管理和物理的保护机制，程序、业务过程和人，这一切一起工作将为环境提供一个保护级别。每个实体在框架中都有一个重要位置，如果一个缺失或不完整，那么整个框架将会受到影响。安全规划应该分层工作：一层为上层提供支持，同时为下一层提供保护。因为安全规划是一个框架，利用框架，组织可以自由插接不同类型的技术、方法和程序，以实现环境所必须达到的保护级别。

基于灵活框架的安全规划，听起来很好，但如何建立呢？在建立堡垒前，建筑师给出了建筑结构的蓝图。我们也需要设计详细的计划，使用该计划恰当地建设安全工程。这里特别感谢为了设计出好的规划而开发行业标准的人们。

2.4.1 ISO/IEC 27000 系列

——英国人似乎知道他们在做什么，跟着他们看看！

英国标准 7799(British Standard 7799，BS7799)是由英国政府工贸部 1995 年开发并由英国标准化机构(British Standard Institution)发布的。这个标准概括出信息安全管理体系(ISMS，又名安全规划)应该如何建立和维护。其目标是指导组织设计、实施和维护策略、过程及技术，以便于管理组织的敏感信息资产面临的风险。

这类标准受欢迎的原因是它能够尝试并集中管理在整个组织中部署的各种安全控制措施。没有安全管理系统，控制措施的实施和管理会相当随意。IT 部门关注安全技术方案，人员安全工作由人力部门负责，物理安全由设施部门负责，业务连续性由运营部门负责。我们需要纵览所有事项并以全盘方式将它们周密结合，而英国的标准就能满足这种要求。

英国标准(British Standard)实际上有两部分：BS7799 第一部分，它描述了控制目标和为实现这些目标可使用的控制措施范围；BS7799 第二部分描述了如何建立和维护安全规划(信息安全管理体系，ISMS)。BS7799 第二部分同时也作为对组织进行认证的基线。

BS7799 被认为是一个事实标准，它没有要求每个组织都必须遵守的详细的标准主体部分，但这个标准看起来很完美，而且能满足行业需求，因此每个组织都想遵守它。当全球的组织机构需要开发一个内部安全规划时，除了 BS7799 没有其他指南或指导可遵守。这个标准列出了安全包括一系列专题，下面列出一些。

- **组织信息安全策略** 业务目标到安全的映射、管理层的支持、安全目标和职责。
- **信息安全框架建立** 建立和维护组织的安全结构可通过以下环节开展，如建立信息安全论坛，设立安全官，定义安全职责、授权流程、业务外包和独立审计。
- **资产分类和控制** 开发安全基础设施去保护组织资产，这包括以下内容：职责、资产清单、分类和操作规程。
- **人员安全** 减少人际活动中固有的风险可通过以下措施：人员筛选，定义角色和职责，正确的安全培训，记录异常情况等。
- **物理和环境安全** 保护组织资产措施有以下例子：正确选择设施地点，建设和维护安全边界，实现访问控制，保护装备。
- **通信和运营管理** 实现运营安全可通过以下方式：运营流程、正确的变更控制、事件处理、职责分离、承载能力规划、网络管理和媒体关系处理。
- **访问控制** 基于业务需求的资产访问控制、用户管理、认证方法和监控。
- **系统开发和维护** 在系统生命周期的各个阶段实现安全，包括：安全需求开发、加密、完整性保护和软件开发流程。
- **业务连续性管理** 通过连续性计划和测试来应对正常运行的中断。
- **合规** 通过采用技术控制、系统审计和法律意识普及来遵循管理、合同和法律方面的要求。

对 BS7799 进行升级和全球标准化由 ISO(国际标准化组织)和 IEC(国际电工委员会)提出并开展。ISO 是全球最大的国际标准开发和发行者。这个组织提供的标准从气象学、食品科学、农业到太空交通工程学、采矿及信息技术。ISO 组织由 159 个国家的标准化协会构成，因此它有一批

能够提出解决问题好方法的优秀人才，其中工作的一个方向是如何建立组织的信息安全规划。IEC 则开发和发布有关电、电子及相关技术的国际标准。这两个组织在 BS7799 基础上开展联合工作，发行了一个新的全球化标准，即 ISO/IEC 27000 系列。

在 BS7799 发展的过程中，它经历了名字和版本号上的巨变，因此能看到像 BS7799、BS7799 V1、BS7799 V2、ISO17799、BS7799-3:2005 等称呼。最初的 BS7799 有多种功能部分，演变到 ISO/IEC 标准后，则该标准变成了一套系列标准，该标准将信息安全管理体系必要的组件划分为不同的模块，具体划分如下：

- ISO/IEC 27000 概述和词汇
- ISO/IEC 27001 ISMS 要求
- ISO/IEC 27002 信息安全管理实践代码
- ISO/IEC 27003 信息安全管理体系实施指南
- ISO/IEC 27004 信息安全管理衡量指南与指标框架
- ISO/IEC 27005 信息安全风险管理指南
- ISO/IEC 27006 信息安全管理体系审核与认证机构指南
- ISO/IEC 27011 远程通信组织信息安全管理指南
- ISO/IEC 27031 业务连续性的 ICT(信息和通信技术)准备能力指南
- ISO/IEC 27033-1 网络安全指南
- ISO/IEC 27799 医疗机构信息安全管理指南

下面的 ISO/IEC 标准在本书编写时还在开发中：

- ISO/IEC 27007 信息安全管理体系审核指南
- ISO/IEC 27013 ISO/IEC20000-1 和 ISO/IEC27001 一体化实施指南
- ISO/IEC 27014 信息安全治理指南
- ISO/IEC 27015 金融及保险行业信息安全管理指南
- ISO/IEC 27032 网络空间安全指南
- ISO/IEC 27033 IT 网络安全指南，它是一个基于 ISO/IEC 18028:2006 的由多部分组成的标准。
- ISO/IEC 27034 应用安全指南
- ISO/IEC 27035 安全事件管理指南
- ISO/IEC 27036 外包安全指南
- ISO/IEC 27037 识别、收集、获取和保存数字证据指南

这组标准就是著名的 ISO/IEC 27000 系列，是世界上从全盘考虑的安全控制管理的最佳行业实践。ISO 遵循戴明环(计划—执行—检查—处理)，该环是一个迭代过程，经常用于业务流程质量控制程序。“计划”组件是指建立目标和制订计划，“执行”组件负责计划的实施，“检查”组件是指衡量结果以验证目标是否实现，最后一个环节“处理”提供了如何纠正和改善计划以便更容易获得成功。图 2-4 描绘了这个循环，同时还描述了它与 ISO/IEC 27000 系列中列出的开发和维护信息安全管理体系的关系。

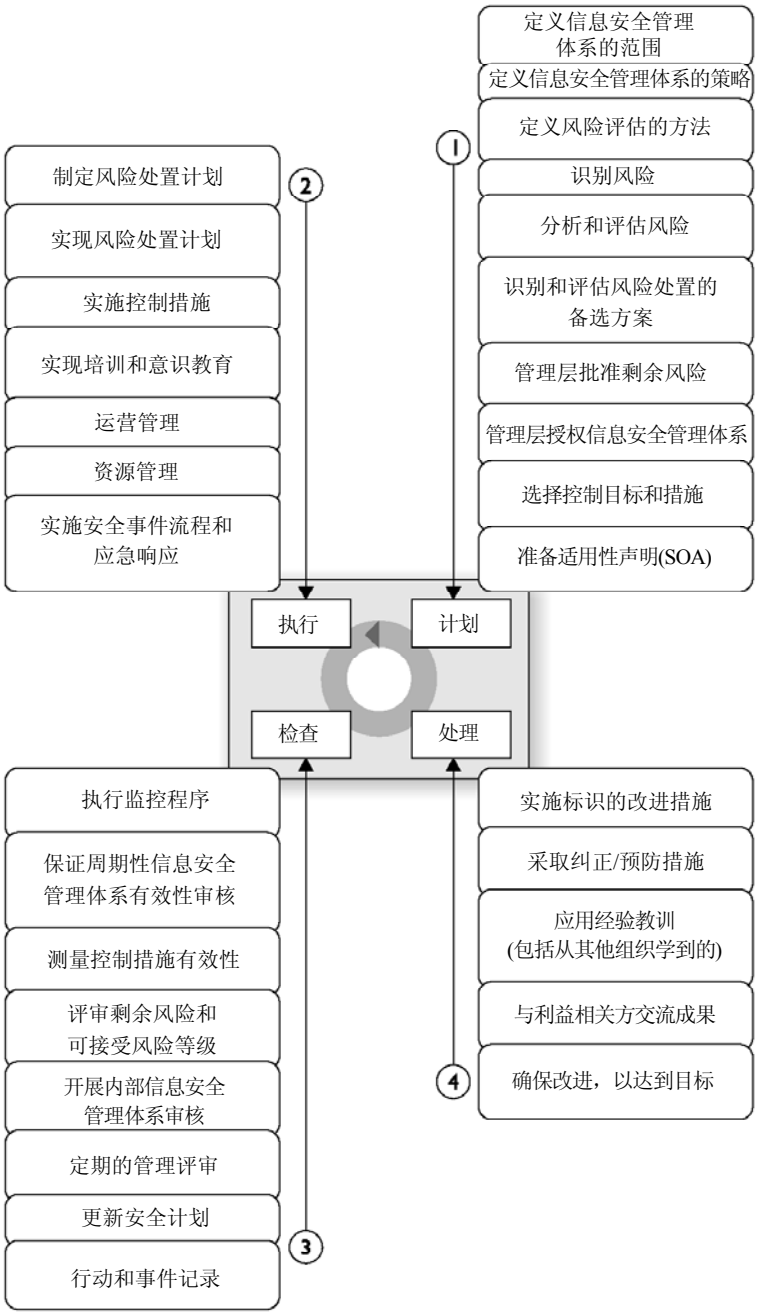

图 2-4　ISO/IEC 27000 系列中使用的 PDCA 环

经常有组织向获得认可的第三方机构寻求 ISO/IEC 27001 认证证书。第三方认证机构会根据 ISO/IEC 27001 列出的 ISMS 要求评估该组织，并证明该组织的符合性水平。正像一个人通过 CISSP 考试后，$(ISC)^2$ 证明他具备了相应的安全知识一样，第三方机构为评估的公司证明其公司范围内的安全实践水平。

众多标准、最佳实践和框架

在后面的章节中，各种盈利和非盈利组织机构开发了自己的安全管理方法、安全控制目标、过程管理和企业发展。下面研究他们的相似之处和区别，同时举例说明各自在行业中的应用场合。

下面是一个基本的明细对比：

- **安全规划开发**

  ISO/ IEC 27000 系列　ISO 和 IEC 联合开发的关于如何开发和维护信息安全管理体系的国际标准。

- **企业架构开发**
  - **Zachman 框架**　由 John Zachman 开发的企业框架开发模型。
  - **TOGAF**　开放群组(The Open Group)开发的用于企业架构开发的模型和方法论。
  - **DODAF**　DODAF 是美国国防部架构框架，用于保障军事任务完成过程中系统间的互操作性。
  - **MODAF**　MODAF 是英国国防部开发的架构框架，主要应用在军事任务支持方面。
- **安全企业架构开发**
  - **SABSA 模型**　用于企业信息安全架构开发的模型和方法论。
- **安全控制开发**
  - **CobiT**　由国际信息系统审计协会(ISACA)和 IT 治理协会 ITGI 联合开发的 IT 管理控制目标集。
  - **SP 800-53**　它是由美国国家标准与技术研究院(NIST)开发的保护美国联邦系统的控制集。
- **公司治理**
  - **COSO**　由反欺诈财务报告全国委员会发起组织委员会(COSO)开发，旨在帮助降低财务欺诈风险的国内公司控制集。
- **过程管理**
  - **ITIL**　它是由英国商务部开发的用于 IT 服务管理的过程。
  - **Six Sigma**　它是被用来开展过程改进的业务管理策略。
  - **CMMI**　(Capability Maturity Model Integration，能力成熟度模型集成)模型由卡内基・梅隆大学开发，目的是实现组织的开发过程改进。

注意：

CISSP 知识纲要把所有架构内容(包括企业架构和系统架构)都放在了“安全架构和设计”一章中。由于企业架构与贯穿整章的企业安全规划直接相关，所以将这块内容放在了本章中。“安全架构和设计”中还专门讲述了用于软件工程和设计的系统架构知识。

2.4.2 企业架构开发

——应该将所有的安全努力与业务集成起来吗？

——不，我们更喜欢混乱和浪费金钱。

组织在试图从整体上保护环境时往往要进行选择。一种方式，他们提出单一解决方案或整体解决方案，随处放置产品，期望通过临时性的方法魔术般地保护环境安全并能覆盖到组织中的所有弱点。第二种方式，组织花时间理解环境，理解业务和环境的安全需求，并布置可以将这两个方面映射到一起的总体框架和策略。很多组织选择方式一，但这种方式属于“不断救火”的方法。这会让安全压力不断增加且安全需求也得不到满足，反而会让困惑和混乱常态化。

第二种方法将会定义企业的安全架构，也可以将其作为实施解决方案时的指南，以确保业务需求被满足，同时可以提供针对环境的标准保护，降低组织发生安全意外事件的几率。尽管实现企业安全架构后不会实现真正意义上的“乌托邦”，但它确实能够在从整体上应对安全问题时抑制混乱，使安全人员和组织更加积极主动和形成成熟的观念模式。

从头开始开发架构并非易事。当然，仅仅在大盒子里面画一些小盒子比较容易，但这些盒子代表什么呢？盒子之间的关系是什么样的？盒子之间的信息流是如何流转的？谁需要查看这些盒子以及他们在做决定时需要考虑哪些方面？架构是一种概念性的结构，它是一种帮人们以可理解数据块的方式理解复杂事物(如企业)的工具。如果熟悉 OSI 网络模型，会发现它是一个用于阐明网络栈架构的抽象模型。计算机内的网络栈很复杂，它有很多协议、接口、服务和硬件规范。以模块框架(七层)考虑它时，将能更好地从整体上理解网络栈及其每个组件间的关系。

注意：

OSI 网络栈将在第 6 章重点讲解。

一个企业架构包含组织的基本及一体化的组件，它表达了企业结构(窗体)和行为(功能)，它包含了企业组件、彼此间的关系以及与环境的关系。

本节涉及了几个不同的企业框架，虽然每个框架都有自己的特别关注点，但它们都提供了如何建立单个架构的指南，因此对于建立不同的框架它们都十分有用。要注意架构框架和实际架构是有区别的。使用框架可以指导如何建立一个最适合公司需求的架构。每个公司的架构都不同，原因在于它们有不同的业务驱动、安全和规定需求、文化和组织结构，但如果每个公司都以相同的架构框架为指导，那么它们的架构将有相似的结构和目标。这种情况就像 3 个人根据一个两层农场式房子的设计图建房子一样。一个人由于有 3 个孩子，因此选择构建 4 个卧室的房子。一个人选择建一个大的起居室和 3 个卧室，还有一个人选择建两个卧室和两个起居室。每个人都从相同的设计图(框架)出发，并根据自己的需求修改它(框架)。

要开发一个架构，首先要识别出关注和使用这个架构的利益相关者。然后需要开发不同的视角，视角将能够以最有效的方式解释不同的利益相关方最关注的信息。如图 2-5 所示，公司有几个不同的视角观点，管理层人员需要从业务角度理解公司，业务流程开发人员需要理解务必收集什么类型的信息来支撑业务活动，应用程序开发人员需要理解维护和处理信息的系统需求，数据建模人员需要理解如何构建数据元素，技术团队需要理解支撑上述层面的网络组件。上述人员都在同一个公司理解架构，这表明了从他们理解的视角，以及组织内与他们的职责直接相关的视角开发。

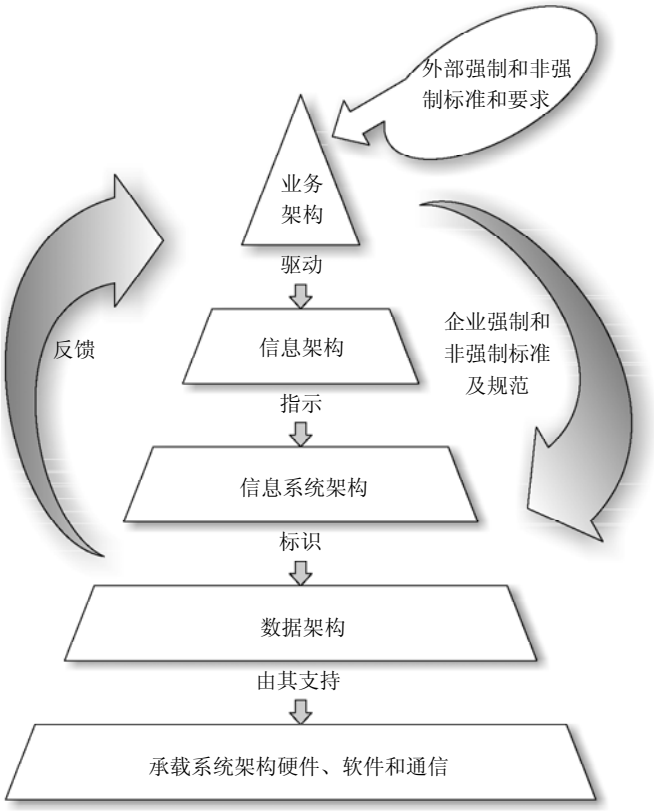

图 2-5　美国国家标准与技术研究院架构框架

企业架构让你不仅从不同视角理解公司，还能帮助你理解一个层面发生变化将如何影响其他层面。例如，如果有一个新的业务需求，企业的每个层面是如何支撑的呢？必须收集和处理什么类型的新信息？是否需要购买新应用程序或对当前的应用程序进行修改？需要新的数据元素吗？需要新的网络设备吗？架构能够帮助理解需要变化的所有事情，只为支持新的业务功能。架构同样也能在相反方面起作用。如果一个公司计划进行技术革新，在技术层面之上新系统仍能够支持所有必须的功能吗？架构允许将组织理解为完整的有机体，它也阐明了一个内部组件的变化如何直接影响的另外一个组件。

1. 为何需要企业架构框架

就如你所经历的那样，业务人员和技术人员有时候看起来是完全不同的两类人。业务人员使用“纯利润”“风险空间”“投资策略”“套期保值”“商品”等术语，技术人员使用“深度数据包监测”“三层设备”“跨站脚本”“负载均衡”等术语。缩写词汇随手可得，如 TCP、APT、ICMP、RAID、UDP、L2TP、PPTP、IPSec、AES 和 DES。我们之间可以不用说任何实际词语就可以成功交流。甚至业务人员和技术人员使用完全相同的词语，但对于对方来讲却有完全不一样的意思。对业务人员而言，“协议”是为完成任务而必须遵循的一套流程。对于技术人员而言，“协议”是计算机或应用程序间通信的一种标准化的方式。业务人员和技术人员都使用术语“风险”一词，但双方针对的是公司面临的截然不同的风险——市场份额和安全漏洞。甚至即使他们使用的“数据”术语意思是相同的，业务人员仅仅是从功能的角度关注，安全人员则是从数据的风险视角关注。

业务人员和技术人员对问题看法的分歧不仅会引发混乱和失败，还会造成资金浪费。如果房子的业务人员想为客户提供一种新型的服务，如在线账单支付，那么肯定会在以下方面产生较大变化：当前的网络基础设施、应用程序、Web 服务器、软件逻辑、加密功能、认证方法、数据库结构等。业务人员的提议看似一个很小的变化，在实现时将会花费大量的资金，去购买和实现新技术、实施编程以及重新架构网络等。业务人员经常感觉 IT 部门在业务革新和成长时是一种障碍，反过来，IT 部门也感觉到业务人员经常会提出一些古怪和不切实际的要求，并且这些要求没有预算支持。

鉴于业务人员和技术人员之间的这类冲突，世界各地的组织实施了很多错误的解决方案，其原因在于与技术规范对应的业务功能没有被理解。结果导致不得不重新购买新的解决方案、实施返工，浪费大量时间。组织不仅会支付比最初计划多的资金，而且很可能会丧失业务机会，进而减少市场份额。这类浪费频频发生，以致美国国会通过了《克林格-科恩法案》(Clinger-Cohen Act)，法案要求联邦政府提高 IT 开销。因此需要一个工具，能让业务人员和技术人员都可使用它来减少冲突，优化业务功能，避免浪费时间和金钱。以上就是企业架构发挥作用的地方。它能让业务人员和技术人员双方以能理解的方式审视同一个组织。

当你进入医生的办公室，会发现一面墙上挂着一张骨骼系统的贴画，在另外一面墙上挂着一张循环系统的贴画，还有一面墙上挂着人体器官的贴画。它们是对同一事物(人体)从不同视角的观察。企业架构框架提供了相同的功能：对同一事物从不同视角关注。在医疗领域，有专科医生，如足科医生、脑外科医生、皮肤科医生、肿瘤科医生、眼科医生等。每个组织也都有它自己的专家，如人力资源、市场、会计、IT、研发、管理人员等。但组织也有对实体从全面理解的问题(不管实体对象是人体还是公司)，这就是企业架构试图解决的问题。

2. Zachman 架构框架

——每个人都理解组织中的所有组件如何共同工作吗？

——那要看在这儿工作了多久。

Zachman 架构框架是创建的第一个企业架构框架，由 John Zachman 开发，内容见表 2-2(完整的框架参见 www.zafa.com)。

表 2-2　企业架构的 Zachman 框架

序号	层次	什么(数据)	如何(功能)	哪里(网络)	谁(人)	何时(时间)	为何(动机)
1	工作范围 ● 计划人员	对业务而言重要的事物清单	业务执行过程的清单	业务运营中所在位置的清单	对业务而言重要的组织清单	重要业务事件清单	业务目标和战略清单
2	业务模型概念 ● 所有者	如语义或实体关系模型	如业务过程模型	如业务逻辑模型	如工作流模型	如主日程表	如业务计划
3	系统模型逻辑 ● 设计人员	如逻辑数据模型	如应用架构	如分布式系统架构	如人员接口架构	如工序结构	如业务规则模型
4	技术模型物理逻辑 ● 建设人员	如物理数据模型	如系统设计	如技术架构	如呈现架构	如控制结构	如规则设计
5	组件配置 ● 实施人员	如数据定义	如程序	如网络架构	如安全架构	如时序定义	如规则说明
6	企业功能实例 ● 工作人员	如数据	如功能	如网络	如组织	如进度表	如战略

Zachman 框架是一个二维模型，它使用了 6 个基本的疑问词(什么、如何、哪里、谁、何时、为何)和不同的视角观点(计划人员、所有者、设计人员、建设人员、实施人员和工作人员)二维交叉，它给出了企业的一个整体性理解。该框架在 20 世纪 80 年代开发出来，内容基于典型的业务架构，其中包含了管理一套有序关系的规则。

该模型的目标是让人们能够从不同视角(包括计划人员、所有者、设计人员和建设人员等)出发了解同一个组织。公司中不同类型的人员需要相同的信息，但这些信息分别以和他们职责直接相关的方式表示。CEO 需要财务报表、绩效考核、资产负债表。网络管理员需要网络图，系统工程师需要接口需求，运维部门需要配置需求。如果你曾经实施过基于网络的弱点测试，就会知道不可以告诉 CEO 有些系统在基于 SYN 的攻击方面存在隐患，你也不能说公司软件存在客户端浏览器注入攻击漏洞，同样也不能说基于 Windows 的应用程序存在数据流被修改的可能。CEO 需要知道这些信息，但必须以其可以理解的语言叙述。组织中每个层次的人工作所需的信息必须以对应的语言和格式来提供。

企业架构经常被用来将支离破碎的过程(包括人工和自动的)优化到一个集成的环境中，该环境能够响应变化，支持业务战略。Zachman 框架已存在数年并已成功应用于众多组织中，主要用于建立或更好地定义组织业务环境。这个框架不是面向安全的，但它却是一个用于工作的好模板，因为对如何模块化理解真实企业提供了指导方向。

3. 开放群组架构框架

——业务过程、数据流、软件程序和网络设备像意大利面一样串在一起。

——可能需要实现一些结构。

另外一个企业架构框架是开放群组架构框架(The Open Group Architecture Framework，TOGAF)，它由美国国防部开发并提供了设计、实施和治理企业信息架构的方法。

TOGAF 用来开发以下架构类型(如图 2-6 所示)：

- 业务架构
- 数据架构
- 应用程序架构
- 技术架构

图 2-6　TOGAF 3 开发的架构

利用架构框架，运用其架构开发方法(Architecture Development Method，ADM)则可以创建单个的架构，这种方法是一个迭代和循环过程，它允许不断地重复审核需求，以及根据需求更新单个架构。这些不同的架构允许技术架构设计师从企业的不同视角(业务、数据、应用程序和技术)去理解企业，以确保开发出环境及组件所必需的技术，最终实现业务需求。这个技术需要跨越不同的网络类型，实现各种各样的软件组件间的互联以及在不同业务单元内工作。打个比方，在一座新城市构建时，人们不会立即到处建房子，城市设计师们则会设计出道路、桥梁、水路、商业及居民区。大型组织机构环境往往分布在各个地方而且种类繁多，这些环境要支撑大量不同的业务功能，和城市一样复杂。因此，在程序员开发代码前，需要根据组织工作背景开发软件架构。

注意：

很多技术人员对上述模型持有负面的本能反应。他们感觉要做的工作太多，太麻烦没什么直接的实质意义等。如果你用含有防火墙、入侵检测系统和 VPN 系统的示意图来和他们交涉，他们会说：“现在我们才是讨论安全。”因为安全技术被应用于组织结构内，所以必须理解组织。

4. 面向军事的架构框架

——我们的侦察队伍搜集了有关敌人的重要情报，但一个小的软件错误导致攻击错了村子。
——责任在于 NATO。

为一个组织构建企业范围的解决方案和技术难度系数很大，其原因是这个架构需要跨越多个不同的复杂政府机构，以允许实现它们之间的互操作性和适当的分层通信信道。这正是美国国防部架构框架(Department of Defense Architecture Framework，DoDAF)发挥作用的地方。在美国国防部购买技术产品和武器系统时，必须依据 DoDAF 标准起草企业架构文档，这些文档将用来阐述购买的产品、系统如何恰当地集成到当前基础设施中。这个架构框架的焦点集中在指令、控制、通信、计算机、情报、监视和侦察系统与过程。重要的是，不仅不同设备间使用同一协议类型和可互操作的软件组件通信，而且使用相同的数据元素。如果间谍卫星抓取了一张图片，图片将被下载到中央数据仓库，然后它会被加载入软件系统中来指挥无人驾驶飞机，军事人员无法中断这个操作，因为软件无法读取另外一个软件的数据输出。DoDAF 能够确保所有的系统、过程和人员协调一致地共同完成使命。

英国国防部架构框架(British Ministry of Defence Architecture Framework，MODAF)是被众人认可的另外一个企业架构框架，它是基于 DoDAF 的。这个框架的关键是使之能够以正确的格式来获取数据并以最快的速度传给正确的人。现代战争具有复杂、行动快速的特点，这就要求人员和系统比以前适应能力更强。需要正确捕获及呈现数据，以便让决策者快速理解复杂问题，这样将能快速精准地做出决策。

注意：

在 DoDAF 和 MODAF 被开发运用于支持军事任务时，它们同时也被扩展和变革，运用到商业领域。

试图找到最适合其组织的系统架构时，需要明确有哪些利益相关方，以及他们需要从系统中

获得什么信息。这个架构能以最实用的方式把公司展现在最想了解公司的人面前。假如公司有些利益相关者想从业务过程的角度了解公司，架构就应从那个角度提供信息。如果有些人想从应用程序的角度了解公司，架构就要从那个角度阐述相应的信息。如果人们想从安全的角度了解公司，你就要从这个特别的角度来提供信息。所以各种企业架构框架的主要区别在于它们提供什么类型的信息以及如何提供信息。

5. 企业安全架构

企业安全架构是企业架构的一个子集，它定义了信息安全战略，包括各层级的解决方案、流程和规程，以及它们与整个企业的战略、战术和运营链接的方式。这是用全面的、严格的方法描述了组成完整的信息安全管理体系(ISMS)所有组件的结构和行为。开发企业安全架构的主要原因是确保安全工作以一个标准化的和节省成本的方式与业务实践相结合。架构在抽象层面工作，它提供了一个可供参考的框架。除了安全性之外，这种类型的架构让组织更好地实现互操作性、集成性、易用性、标准化和便于治理性。

如何知道一个组织是否部署企业安全架构呢？如果对于以下大多数问题的回答是肯定的，那么这类架构就没有部署。

- 在整个组织中安全是在单独区域范围发生的吗？
- 在高级管理人员和安全人员之间是否有持续的脱节？
- 为不同部门重叠的安全需求购买冗余产品了吗？
- 制定的安全规划仅仅由主要的安全策略组成，而没有实际的实施和强制执行吗？
- 当因为业务需要，用户访问需求增加时，网络管理员未经客户经理的书面批准就可以修改访问控制吗？
- 当一个新产品推出时，会弹出意想不到的互操作性问题，而需要更多的时间和金钱来解决吗？
- 当安全问题出现的时候，会有很多的“一次性”努力而不是按照标准过程进行的吗？
- 业务部门经理是否不知道他们的安全责任以及自己的安全责任如何映射到法律和监管需求？
- “敏感数据”在策略中有定义，但必要的控制没有得到充分实施和监控吗？
- 实施的是单点解决方案而不是企业级解决方案？
- 同样昂贵的错误持续发生？
- 因为企业没有以标准的、全面的方式检查或监控，所以安全治理通常无效？
- 所做的业务决定没有考虑到安全要素？
- 安全人员通常是去“紧急扑灭大火”，并没有真正花时间来顾及和开发信息安全战略？
- 安全努力发生在某些业务部门，而其他业务部门对此却一无所知？
- 越来越多的安全人员开始寻求精神科医生帮助或寻找抗焦虑的良药？

如果这些问题的答案是“是的”，说明没有部署有效的架构。现在看下这些年笔者发现的非常有趣的事情。大多数组织都有前面列出的问题，但这些组织仅仅关注每个单独的问题，好像问题之间没有任何关联。CSO、CISO 和/或安全管理员他们往往不会理解这些问题仅仅是疾病的表面现象。“治疗”是让一个人负责团队，针对企业安全架构的推广计划开发一个分阶段性的方法。

目标是集成面向技术、以企业为中心的安全过程；综合管理、技术和物理控制以实现正确管理风险；同时将这些过程集成到 IT 基础设施、业务流程和组织文化中。

组织不开发或不推出企业安全架构的主要原因是，他们并不完全了解企业架构是什么，甚至有的组织认为它是一项艰巨的任务。“救火”行为更容易理解和方便开展，所以许多公司继续在使用这个熟悉的方法。

一个团队开发了舍伍德的商业应用安全架构(Sherwood Applied Business Security Architecture，SABSA)，正像在表 2-3 中所示，它类似于 Zachman 框架。它是一个分层模型，它在第一层从安全的角度定义了业务需求。模型的每一层在抽象方面逐层减少，细节逐层增加，因此，它的层级都是建在其他层之上的，从策略逐渐到技术和解决方案的实施实践。其思路上创新提出了一个包括战略、概念、设计、实施、度量和审计层次的安全链条。

表 2-3　SABSA 架构框架

	资产(什么)	动机(为什么)	过程(如何)	人(谁)	地点(何地)	时间(何时)
上下文	业务	业务风险模型	业务过程模型	业务组织和关系	业务地理布局	业务时间依赖性
概念层	业务属性配置文件	控制目标	安全战略和架构分层	安全实体模型和信任框架	安全域模型	安全有效期和截止时间
逻辑层	业务信息模型	安全策略	安全服务	实体概要和特权配置文件	安全域定义和关系	安全过程循环
物理层	业务数据模型	安全规则、实践和规程	安全机制	用户、应用程序和用户接口	平台和网络基础设施	控制结构执行
组件层	数据结构细节	安全标准	安全产品和工具	标识、功能、行为和访问控制列表(ACL)	过程、节点、地址和协议	安全步骤计时和顺序
运营层	业务连续性保障	运营风险管理	安全服务管理和支持	应用程序和用户管理与支持	站点、网络和平台的安全	安全运营日程表

下面列出的一问一答是在框架的每个级别上提出的：

- **想在这一层努力做到什么？**通过安全架构来保护资产。
- **为什么要这么做？**运用安全的动机是用这层的术语来表达。
- **如何做？**在这一层要实现的安全功能。
- **都涉及谁？**在这一层上与安全有关的人和组织部门。
- **在哪里做？**与这层有关的应用安全的位置。
- **什么时候做？**与这层有关的安全的时间要素。

SABSA 是用于企业安全架构和服务管理的框架和方法论。由于它是一个框架，这就意味着它为构建架构提供了一种结构。由于它也是一种方法论，这意味着它提供了建立和维护架构要遵循的过程。SABSA 提供了一个生命周期模型，这样，随着时间的推移，可以对架构持续监控和改进。

要成功开发和实现企业安全架构，必须理解并遵循下面的要点：战略一致性、过程强化、促

进业务和安全有效性。

战略一致性是指企业安全架构必须能够满足业务驱动、监管和法律的要求。要让公司能够生存并能繁荣，必须为其环境付出安全努力。安全行业仅在技术和工程界有所发展，但在商业业务领域没有进展。在很多组织中，IT 安全人员和业务人员虽然可能工位彼此靠近，但通常，在如何看待自己所工作的单位方面有着天壤之别。技术仅仅是支撑业务的工具，但它不是业务本身。IT 环境类似于人体内的循环系统，它的存在是用来支持身体——而身体的存在不是为了支持循环系统。安全类似于身体的免疫系统——它的存在目的在于保护整体环境。如果这些关键系统(业务、IT、安全)不一起工作，齐心协力，那么将会出现缺陷和失调现象。人体中的不足和失调现象会导致体内疾病，而组织内的不足和失调现象可能会导致风险和遭受安全入侵。

ISMS(信息安全管理体系)与企业安全架构

——我们需要开发素材，并将其固定到组织容器中。

ISMS 和企业安全架构有什么区别呢？ISMS 概括出了需要部署的控制(如风险管理、脆弱性管理、业务连续性计划、数据保护、审计、配置管理和物理安全等)，同时还为如何在控制的生命周期中管理它们指明了方向。ISMS 还从组织全局出发指定了为能够提供全面安全规划需要部署的各个组成部分，还指定了如何维护这些组成部分。企业安全架构说明了这些组件是如何被集成到当前业务环境的不同层次中的。ISMS 的安全组件必须交织贯穿于业务环境中，而不能与公司内各部门相互孤立。

例如，ISMS 指出了需要部署的风险管理，企业架构则细化了风险管理的组件，并阐明了如何从战略、战术和运营层面开展风险管理。另外一个例子是，ISMS 指出了需要部署的数据保护。架构则展示了在基础设施、应用程序、组件和业务级别上如何实现保护数据。在基础设施层，可以使用数据防丢失保护技术来检测敏感数据如何在网络中传输。包含敏感数据的应用程序必须拥有必要的访问控制和加密功能。应用程序内的组件可以实现特定的加密功能。保护敏感的公司信息可以与业务驱动直接连在一起，这一点会在架构的业务层面说明。

ISO/IEC 27000 系列(概述了 ISMS)是面向策略的，并概述了安全规划的必要组件。这意味着，ISO 标准本质上是通用的，当然这不是一个缺陷，它们创建了一种方法，使它们适用于不同类型的业务、公司和组织。但是，既然这些标准是通用性的，就很难知道如何实现它们以及如何将它们映射到你公司的基础设施和业务需求。以上就是企业安全架构发挥作用的地方。架构是一种工具，用于确保安全标准概括出的内容能够在组织的不同层面实现。

审视企业安全架构业务促进需求时，我们需要提醒自己，公司开展业务是为了赚钱。公司和组织都不能只为安全目的而存在的。安全不能堵塞业务过程，反而应更好地促进业务。

业务促进功能则要求核心业务流程应该集成到安全运营模型——它们是基于标准设计的而且能遵循风险容忍标准。在现实世界中这是什么意思呢？例如，公司的会计师指出，如果允许客户服务和技术支持人员在家办公，那么公司将节省大量的资金，如办公室租金、公用设施和日常开支，同时由此产生的保险金也会很便宜。这时公司可能会采取使用了 VPN、防火墙、内容过滤等的新模型。通过提供必要的保护机制，安全使公司转移到另外一个工作模型。如果金融机构计划允许客户能够查看账户信息和转账，则只要部署了正确的安全机制(如访问控制、认证、安全连接机制等)，就能提供这项服务。安全应该通过所提供的机制让组织能安全地开展新业务，实现组织的繁荣。

如果过程强化优势充分发挥，将对组织有很大的帮助。当组织不知道如何保障它们环境时，则必须细致查看正在进行的每个业务过程。很多时候都需要从安全角度来审视业务过程，因为这正是开展过程强化的原因，但这同时也是加强和改进同一个过程进而提高生产率的最佳机会。分析各类组织的业务过程时，通常会发现有很多重复劳动，很多手工劳动完全可自动化，或者有些任务完全可以重新安排工序，节省时间和劳动量。这就是经常提及的过程重构概念。

在一个组织开发企业安全组件时，这些组件必须能够高效集成到业务过程中。这样就能实现过程管理重新精化和调整，同时也能将安全集成到系统生命周期和日常运营中。因此业务促进意味着“可以开展新业务”，过程强化意味着“可以将工作开展的更好”。

安全有效性涉及度量、满足服务水平协议(Service level agreement，SLA)需求、实现投资回报率(return on investment，ROI)、满足设置基线、使用仪表盘或平衡计分卡系统提供管理。以上都是用来从整体上判断现行的安全解决方案和架构有效性的方法。

很多组织既要确保部署的控制措施能够提供必要的保护水平，又需要确保有限的资金恰当使用，因此才开始接触架构的安全有效性观点。一旦设置好基线，就可以开发度量指标来验证基线的合规性。然后，将这些指标以管理层可以理解的形式报告上去，让他们能够掌握组织的安全发展状况和合规水平。这也使得管理层能够做出明智的业务决策。安全影响今天几乎所有的业务，因此安全有效性信息应该很容易地让高级管理人员以他们实际使用的方式读取。

6. 企业架构与系统架构

——运营系统遵循严谨的层次结构，公司则比较随意。

虽然企业架构和系统架构确实有重叠之处，但是它们之间还是有区别的。企业架构解决的是组织的结构，系统架构解决的是软件和计算组件的结构。虽然这些不同的架构有不同的关注点(组织和系统)，但它们还是有直接的联系，因为系统必须能够支持组织及其安全需求。软件架构师如果不理解公司需要应用程序来做什么，那么他就不能设计出用于公司内部的应用程序。因此，软件架构师需要了解公司的业务和技术背景，以确保开发的软件能够满足组织的需求。

重要的是要认识到，在组织的安全策略中列出的规则必须支持所有应用程序代码、操作系统安全内核、计算机 CPU 提供的硬件安全。如果要成功实施安全，必须确保安全能够被集成到组织和技术的每一个层面中。这就是为什么一些架构框架涵盖的公司功能范围从业务过程层面到组件在应用程序中是如何工作的。必须详细理解以上这些相互作用、相互依存的关系。否则，会出现以下情况：开发错误的软件，购买错误产品，最终导致互操作性问题的增多，软件也仅能支持企业的部分业务。

做一个形象比喻，企业和系统架构的关系类似于太阳系和单个行星之间的关系。太阳系是由行星组成的，就像一个企业是由系统组成的。把太阳系作为一个整体去理解单个行星土壤补偿、大气层等的复杂性也是非常困难的。每个观点(太阳系与行星)都有其重点和作用。当看企业与系统架构的时候，原理是类似的。企业的观点是看整体，而系统的视角则是看组成整体的各个部分。

注意：

在本章中主要是从企业的观点讲解了安全架构，第 4 章将介绍更多的系统专有架构框架，如 ISO/IEC42010:2007。

企业架构：可怕的野兽

如果没有接触过这些企业架构模型而且感到有些混乱，也不必要担心，这种现象很常见。由于企业架构框架是一个了不起的工具，可以用于理解和帮助控制组织内所有复杂的事务，所以安全行业仍在完善这类架构的使用。大多数企业制定策略后重点研究技术以求加强这些策略，直接略过了企业安全架构开发的全过程。这主要是因为信息安全领域仍然在探索学习如何从 IT 部门脱离出来并融入既定的企业环境。由于安全和业务的联系日益密切，这些企业框架看起来就不会那么抽象和陌生了，反而将成为卓有成效的好工具。

2.4.3　安全控制开发

——有了架构，现在往里放什么？

——整理、安排。

到目前为止，已经有了 ISO/IEC 27000 系列，其中概述了组织安全规划的必要组成部分。也有了企业安全架构，帮助汇总安全规划中所列出的要求，并将之集成到公司现有业务结构中。现在，关注一下要落实到位的控制目标，以达成安全规划和企业架构所列出的目标。

1. CobiT

CobiT(Control Objectives for Information and related Technology，信息及相关技术的控制目标)是一个框架，是一组由国际信息系统审计与控制协会(ISACA)和 IT 治理协会(ITGI)制定的控制目标集，它定义了控制目标，使用这些控制目标可以正确管理 IT 并能确保 IT 到业务需求的映射。CobiT 分成 4 个领域：计划和组织(Plan and Organize)、获得与实现(Acquire and Implement)、交付与支持(Deliver and Support)、监控与评价(Monitor and Evaluate)。每个类别又细分为子类别。举例来说，获得与实施包含以下子类别：

- 获得和维护应用程序软件
- 获得和维护技术基础设施
- 开发和维护规程
- 安装和认可系统
- 管理变更

从上面可以看出，CobiT 域为公司提供了目标和指导，可以按照这些规则购买、安装、测试、认证和认可 IT 产品。这是相当强大的，因为现在大多数公司都在使用临时的和非正式的方式进行采购和开展流程。对于 IT 治理，CobiT 提供了一个“检查列表”的方法，也就是在实现不同的 IT 功能时，需要提供一系列经过深思熟虑完成的材料。

CobiT 规定了执行摘要、管理指南、框架、控制目标、实现工具集、性能指标、成功因素、成熟度模型和审计准则。它勾画出一个完整的可以遵循的路线图来完成这种模式涉及的 34 个控制目标中的每一个。图 2-7 展示了 CobiT 框架如何将业务需求、IT 资源和 IT 过程连接在一起。

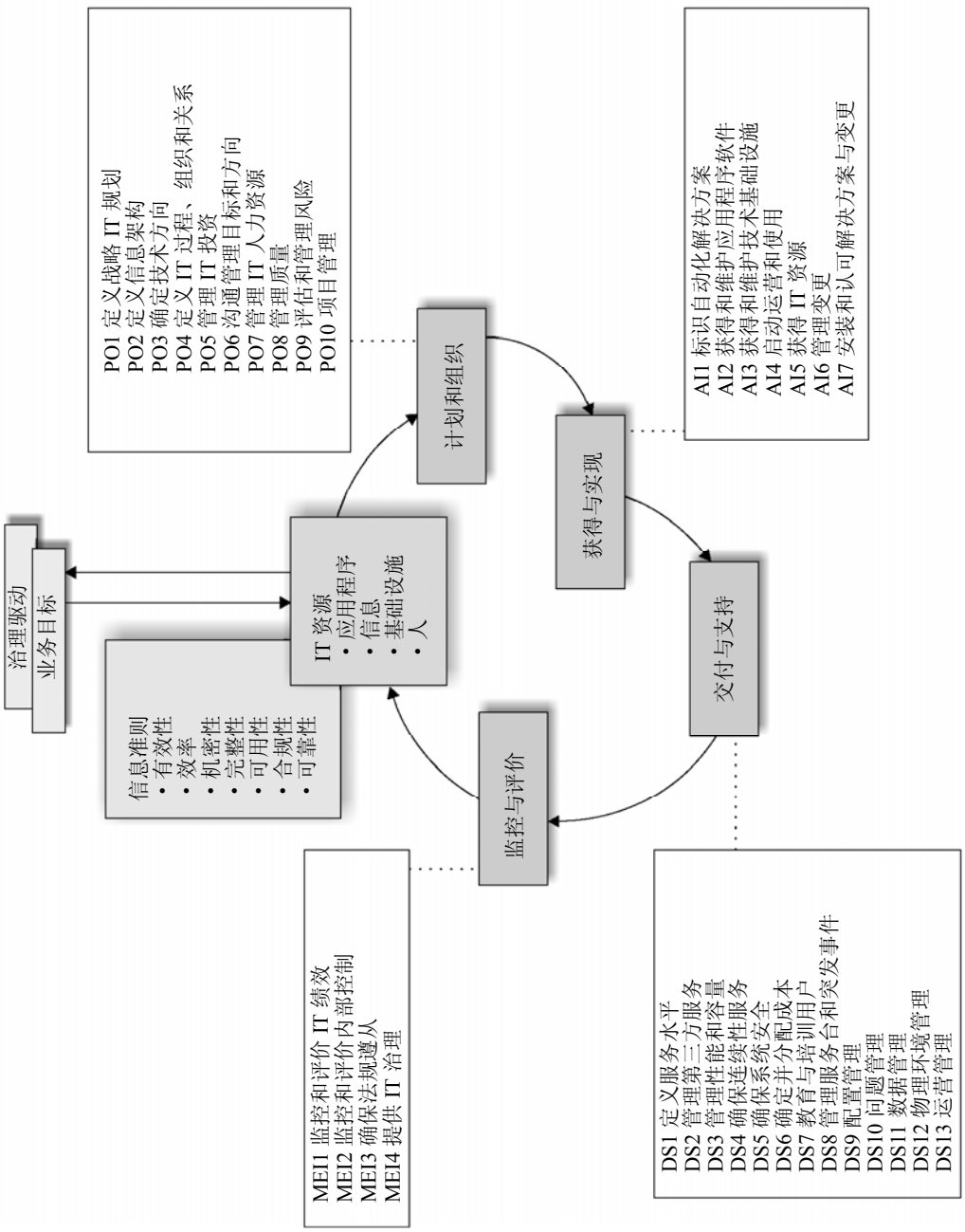

图 2-7　CobiT 框架

那么，CobiT 是如何融入全局呢？按照 ISO/IEC27000 系列标准开发安全策略时，高层次的文件会有类似的声明“不允许非授权的访问”，但谁被授权了？如何授权？如何实现访问控制确保不会发生非授权访问？如何判断访问控制组件在正确工作？以上都是理论联系实际的地方，也正是策略文件中的描述在现实中如何付诸实施的问题。CobiT 提供了选取的控制措施在现实中部署后需要实现的目标。例如，CobiT 列出了以下用户账户管理的控制实践：

- 使用唯一的用户 ID，以使用户被关联到其行为并为之承担责任。

- 校验那些需要使用信息系统或服务的用户是否获得了系统所有者的授权，获得的授权访问级别是否适合业务目标，是否符合组织的安全策略。
- 要求用户理解并确认访问权限和访问条件的规程。
- 确保在授权流程完成前，内部和外部服务供应商不能访问。
- 维护一个包含所有使用服务的注册用户及访问级别的正式记录。
- 及时并定期审查用户 ID 和访问权限。

当涉及用户账户管理时，组织应该确保它至少满足这些目标，反过来，这也是审计师审计要依照的东西，确保组织正确地实践安全。在行业中，目前使用的大部分安全合规性审计实践都是基于 CobiT 的。所以，如果要想使审计师高兴，并审核通过组织的合规性评估，应该学习、实践并实现 CobiT 中列出的控制目标，这被认为是行业的最佳实践。

注意：

在安全行业，许多人错误地认为，CobiT 纯粹以安全为目标，但现实中，它涉及信息技术的各个方面，安全性只是它的一个组成部分。CobiT 是一套实践，可以遵循它来进行 IT 治理，它要求有正确的安全实践部分。

2. NIST 800-53

——有解锁政府系统的标准方法吗？

CobiT 包含有私营部门使用的控制目标，但当涉及联邦信息系统和组织的控制时，美国政府有其自己的一套要求。

NIST(国家标准与技术研究所)是美国商务部的一个非监管机构，它的使命是“通过推进测量科学、标准和技术的方式促进美国的创新和产业竞争力，提高经济安全，改善生活质量。”

NIST 负责制定的标准之一被称为 Special Publication(特别发表刊物)800-53，其中概述了机构要部署的控制，以符合 Federal Information Security Management Act of 2002(联邦信息安全管理法案 2002)。表 2-4 列出了本发布中所讨论的控制类别。

表 2-4　NIST 800-53 控制类别

标 识 符	系　　列	类
AC	访问控制	技术类
AT	意识教育和培训	运营类
AU	审计和问责	技术类
CA	安全评估与授权	管理类
CM	配置管理	运营类
CP	连续性计划	运营类
IA	身份认证与验证	技术类
IR	事件响应	运营类
MA	维护	运营类
MP	媒体保护	运营类
PE	物理和环境保护	运营类
PL	计划	管理类
PM	规划管理	管理类

(续表)

标 识 符	系 列	类
PS	人员安全	运营类
RA	风险评估	管理类
SA	系统和服务获取	管理类
SC	系统和通信保护	技术类
SI	系统和信息完整性	运营类

这些控制类别(系列)是为信息系统准备的管理、运营和技术控制，用来保护系统及其信息的保密性、完整性和可用性。

就像是在商业领域，审计人员按照 CobiT 为他们提供的“检查列表”方式用面向商业的规则来评估一个组织的法规遵从性，政府审计人员使用 SP 800-53 作为“检查列表”方式，以确保政府机构能够符合面向政府的规则。虽然这些控制目标检查列表(CobiT 与 SP 800-53)不一样，但它们仍有很多部分重叠，因为不管它们处于什么类型的组织，都需要以类似的方式保护系统和网络。

警告：

在 CISSP 考试中，你可以看到控制类别细分为行政管理、技术和物理类别以及 NIST 中列出的类别，如管理、技术和运营。要熟悉这两种控制类型分类方法。

2.4.4 COSO

——将费用都用在收益列表中，因此看上去我们有很多钱。

——是，没人会发现。

CobiT 派生于 COSO 框架，是由反欺诈财务报告全国委员会发起组织委员会(Committee of Sponsoring Organizations，COSO)于 1985 年开发的，是用来处理财务欺诈活动并汇报。COSO 框架由以下组件构成。

- 控制环境
  - 管理哲学和运营风格
  - 涉及道德和欺诈的企业文化
- 风险评估
  - 建立风险目标
  - 管理内部和外部变化的能力
- 控制活动
  - 为降低风险制定的策略、规程和实践
- 信息和通信
  - 确保正确的人在正确的时间获得正确信息的结构
- 监控
  - 检测和应对控制不足的响应

COSO 是企业治理模型，而 CobiT 是 IT 治理模型。COSO 处理的更多是战略层的事情，而 CobiT 更关注运作层面。可以将 CobiT 视为满足许多 COSO 目标的一种方式，但它仅从 IT 角度来满足。COSO 也处理非 IT 事项，如公司文化、财务会计原则、董事会董事责任和内部沟通机制。

COSO 是为向虚假财务报告全国委员会(National Commission on Fraudulent Financial Reporting，一个研究虚假财务报告及其诱发因素的组织)提供资助而形成的。

关于欺诈问题，20 世纪 70 年代已经有法律出台，明确规定一个公司编造账簿(人为操纵自己的收入和盈利报告)是违法行为，但是直到 2002 年，萨班斯-奥克斯利法案(Sarbanes-Oxley Act，SOX)才真正成为强制执行的法律。SOX 是美国联邦法律，除了其他规定之外，还包括如果公司向证券交易委员会(Security Exchange Commission，SEC)提交虚假的会计报告被发现，则可以让高管坐牢。SOX 是基于 COSO 模型的，到目前为止，符合 SOX 的公司必须遵照 COSO 模型。企业普遍实施了 ISO/ IEC27000 标准和 CobiT，以帮助建立和维护内部 COSO 结构。

注意：

CISSP 考试不涉及具体的法律，如联邦信息安全管理法案和 SOX，但却涉及了安全控制模型框架，如 ISO 标准、CobiT 和 COSO。

2.4.5　流程管理开发

确保部署了适当的控制后，还希望以结构化和可控的方式构造和完善业务、IT 和安全过程。可以认为安全控制是“工具”，过程则是如何使用这些工具。要正确、有效、高效地使用它们。

1. ITIL

——如何确保 IT 部门支持业务单位？

——有无数方法。

ITIL(Information Technology Infrastructure Library，信息技术基础设施库)是 IT 服务管理的最佳实践的事实标准。ITIL 的产生源于业务需求对信息技术的依赖不断增加。不幸的是，大多数组织中的业务人员和 IT 人员之间存在着天然的鸿沟，因为他们在组织内使用不同的术语，有不同的侧重点。缺乏共同的语言和对另外一方领域(业务和 IT)的理解已导致许多企业不能有效融合业务目标和 IT 功能。这种错误的融合，通常会产生混淆、错误通信、错过最后期限、错过机会、增加时间和劳动成本以及在业务和技术层面上的挫折。ITIL 是以图书或在线形式提供可定制框架。它提供了目标、实现这些目标需要的一般活动、要满足既定目标的每个过程的输入和输出值。虽然 ITIL 拥有处理安全的组件，但其重点倾向于 IT 部门和它所服务的“客户”之间的内部服务水平协议，“客户”通常是指组织内部部门。图 2-8 所示为 ITIL 的主要组件。

2. 六西格玛

——我在业务改进上有盲点。

——为什么不再多想想？

六西格玛是一种过程改进方法论，也是一种“新的和改进的”全面质量管理(Total Quality Management，TQM)，它曾在 20 世纪 80 年代轰动了业务部门。它的目标是通过使用测量运营效率，减少变异、缺陷和浪费的统计方法来实现改善过程质量。在某些情况下，安全保障行业用六西格玛来度量不同的控制措施和过程的成功要素。六西格玛是由摩托罗拉公司开发的，其目标是在生产过程中识别和消除缺陷。西格玛层级描述了过程的成熟度——它代表着过程中包含缺陷的百分比。在运用于生产时，六西格玛已经被应用到多种类型的业务功能中，包括信息安全和保证。

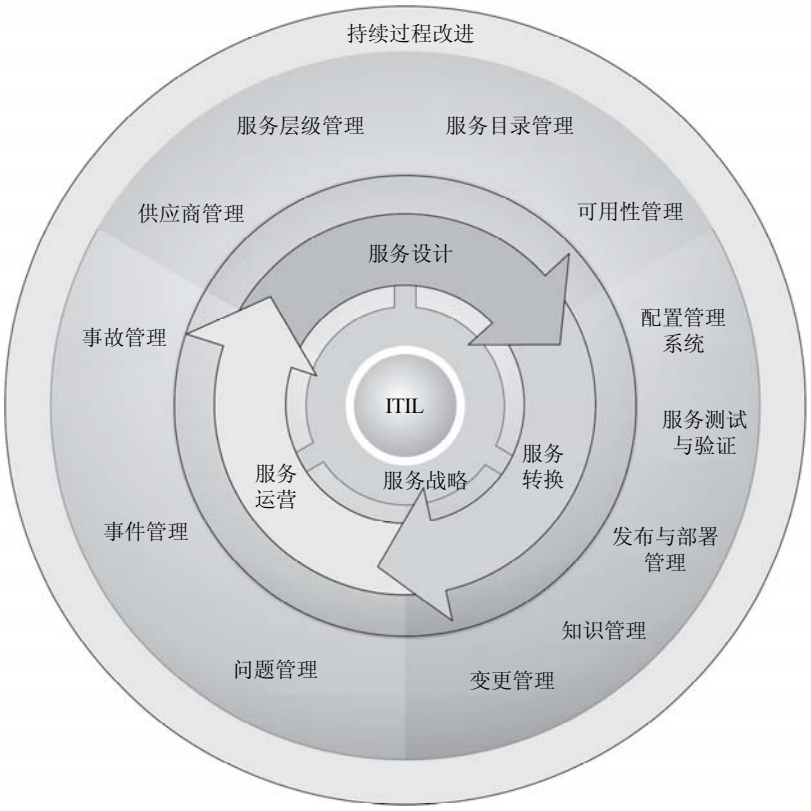

图 2-8　ITIL

3. CMMI

——我只想要更好的、更好的、更好的！

——走开。

CMMI(Capability Maturity Model Integration，能力成熟度模型集成)来自于安全工程界，在第 10 章中将深入讲解这个模型，但这个模型也可以用在组织内，帮助组织铺平持续改进之路。

虽然知道需要使安全规划更好，但是这并不总是很容易做到，因为“更好”是一个模糊和不可计量的概念。可以真正得到提高的唯一方法是：知道从什么地方开始，需要到什么地方，以及需要在这两者之间采取的步骤。正如如图 2-9 所示，每个安全规划都有成熟度级别。在 CMMI 模型里的每个成熟度等级代表一个改进阶段。有些安全规划是混乱的、临时的、不可预测的，而且通常是不安全的。有些安全规划创建了文档，但在实际过程中并没有发生；而一些安全规划却是十分先进、精简和高效。

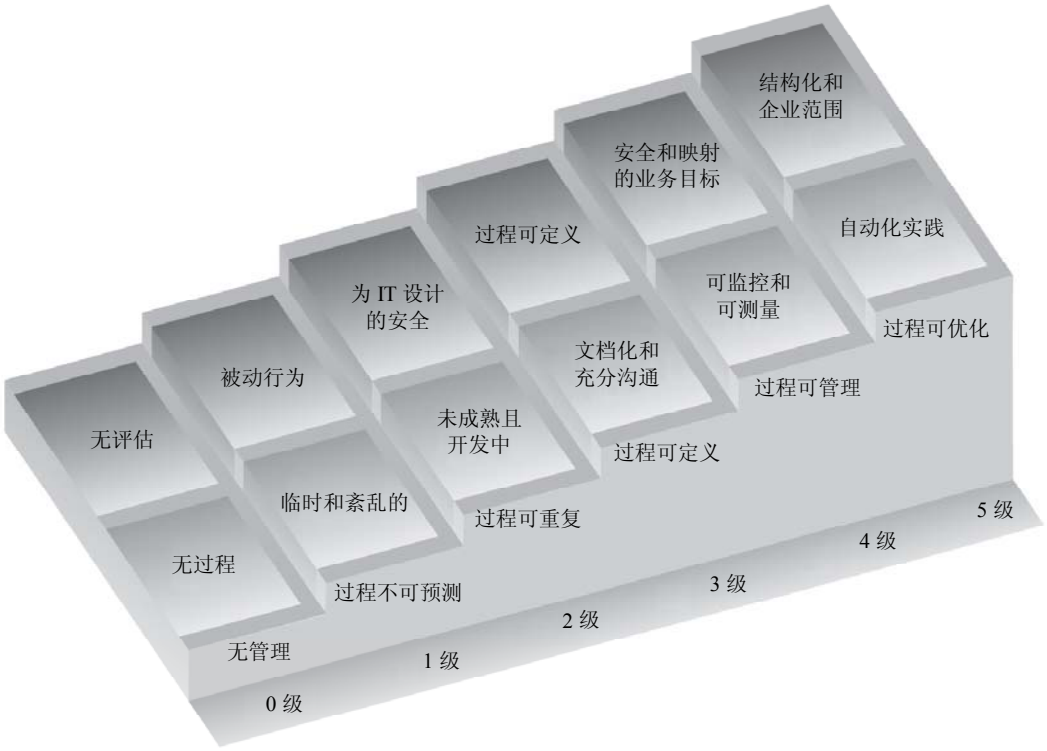

图 2-9　安全规划的能力成熟度模型

安全规划开发

没有一个组织打算把前面列出的所有标准及架构框架(ISO/IEC 27000、COSO、Zachman 框架、SABSA、COBIT、NIST 800-53、ITIL、六西格玛，CMMI)都能部署上。它们是很好的工具箱，打开它，会找到一些更加适合于所在组织的工具。还会发现当所在组织的安全规划日趋成熟时，这些不同的标准、框架和管理组件会在哪里发挥作用。虽然这些标准和框架都是独立和独特的，但是对于任何安全规划和相应的控制，它们都是要建立的基本内容。这是因为无论它们被部署在公司、政府机构、企业、学校还是非盈利组织中，安全的基本原则都是通用的。每个组织实体都是由人员、流程、数据及技术组成的，这些元素都需要得到保护。

CMMI 的关键是开发出可以遵循的结构化步骤，依据它，组织就可以从一个层次升级到下一个层次，并能不断改进流程和安全态势。安全规划包含了很多元素，但如果期待所有组件在部署第一年都被恰当地实施是不现实的。某些组件(如取证能力)在一些基本工作(如事件管理)建立起来前，是不可能部署到位的。这正像想让小孩学会跑步之前，必须列出学习走路的方法一样。

自顶向下的方法

——门卫说应该把计算机都打包起来，以满足安全需求。

——可能要先问问管理层。

安全规划应使用自顶向下的方法，这意味着启动、支持和方向都来自于高层管理人员；中层管理人员传达高层意图，最后下达到一线工作人员。与此相反，一个自底向上的方法是指工作人员(通常是 IT 人员)在没有得到足够的管理支持和指导的情况下，开发安全规划。自底向上的方法通常是彻底无效的，而且没有全面解决所有的安全风险，最后注定是要失败的。自顶向下的方法是确保人们真正保护公司的资产，它是由高级管理人员所驱动。高级管理人员不仅要最终负责保护组织，而且有必要的资金财政大权，有权分配所需要的资源，并且是唯一可以保证安全规则和策略真正执行的人。管理层的支持是安全规划最重要的部分之一。简单的点头和眼神交流不会提供安全规划所需要的支持。

虽然这些不同的安全标准和框架的核心是相似的，重要的是要理解安全规划都具有不断循环的生命周期，因为应该不断对其进行评估和改进。任何进程中的生命周期都可以用不同的方式描述。通常使用下面的步骤：

(1) 计划和组织
(2) 实现
(3) 运营和维护
(4) 监控和评估

如果安全规划和安全管理没有使用生命周期方法来维护程序，组织注定只是像对待另外一个项目那样对待安全。任何被视为项目的东西都有开始日期和结束日期，并且在到达结束日期时每个人都被分散到其他的项目中。许多组织都雄心勃勃地开始安全计划，但由于没有实现正确的结构以确保安全管理的持续进行和不断改进，结果造成多年来大量的启动和停止。重复性的工作花费比本应该的花费多很多，但效果却降低。

以下提供的是每个阶段的主要组件。

- 计划和组织
  - 建立管理承诺
  - 建立监督指导委员会
  - 评估业务驱动
  - 开发组织的威胁配置文件
  - 开展风险评估
  - 在业务、数据、应用程序及基础设施层面开发安全架构
  - 确定每个架构层面的解决方案
  - 获得管理层的批准后向前发展
- 实施
  - 分配角色和职责
  - 开发和实现安全策略、规程、标准、基准和指南
  - 识别静态和传输中的敏感数据。

- 实现下列蓝图：
  - 资产识别和管理
  - 风险管理
  - 脆弱性管理
  - 合规
  - 身份管理和访问控制
  - 变更控制
  - 软件开发生命周期
  - 业务连续性计划
  - 意识教育和培训
  - 物理安全性
  - 事件响应
- 每个蓝图的实现解决方案(管理、技术、物理)
- 为每个蓝图开发审计和监控解决方案
- 为每个蓝图建立目标、服务水平协议(SLA)和度量指标

- 运营和维护
  - 遵循程序，以确保在每个已实现的蓝图满足所有基准
  - 进行内部和外部审计
  - 执行每个蓝图所述的任务
  - 管理每个蓝图的服务水平协议(SLA)
- 监测与评估
  - 审查日志、审计结果、收集的度量值和每个蓝图的服务水平协议(SLA)
  - 评估每个蓝图的目标完成情况
  - 每季度与指导委员会开会
  - 制定改进步骤，并融入计划和组织阶段

上面列出的许多项都贯穿在整本书中。提供的列表展示了所有这些项是如何以有序和可控的方式推进的。

虽然前面介绍的标准和框架非常有用，但它们的水平非常高。例如，如果一个标准简要地指出一个组织必须确保其数据的安全，需要投入大量的工作。这就是安全专业人员为开发安全蓝图卷起衣袖大干一场的地方。为特定业务需求识别、开发和设计安全需求时，蓝图成为重要工具。组织基于管理责任、业务驱动和法律义务提出了自己的安全需求，则必须定制蓝图以满足这些需求。例如，Y 公司有数据保护策略，其安全团队也已经开发了该公司应遵循的数据保护战略的标准和程序。这时，就需要设计出更加细化的蓝图、必要的过程和组件来满足在策略中所述的要求、标准和需求。其中，至少包括一个公司网络的示意图。

- 敏感数据存放在网络的什么位置
- 敏感数据跨越的网络分段
- 为保护敏感数据而采用不同的安全解决方案(如 VPN、SSL 和 PGP)
- 共享敏感数据的第三方连接
- 为第三方连接采用的安全措施
- ……

要开发和遵循哪些蓝图取决于组织的业务需求。例如，Y 公司要使用身份管理，那么必须要有一个蓝图勾勒出角色、注册管理、授权来源、身份信息库和单点登录解决方案等。如果 Y 公司不使用身份管理，那么就没有必要为此建立蓝图。

因此，蓝图须列出安全解决方案、过程和组件，供组织用于满足自身的安全和业务需求。蓝图必须应用在组织内不同的业务部门中，例如，在不同部门实行身份管理都应遵循绘制好的蓝图。在整个组织中遵循统一的蓝图，将方便实施标准化，更容易进行度量指标收集和治理工作。图 2-10 说明了开发安全规划时，蓝图会在哪里发挥作用。

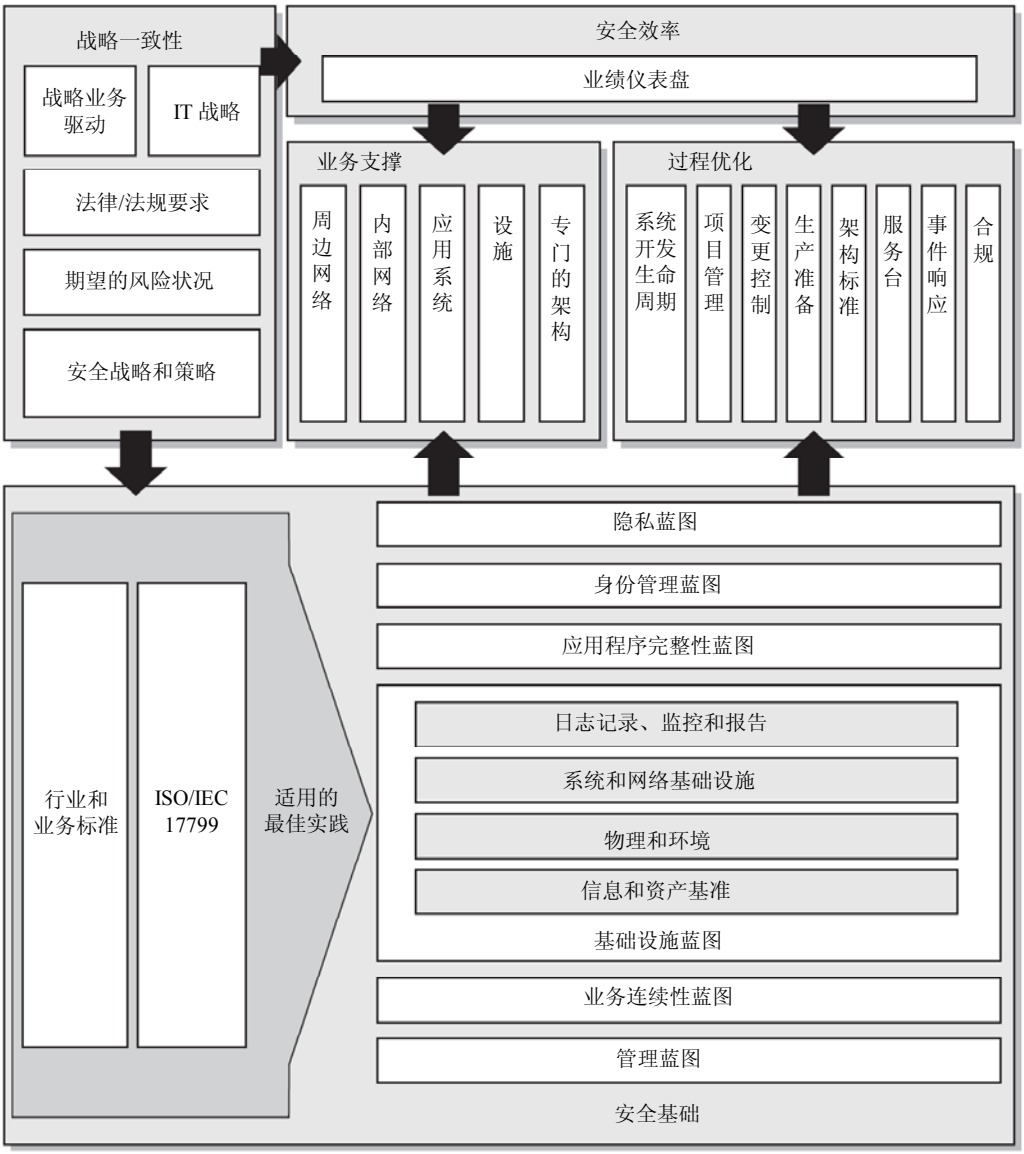

图 2-10　蓝图必须与安全、业务需求相对应

为将这些紧密联系在一起，可以考虑 ISO/IEC27000，它主要在策略层工作，就像说明想建造的房屋的类型(二层、牧场式、5 间卧室和 3 间浴室)。企业安全框架像是房子的建筑布局(基础、

墙壁和天花板)。蓝图好比是房子特定组件(窗户类型、安全系统、电气系统和管道等)的详细说明。控制目标好比是为保障安全而规定的建设规范和条款(包括电气接地、布线、建材、保温和防火等)。建筑检查员将使用他的检查列表(建筑规范)以确保在安全地建造自己的房子。这就如同审计师用他的检查列表(COBIT 或 SP 800-53)确保安全地建立和维护安全程序。

一旦房子建成了，你的家人会搬进去，将会设置时间表和日常生活的流程，这些事情的发生是可预见的，而且是高效的(如爸爸接孩子放学，妈妈做饭，大一点的孩子洗衣服，爸爸支付账单，每个人都做院子里的工作)。这类似于 ITIL——流程管理和改进。假如家庭是由一些优秀工作人员组成，而他们的目标是尽可能高效地优化日常活动，因此很可能会采纳六西格玛方法，该方法以持续过程改进为重点。

关键术语

- **隐匿安全**　依赖于措施的保密和复杂性实现安全，而非采用最佳安全实践。
- **ISO / IEC 27000 系列**　业界公认的最佳实践用于 ISMS 的开发与管理。
- **Zachman 框架**　该企业架构框架由 John Zachman 开发，用于定义和理解商业环境。
- **TOGAF**　该企业架构框架由开放群组(Open Group)开发，用于定义和理解商业环境。
- **SABSA 框架**　风险驱动的企业安全架构，它将安全映射到商业计划，与 Zachman 框架相似。
- **DoDAF**　美国国防部架构框架，用以确保系统的互操作性，以满足军事任务的目标。
- **MODAF**　这个架构框架由英国国防部开发的，主要用于军事任务支援。
- **COBIT**　它是一组控制目标集，用来作为 IT 治理的框架，是由 ISACA 和 ITGI 开发的。
- **SP 800-53**　由 NIST 开发的用于保障美国联邦系统安全的控制集。
- **COSO**　是由反欺诈财务报告全国委员会发起组织委员会(COSO)开发的，用于公司治理以帮助防止欺诈行为的内部控制。
- **ITIL**　信息技术服务管理流程的最佳实践，是由英国政府商务办公室开发的。
- **六西格玛**　由摩托罗拉公司开发的企业管理战略，目的是改善业务流程。
- **CMMI**　卡耐基梅隆大学开发的过程改进模型。

2.4.6　功能与安全性

——安全了，但什么也做不了！

任何一个参与到安全计划的人都能理解，在保障组织信息安全和提供必要的功能性之间需要平衡，只有这样才能不会影响生产效率。在许多安全项目启动之初，往往有一个常见的场景：项目负责人清楚想要达到的最终结果，而且对于如何快速、高效地部署安全方案有很理想化的想法，但是他们跟用户协商失败了，因为用户认为自己会被限制所束缚。在用户听到约束条件后，会通知项目经理，如果按照安全计划实施，他们将无法完成某些部分的工作。这通常会导致该项目紧急刹车而停止运转。项目经理必须重新开展可行性评估、评价以及规划如何循序渐进的保护组织环境，如何有技巧地让用户和任务接受新的安全约束和业务。在规划阶段如果与用户沟通失败或用户没有充分了解业务流程，则会造成许多麻烦，浪费时间和金钱。安全管理活动的负责人必须认识到，他们需要理解环境，并在开始安全规划实施阶段之前做好充分的计划。

2.5 安全管理

——既然创造了这个东西，如何管理它呢？

——踢它行吗。

我们听说过许多故事：病毒造成数百万美元的损失；外国黑客从金融机构盗取信用卡信息；大公司和政府的网站因为政治问题而受到攻击；黑客被捉拿归案并送入监狱。这些都是与信息安全相关的有趣信息，但实际上，以上活动并不是普通公司或安全部门的专家在日常安全任务中需要处理的问题。虽然病毒和黑客攻击占据了头条新闻的位置，但安全管理才是公司业务和信息安全结构的核心。

安全管理会随着时间发生变化，因为联网环境、计算机以及保留信息的应用程序都在变化。过去，信息存储在大型机上，这种大型机采用了更集中的网络结构。大型机以及用于访问和配置大型机的管理控制台都在一个相对集中的区域内，而不是像今天看到的分布式网络。只有特定的人能够访问大型机，只有一小部分人才知道大型机的工作方式，这就大大降低了安全风险。用户能够通过“哑”终端(由于没有或只有很少的内部逻辑而得名)访问大型机上的信息。也不需要安排多少严格的安全控制，因为这种封闭的环境提供了类似茧一样的保护环境。然而，计算领域并非总是这种架构。现在，大多数网络都容纳了许多个人计算机，个人计算机拥有高级逻辑和处理能力，用户对系统的熟悉程度足以让他们危及系统本身，信息也再不是只集中于某个“玻璃屋”内。相反，信息分布在服务器、工作站、笔记本、无线设备、移动设备、数据库及其他网络中。信息通过有线和无线方式传输的速度在 10～15 年前是无法想象的。

Internet、外联网(公司合伙人的网络)与内联网不仅让安全更为复杂，而且让安全问题显得更为关键。核心网络架构已经从本地独立计算环境变成了分布计算环境，随着这种变化呈指数增长，网络复杂性也随之增加。虽然将网络接入 Internet 能够为用户提供更多的功能和服务，并且能够让公司在 Internet 世界中开阔视野，但是也为潜在的安全风险敞开了大门。

今天，如果失去了计算机和处理能力，那么许多组织就无法运转。计算机已融入商业和个人日常生活之中，突然失去它们，人们将遭受极大的痛苦和损失。许多大企业已经认识到，数据应当像物理建筑、工厂设备和其他物理资产那样作为资产而受到保护。多数情况下，组织的敏感数据甚至比物理资产更重要，成为组织的“皇冠珠宝”。随着网络和环境的变化，安全也需要变化。安全不只是为保护组织资产所采用的技术控制，要对这些控制方法进行管理，并且安全工作的很大一个方面就是管理用户的活动以及所采取的措施。安全管理实践侧重于持续保护公司资产和资源。

安全管理包括所有为保持程序安全启动、运行和演变所需要的活动。它包括风险管理、文档化、安全控制实现和管理、流程和过程、人员安全、审计和持续的安全意识培训。风险分析标识出关键资产，发现对它们构成威胁的风险，并估计在风险成为现实时公司可能承受的危害和损失。风险分析将帮助管理层构造预算，从而有足够的资金能够用于保护被识别的资产不会遭受威胁，以及开发可行的、指导安全活动的安全策略。标识、实现和维护保护控制措施，使组织的安全风险维持在可接受的水平。安全教育和意识培训将信息安全灌输给公司内的每位员工，因此每个人都受到了安全教育，从而能够更容易地朝着相同的安全目标前进。

下面将就安全项目管理中所涉及的最重要的组件进行讨论。

2.6 风险管理

——生活充满风险。

安全环境下的风险指的是破坏发生的可能性以及破坏发生后的衍生情况。信息风险管理

(Information Risk Management，IRM)是识别并评估风险、将风险降低至可接受级别、执行适当机制来维护这种级别的过程。百分之百安全的环境是不存在的。每种环境都具有某种程度的脆弱性，都面临一定的威胁。问题的关键在于识别这些威胁，估计它们实际发生的可能性以及可能造成的破坏，并采取恰当的措施将系统环境的总体风险降低至组织机构认为可接受的级别。

公司面临的风险具有各种形式，它们并非都与计算机有关。例如，某家公司并购另一家公司，在希望此举动将扩大市场份额、提高生产效率、增加利润的同时，前者也将承担大量风险。如果一家公司扩大生产线，那么就可能会增加管理费用、招聘新员工、购置设施以及投入更多资金购买原材料，而且还可能需要增加保险金以及营销活动开支。在这种情况下，潜在的风险在于：管理费用的提高可能不会导致销售的增长，因而利润反而会降低，或者无法取得预期的效益。

当考虑信息安全时，企业需要了解并正确处理几种类型的风险。下面列出了几种主要的风险：

- **物理破坏**　火灾、水灾、蓄意毁坏、停电和自然灾害。
- **人为破坏**　意外或有意行为，或者可能降低生产效率的懒散工作态度。
- **设备故障**　系统或外围设备故障。
- **内部与外部攻击**　黑客、破解和攻击行为。
- **数据误用**　共享商业秘密、欺诈、间谍活动和盗窃。
- **数据丢失**　通过破坏性方法有意或无意地造成信息丢失。
- **应用程序错误**　计算错误、输入错误和缓冲区溢出。

我们需要识别这些威胁，对它们进行分类和评估，从而计算出威胁可能对公司造成的损失程度。虽然实际风险很难衡量，但是我们可以根据潜在的风险大小来决定处理各种风险的优先顺序。

2.6.1　谁真正了解风险管理

可惜的是，在安全领域内外，很少有人真正了解风险管理。虽然如今信息安全是一宗“大生意”，但其焦点更多是放在应用程序、设备、协议、病毒与黑客行为上。尽管在风险管理过程中仍然需要考虑并权衡所有这些内容，然而就总体安全而言，它们只是次要问题，而不是风险管理的重心所在。

安全已成为一个商业问题，但商业运作的目的在于盈利，而不只是确保安全。只有当潜在风险威胁到它的根本利益时，公司才会关注安全问题。风险以各种形式存在，例如信用卡号码数据库泄露引发机构声誉下降和客户流失；一种新的计算机蠕虫病毒造成几千美元的运作费用损失；成功的公司间谍行为导致专利信息泄露；有效的社会工程攻击造成机密数据丢失。对安全专家来说，理解每个威胁极为重要。然而更重要的是，他们必须了解如何计算这些威胁造成的风险，并将其转换成公司应对安全威胁的推动力。

了解“脆弱性”、“威胁”和“风险”这些定义之间的差异对你而言可能无关紧要，但它确实比大多数人所认为的要重要得多。脆弱性扫描器能够识别正在运行的危险服务、多余账户以及存在安全漏洞的系统。这只是简单的工作。但是，如果只有 12 万美元的安全预算，但却需要处理大量的脆弱性，那么你是否具备决定首先处理哪些脆弱性的相应技能呢？既然资金有限，而脆弱性的数量几乎是无限的，你如何才能确定关键脆弱性的处理顺序、保证公司优先解决最紧迫的问题并获得最大投资回报呢？这才是风险管理的关键所在。

正确地实施风险管理意味着你全面了解组织，了解它所面临的威胁，知道应该采取什么样的应对措施来处理这些威胁，并持续监控以确保风险级别处于可接受的级别。

2.6.2　信息风险管理策略

——如何拼凑所有这些风险管理片段？

——看看策略吧。

恰当的风险管理需要高级管理层的坚定承诺和一个文本化过程，这个过程为组织机构的使命、IRM 策略和委任的 IRM 团队提供支持。

IRM 策略应成为组织机构总体风险管理策略的一部分(公司风险不仅限于信息安全问题)，并且应当在组织机构的安全策略中体现出来。IRM 策略应当涉及下列内容：

- IRM 团队的目标
- 公司可接受的风险级别及其定义
- 风险识别的形式化过程
- IRM 策略与组织机构的战略规划过程之间的联系
- IRM 的职责以及履行这些职责的角色
- 风险和内部控制之间的映射关系
- 为响应风险分析而改变员工行为和资源分配的方式
- 风险与业绩目标和预算之间的映射关系
- 监控控制效率的主要指标

IRM 策略为组织的风险管理过程及措施奠定基础并指明方向，并应解决一切信息安全问题。同时，IRM 策略还应为 IRM 团队如何向高级管理层通报公司风险信息以及如何正确执行管理层决定的风险缓解任务提供指导。

2.6.3 风险管理团队

——Fred 胆子小，什么都怕，他要担任我们风险团队的头儿了。

——挺好。

每个组织机构在公司规模、安全态势、威胁情况与安全预算方面各有差异。一个组织机构可能只有一名员工负责 IRM，或者拥有一个协同合作的 IRM 团队。IRM 团队的总体目标在于以最低预算确保公司安全。只有完成下列工作，这一目标才有可能实现：

- 由高级管理层提供明确的风险接受级别。
- 记录风险评估过程与措施。
- 识别和缓解风险的措施。
- 由高级管理层适当分配资源与资金。
- 对所有与信息资产有关的员工进行安全意识培训。
- 如有必要，能够成立特殊领域内的改进(或风险缓解)团队。
- 制定法律及法规遵从要求计划，以控制和履行这些要求。
- 开发衡量标准和业绩指标，以衡量和管理各种类型的风险。
- 能够随环境和公司变化识别和评估风险。
- 集成 IRM 与组织机构的变更控制过程，保证这些变更不会形成新的脆弱性。

显而易见，这个列表所包含的内容并不仅仅是购买一款新的防火墙并宣称它能保证公司安全那么简单。

在大多数情况下，IRM 团队成员并非由专门从事风险管理工作的员工组成。相反，团队成员已在公司拥有一份全职工作，他们只是暂时承担风险管理任务。因此，有必要获得高级管理层的支持，从而对资源进行合理的分配。

当然，任何团队都需要一名领袖，IRM 团队也不例外。公司应该挑选一名成员来管理这个团队，在大型组织机构内，这名成员应当使用 50%～70%的时间来处理风险管理工作。管理层必须

投入资金对此成员进行必要的培训，为其提供风险分析工具，以确保风险管理工作的顺利进行。

2.7　风险评估和分析

——我已确定我们所面临的最大风险是这个曲别针。

——发现得好！

风险评估(实际上是一种风险管理工具)方法能够识别脆弱性和威胁以及评估可能造成的损失，从而确定如何实现安全防护措施。对风险进行评估，之后分析结果。风险分析用于确保安全防护措施是划算的、相关的、及时的并能响应特定威胁。安全问题可能会非常复杂，即使对熟练的安全专家来说也是如此，而且其容易造成如下的问题：使用太多的安全限制，安全措施不足，使用了错误的安全组件，在实现安全的过程中花费了太多的资金却没有达到既定的目标。风险分析帮助公司将面临的风险区分出优先次序，向他们说明投入一定的资金就可以明智地保护自己不受这些风险的影响。

风险分析有下列 4 个主要目标：

- 标识资产和它们对于组织机构的价值。
- 识别脆弱性和威胁。
- 量化潜在威胁的可能性及其对业务的影响。
- 在威胁的影响和对策的成本之间达到预算的平衡。

风险分析提供了一种成本/收益比(cost/benefit comparison)，也就是用来保护公司免受威胁的防护措施的费用与预料中的损失所需要付出的代价之间的比值。在大多数情况下，如果损失的代价没有超过防护措施本身的费用，那么就不应该实行该防护措施。这意味着，如果某个设施价值 10 万美元，那么花 15 万美元保护它就没有任何意义。

在开始工作之前，你必须明白应该做些什么。任何没有正确定义项目范围就匆忙开始工作的人都能够证实这种说法的正确性。在评估和分析之前，安全团队必须估计项目的规模，以确定应评估哪些资产和威胁。大多数评估主要针对物理安全、技术安全和人员安全。试图同时评估所有这些项几乎是不可能的。

安全团队需要完成的一项任务是生成一份详细说明资产评估结果的报告。高级管理层应审核和接受这份报告，并将其确定为 IRM 项目的范围。如果管理层在这样的早期阶段就确定一些资产并不重要，那么风险评估团队就不应花费额外的时间或资源来评估这些资产。在与管理层讨论的过程中，参与讨论的每一名成员都必须清楚地了解 AIC 安全三元组(可用性、完整性和机密性)的重要性，以及它们与业务需求的直接关系。

管理层应简要说明项目范围，它很可能会受到组织化治理、风险管理以及法规和资金的限制。如果在项目开始之初没有认真评估项目的规模，那么项目随后就会因为缺乏资金而停止。千万不要让这种情况发生在自己身上。

风险分析能够帮助将安全计划目标整合到公司的业务目标和需求中。业务目标和安全目标越一致，两者就会越成功。风险分析还能够帮助公司为安全计划及构成安全计划的组件制订合理的预算。一旦公司了解了自己资产的价值以及它们面临的潜在威胁，它就能够在花多少金钱保护这些资产的问题上作出明智的决策。

如果想获得成功，那么风险分析就必须得到高级管理层的支持和指导。管理层需要确定风险分析的目的和范围，需要指定一个团队来执行这项评估，还需要有必要的时间和资金进行分析工作。对于高级管理层来说，查看风险评估和分析的结果并根据其发现的问题进行相应的行动是非

常重要的。仔细检查了风险评估发现的所有问题，但是却没有根据结果有所行动，那么又有什么用呢？然而，这样的情况的确时有发生。

2.7.1 风险分析团队

每个组织机构都有各种部门，每个部门都有自己的职能、资源、任务和特点。要实现最有效的风险分析，就需要建立一个风险分析团队，其中包括来自许多或全部部门的人员，以保证能够识别和处理所有的威胁。风险分析团队的成员可以是管理人员、应用程序编程人员、IT 人员、系统整合人员或运营部经理，事实上就是任何来自组织机构关键领域的关键人员。这是必要的人员组成方式，因为如果风险分析团队中只有来自 IT 部门的人员，那么他们可能不了解会计部门遇到的有关数据完整性问题的风险，或者会计部门的数据文件在一次意外或蓄意事件中丢失对于整个公司将意味着什么。在另一个示例中，IT 人员也可能不会明白，如果发生了自然灾害，那么仓库人员将遇到怎样的风险，这场灾害对于公司的工作效率和整个公司会造成什么影响。许多时候，风险分析团队都由各部门的人员组成。如果不能做到这一点，那么风险分析团队至少应当确保与各部门的人员面谈，从而能够充分了解和量化所有的威胁。

风险分析团队还必须包括了解各自部门工作流程的人，也就是每个部门中适当级别的人员。这是一项困难的任务，因为经理往往将所有风险分析任务都委托给部门中较低级别的人员，然而，这些较低级别的人员无法充分了解风险分析团队可能处理的工作流程。

在评估风险时，应当始终记住几个问题。这些问题有助于确保风险分析团队和高级管理层不会偏离工作重心。团队成员应提出以下问题：可能会发生哪些事件(威胁事件)？其潜在的影响(风险)是什么？它们多久发生一次(频率)？对于前面 3 个问题的答案的正确性有多大的把握(确定性)？通过进行内部调查、面谈或举办研讨会，可以收集到许多类似的信息。

在分析风险时，记住这些问题有助于团队集中注意手头的任务，并做出更加准确和合理的决策。

2.7.2 信息和资产的价值

——如果信息没有价值，那谁还愿意保护它呢？

附加于信息之上的价值与涉及信息的参与方、为开发信息而付出的劳动、为维护信息而花费的资金、信息丢失或遭到破坏所带来的损失、竞争对手为得到信息所付出的代价以及可能遭受的债务处罚相关。如果公司不知道它正在保护的信息和其他资产所具有的价值，那么就不会知道要花费多少资金和时间来保护它们。如果你的职责是确保俄罗斯无法获知美国的间谍卫星在发送和接收信息时所使用的加密算法，那么所运用的安全措施可能就要比保护自己的花生酱和香蕉三明治食谱不被邻居知道更为极端和昂贵。信息的价值决定了所要采取的安全举措。

上面的示例指的都是评估信息的价值并加以保护，不过这种逻辑只适用于保护一个组织机构的设施、系统和资源。公司设施的价值必须与其所有的打印机、工作站、服务器、外围设备、供应品和雇员一起评估。如果事先不了解你拥有什么资产及其价值，那么你就不会知道有多少资产面临着损失风险。

2.7.3 构成价值的成本

资产可以进行定量和定性度量，不过这些度量标准应当有根有据。资产的实际价值是由它对整个组织的重要性来决定的。资产的价值应该反映出当该资产真正遭受损失时所产生的所有可识别成本。如果一台服务器价值 4000 美元，那么在进行风险分析时，这个价值不应当作为该服务器的价值。如果该服务器出现故障，那么更换或修复费用、工作效率损失、任何可能崩溃或丢失的

数据的损失也应该考虑进来，这样才能得出公司在该服务器发生故障的情况下会遭受多大的损失。

在为资产定价时，应当考虑下面的问题：

- 获取或开发该资产的成本
- 维护和保护该资产的成本
- 该资产对所有者和用户具有的价值
- 该资产对竞争对手具有的价值
- 其他人为购买该资产愿意付出的价格
- 在损失的情况下更换该资产所需的费用
- 在该资产不可用的情况下损失的运作和生产能力
- 该资产贬值的债务问题
- 该资产在组织结构中的用处和角色

了解资产的价值，这是理解应当采取何种安全机制以及应当花费多少资金来进行保护工作的第一步。一个非常重要的问题是：如果公司不保护这些资产，那么将会造成多大的损失？

确定一项资产的价值有助于完成公司的各种工作，包括下列工作：

- 执行有效的成本/收益分析
- 选择特定的对策和防护措施
- 决定购买的保险范围
- 了解什么资产正在面临风险
- 遵循“应有的注意”，遵守法律和法规要求

资产包括有形资产(计算机、设施、供应品)和无形资产(声誉、数据、知识产权)。由于无形资产的价值会随着时间而变化，因此很难对其进行量化。应该如何评估公司声誉的货币价值呢？这个问题不容易回答，但重要的是要做这么做。

2.7.4　识别脆弱性和威胁

——呃，　应该害怕什么呢?

在前面部分中，我们为风险给出的定义是：威胁主体利用脆弱性对资产造成伤害的可能性以及导致的业务影响。有多种威胁主体可以利用若干种脆弱性，从而可能导致如表 2-5 所示的各种特定威胁。表 2-5 只是列举了许多组织在它们的风险管理计划中都会处理的一些风险示例。

表 2-5　威胁和脆弱性之间的关系

威 胁 主 体	可能利用的脆弱性	导致的风险
恶意软件	缺少防病毒软件	病毒感染
黑客	服务器上运行的功能强大的服务	对机密信息的未授权访问
用户	操作系统中配置错误的参数	系统故障
火灾	缺少灭火器材	设施和计算机受到破坏，可能付出生命代价
雇员	缺少训练或实施标准 缺少审计	共享至关重要的信息 在数据处理应用程序中更改输入和输出
承包商	松懈的访问控制机制	窃取商业秘密
攻击者	编写较差的应用程序 缺少严格的防火墙设置	造成缓冲区溢出 进行拒绝服务攻击
入侵者	缺少保安	打破窗户，盗窃计算机和设备

在计算机化的系统环境中还会出现其他一些威胁，这些威胁比表 2-5 中列出的威胁更加难以识别。这些威胁都与应用程序和用户错误有关。如果某个应用程序使用若干复杂的公式计算结果，那么在公式不正确或应用程序使用错误输入数据的情况下，要发现并隔离具体的威胁就可能会很困难。因为不正确的结果会传递给另外一个过程，所以可能导致不合逻辑的处理和级联错误。这种问题存在于应用程序代码的内部，并且非常难以发现。

通过监控和审计用户活动，比较容易识别用户有意或无意的错误。必须进行审计和复查，以便发现雇员是否在程序中输入了错误值、误用技术或以不合理的方式修改了数据。

一旦识别脆弱性及相关的威胁，还需要研究由此脆弱性衍生的问题。风险具有潜在损失，这意味着如果威胁主体确实利用了脆弱性，那么公司就会遭受损失。这种损失可能是数据的破坏、系统和/或设施的损毁、机密信息的未授权泄露以及雇员生产能力的下降等。当进行风险分析的时候，分析团队在评估某种风险可能造成的损害的同时，还必须考虑到延时损失。延时损失是次生灾害，发生在脆弱性被利用之后。延时损失包括公司声誉受损、市场份额减少、延时处罚增加、民事诉讼和从客户手中回笼资金出现延迟等。

例如，如果某个公司的 Web 服务器因遭受攻击而无法正常工作，那么最直接的损失(潜在损失)可能是数据讹误、修复服务器所需要的人力成本、替换代码和组件所需要的成本等。如果该公司通过自己的网站接受订单和付款，那么它的收益就会遭受损失。如果需要花费一整天时间修复 Web 服务器，那么该公司就可能损失大量的销售额和收益。如果需要花费一个星期修复 Web 服务器，那么该公司损失的销售额和收益就有可能不足以支付其他账目和花费。这些就是延时损失。如果该公司的客户因为这样的事情而对其失去信心，那么公司就会成年累月地遭受商业损失。这是延时损失的一种极端情况。

以上这些问题使得正确量化特定威胁可能造成的损失变得更加复杂，然而，必须将这些问题考虑进来，以保证这种分析能够反映事实。

2.7.5 风险评估方法

——有没有对待风险的方式方法？还是车到山前必有路？

对于风险评估来说，业内有不同的标准化方法。各个方法都包含相同的基本核心组件(识别脆弱性、分析威胁、计算风险值)，但各个方法又各有侧重。作为安全专业人士，你有责任知道哪个方法最适合你的组织及其需要。

NIST 开发了一套风险方法，出版在 SP 800-30 文档中。这套 NIST 方法叫做信息技术体系风险管理指南(Risk Management Guide for Information Technology System)，被认为是美国联邦政府标准。NIST 方法专门针对 IT 威胁及其与信息安全风险的关联方式。这种方法使用下列步骤：

(1) 系统特征描述
(2) 威胁识别
(3) 脆弱性识别
(4) 控制分析
(5) 可能性确定
(6) 影响分析
(7) 风险确定
(8) 控制建议
(9) 结果记录

NIST 风险管理方法主要关注计算机系统和 IT 安全问题。它不包括大型组织所面临的诸如自

然灾害、继任规划、环境问题以及安全风险与商业风险的关系等威胁类型。它是一个只关注企业运营层面而不是较高战略层面的方法。该方法勾勒了具体的风险方法，如图 2-11 所示，图中标明了相关联的输入值和输出值。

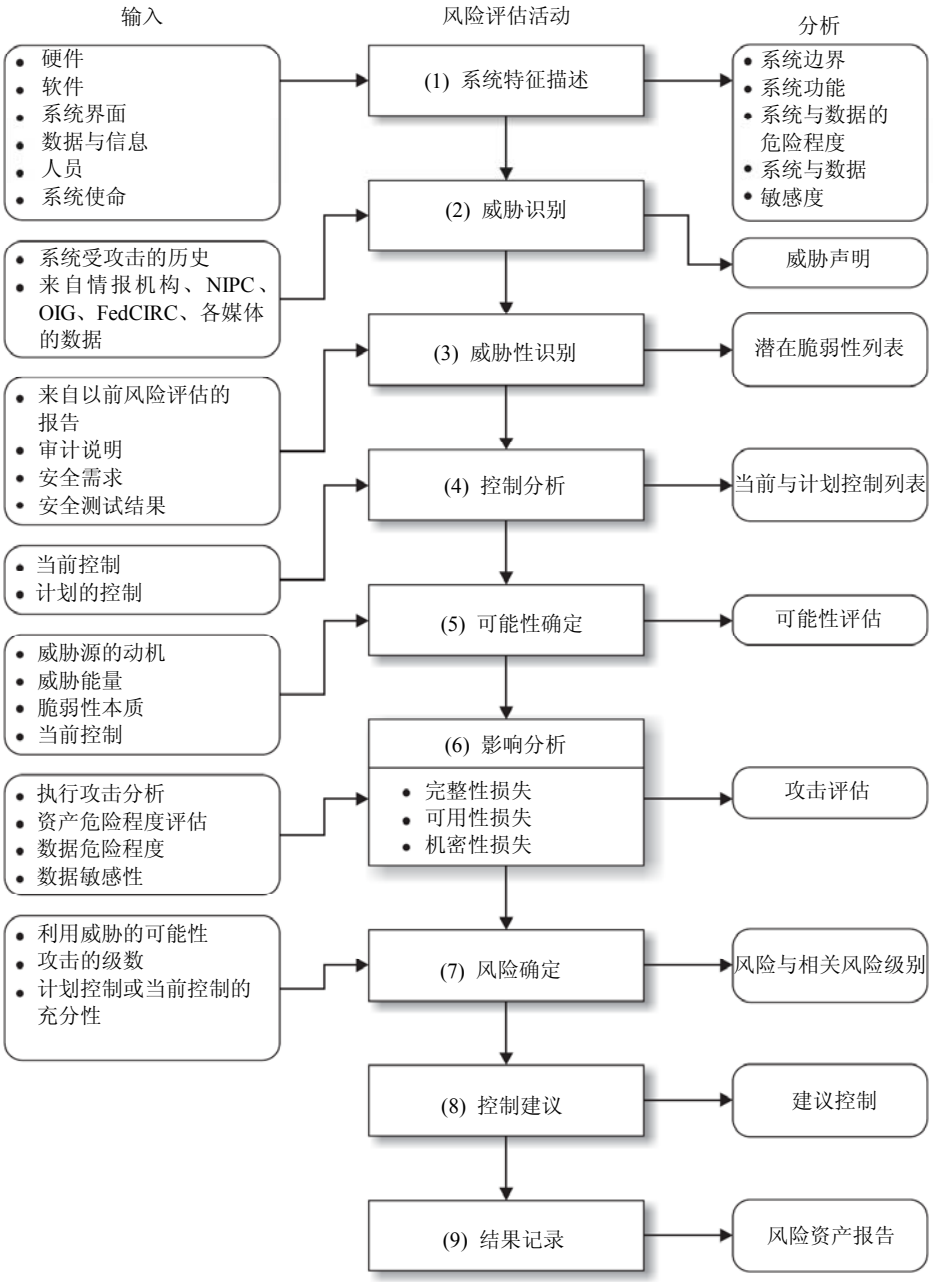

图 2-11　NIST SP 800-30 中的风险管理步骤

第二种风险评估方法是 FRAP，即便利的风险分析过程(Facilitated Risk Analysis Process)。这种定性方法的核心是只关注那些的确需要评估以降低成本和时间的系统。这种方法强调对活动进行筛选，从而只对最需要进行风险评估的项目进行评估。它可以用来一次分析一个系统、应用程

序或业务流程。数据收集起来之后，会根据它们的关键性对业务操作所面临的威胁进行排序，确定优先级。风险评估团队记录下为降低可识别风险而需要采取的控制措施，制定为实现控制措施而需要采取的行动计划。

这个方法不计算风险被利用的概率和年度预期损失。团队成员根据经验来决定这些风险的关键程度。这个方法的开发者(Thomas Peltier)认为用数学公式计算风险太耗时耗神。其目的是把评估控制在小范围内，简化评估流程，提高效率和降低成本。

另一种方法叫做 OCTAVE(Operationally Critical Threat, Asset, and Vulnerability Evaluation，操作性关键威胁、资产和脆弱性评估)，它由 Carnegie Mellon 大学的软件工程学院设计。这种方法专门为管理和指导公司内的信息安全风险评估的人员设计，它将组织机构内的工作人员放在权力位置，使其能够决定评估组织机构安全的最佳方式。这种方法源于一个理念，即在具体环境中工作的人最能理解组织机构的需要及其面临的风险。风险评估团队成员一轮轮的开研讨会。协调者帮助团队成员了解该风险方法，以及如何将其应用于特定业务部门内标识出的脆弱性和威胁。这个方法强调自我引导的团队方法。OCTAVE 的评估范围往往较大，相比之下，FRAP 更专注于方法。FRAP 只用于评估系统或者应用程序，而 OCTAVE 可以用于评估所有系统、应用程序和组织内的业务流程。

NIST、FRAP 和 OCTAVE 方法关注 IT 威胁和信息安全风险，而 AS/NZS 4360 则采取了一种更广泛的方式来进行风险管理。这种澳大利亚和新西兰的方法可用于了解公司的财务、资本、人员安全和业务决策风险。尽管也能够用于分析安全风险，但是它并非专门为该目标而创建的。这个方法更从商业的角度而不是安全的角度来关注公司的健康情况。

如果需要一个集成到安全计划的风险方法，可以在之前提到的 ISO/IEC27000 系列中选择一个。ISO/IEC27005 是一个国际标准，规定在 ISMS 框架内如何进行风险管理。如果说 NIST 风险方法主要侧重 IT 和操作层面，这个方法则侧重 IT 和较软的安全问题(文档、人员安全和培训等)。在组织安全计划中集成方法，可以应对组织面临的所有安全威胁。

注意：

深入了解有关这些风险方法的详细信息，参阅题为 “Understanding Standards for Risk Management and Compliance” 的文章，网址: http://www.logicalsecurity.com/resources/resources_articles.html

失效模式和影响分析(Failure Modes and Effect Analysis，FMEA)是一种确定功能、标识功能失效并通过结构化过程评估失效原因和失效影响的方法。它常用于产品开发和运营环境中。其目标是标识最容易出故障的环节，之后或者修复故障或者实施控制以降低故障的影响。比如，可以在组织的网络上执行 FMEA 来识别单点故障。这些单点故障意味着能够直接影响网络整体效率的脆弱性。可以使用这种结构化方法来标识这些问题(脆弱性)、评估它们的关键性(风险)并标识应该采取的必要控制措施(降低风险)。

FMEA 方法使用失效模式(事物出故障或者失效的方式)和影响分析(故障或者失效所带来的影响)。将这种过程应用于某个长期失效，可以确定最有可能发生失效的地方。我们既可以认为 FMEA 能够洞察未来并确定潜在的失效领域，也可以认为它能够发现脆弱性，并且在脆弱性转变为真正的障碍之前采取纠正措施。

按照下面特定的步骤，可以取得失效模式分析的最佳结果：

(1) 绘制一幅系统或控制的结构图。

(2) 设想一下，如果图中的每一个方框失效，将会出现什么情况。

(3) 绘制一张表，将失效的影响和影响评估对应起来。

(4) 修改系统设计，对表进行调整，直到系统中不再存在无法接受的问题。

(5) 让几位工程师检查失效模式和影响分析。

表 2-6 举例说明了如何执行和记录 FMEA。虽然大多数公司都没有足够的资源为每个系统和控制进行如此细致的工作，但是我们应当对可能给公司造成重大影响的关键功能和系统进行分析。

表 2-6　如何执行和记录 FMEA

准备人：							
批准人：							
日期：							
修改：							
				失效的影响			
项 识 别	功　　能	失 效 模 式	失 效 原 因	组件或功能集合	下一个更高集合	系　　统	失效检测方法
IPS 应用程序内容过滤器	内联周边保护	无法关闭	流量超载	单点失效拒绝服务	IPS 阻塞输入的流量流	IPS 中断	将健康检查状况发送至控制台，并且向安全管理员发送电子邮件
中央防病毒软件特征库更新引擎	将已更新的特征库传送到所有服务器和工作站	无法就阻止恶意软件提供足够、及时的保护	中央服务器停止运行	单个节点的防病毒软件没有更新	网络被恶意软件感染	中央服务器可能被感染或感染其他系统	将活动信号状况检查结果发送至中央控制台和页面网络管理员
消防水管	扑灭建筑物 1 中 5 个区域的火灾	无法关闭	水管中的水结冰	无	建筑物 1 中没有可用的灭火装置	灭火系统水管破裂	灭火传感器直接连入消防系统中央控制台
……							

FMEA 最初是为系统工程而开发的，目的是检查产品中潜在的失效以及涉及这些失效的过程。这种方式被证明是成功的，最近人们对其进行了修改，并将其用于评估风险管理优先级以及缓解已知的威胁脆弱性。

使用 FMEA 保证风险管理的原因是：随着企业更细化地理解风险，风险管理的详细程度、使用的变量和复杂程度也持续增加。随着人们的风险意识(细化到战术和操作层面)不断增强，这种确定潜在缺陷的系统方式正发挥着越来越大的作用。

尽管 FMEA 作为一种调查方法在识别某个系统的主要失效模式时非常有用，但是它在查找多个系统或子系统中存在的复杂失效模式方面还有所欠缺。事实证明，在确定更加复杂的环境和系统中可能发生的失效方面，故障树分析方法更为有用。故障树分析过程可以概括如下：首先，以一种不希望产生的影响作为逻辑树的根部或顶部事件；然后，将可能造成这种影响的每一种情形作为一系列逻辑表达式添加到树中；最后，使用与失效可能性有关的具体数字来标记故障树。通常，使用计算机程序就能够计算出某个故障树的失效可能性。

图 2-12 显示了一个简单的故障树和不同逻辑符号，这些符号用于代表在某一特殊的失效事件发生时必然出现的情况。

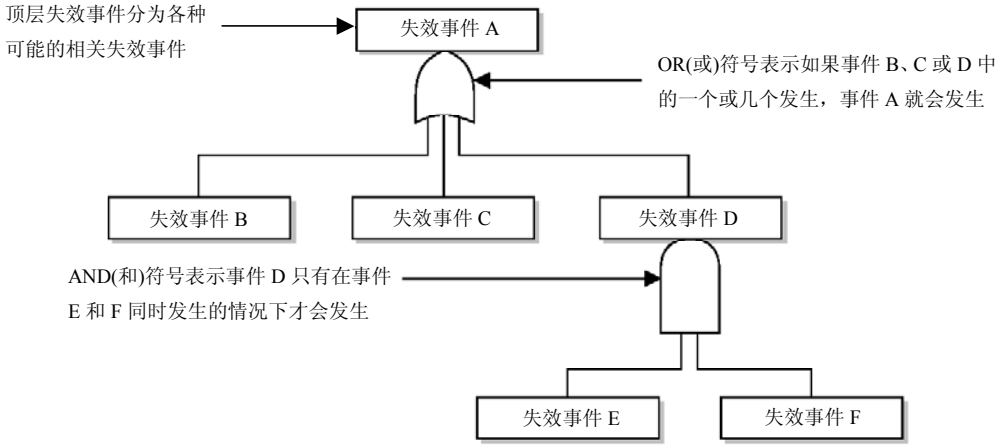

图 2-12　故障树与逻辑组件

在绘制故障树时，必须准确列出一个系统中可能出现的所有威胁或故障。故障树的枝干可以分成不同的通用类别，如物理威胁、网络威胁、软件威胁、Internet 威胁和组件失效威胁。确定所有可能的威胁类别后，就可以对它们加以整理，并从故障树上去除不适用于该系统的枝干。一般来说，如果一个系统没有以任何方式连接到 Internet，那么就可以从故障树上删除代表 Internet 威胁的枝干。

下面列出了一些可以通过故障树分析确定的、最常见的软件失效事件：

- 错误警报
- 不充分的错误处理
- 先后顺序或次序
- 不正确的计时输出
- 有效但非预期的输出值

当然，由于软件和异构环境的复杂性，上面只列出了一小部分软件失效事件。

为以防万一，若这些备选的风险评估方法还不够多，也可以考虑一下 CRAMM(Central Computing and Telecommunication Agency Risk Analysis and Management Method，中央计算和电信机构风险分析与管理方法)， 该方法由英国创建，其自动化工具由西门子公司负责销售。该方法分为 3 个不同的阶段：定义目标、评估风险和标识对策。称其为独一无二的方法的确有失公允，因为它和其他任何风险方法的基本结构是一样的。它的独特之处在于它的每样东西(问卷、资产依赖建模、评估公式和合规报告)都是自动化工具格式。

2.4 节中包含 ISO/IEC 27000、CobiT、COSO、Zachman、SABSA、ITIL 和六西格玛等方法，而本小节中所包含的风险方法也一样，是一堆容易混淆的标准和指南。记住，这些方法有很多相互重叠的共同点，因为几乎每一个方法的具体目标都是标识对组织可能造成伤害的东西(脆弱性和威胁)和解决这些问题(降低风险)。使这些方法相互区别的是它们各自所具有的独特方法和关注点。如果需要在全组织范围内部署风险管理程序并把它集成到安全计划中，应该遵循 ISO/IEC 27005 或者 OCTAVE 方法。如果需要在评估过程中重点关注 IT 安全风险，则遵循 NIST800-30。如果预算有限，并且需要重点评估一个单独的系统或进程，则遵循 FRAP(Facilitated Risk Analysis

Process)。如果想深入了解某一个具体系统内的安全缺陷是如何造成衍生效应的，你可以使用FMEA(Failure Modes and Effect Analysis，失效模式和影响分析)或者失效树分析。如果需要了解所在公司的商业风险，则遵循 AS/NZS4360 方法。

现在，将过程总结如下：

(1) 制定风险管理政策。
(2) 组建风险管理团队。
(3) 标识公司待评估的资产。
(4) 计算每个资产的价值。
(5) 标识能够影响已确定资产的脆弱性和威胁。
(6) 选择最适合需要的风险评估方法。

关键术语

- **NIST 800-30 Risk Management Guide for Information Technology System**：关注 IT 风险的美国联邦标准。
- **FRAP(Facilitated Risk Analysis Process)**：专用的定量方法，先进行预筛选以节省时间和金钱。
- **OCTAVE(Operationally Critical Threat, Asset and Vulnerability Evaluation)**：面向团队的方法，通过有组织的研讨会来评估组织风险和 IT 风险。
- **AS/NZS 4360**：澳大利亚和新西兰的一种业务风险管理评估方法。
- **ISO/IEC 27005**：在 ISMS(信息安全管理系统)中实现风险管理计划的一个国际标准。
- **FMEA(Failure Modes and Effect Analysis，失效模式和影响分析)**：利用组件的基本功能来识别缺陷及其影响的一种方法。
- **故障树分析**：分析具体缺陷在复杂系统中出现的根本原因的一种方法。
- **CRAMM**：Central Computing and Telecommunications Agency Risk Analysis and Management Method，中央计算和电信机构风险分析管理方法。

接下来需要确定风险分析方法应该是定量的还是定性的，下面将会对此展开讨论。

注意：

风险评估用来收集数据。风险分析对收集的数据进行研究，以确定应该采取什么行动。

2.7.6　风险分析方法

——一个咨询师说这个威胁会使我们损失 15 万美元，另外一个咨询师说它达到了红色警告的级别，可审计团队的说法又不同，我们是当回事还是不当回事呢？

风险分析具有定量和定性两种方法。定量风险分析会尝试为风险分析过程的所有元素都赋予具体的和有意义的数字。分析中的每个元素(资产价值、威胁频率、脆弱性的严重程度、损失影响、防护成本、防护有效性、不确定性和可能性)都被量化并输入公式，然后计算出总风险和剩余风险。与定性方法相比，定量的风险分析方法是一种数学方法，更为科学。定性风险分析对风险分析中的数据元素采用“较软”的方法。它不量化那些数据，即它并不赋予那些数据数值以放到公式中

计算。比如，对一个组织进行量化的风险分析后，可能得到这样的结果：如果 Web 服务器上的缓冲区溢出被利用，损失 10 万美元；如果数据库遭到破坏，损失 2.5 万美元，如果文件服务器遭到破坏，损失 1 万美元。定性的风险分析不会呈现这样的用金钱来衡量的结果，只是给风险评级，如红、黄和绿。

定量分析使用风险计算来预测经济损失的程度以及每种威胁发生的可能性。相反，定性分析并不使用计算，而是更多地以观点和场景为基础，使用评级的方式来评定风险的关键性级别。

定量的方法和定性的方法都具有各自的优缺点，分别适用于特定的场合。公司管理层、风险管理团队以及他们决定使用的工具将确定哪一种方法是最好的。

下面将深入讨论定量分析并重温定性方法，然后对比二者的属性。

1. 自动风险分析方法

如果手动收集所有在风险分析公式中需要的数据以及合理说明结果，那么所需要的工作量将是惊人的。市场上有若干种自动风险分析工具，它们可以让这项工作更容易或更精确。收集的数据可以重复使用，这样就能够大大减少进行后续分析所需要的时间。此外，这些工具还可以为管理层打印出报告和全面的图表。

注意：

记住，脆弱性评估不同于风险评估。脆弱性评估只是找出脆弱性(漏洞)。风险评估计算脆弱性被利用的可能性以及产生的相关的业务影响。

自动风险分析工具的目的是：减少风险分析任务的手动难度，进行快速计算，估计未来可能的损失，以及确定选用的安全对策的有效性和优点。大多数自动风险分析工具都将信息存入一个数据库，并且使用不同的参数运行若干场景，从而给出不同威胁结果的全景图。例如，在某种自动风险分析工具中输入了所有必要的信息之后，就能够计算出一场大火灾的潜在后果；使用不同的参数运行该工具一次，就能够计算出病毒毁坏主文件服务器上40%的数据时会带来的潜在损失；再使用另一组参数运行该工具一次，又能够计算出攻击者窃取了 3 个数据库中所有客户的信用卡信息时公司将遭受多大的损失。采用各种不同的风险可能性运行这种工具，能够让公司详细地了解哪些风险比其他风险更严重，从而可以确定应该首先处理哪些风险。

2. 风险分析的步骤

前面已经进行了风险评估，即收集数据用于风险分析。已经标识了待评估的资产，为每项资产赋予了一个相关数值，确定了影响这些资产的脆弱性和威胁。现在需要进行风险分析了，意味着需要找出诠释评估过程中所收集的数据的方法。

如果进行定量分析，需要用数学公式来诠释这些数据。最常用的公式是单一损失期望(single loss expectancy，SLE)和年度损失期望(annual loss expectancy，ALE)。

SLE 是为某个事件赋予的货币价值，表示特定威胁发生时公司潜在损失的金额：

资产价值×暴露因子=SLE

暴露因子(Exposure Factor，EF)表示某种特殊资产被已发生的风险损坏所造成损失的百分比。例如，如果某个数据仓库的资产价值为 15 万美元，发生火灾后，该数据仓库大约有 25%的价值遭到破坏，那么 SLE 就是 37 500 美元。

资产价值(15 万)×暴露因子(25%)=37 500

这个结果告诉我们，如果该公司发生火灾，可能损失 37 500 美元。但由于按年度制定和使用安全预算，所以需要知道年发生比率是多少。这是需要用到 ALD 公式，即：

SLE×年发生比率= ALE

年发生比率(ARO)表示一年时间内发生特定威胁的预计频率。该值的范围可以是从 0.0(不发生)到 1.0(一年一次)乃至大于 1 的数字(一年若干次)之间的任何值。例如，如果数据库发生火灾并造成损坏的概率是十年一次，那么 ARO 值是 0.1。

因此，如果公司的数据仓库设施发生火灾可能造成 37 500 美元的损失，发生火灾的频率即 ARO 值为 0.1(表示 10 年发生一次)，那么 ALE 值就是 3750 美元(37 500×0.1 = 3750)。

ALE 值告诉该公司，如果想采取控制或防护措施来阻止这种损失的发生，那么每年就应当花费 3 750 美元或者更少的费用来提供必要的保护级别。了解某个风险的实际发生可能性以及威胁可能造成的损失金额是非常重要的，这样我们就能够知道应该花多少钱首先保护资产不受威胁。如果公司每年花费超过 3750 美元来保护自己不受该威胁的影响，那么是没有什么商业价值的。

既然拥有了所有数据，那么应当如何进行处理呢？让我们看一下表 2-7 中的示例，该表显示了一个定量风险分析的结果。有了这些数据，公司就能够根据威胁的严重程度、威胁发生的可能性以及威胁发生时可能造成的损失作出明智的决定，从而确定应当首先处理哪些威胁。此时，公司也会了解到要免受每种威胁的影响应当各投入多少资金。因此，公司能够作出有益的商业决定，而不是为了安全到处花钱，却没有清楚了解整个情况。如果病毒渗透造成的数据讹误使得该公司承担的风险是损失 6500 美元，那么为确保不发生病毒攻击而用于购买防病毒软件和方法的资金最多不超过这个金额。

表 2-7　如何使用 SLE 和 ALE 进行风险分析

资　　产	威　　胁	单一损失期望(SLE)	年发生比率(ARO)	年度损失期望(ALE)
设施	火灾	230 000 美元	0.1	23 000 美元
商业秘密	盗窃	40 000 美元	0.01	400 美元
文件服务器	故障	11 500 美元	0.1	1150 美元
数据	病毒	6500 美元	1.0	6500 美元
客户信用卡信息	盗窃	300 000 美元	3.0	900 000 美元

因为定量分析的数据都是以数值的方式来体现，所以有些人错误地认为这个过程是绝对客观和科学的。但因为数据本身多少会有一些主观性，所以要做到完全客观是很难的。如何精确地知道火灾每 10 年发生一次呢？怎能知道每发生一次火灾会有 25%的资产价值遭到破坏呢？不知道这些数字的精确值，只是根据历史数据和业内经验推测出来。在定量风险分析过程中，可以尽力提供正确信息，尽可能得出较精确的风险值，但是不能预见未来，也不知道究竟在未来我们或者我们的公司将要付出什么代价。

不确定性

——我编造了所有的数字。

——看起来还挺真的。

在风险分析中，不确定性指的是对估计缺乏信心的程度，它使用百分比表示：0～100%。如果对某件事的信心程度为 30%，那么就可以说不确定程度为 70%。执行风险分析时，了解不确定性非常重要，因为它表明团队和管理层对于分析数据的信心水平。

3. 风险分析的结果

风险分析团队应当具有定义清楚的目标。下面简单列出了从风险分析中通常期望得到的结果：

- 赋予资产的货币价值。
- 所有可能威胁和重要威胁的综合列表。
- 每种威胁的发生概率。
- 12 个月时间内公司在每种威胁下能够承受的潜在损失。
- 建议的防护措施、对策和行动。

虽然上面的列表显得较短，但是实际上每一项下面往往都有数量众多的子项。这种报告应当提交至高级管理层。高级管理层将会非常关心可能的财产损失和缓解这些威胁所需的费用。虽然该报告应该尽可能详细，不过最好还是列出执行摘要，以便帮助高级管理层快速了解风险分析的整个发现结果。

2.7.7 定性风险分析

——我自我感觉很安全。

——太棒了，那我们可以回家了！

另外一种风险分析方法是定性分析，这种方法不会为各个组件和损失赋予数值和货币价值。相反，定性方法将考查各种风险可能发生的场景，并基于不同的观点对各种威胁的严重程度和各种对策的有效性进行等级排列(一个全面的分析可能包含几百种场景)。定性分析技术包括判断、最佳实践、直觉和经验。收集数据的定性分析技术示例有 Delphi、集体讨论、情节串联、焦点群体、调查、问卷、检查表、单独会谈以及采访。风险分析团队将决定对需要进行评估的威胁所使用的技术以及在分析中融入的公司和个人的文化元素。

进行风险分析工作的团队首先会召集那些在威胁评估方面受过教育、富有经验的人员。当这个团队了解描述威胁和潜在损失的场景时，他们就能够根据自己的感觉判断出该威胁实际上将如何发生以及将会带来多大程度的损失。

接下来，为每一个可识别的脆弱性撰写一个场景，并且研究它是如何被利用的。最熟悉某种威胁的“专家”应当复查相应的场景，以保证它反映了实际威胁发生时的情况。然后，评估能够减少这种威胁所造成损失的防护措施，并且针对每种防护措施都应用该场景。暴露可能性和损失可能性既可以使用高、中、低排序，也可以使用 1～5 或 1～10 的等级排序。常见的定性分析矩阵如图 2-13 所示。一旦被选定的人员对威胁的发生可能性、潜在损失、每种防护措施的优点进行等级排列之后，这些数据就应当写入报告，随后再提交给管理层，以帮助他们更好地决定如何使用防护措施才能最好地保护系统。这种分析方法的好处在于，为风险、防护措施力度和缺陷识别进行等级排序的团队工作人员必须与懂得这些知识的人员交流，这样才能向管理层提供自己的意见。

可能性	后果				
	微不足道	很小	中等	很大	严重
几乎一定	中	高	高	天	天
很有可能	中	中	高	高	天
有可能	低	中	中	高	天
不太可能	低	中	中	中	高
几乎不可能	低	低	中	中	高

图 2-13　定性风险矩阵，概率与后果(影响)

让我们看一个定性风险分析的简单示例。

风险分析团队撰写了一页场景，说明了黑客访问公司内部 5 台文件服务器上所保存的机密信息的威胁。随后，风险分析团队将这页场景分发给一个 5 人团队(IT 经理、数据库管理员、应用程序编程人员、系统操作员和运营部经理)。这个 5 人团队会对威胁的严重程度、潜在损失和每种防护措施的有效性进行 1～5 的等级排列，其中 1 代表最不严重、最无效或最不可能。表 2-8 给出了结果。

表 2-8　定性分析示例

威胁=黑客访问机密信息	威胁的严重程度	威胁发生的可能性	给公司造成的潜在损失	防火墙的有效性	入侵检测系统的有效性	蜜罐计算机的有效性
IT 经理	4	2	4	4	3	2
数据库管理员	4	4	4	3	4	1
应用程序编程人员	2	3	3	4	2	1
系统操作员	3	4	3	4	2	1
运营部经理	5	4	4	4	4	2
结果	3.6	3.4	3.6	3.8	3	1.4

这些数据被编入报告并提交给管理层。管理层收到这些信息后，就会知道自己的职员(或选择的安全专业人员团队)认为购买防火墙比购买入侵检测系统或设置蜜罐计算机能够更加有效地保护公司资产免受威胁影响。

这只是针对特定威胁的结果。管理层将会查看所有威胁的严重程度、每种威胁的可能性和潜在损失，这样他们就知道哪些威胁能够造成最大的风险，从而应该首先处理它们。

1. 定量与定性的对比

——我们应该用哪种方法？

定量方法和定性方法都具有各自的优缺点，表 2-9 对这两种方法进行了比较。

表 2-9　定量分析和定性分析的特征

特　　征	定 量 分 析	定 性 分 析
不需要计算		×
需要更复杂的计算	×	
涉及大量猜想工作		×
提供一般风险领域和指标		×
更易于自动化和评估	×	
用于风险管理性能追踪	×	
提供可信的成本/收益分析	×	
使用独立可验证的和客观的衡量标准	×	
提供非常清楚该过程的职员的意见		×
指出在一年之内可能招致的明确损失	×	

风险分析团队、管理层、风险分析工具以及公司的文化将决定是使用定量的方法还是使用定性的方法。每种方法的目标都是评估公司面临的实际风险并给出威胁的严重程度等级，以便在实际预算范围内启用适当的防护措施。

表 2-9 列出了定量方法与定性方法的一些优势，但选择一种适合的方法并不容易。在决定使用定量方法还是定性方法时，应考虑下面的问题。

2. 定性方法的缺点

- 评估方法及结果相对主观。
- 无法为成本/收益分析建立货币价值。
- 使用主观衡量很难跟踪风险管理目标。
- 没有相应的标准。每个供应商解释其评估过程和结果的方式各不相同。

Delphi 技术

——Oracle Delphi 的结果显示大家都同意我的看法。

——那再匿名投票一次看看结果如何？

Delphi 技术是一种群体决策方法，它用于保证每一位成员都将自己对某个特定威胁会带来的后果的真实想法表达出来。这就避免了团队中的个人在赞同其他人的想法时感到有压力，并使得他们能够以独立和匿名的方式参与工作。团队中的每位成员都提供自己对某个特定威胁的意见，然后提交到执行分析的团队手中。结果将被编译并分发给团队成员，随后团队成员将自己的评论匿名写在纸上，再将它提交给分析团队。这些评论再次被编译和分发，以获得更多的评论，直至形成一致意见。这种方法用于在成本、损失价值和发生可能性等问题上达成一致，个人并不需要在口头上表示同意。

3. 定量方法的缺点

- 计算更加复杂。管理层能够理解这些值是怎么计算出来的吗？
- 没有可供利用的自动化工具，这个过程完全需要手动完成。

- 需要做大量基础性的工作，以收集与环境相关的详细信息。
- 没有相应的标准。每个供应商解释其评估过程和结果的方式各不相同。

注意：

既然完全定量评估几乎不可能而定性方法又不能为财务决策提供统计数据，那么可以考虑两种方法结合起来使用。定量方法可以用于有形资产(货币值)， 定性方法可以用于无形资产(优先级值)

2.7.8　保护机制

——我们知道我们现在很危险，也知道危险发生的概率，接下来该怎么办？

——跑呗！

下一步是确定现行的安全机制并评估它们的有效性。

由于公司面临的威胁是多种多样的(并不只是计算机病毒和攻击者)，因此每种威胁都需要分别处理和作出规划。用作安全防护措施的访问控制机制将在第 3 章进行讨论。第 4 章和第 10 章阐述了软件应用和数据故障问题。第 5 章将介绍站点位置、火灾防护、站点建设、电气问题和设备故障。通信和网络问题将在第 6 章分析和介绍。第 8 章介绍了灾难恢复和业务连续性。所有这些问题都有自己的关联风险和规划需求。

本节涉及如何为计算机系统识别和选择正确的对策，以及在比较各种不同的软件对策时，如何找出所需的最佳特征和进行调查的所有成本概况。对可选择对策进行分析的最终结果应当表明为什么所选的对策对于公司来说是最有利的。

1. 对策的选择

一项安全对策必须有很好的商业意义，这意味着该对策是非常划算的(收益大于成本)。这就需要另一种分析：成本/收益分析。通常，对某个给定的防护措施所使用的成本/收益计算公式如下所示。

(实现防护措施前的 ALE)–(实现防护措施后的 ALE)–(防护措施每年的成本)
=防护措施对公司的价值

例如，如果在实现推荐的防护措施之前，黑客攻击一台 Web 服务器的威胁的 ALE 为 12 000 美元，而实现防护措施之后的 ALE 为 3000 美元，该项防护措施每年的维护和运行成本是 650 美元，那么这项防护措施每年对公司的价值就是 8350 美元。

对策的成本并不只是在购买订单上填写的金额。在计算一项对策的全部成本时，应当考虑下列因素：

- 产品成本
- 设计/规划成本
- 实现成本
- 环境更改
- 与其他对策的兼容性
- 维护需求
- 测试需求

- 修复、替换或更新成本
- 运行和支持成本
- 对工作效率的影响
- 预订成本
- 监控和响应警报所需的额外人工成本
- 解决这款新工具带来的问题的成本

许多公司都经历过这种痛苦：在购买新的安全产品时并没有意识到还需要员工来维护这些产品。虽然使用工具可以自动完成这些任务，但是许多公司以前从未执行过这些任务。因此，很多时候购买安全产品并不能节省人力，相反还需要更多人力。例如，公司 A 决定保护他们的大量资源和网络流量，这需要购买入侵检测系统(IDS)。因此，这个公司花 5500 美元购买了该软件。这就是总的成本吗？完全不是。该软件应该在非生产环境中进行测试，以发现意想不到的行为。在测试完成并且 IT 团队觉得将 IDS 加入自己的生产环境比较安全之后，他们还必须安装监控管理软件和传感器，并正确指定从传感器到管理控制台的通信通道。此外，可能还需要重新配置路由器以重定向流量，这时必须保证用户不能访问 IDS 管理控制台。最后，IT 团队需要配置一个数据库来记录所有的攻击记录，并且需要运行模拟程序。

与 IDS 警报响应相关的成本也应明确考虑在内。即使公司 A 部署了一个 IDS，安全管理员仍然可能需要其他报警设备，如手机。与 IDS 事件相关联的时间成本也应当考虑进来。

在 IT 团队中工作过的人都知道，在这种情况下几乎总是存在一些不利因素。在安装该软件之后，网络性能也许就变得无法接受了。由于某种很严重的原因，用户可能再也不能访问 Unix 服务器。IDS 供应商也许不会说明要使整个软件正常运行，还需要两个服务补丁程序。此外，还需要耗费一定的人力来应付这个新 IDS 发出的正确和不正确的警报。

例如，该项对策的各种费用如下：软件费用为 5500 美元，培训费为 2500 美元，实验室和测试费用为 3400 美元，使用该软件后用户的工作效率损失为 2600 美元，路由器重新配置、产品安装、故障检测和修理以及安装两个服务补丁程序的总费用为 4000 美元。因此，该项对策的真实成本就是 18 000 美元。如果我们的总潜在损失经过计算是 9000 美元，那么针对该风险使用这项对策的成本就会超出预算一倍。有些费用在发生之前难以或无法预测，但是有经验的风险分析师能够考虑到许多这样的可能性。

2. 对策的功能和有效性

——对策根本不奏效，但它的界面不赖！

——的确不错！

风险分析团队必须评估防护措施的功能和有效性。在选择防护措施的时候，某些特征更优于其他特征。表 2-10 列出了在购买和使用某种安全保护机制之前应该考虑的特征。

表 2-10　购买防护措施之前应该考虑的特征

特　征	描　述
基础模块	能够从环境中安装和卸载保护机制而不会危及其他机制
提供统一的保护	同一个安全级别以一种标准化的方式应用于它要保护的所有机制
提供重写功能	必要情况下管理员可以重写限制
默认为最小权限	在安装之后，默认为缺少许可权限，而不是每个人都能够完全控制它
防护措施及其保护的资产相互独立	防护措施可以用来保护不同资产，不同资产也可以被不同防护措施所保护

(续表)

特　　征	描　　述
灵活性和安全性	防护措施提供的功能越多越好。这些功能应该有灵活性，从而我们可以选择不同的功能，而不是必须全选或是一个功能都不能选择
用户交互	用户不会恐慌
用户和管理员之间有清楚的界限	当涉及到配置或关闭保护机制的时候，用户应该有较少的权限
最少的人为干预	当不得不需要人为配置或修改控制的时候，就为错误开启了方便之门。防护措施应该能够自己进行设置，能够从环境中获取所需的信息，并且需要尽可能少的人为输入
资产保护	即使需要重新设置对策，资产也仍然受到保护
容易升级	软件总是不断发展的，所以应该能够方便地进行升级
审计功能	防护措施需要包含一个机制，用于提供最少的和/或详细的审计
最小化对其他组件的依赖性	防护措施应该具有灵活性，不应该对自己的安装环境有严格的要求
容易被职员使用和接受，并能容忍错误	如果防护措施对工作效率造成障碍，或是在简单的任务中需要添加额外的步骤，用户就不能容忍它
必须产生可用的和可以理解的输出	应该给出重要信息，从而让人们能够很容易地理解它，并且将其用于趋势分析
必须能够重启防护措施	安全机制应该能够重新启动，并在不影响其保护的系统和资产的情况下恢复原有的配置和设置
可测试	应该能够在各种情况和各种环境下对防护措施进行测试
不引入其他危害	防护措施不应该提供任何隐蔽通道或后门
系统和用户性能	系统和用户的性能不应该受到很大影响
普遍应用	在环境中实施保护措施时，不能有许多(甚至一个)例外情况
恰当的报警	应该能够设定一个阀值，确定什么时候警报相关人员发生了违反安全的行为，这种警报应该是可接受的
不影响资产	环境中的资产不应该受到防护措施的负面影响

如果防护措施的功能显著，那么就能够提供有效的屏障。这就会告诉那些做坏事的人，这里有足够的保护，他们最好改为攻击那些更容易的目标。虽然防护措施应该有显著的功能，但是它的工作方式应当不可获取，从而使那些心怀恶意的人不能更改防护措施或是知道如何接近保护机制。如果用户知道如何禁用占用 CPU 周期的防病毒程序，或是了解如何避开代理服务器以自由访问 Internet，那么他们就会这样做。

2.7.9　综合考虑

因此，要进行一项风险分析，公司就应当首先确定必须保护哪些资产以及保护的程度如何，应该说明保护具体资产所需的金额。接着，评估可用防护措施的功能，确定哪些防护措施对环境最有利。最后，公司需要评估各种防护措施的成本，并且进行比较。这些步骤和结果信息将帮助管理层在选择和购买防护措施上作出最明智和最有远见的决定。

2.7.10　总风险与剩余风险

一个公司实现安全对策的原因是将整体风险降低到一个可接受的级别。前面已经介绍过，没有百分之百安全的系统和环境，这意味着我们总是漏掉了一些需要预防的风险。这些风险称为剩余风险。

安全工作永无止境

仅仅通过定期重新评估风险即可确定防护措施的效果。如果风险并未发生变化，而且所实现的防护措施运转正常，那么就说明风险已经得到了合理的缓解。定期的 IRM 监控可以为信息安全风险评级提供支持。

脆弱性分析以及持续的资产识别和估价也是重要的风险管理性能和监控任务。要确定所采用的防护措施是否能够为资产和环境提供适当和必要的保护，持续的风险分析非常重要。

剩余风险与总风险不同，总风险指的是公司在不实现任何防护措施的情况下所面临的风险。如果成本/收益分析的结果表明最好不采取任何动作，那么组织机构就可能选择接受总风险。例如，如果某公司的 Web 服务器发生问题的可能性很小，而提供更高级别的保护所需的成本将会超过该风险造成的潜在损失，那么该公司就会选择不实现防护措施，从而承担了总风险。

总风险和剩余风险之间存在重要差别，这取决于公司愿意承担的风险大小。下面给出了两者的概念化公式：

威胁×脆弱性×资产价值=总风险

(威胁×脆弱性×资产价值)×控制间隙=剩余风险

这些概念还可以使用如下公式表示。

总风险–对策=剩余风险

注意：

你不能在前面的公式中插入数字。相反，该公式只是用于从概念上解释构成风险的不同项之间的关系，这意味着不存在乘法或数学函数。该公式只是一个工具，可以帮助你理解定义总风险或剩余风险时会涉及哪些项。

风险评估期间已经识别了威胁和脆弱性。这些脆弱性被利用的可能性乘以遭受风险的资产的价值，就得到了总风险。在将控制间隙(控制不能提供的保护)考虑进来以后，结果就是剩余风险。实现防护措施是缓解风险的途径。由于没有公司能够消除所有的威胁，因此这意味着总是存在某种剩余风险。问题是该公司愿意承担多大程度的风险。

2.7.11 处理风险

——我们既然已经知道了危险所在，怎么办呢？

——把它藏在那棵大树后面。

一旦公司了解了他们所面临的总风险和剩余风险，就必须决定如何处理这些风险。处理风险的基本方式有下列 4 种：转移、规避、缓解、接受。

公司可以通过多种保险来保护自己的资产。如果公司觉得总风险或剩余风险太大，无法承担，那么可以购买保险，也就是将风险转移给保险公司。

如果公司决定终止引入风险的活动，那么这种行为称为风险规避。例如，如果某公司允许员工使用即时通信(IM)工具，那么可能带来与这种技术相关的许多风险。因为没有足够多的业务需求要求继续使用即时通信服务，所以该公司可能会决定不允许用户进行任何 IM 活动。停止 IM 服务就是风险规避的示例。

另一种方式是风险缓解，就是风险被降低至可接受的级别，从而可以继续开展业务。安装防火墙、进行培训以及部署入侵/检测保护系统，这些都是典型的风险缓解方式。

最后一种方式是接受风险，这意味着公司理解自己所面临的风险级别以及风险带来的潜在损失，并且决定在不采取任何对策的情况下接受风险。在成本/收益率表明采取对策的成本超出潜在的损失价值时，许多公司都会接受风险。

理解为何接受风险是某种特定情况下的最佳方式，这是至关重要的问题。但是，如今公司中的许多人接受风险，却没有完全理解接受的是什么。这种情况通常与安全领域中的风险管理不成熟、风险决策人员缺乏培训和经验有关。当业务经理被赋予处理其部门所面临的风险的责任时，多数场合他们会接受面临的任何风险。这是因为业务经理的真正目的是完成项目，他们并不想陷入愚蠢而又令人烦恼的安全问题。

接受风险应基于几个因素。例如，潜在的损失是否低于对策成本？组织机构是否能够应付接受风险所带来的“阵痛”？第二个考虑事项并不是一个纯粹的成本决策，而是需要考虑与决定接受风险有关的非成本问题。例如，如果接受风险，那么就必须在生产过程中增加另外 3 个步骤。这对我们有意义吗？或者，如果接受风险，那么可能发生更多的安全事故，我们准备好处理这些事故了吗？

接受风险的个人或团体还必须理解这个决策的潜在可见性。假设公司已经决定不保护客户的姓名，但是必须保护客户的其他信息(如社会安全号、账号等)。虽然这些行为符合法律法规的要求；然而，如果客户发现公司没有正确保护他们的姓名，并且由于缺乏相关知识而将这一行为与身份欺诈联系起来，那么该怎么办呢？即使一切问题得到适当的处理，但公司可能无法处理潜在的声誉影响。公司客户群体的认知并不总是基于事实，但是，客户可能会将他们的业务交给另一家公司，这是我们必须认识到的一个潜在事实。

图 2-14 说明了如何结合本小节讨论的所有概念来制订一个风险管理计划。

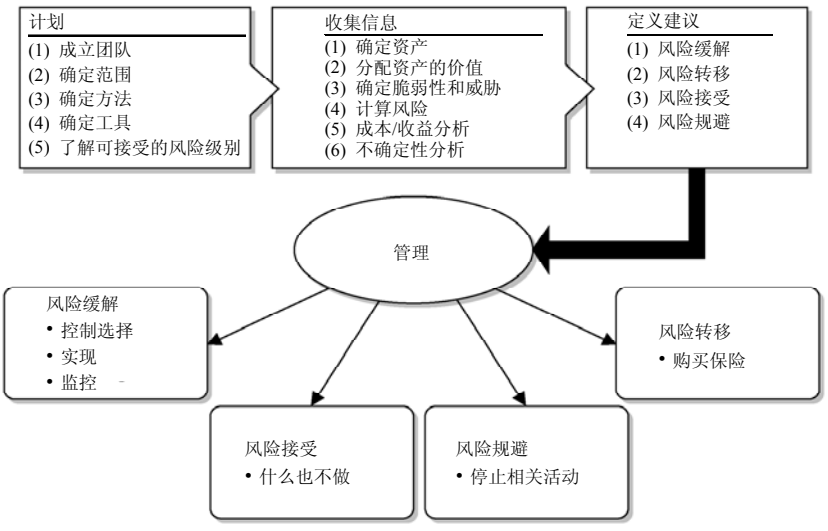

图 2-14　如何制订一个风险管理计划

关键术语

定量风险分析：将货币价值和数值赋予风险评估的所有数据元素。

定性风险分析：根据情境和等级来分析风险的一种意见型方法。

单一损失期望(SLE)：某一个特定的脆弱性被利用而预期产生的单次损失和对单一资产的预期影响。

资产价值×暴露因子=SLE

年度损失期望(ALE)：某一个特定的脆弱性被利用而预期产生的年度损失和对单一资产的预期影响。

SLE×ARO = ALE

不确定性分析：给数据元素赋予数值的信心程度。

Delphi 方法：匿名方式收集数据的方法。

成本/收益分析：计算控制措施的价值。

(实现控制措施前的 ALE)–(实现控制措施后的 ALE)–(控制措施每年的成本)=控制措施对公司的价值

控制措施的功能性与有效性：功能性指控制措施是什么，有效性是它发挥的效果如何。

总风险：控制措施实施前的全部风险数量。

威胁×脆弱性×资产=总风险

剩余风险：实施控制措施后剩余的风险。

威胁×脆弱性×资产×控制间隙=剩余风险

处理风险：接受、转移、缓解和规避。

2.7.12 外包

——我确保在我们从未见过、从未听说过的公司的基础上成立的公司能够很好地保护我们的敏感信息！

——是的，我看也不错！

越来越多的组织机构把一些业务外包出去，自己专门从事核心业务功能。他们让托管公司维护网站和电子邮件服务器，让服务提供商提供不同的电信连接，让灾难恢复公司提供协同功能，让云计算提供者提供基础设施或应用程序服务，让开发人员创建软件，让安全公司执行脆弱性管理。但理解这一点很重要：可以外包功能，但不能外包风险。虽然公司可以让第三方公司提供这些服务，但是如果出现数据泄露这类事情，你的公司还要最终为其负责。第 9 章将从法律的角度(下游责任)深入探讨这类问题，现在列一下公司在外包业务时为降低风险应该做的事情：

- 审核服务提供者的安全计划。
- 进行现场检查和采访。
- 审核合同以确保就安全和保护级别达成一致意见。
- 确保服务级别协议已就绪。
- 审核内部、外部审计报告和第三方审查报告。
- 审核介绍材料并与以前和现在的顾客沟通。
- 浏览商业改进局报告。
- 确保拥有业务连续性计划。
- 签署保密协议。
- 了解提供者的法律和法规要求。
- 需要审计标准声明(SAS)70 审计报告。

注意：

SAS70 是一个由第三方审计机构进行的内部控制措施审计。

如今外包在组织机构中非常盛行，以至于人们忘记了安全和合规的要求。外包一些功能从经济上可能比较划算，但如果引起安全泄露问题，则需付出昂贵的代价。

2.8　策略、标准、基准、指南和过程

——风险评估终于结束了，休息一下吧。

——不行，还有好多事要做呢。

计算机以及在计算机上处理的信息与公司面临的关键任务和目标有直接的关系。由于具有这样的重要意义，因此高级管理层应当优先考虑保护计算机和信息，并提供足够的支持、资金、时间和资源，从而保证以最合理、最划算的方式保护系统、网络和信息。要成功实现这些目标，必须采取全面的管理方法。这是因为从环境安全角度看，组织机构内的每位员工都具有不同的个人价值和经验。同时，组织机构还必须确保每位员工都从满足组织机构要求的层面上看待安全，而组织机构的这些要求由法律、法规、需求以及组织机构环境风险评估的目标和要求决定。

为了能够在公司内最终圆满解决安全问题，就需要从最高层做起，并且安全计划能够在组织机构内的每一层都起到应有的作用和功能。高级管理层应该定义安全问题的范围、需要保护哪些资产以及需要保护到什么程度。在涉及安全问题时，管理层必须了解他们负责的规章、法律和责任问题，并确保整个公司都完成了所有这些责任和义务。高级管理层还必须确定雇员应该遵守的规范以及违反规范的处理方法，这些决策应当由那些在出现问题时能够担负最终责任的人员来制订。然而，较为常见的做法是：利用安全人员的专业技能，确保正在实施足够的策略和控制，从而能够实现高级管理层制定和确定的目标。

一个安全计划包含为公司提供全面保护和长远安全策略所需的所有条款。安全计划应当具有安全策略、措施、标准、指南和基准。人力资源部门和法律部门必须加入到开发和实施某些规则的活动中，满足这些文档中所列出的要求。

策略开发人员应当检查语言、详细程度、策略的形式以及支持机制。应该从实际的角度开发安全策略、标准、指南和措施和基准，以达到最佳效果。高度结构化的组织机构通常都会更加规范地遵守指南。结构化程度稍差的组织机构可能需要更多的解释和强调，从而促进规范的遵守。规则越详细，就越容易判断一个人是否违规。然而，过分琐碎的文档和规则可能会增加负担，反而没有益处。在撰写安全文档时，必须评估业务类型、公司文化及其目标，从而保证使用正确的语言。

围绕安全文档有很多的法律责任问题。如果你的组织有政策规定应该如何保护敏感信息，然后又发现你的公司没有践行它的政策，那么刑事诉讼和民事诉讼就可以成功执行。所以重要的是，公司的安全不能只是纸上谈兵，要落实到实处。

2.8.1　安全策略

——瞧，这个文件上载明了我们需要做什么，我要给它贴满小笑脸。

安全策略是高级管理层(或是选定的董事会和委员会)制定的一个全面声明，它规定安全在组织机构内所扮演的角色。安全策略可以是组织化策略，也可以是针对特定问题的策略或针对系统

的策略。在组织化安全策略中，管理层规定了应该如何建立安全计划，制定安全计划的目标，分配责任，说明安全的战略和战术价值，并且概述了应该如何执行安全计划。这种策略必须涉及相关法律、规章、责任以及如何遵守这些规定。组织化安全策略为组织机构内部未来的所有安全活动提供了范围和方向，还说明了高级管理层愿意接受多大的风险。

组织化安全策略具有一些必须理解和实现的重要特征：

- 业务目标应促进策略的制定、实现和执行。该策略应当不规定业务目标。
- 组织化安全策略应当是一份易于理解的文档，为管理层和所有员工提供参考。
- 应当开发和用于将安全整合到所有业务功能和过程中。
- 应当源于并支持适用于公司的所有法律法规。
- 应当随公司的发展变化(如采用新的商业模式、与其他公司合并或者所有权发生变更)进行审核和修订。
- 组织化安全策略的每次更迭都应当注明日期并在版本控制下进行。
- 受该策略监管的部门和个人必须能够查看适用于他们的策略内容，并且不必阅读整个策略材料就能找到指导和答案。
- 制定策略应以该策略一次性能够使用几年为目的。这将有助于确保策略具有足够的前瞻性，从而能够处理将来的安全环境中可能出现的任何潜在变化。
- 策略表述的专业水平能够强化其重要性以及遵守的必要性。
- 策略中不应包含任何人都无法理解的语言。必须使用清楚的、易于理解和接受的陈述性声明。
- 定期对策略进行审核，并根据自上一次审核和修订以来发生的事故加以改编。

必须针对不遵守安全策略的个人开发和实施一个过程，从而对他们的不合规采取一种结构化的响应方法。这将建立一个其他人都能够理解的过程，使他们不仅了解组织期待其如何遵守安全策略，而且知道在不遵守安全策略时将会受到怎样的惩罚。

组织策略也指主要的安全策略。组织有许多安全策略，这些策略应该按层级化的方式建立。组织(主要)策略位于最高层，然后下面是针对具体安全问题的策略。后者称为针对专门问题的策略。

针对专门问题的策略也称为功能实现策略，主要处理管理层认为需要更多详细解释和关注的特定安全问题，从而保证能够建立一个全面的安全结构，并且所有雇员都知道自己应当如何遵循这些安全问题。例如，某个组织机构可能会选择如下的电子邮件安全策略：它规定管理层在监控时能够和不能够查看员工的哪些电子邮件信息，规定雇员能够或者不能够使用哪些电子邮件功能，并且解决特殊的隐私问题。

再具体一些，某个电子邮件策略可能规定，管理层可以查看邮件服务器上的任何雇员的电子邮件信息，但是不能查看用户工作站上的电子邮件。该策略还可能规定，雇员不能使用电子邮件共享机密信息或者传播不适当的内容。员工会因为这些活动而受到监控。在雇员使用电子邮件客户端之前，应要求他们要么签署一份确认文档，要么在确认对话框中单击“Yes”按钮表示确认。这种策略为雇员提供了指导和规定，说明他们能做什么以及不能做什么，并且告知用户他们的行为将会有怎样的后果。此外，这种策略还能够提供责任保护，以防止雇员在处理电子邮件时由于种种原因而抱怨。

注意：

安全策略不应受技术和解决方案的约束。它必须列出目标和任务，但不得规定组织机构在完成这些目标和任务时应采用哪些具体的做法。

下面列出了常见的安全策略层级图，说明了主要策略和支持它的针对具体问题的策略之间的关系：

- 组织策略
  - 可接受的使用策略
  - 风险管理策略
  - 脆弱性管理策略
  - 数据保护策略
  - 访问控制策略
  - 业务连续性策略
  - 日志聚集和审计策略
  - 人员安全策略
  - 物理安全策略
  - 安全应用程序开发策略
  - 变更控制策略
  - 电子邮件策略
  - 事件响应策略

针对系统的策略是管理层的决策，这些决策与实际的计算机、网络和应用程序有关。组织中针对系统的策略既可以规定应该如何保护包含敏感信息的数据库、谁可以访问它和如何对它进行审计，也可以规定应该如何锁定和管理笔记本。这种策略针对的是一个或一组相似系统，规定应该如何保护它们。

使用广义的术语编写策略，以便涵盖多个主题。通过使用措施、标准和指南，可以为策略提供更细粒度的支持。策略提供基础，而措施、标准和指南提供安全架构。在安全架构内填充必要的安全防护措施(行政的、技术的和物理的)，从而制定全面的安全计划。

策略的种类

安全策略可以分为下列几种类别：

- **规章性策略**　这种策略用于确保组织机构遵守特定的行业规章建立的标准(HIPAA、GLBA、SOX 和 PCI-DSS 等)。这种策略一般都很详细，并且针对专门的行业。这种策略用在金融机构、卫生保健机构、公共设施和其他政府控制的行业中。
- **建议性策略**　这种策略用于强烈推荐雇员在组织机构中应该采取的某些行为和活动。它也对雇员不遵守规章的情况进行了相应规定。这种策略用在医疗信息处理和金融信息处理中。
- **指示性策略**　这种策略用于告知雇员相关信息。它不是一种强制性策略，而是用来指导个人与公司相关的特定问题。该策略会解释公司如何与合伙人打交道、公司的目标和任务，以及各种情况下的全面报告。

2.8.2 标准

——有些事情必须做！

标准指强制性的活动、动作或规则，它可以为策略提供方向上的支持和实施。组织安全标准可以指定如何使用硬件和软件产品，也可以用于指明期望的用户行为。它们提供了一种方法，从而确保在整个组织机构之间以统一的(标准化的)方式实现特定的技术、应用程序、参数和措施。组织化标准可能会要求所有雇员都必须随时携带公司的身份徽章，在特定区域内应当怀疑陌生人的身份与目的，并对机密信息进行加密。在公司内部，这些规则往往是强制性的，如果公司想获得成功，就必须实施这些规则。

组织可以制定针对具体问题的数据分类策略，规定“必须适当保护所有机密数据”。这还需要一个数据保护标准提供支持，规定应该如何实现和遵循这种保护，如“必须用 AES256 来保护休息中和传输中的机密信息”。

前面已经介绍过，战术和战略目标之间存在差异。战略目标可以视为终极目标，战术目标则是达到终极目标所需要的步骤。如图 2-15 所示，标准、指南和措施是战术工具，用于达到和支持安全策略中的指示，而安全策略被视为战略目标。

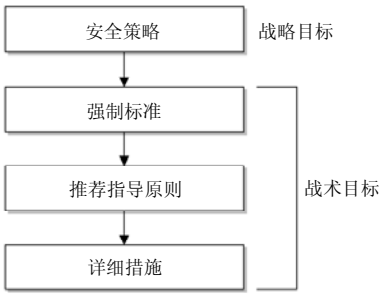

图 2-15　安全策略建立战略规划，底层元素则提供战术支持

警告：

术语“标准”在业内有许多含义。标准是必须遵循的内部文档。但有些时候，ISO/IEC27000 系列中的最佳做法由于是由标准机构制定的也称为标准。第 6 章中会提到具体的技术标准，如 IEEE 802.11。需要了解这个术语使用的上下文。CISSP 考试不会就这个术语迷惑大家，但需要知道行业内使用它的几种不同方式。

2.8.3 基准

“基准”可以指一个用于在将来变更时进行比较的时间点。只要风险得到缓解，而且实现了安全策略，就可以对基准进行正式审核并达成一致意见，之后再进一步通过比较和开发来进行评估。基准可以产生一致的参考点。

假设你的医生告诉你，由于以油炸圈饼、比萨饼和苏打汽水为食，因此你的体重已达 400 磅(这会令你感到沮丧，因为电视广告声称你可以吃自己想吃的任何食物，只要每天服用非常昂贵的药丸就可以减肥)。医生告诉你，你需要每天锻炼身体，将心率提高到正常水平的两倍，每天两次，每次 30 分钟。但是，如何知道自己的心率提高到两倍了呢？使用一条带有小球的臂带可以测出自己的基准(正常心率)。因此，你就从基准开始继续锻炼，直至将心率提高到两倍为止。

基准还用于定义所需要的最低保护级别。在安全领域，可以为每种系统都定义具体的基准，它规定要提供的必要的设置和保护级别。例如，某公司也许要求公司中所有的会计系统都至少达到评估保证级别(Evaluation Assurance Level，EAL)第 4 级的基准。这意味着，只有那些通过通用准则过程并达到该级别的系统才可以用在这个部门评估中。正确配置系统后，这就成为必要的基准。如果安装了新的软件，对现有软件应用了补丁程序或升级，或者系统发生了其他变更，那么很可能系统无法提供必要的最低保护级别(它的基准)。发生变更时，安全人员必须对系统进行评估，并确保作为基准的安全级别始终得到满足。如果技术人员在系统中安装了一个补丁程序，但不能保证基准仍然得到满足，那么就可能在系统中引入新的脆弱性，从而导致攻击者能够轻松访问特定网络。

注意：

组织机构内还应制订和实施非面向技术的基准。例如，某公司可能强制要求所有员工在工作时都要始终佩戴带有照片的身份徽章。它可能还要求访客必须在前台签名，并且在参观公司时有人陪同。如果这些规定得到遵守，那么就会建立一个保护基准。

2.8.4　指南

指导原则是在没有应用特定标准时向用户、IT 人员、运营人员及其他人员提供的建议性动作和操作指导。指南能够处理技术、人员或物理安全方面的各种方法。现实工作中总有不顺畅之处，此时指南就可以作为参考。标准是特定的强制性规则，而指南是为不可预见的情况提供必要灵活性的一般方法。

某个策略可能要求必须审计对机密数据的访问。一个支持性的指南可能会进一步阐明这些审计活动应当包含足够的信息，从而能够与前面的检查情况互相补充。支持措施将概述配置、实现和维护这种审计的必要步骤。

2.8.5　措施

措施是为了达到特定目标而应当执行的详细的、分步骤的任务。这些步骤可以应用于需要完成特定任务的用户、IT 人员、运营人员、安全人员及其他人员。许多组织都有书面的措施，它们规定了应该如何安装操作系统、配置安全机制、实现访问控制列表、建立新用户账户、分配计算机权限、审计各种活动、销毁资料、报告意外事故等很多措施。

因为措施距离计算机和用户最近(相对于策略)，并且提供有关配置和安装问题的详细步骤，所以它被视为策略链中的最低级别。

措施说明了如何将策略、标准和指南应用到实际操作环境中。如果某个策略规定所有访问机密信息的个人都必须经过适当的身份验证，那么作为支持的措施就需要阐明实现这个目标的步骤：为授权定义访问准则，规定如何实现和配置访问控制机制，规定如何审计访问活动。如果某个标准规定应当执行备份操作，那么措施就需要定义进行备份所需的详细步骤、备份的时间、备份的存储介质等。措施应当足够详细，以便于不同的人群都能够理解和使用。

让我们通过一个示例将上面这些内容综合在一起。某家公司的安全策略指出应当适当地保护机密信息，这是一个非常广泛而且笼统的说法。作为支持的标准会强制要求所有客户信息在存入数据库时都必须采用 AES(Advanced Encryption Standard，高级加密标准)算法进行加密，并且只能使用 IPSec 加密技术在 Internet 上传输。该标准说明需要怎样的保护类型，并且提供更加细化的解释。作为支持的措施会阐述如何实现 AES 和 IPSec 技术，指南则说明在数据传输期间发生意外讹误或损失时应当如何进行处理。一旦这些软件和设备都按照上述措施得以配置，我们就说这是必

须总是维护的基准。所有这些工作共同为公司提供了一个安全架构。

2.8.6 实施

——我们的策略信息量非常大，看起来非常的专业。

——无所谓，没有人在乎！

但是，在许多时候，安全策略、标准、措施、基准和指南之所以被写入文档，是因为审计员要求公司将这些项记录成文，不过这些文档最后都会放入文件服务器，并且不会被共享、解释或使用。要使这些文档发挥作用，就必须加以实施。如果人们不知道规则的存在，那么他们就不会遵守规则。因此，我们不仅需要开发安全策略及相关规定，而且还必须加以实现和实施。

为了达到效果，雇员需要了解这些文档涉及哪些安全问题。因此，安全策略及其支持文档必须是可见的。安全意识培训、手册、报告、新闻简讯以及法律标语都可以实现这种可见性。必须明确指出，这些指示来自于高级管理层，所有的管理人员都支持这些策略。雇员必须了解他们的动作、行为、可问责性和表现会有什么样的后果。

实现安全策略及其支持条款表明公司与管理人员行使了“应有的注意”。告知雇员他们应该遵守的规则以及违反规则的后果会涉及责任问题。如果某家公司由于一位雇员在公司的计算机中下载了色情内容而解雇他，该雇员可以将公司告上法庭，只要他能够证明：公司没有明确告诉自己，在使用公司财产时哪些行为是可以接受的、哪些行为是不可以接受的以及相应的后果，那么该雇员就能够胜诉。安全意识培训将在后面部分进行介绍，然而我们必须明白，那些没有向其雇员提供这些信息的公司并未实行“应有的注意 ”，从法律角度看，它们存在疏忽，应当承担相应的责任。

关键术语

- **策略** 描述高层管理者的安全指示的高级文档。
- **策略类型** 组织层面(主要的)、针对具体问题的、针对系统的。
- **策略功能性类型** 规章型、建议型、指示型。
- **标准** 强制性的、为安全策略提供支持的规则。
- **指南** 建议和最佳做法。
- **措施** 逐步的实现指导。

2.9 信息分类

——我写给我家狗狗的情书是最高机密。

——那当然了！

在本章开始部分，简单说明了识别什么信息对于公司是关键信息以及赋予信息价值的重要性。给各种类型的数据赋予价值的基本原因在于：它可以帮助公司调整用于保护各种数据的资金和资源数量，因为并非所有数据对公司都具有同等的价值。确定所有重要信息之后，就应当进行适当的分类。公司建立并维护大量的信息。信息分类是为了根据信息的损失、泄漏或无效的敏感程度来组织信息。一旦根据敏感程度对信息分类，公司就能够决定保护各种信息所需要的安全控制。这样可以确保信息资产得到适当级别的保护，同时分类会指明安全保护的优先顺序。数据分类的主要目的是说明需要为每种数据集设定的机密性、完整性和可用性保护级别。许多人的认识有误区，认为只需要注重保护数据的机密性，但其实还需确保数据未被未经授权的修改和在需要时是可用的。

数据分类有助于保证以成本最为低廉的方式保护数据。保护和维护数据会耗费资金，因此必

须将这笔资金用在确实需要保护的信息上。回到非常复杂的美国间谍卫星以及花生黄油和香蕉三明治食谱的示例。一家公司负责开发与美国间谍卫星进行数据传输所使用的加密算法，它会将此信息列为绝密，并应用复杂的高科技安全控制与措施来保证信息不会被未授权访问并泄露。另一方面，三明治食谱的安全级别就较低，采取的唯一保护方式就是不谈论它。

每种分类都应当具有单独的处理要求和措施，以便说明如何访问、使用和销毁数据。例如，在某家企业内，可能只有高级管理层和其他少数几个人有权访问机密信息，并且需要两个或更多的人输入访问密码才能访问。审计可以非常详细，并且能够对其结果进行每日监控，同时将机密信息的文件副本存放至保险库。为了从介质上完全擦除信息，可能需要采用消磁或归零方法。这家公司的其他信息可以归类为敏感信息，能够进行查看的人也略微多一些。对分类为敏感级别的信息的访问控制可能只要求一组凭证。虽然仍旧需要审计，但只需要每周检查一次，敏感信息的文件副本存放在上锁的文件柜中，并且删除数据时可以使用常规方法。机密和敏感信息之外的信息属于公开信息。所有雇员都有权访问公开信息，不需要特殊的审计或销毁方法。

2.9.1　分类级别

对于组织机构应该使用什么样的分类级别没有硬性和快捷的规定。某家公司可能只选择使用表 2-11 中所列出的任何分类级别。一家组织可能只选用两级分类，而另一家组织可以选用 4 级。表 2-11 阐明了可用的分类类型。需要注意的是，某些分类用于商业公司，而其他分类则用于军事机构。

表 2-11　商业公司与军事机构的数据分类

分　类	定　义	示　例	使用该分类的组织机构
公开	• 泄露不受欢迎，但不会给公司或个人造成不利影响	• 有多少人在完成某个特定的项目 • 即将开工的项目	商业公司
敏感	• 要求采取特殊防范措施，避免未授权的修改或删除，从而保证数据的完整性与机密性 • 要求高于正常的准确性和完整性保证	• 财务信息 • 项目细节 • 利润及其预测	商业公司
隐私	• 在公司内使用的个人信息 • 未授权的泄露可能给公司或个人造成不利影响	• 工作经历 • 人力资源信息 • 医疗信息	商业公司
机密	• 仅在公司内使用的信息 • 《信息自由法案》或其他法律法规豁免泄露的信息 • 未授权的泄露会对公司造成严重破坏	• 商业秘密 • 卫生保健信息 • 程序代码 • 使公司保持竞争优势的信息	商业公司 军事机构
未分类	• 非敏感或机密的信息	• 计算机手册与保修资料 • 招聘信息	军事机构
敏感但未分类(SBU)	• 保密程度不高 • 即使泄露，也不会造成严重破坏	• 医疗信息 • 测试评分答案	军事机构
秘密	• 如果泄露，那么可能会给国家安全造成重大威胁	• 军队驻扎计划 • 核弹部署	军事机构
绝密	• 如果泄露，那么可能会给国家安全造成毁灭性破坏	• 新型战争武器设计图 • 间谍卫星信息 • 间谍行为资料	军事机构

下面的分类由高到低列出商业公司的信息敏感级别：

- 机密
- 隐私
- 敏感
- 公开

下面的分类由高到低列出军事机构的信息敏感级别：

- 绝密
- 秘密
- 机密
- 敏感但未分类
- 未分类

表 2-11 所列出的分类级别是业界常用的方法，但也有很多变体。组织机构需要首先确定分几级才能最适应组织安全的需要，然后指定命名方案，最后定义出每个级别叫什么名称。A 公司可能使用“机密”分类级别代表最敏感信息，B 公司可能用“绝密”“秘密”和“机密”三级分类，而机密代表其最不敏感的信息。每个组织都必须开发最符合自己业务和安全需要的信息分类方案。

重要的是，不要走极端而提出大量的分类方法，这样只会给即将使用分类系统的个人带来混淆与沮丧情绪。另外，由于需要对多种类型的数据进行分类，因此分类也不应有太多限制或过于详细。

每种分类都应唯一且区别于其他分类，同时不能有任何重叠。分类过程还应当简单说明如何通过生命周期(由建立到终止的整个过程)控制并处理信息与应用程序。

确定分类方案后，公司或政府机构必须开发出一套使用准则来说明如何对信息进行分类。下面列出了组织机构可能用于决定信息敏感度的一些准则参数：

- 数据的用途
- 数据的价值
- 数据的寿命
- 数据泄露可能导致的损失级别
- 数据被修改或出现讹误可能导致的损失级别
- 保护数据的法律、法规或合约责任
- 数据对安全的影响
- 谁能够访问这些数据
- 由谁维护这些数据
- 谁能够重造这些数据
- 如果数据不可用或出现讹误，那么造成的机会损失有多少

数据并非唯一需要分类的事物，有时应用程序和整个系统也需要分类。应当对保存和处理分类信息的应用程序进行评估，从而决定它们的保护级别。你肯定不希望使用一个充满安全脆弱性的程序来处理和“保护”最敏感的信息。应用程序的分类应当基于公司对软件的确信(自信程度)及其能够存储和处理的信息类型。

注意：

组织必须保证：任何备份机密信息(和访问备份信息)的人都具有必要的许可级别。如果没有安全许可的底层技术人员在工作中能够访问这些信息，那么就会引起很大的安全风险。

警告：

分类规则必须适用于任何格式的数据，这些格式包括数字、纸张、视频、传真、音频等。

现在我们已经选定了一个敏感性方案，接下来应当详细说明每种分类的处理方式。需要明确说明访问控制、识别与标记的规定，以及如何存储、维护、传输和销毁经过特殊分类的信息。此外，还需要解决审计、监控和法规遵从问题。每种分类都需要不同的安全级别，因而上述条目的要求也各不相同。

2.9.2　分类控制

——我把绝密信息标上“绝密”字样了！

——太棒了，现在人人都想知道它是什么了。干得好！

前面曾经提到过，对每种分类执行何种控制取决于管理层和安全团队决定的保护级别。在本书中，将讨论大量的控制类型。然而，某些应用程序和处理敏感数据的方法为大多数组织所通用：

- 对各种级别的敏感数据和计划采用严格而细粒化的访问控制(参见第 3 章中对访问控制的介绍和文件系统权限的相关介绍)
- 对存储和传输过程中的数据加密(参见第 7 章中对各种类型的加密技术的介绍)
- 审计与监控(确定所需的审计级别以及日志保留时间)
- 责任分离(确定访问敏感信息是否需要两人或两人以上共同参与，以防止欺诈行为。如有必要，还需要定义相应措施并将其文档化)
- 定期审查(审查分类级别及相关数据和计划，从而确保它们仍然与业务需求保持一致；根据实际情况，可能还需要对数据或应用程序进行再分类或解密)
- 备份与恢复措施(定义与文档化)
- 变更控制措施(定义与文档化)
- 物理安全保护(定义与文档化)
- 信息流通道(敏感数据驻留在什么地方和它怎样在网络上流通)
- 数据字典审查
- 正确的处理动作，如粉碎、消磁等(定义与文档化)
- 标记、标签和处理步骤

数据分类措施

下面概述了正确分类计划的必要步骤：

(1) 定义分类级别。
(2) 指定确定如何分类数据的准则。
(3) 任命负责为数据分类的数据所有者。
(4) 任命负责维护数据及其安全级别的数据看管员。
(5) 制订每种分类级别所需的安全控制或保护机制。

(6) 记录上述分类问题的例外情况。
(7) 说明可用于将信息保管转交给其他数据所有者的方法。
(8) 建立一个定期审查信息分类和所有权的措施。向数据看管员通报任何变更。
(9) 指明信息解密措施。
(10) 将这些问题综合为安全意识计划，让所有员工都了解如何处理不同分类级别的数据。

2.10 责任分层

——好，他是负责人，出了错就怪他！

高级管理层和其他级别的管理层了解公司的长远规划、业务目标和目的。下一个层次为职能管理层，其成员了解各职能部门的运作方式、每位员工的工作职能以及公司安全对其所管理部门的直接影响。再下一个层次为运营经理和员工，这个层次与公司的实际运作密切相关。他们详细了解技术和措施要求、系统及系统的使用方式。这个层次中的员工理解安全机制与系统的整合方式、如何配置安全机制及其对日常生产效率的影响。每个层次对安全在组织机构中发挥的作用有着不同见解，并且都应当采用最佳安全实践、措施和选定的控制，以确保一致认可通过的安全级别能够提供必要的保护，同时不会给公司的生产效率带来负面影响。

尽管上述每个层次对于组织机构的总体安全来说都十分重要，但是某些特定角色必须被明确地定义。在小型机构工作的员工(那里的每名员工必须同时担任几个职位)可能会对接下来介绍的角色感到非常困惑。许多商业公司的安全团队并不具备这种安全结构层次，但是大量政府机构和军事部门都采用该结构。你需要了解必须分配的职责，以及这些职责是仅分配给几个人还是分配给一个大型安全团队。这些角色包括：董事会、安全执行官、数据所有者、数据看管员、安全管理员、安全分析员、应用程序所有者、监督员(用户经理)、变更控制分析员、数据分析员、过程所有者、解决方案供应商、用户、生产线经理以及为这些人端送咖啡的服务生。

2.10.1 董事会

——嗨，安然曾经很成功，现在他们的方法出什么问题了？

董事会由企业股东选出的一组人员组成，负责监督企业宪章的执行情况。成立董事会的是为了确保股东的利益得到保护，并且企业能够平稳运行。董事会成员应该是没有偏见的独立个人，他们负责监督行政人员在管理公司方面的表现。

许多年来，董事会成员要么寻求其他方法来防止企业欺诈和管理不善，要么过于依赖执行管理层的反馈，而不是自己动手去发现公司是否正常运营的真相。通过 2002 年被曝光的所有企业丑闻(如安然、WorldCom、Global Crossing 等)，我们能够了解到这种情况。这些公司的董事会负责查明上述欺诈性活动，并阻止它们以保护股东的利益。有许多因素致使董事会无法发挥他们应有的作用。某些因素是有意造成的，另外一些因素则是无意形成的。这些丑闻迫使美国政府和证券交易委员会(Securities and Exchange Commission，SEC)给公开上市的公司董事会提出更多的要求和设置潜在的惩罚条款。因此，如今许多公司发现他们很难找到担任这些角色的候选人，毕竟，身兼数职还得承担个人责任，这确实令人沮丧。

如果要求董事会成员承担起保护股东利益的责任，那么他们的独立性就非常重要。这意味着董事会成员不能是公司员工的直系亲属，不得从公司获得可能干扰其判断或造成利益冲突的经济补贴，也不得有其他活动阻止董事会成员成为公司股东的支持者。如果公司必须遵守 Sarbanes-Oxley(SOX)

法案，那么情况更是如此。该法案规定，如果公司不能适当维护内部的企业治理架构，并且(或者)公司向 SEC 上报的财务报表存在错误，那么董事会成员可能要承担个人责任。

注意：

其他法规(如 Gramm-Leach-Bliley 法案(GLBA))也向董事会提出了要求。但是，SOX 法案规定董事会成员必须承担个人责任，他们可能会因此被判罚金或入狱。

警告：

CISSP 考试并没有与具体法规(如 SOX、HIPPA、GLBA、Basel II、SB 1386 等)相关的题目。因此，在准备考试时，不必研究这些法规。但是，安全专家必须了解公司所在的国家和地区的法律与法规，这一点尤为重要。

2.10.2　执行管理层

——我很重要，但我的头衔里没有“C”。

——那就不重要！

执行管理层由头衔以字母“C”开头的个人组成。CEO(chief excutive officer，首席执行官)负责组织机构的日常管理工作。CEO 通常由董事会主席担任，是公司内地位最高的人。担任这个角色的人负责从宏观角度监督公司的财务、战略规划和运营。CEO 常被视为公司的远景规划者，负责制订和修改公司的业务计划。他们完成预算，确定伙伴关系，决定进入哪些市场，生产哪些产品以及公司如何将自己与其他公司区分开来等。这个角色的总体责任在于确保公司的发展和繁荣。

注意：

CEO 可以委托分派任务，但是不分派责任。越来越多与信息安全有关的法规要求这个角色承担更多责任。因此，国家的安全部门获得了更多的资金，决策者和财政官员承担的个人责任使得他们放松了钱袋。如今，公司也愿意在安全方面投入更多资金。

CFO(chief financial officer，首席财务官)负责公司的账目和财务活动以及组织机构的总体财务结构。他负责决定组织机构的财务需求，以及如何为这些需求提供资金。CFO 必须创建和维护公司的资金结构，这一结构由证券、存款、现金和债务融资组合而成。他监督公司的运营预测和预算，负责向 SEC 和股东提交季度和年度财务报表。

CFO 和 CEO 负责向股东(债权人、分析师、员工、管理层、投资者)通报公司的财务状况和健康水平。2002 年的企业经济丑闻被查出后，美国政府和 SEC 对担任这些角色并滥用职权的个人进行了严厉的惩罚，下面列出了一些示例：

- 2004 年 1 月——安然前任 CFO Andrew Fastow 因为财务丑闻被判入狱 10 年，他的刑期由于与起诉人合作而得到减免。
- 2005 年 6 月——Adelphia Communications Corp 的 CEO John Rigas 由于任职期间的贿赂与隐藏债务丑闻(致使该公司破产)而被判入狱 15 年。他的儿子(曾在该公司担任管理职位)被判 20 年监禁。
- 2005 年 7 月——WorldCom 的前任 CEO Bernard Ebbers 因组织美国有史以来最大的企业欺诈而被判入狱 25 年。

- 2005 年 8 月——WorldCom 前任 CFO Scott Sullivan 因为参与导致这家电信巨头破产的、金额达 110 亿美元的财务欺诈而被判入狱 5 年。
- 2005 年 12 月——HealthSouth Corp 的前任 CEO 因为参与金额达 27 亿美元的财务丑闻而被判入狱 5 年。

这些仅仅是被各大新闻媒体争相报道的首席官员，此外还有其他 CEO 和 CFO 也因为“创造性的财务”和欺诈活动而受到惩罚。

注意：

尽管上面介绍的示例都发生在数年以前，但是这些事件推动了美国政府制定新的法律法规来控制不同类型的欺诈行为。

图 2-16 说明了董事会成员应当如何为设置组织机构的战略和风险偏好(公司应承担多大风险)而承担责任。董事会还负责接收执行管理层和保障部门(审计委员会)上报的信息。借助这些信息，董事会能够确保公司的平稳运营，从而保护股东的利益。此外还需要注意的是，业务单位所有者(而非安全部门)也是风险所有者。由于许多公司没有将风险责任扩大到业务单位，因此 CISO 这个职位常常被称为“替罪羊”。

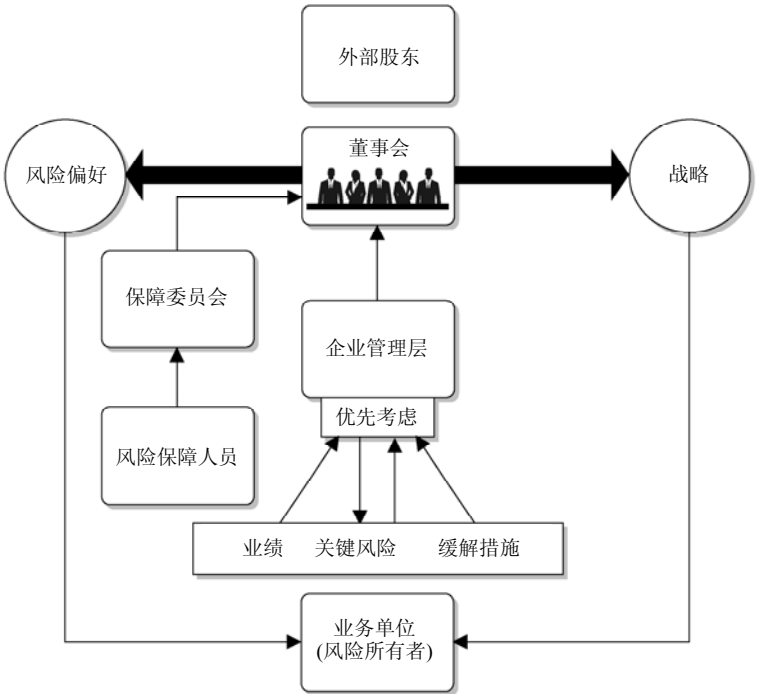

图 2-16 不同部门和层级都必须理解风险

2.10.3 CIO

CIO(Chief Information Officer，首席信息官)处于公司组织结构的较低层。根据企业结构，他们负责向 CEO 或 CFO 上报，并且负责组织机构内部信息系统和技术的战略使用与管理。随着时间的推移，在许多组织机构中，这个职位已更多地注重战略问题，而更少地关注运营管理。CIO 监督和负责公司的日常技术运作，但是由于组织机构对技术的依赖很强，因此越来越多的组织机

构要求 CIO 进入高级管理层。

CIO 的职责已经扩展到在业务流程管理、收入来源以及如何利用公司的内在技术实现业务战略方面与 CEO(和其他管理层)进行合作。通常，因为必须沟通两个截然不同的领域，所以 CIO 既要涉足技术管理，又要参与业务运营。

CEO 会为保护公司的资产设置阶段，并最终负责公司安全计划的有效执行。CEO 应当就各种问题向下层做出指示；同时，董事会、头衔以字母 C 开头的主管与中层管理人员之间应建立明确的沟通渠道。SOX 法案中列出了 CEO 和 CFO 不能有效执行上述职责而可能需要承担的责任与处罚。SEO 则希望，如果 CEO 和 CFO 行为不端，那么不能仅仅以公司缴纳罚金了事。依据 SOX 法案，他们可能要缴纳数百万美元的罚金和/或被判入狱。这些规定使得 CEO 和 CFO 在管理公司方面丝毫不敢懈怠。

2.10.4　CPO

CPO(Chief Privacy Officer，首席隐私官)是一个较新的职位，设立该职位主要是因为公司在保护各种类型数据方面面临日益增长的需求。这个角色负责确保客户、公司和雇员数据的安全，避免公司陷入刑事和民事诉讼，并防止公司由于数据泄露而登上新闻头条。这个职位通常由律师担任，并直接参与有关数据收集、保护和将数据交付给第三方的策略制订。CPO 一般向 CSO(首席安全官)提交报告。

公司必须理解组织机构应当遵守的隐私、法律和法规要求，这是十分重要的一点。了解这些要求后，就可以制订组织机构的策略、标准、措施、控制与合同协议，确定隐私要求是否得到满足。此外还需要记住的是，组织机构有责任了解他们的供应商、合作伙伴和其他第三方如何保护这些敏感信息。很多时候，公司需要对上述其他各方(他们拥有需要保护的数据的副本)进行审查。

某些公司在执行风险评估时并没有包括他们没有正确保护所负责信息而要承担的惩罚和后果。如果没有包括这些责任，那么就不能正确地评估风险。

组织机构应当就如何收集、使用、披露、归档和销毁隐私数据作出明确规定。如果雇员没有遵守组织机构为处理这类信息而制订的标准，那么他们应当承担责任。

注意：

从保护敏感数据的角度执行风险评估称为隐私影响分析(privacy impact analysis)。阅读网站 www.actcda.com/resource/multiapp.pdf 上的 “How to Do a Privacy Assessment” 部分，读者可以了解相关的步骤。

2.10.5　CSO

——嘿，为防万一，我们需要个替罪羊。

——我们有了，就是首席安全官。

CSO(Chief Security Officer，首席安全官)负责了解公司面临的风险和将这些风险缓解至可接受的级别。这个角色要了解组织机构的业务推动力，并为促进这些推动力而制订和维护一个安全计划，同时还负责提供安全、确保遵守大量法律法规以及满足客户需求或合约义务。

这个角色的设立是安全行业取得胜利的标志，因为这意味着安全最终被视为一种业务问题。以前，安全仅限于 IT 部门，而且被视为纯粹的技术问题。随着组织机构了解到需要整合安全需求和业务要求，在执行管理团队中设立安全职位的要求越来越迫切。CSO 的工作是确保业务不会因

为安全问题而出现任何形式的中断。这个工作已扩展到 IT 部门之外，延伸至业务流程、法律问题、运营问题、收入来源和声誉保护等领域。

隐私

隐私不同于安全。隐私指一个人应该能够拥有和认为自己会拥有的自身敏感信息的控制权。安全是用来提供这种控制权的机制。

由于身份盗窃和金融欺诈威胁的日益增多，保护个人身份信息(PII)变得越来越重要(也越困难)。PII 是个人信息的综合(姓名、地址、电话号码和账户号码等)。组织机构必须制定隐私策略和控制措施来保护员工和顾客的 PII。

CSO 与 CISO 的对比

CSO 和 CISO(Chief Information Security Officer，首席信息安全官)可能承担着类似或截然不同的职责。如何明确两者的职责呢？定义两个角色的职责，是否同时设立这两个角色，仅设立一个角色或不设立任何角色，这些都由组织机构自行决定。大体而言，与 CISO 角色相比，CSO 角色的职责更为广泛深入。CISO 通常更加关注技术问题，并且具有 IT 背景。CSO 则通常需要更深入地理解业务风险，包括物理安全(而不仅仅是技术风险)。

CSO 更多时候是一名商人，通常只有大型组织机构才会设立这个职位。如果某个公司同时设立了这两个角色，那么 CISO 应当直接向 CSO 报告。

CSO 往往负责整合(convergence)，即把以前脱节的安全功能正式组合起来。这主要是指让物理安全和 IT 安全以更为协调的方式运作，而不是各自为政。一些问题如损失预防、欺诈预防、业务连续性计划、法律法规遵循和保险等都涉及物理和 IT 安全两个方面的要求。因此，CSO 监管和整合这些不同的安全原则，从而可以全面而整体地实施安全计划。

2.11 安全指导委员会

——我们的指导委员会领着我们撞了南墙。

信息系统安全指导委员会负责就企业内部的战术和战略安全问题做出总体决策，并且不可以与任何一个或者多个业务部门有联系。这个委员会的成员应由来自组织机构各部门的人员组成，因此他们能够从个别部门和组织机构整体的角度来看待风险和安全决策的影响。该委员会应当由 CEO 领导，同时 CFO、CIO、各部门经理和首席内部审计员都应参与其中。

信息系统安全指导委员会应当至少每季度召开一次会议，并制订明确的议程。下面列出了这个委员会的一些职责：

- 定义组织机构的可接受风险级别。
- 确定安全目标和战略。
- 根据业务需求决定安全活动的优先级别。
- 审查风险评估和审计报告。
- 监控安全风险的业务影响。
- 审查重大的安全违规和事故。
- 批准安全策略和计划的任何重要变更。

他们还应当定义一个明确的远景声明，以推动和支持组织机构的业务目标。如果涉及组织机

构的业务目标，那么这个声明还应为组织机构的机密性、完整性和可用性目标提供支持。支持和定义适用于组织机构并允许其实现业务目标的任务声明也应遵从或支持上述远景声明。

2.11.1　审计委员会

审计委员会应由董事会任命，以帮助其审查和评估公司的内部运作、内部审计系统以及财务报表的透明度和准确性，使公司的投资者、客户和债权人继续保持对组织机构的信心。

通常，这个委员会至少应负责以下问题：

- 公司财务报表以及向股东和其他人提供的财务信息的完整性
- 公司的内部控制系统
- 独立审计员的雇用和表现
- 内部审计功能的表现
- 遵守与道德有关的法律要求和公司策略

审计委员会的目标是在董事会、公司管理层、内部审计员和外部审计员之间提供独立而开放的通信渠道。财务报表的完整性和可靠性对于每个组织机构来说都至关重要。很多时候，来自股东、管理层、投资者和公众的压力能够直接影响这些财务文档的客观性和准确性。在发生备受关注的企业丑闻之后，审计委员会的角色已经由监督、监察公司管理层并为其提供建议转向实施和确保所有相关人员的可问责性。这个委员会还必须接受来自外部和内部审计员以及外部专家的建议，以帮助确保公司制订适当的内部控制过程与编写正确的财务报表。

2.11.2　数据所有者

数据所有者(也称为信息所有者)通常是一名管理人员，他负责管理某个业务部门，对特定信息子集的保护和应用负最终责任。数据所有者具有“应有的注意”职责，因此，如果由于任何疏忽行为导致数据讹误或泄露，那么他必须承担责任。数据所有者决定其负责的数据的分类，如果公司需要，那么还应改变数据的分类。他还负责确保实施必要的安全控制，定义每种分类的安全需求和备份需求，批准任何泄露活动，保证应用适当的访问权限，以及定义用户访问准则。数据所有者有权准许访问请求，也可以选择将这一职权委托给业务部门经理。同时，数据所有者还要处理与其所负责数据有关的安全违规行为，以对数据进行保护。如果数据所有者工作繁忙，那么可以将数据保护机制的日常维护工作委托给数据看管员完成。

2.11.3　数据看管员

——嘿，看管员，帮我收拾一下这些破烂！

——我可不管那闲事！

数据看管员(也称为信息看管员)负责数据的保护与维护工作。这个角色通常由 IT 或安全部门员工担任，其职责包括：实施和维护安全控制措施、执行数据的常规备份，定期验证数据的完整性，从备份介质还原数据，保存活动记录，以及实现公司关于信息安全和数据保护的信息安全策略、标准和指南所指定的需求。

2.11.4　系统所有者

——我是管理这个系统的大王！

——你管这个打印机？你妈妈肯定很自豪！

系统所有者负责一个或多个系统，每个系统可能保存并处理由不同数据所有者拥有的数据。

系统所有者负责将安全因素集成到应用程序和系统购置决策及项目开发中。他还负责通过必要的控制、密码管理、远程访问控制、操作系统配置等措施保证足够的安全。这个角色必须确保系统的脆弱性得到正确评估，并且向事故响应团队和数据所有者报告所有的系统脆弱性。

数据所有者问题

每个业务部门都应当设立一名数据所有者，由他保护该部门最重要的信息。公司的策略必须赋予数据所有者完成任务的必要权力。

数据所有者并非一个技术角色，而是一个业务角色。他必须理解部门成功与保护数据这一重要资产之间的关系。并非所有商人都理解这个角色，因此必须对他们进行必要的培训。

2.11.5 安全管理员

安全管理员负责实施和维护企业内具体的安全网络设备和软件。这些控制措施通常包括：防火墙、IDS、IPS、反恶意软件、安全代理、数据损失防御等。人们经常区分开安全管理员和网络管理员的职责。安全管理员主要侧重维护网络的安全，而网络管理员侧重网络的更新和运行。

安全管理员的任务往往包括创建新系统用户账户，实现新的安全软件，测试安全补丁与组件，以及发放新密码(安全管理员不能真正批准新系统用户账户，这是监督员的职责)。安全管理员必须确保为用户授予的访问权限支持公司策略和数据所有者的指示。

2.11.6 安全分析员

——我分析了你的安全状况，发现一塌糊涂。

——太奇怪了！

与上述角色相比，安全分析员角色完成更高级的、更策略化层次的工作。安全分析员帮助制订策略、标准和指南，并设立各种基准。前面介绍的角色主要负责与安全计划有关的工作，安全分析员则帮助定义安全计划基本要素，并进一步保证这些要素得到正确执行与实践。这个角色的工作主要在设计层面，而非实现层面。

2.11.7 应用程序所有者

某些应用程序专门为单独的业务部门而设计。例如，财务部门使用财务软件，研发部门使用测试与开发软件，而质保部门则应用某种自动化系统。应用程序所有者往往是业务部门经理，负责规定哪些人有权访问他们的应用程序(当然必须遵守公司的安全策略)。

因为每个部门都拥有其专有应用程序的所有权，所以每个部门的应用程序所有者必须负责该部门应用程序的安全。这包括测试、修补、执行计划变更控制，并且还要保证实施正确的访问控制以提供必要的保护级别。

2.11.8 监督员

监督员角色也称为用户经理，主要负责所有用户活动以及由这些用户建立并拥有的资产。例如，假设 Kathy 是 10 名雇员的监督员，那么她的职责包括：确保这些雇员了解他们的安全职责，保证雇员账户信息的更新，以及在员工被解雇、停职或调职时向安全管理员进行通报。公司内任何一位雇员的角色变化都会影响到他们的访问权限，因此用户经理需要及时向安全管理员通报这些角色变化信息。

2.11.9　变更控制分析员

——我分析了你的变更请求，认为它会毁掉这个公司。

——无所谓啊。

变化是唯一永恒的事物。因此，在发生变更时，必须有人来保证变更的安全。变更控制分析员负责批准或否决变更网络、系统或软件的请求。这个角色必须确保变更不会引入任何脆弱性，并保证对变更进行适当测试，使其得以顺利实施。变更控制分析员需要了解各种变更对安全、互操作性、性能和生产效率的潜在影响。否则，公司只能先进行变更，然后再观察其造成的后果。

2.11.10　数据分析员

对于公司而言，数据的合理结构、定义和组织非常重要。数据分析员负责保证以最佳方式存储数据，从而为需要访问和应用数据的公司与个人提供最大的便利。例如，薪金信息不能与存货信息混杂在一起，采购部门需要以货币方式列出产品的价值，而存货系统需要遵循一个标准化的命名方案。数据分析员还可能负责构造一个保存公司信息的新系统，或者建议购买一款完成该项工作的产品。

数据分析员与数据所有者共同合作，帮助保证建立的数据结构符合并支持公司的业务目标。

2.11.11　过程所有者

你是否听说过现在流行的一句口号：“安全不是一款产品，而是一个过程。”这个说法非常正确。我们应当将安全视为另一个业务过程，而不是将其当做一款产品。

所有组织机构都具有许多过程：如何接受来自客户的订单；如何生产产品以完成订单；如何向客户交付产品；客户欠账时如何催收等。没有定义明确的过程，组织机构就无法正常运转。

过程所有者负责正确定义、改进并监控这些过程。过程所有者不必局限于某个业务部门或应用程序。复杂的过程涉及许多变量，可能涵盖了许多不同的部门、技术和数据类型。

2.11.12　解决方案提供商

——我原来想出了维护世界和平的解决方案，只是现在又忘了。

——下次把它写在纸巾上。

你遇到的每位供应商都声称自己是能够为你解决一切烦恼的解决方案提供商。事实上，由于世界上的问题多种多样，因此存在各种不同的解决方案提供商。当公司遇到问题或需要改进某个过程时，就需要由这个角色解决。例如，如果 A 公司需要一个支持数字签名电子邮件和身份验证架构的解决方案，那么就会求助于一家公共密钥基础设施(PKI)解决方案提供商。解决方案提供商与业务部门经理、数据所有者和高级管理层合作，开发并配置一个解决方案，从而解决公司面临的问题。

2.11.13　用户

——我发现我们公司要是没有用户的话就安全多了。

——我马上走人。

在与工作关联的任务中，任何例行使用数据的个人都是用户。用户必须拥有必要的数据访问级别，才能完成职权范围内的本职工作。他有义务遵守操作安全措施，从而保证数据对其他人的机密性、完整性和可用性。

2.11.14 生产线经理

谁负责向供应商阐明公司的需求，并且不会被他们的花言巧语所打动，从而确定其产品是否符合公司要求？谁负责保证遵守许可协议？谁负责将公司的需求转化为针对产品开发人员或解决方案提供商的目标和规范？每当 Microsoft 推销其产品时，谁负责决定是否确实需要升级操作系统版本？这个人就是生产线经理。

这个角色必须了解业务推动力、业务过程以及支持两者所需的技术。生产线经理要评估市场上的各种产品，与供应商合作，全面了解公司能够采用的各种选择，并向管理层和各业务部门提出满足其目标的解决方案购置建议。

2.11.15 审计员

——审计员来了！赶快把他去年让我们做的事做了！

审计员的职能是定期巡查，确保你正在做你该做的事情。他们确保采取并安全地维护了正确的控制措施。审计员的目标是确保组织机构遵循了自己制定的策略和适用的法律法规。组织可以拥有内部审计员和/外部审计员。外部审计员往往代表法律机构，确保组织符合法规要求。前面提到的 CobiT 是多数信息安全审计员在评估安全规划时用的模型。

虽然许多安全专业人士都害怕审计员，但审计员的工作在确保组织的整体安全性方面非常有价值。他们的目标是找出你忽视的问题并帮助你了解如何修复这些问题。

2.11.16 为何需要这么多角色

虽然大多数公司没有设立上面提及的所有角色，但是重要的是要构建一个组织结构，包含所有必要的角色并给这些角色分配正确的安全职责。这个结构要清晰地定义职责、指令线和沟通渠道以及实施能力。结构清晰意味着人们清楚地知道在不同情况下谁做什么和怎么做。

2.11.17 人员安全

人员责任的许多方面都在管理的保护伞之下，还有几个方面与整体的安全环境有着直接的关系。

虽然社会已经发展成在工作场所非常依赖于技术，但是人仍然是公司成功的关键因素。在安全领域，人往往是最薄弱的环节。意外的错误、缺乏培训、故意弄虚作假或恶意企图，人员会造成更严重和难以检测的安全问题，这些甚至比黑客攻击、外界间谍活动或者设备故障带来的后果更严重。虽然不能预测员工未来的行动，但是可以通过实施预防性措施把风险降至最低。这些措施包括聘请最有资历的人，进行背景调查，使用详细的岗位说明，提供必要的培训，实施严格的访问控制，以及在辞退人员时采取保护各方利益的方式。

如果几种措施落实到位，则可以减少欺诈、破坏、信息滥用、盗窃和其他安全隐患的可能性。职责分离(separation of duties)可以确保一项重要的任务不是由一个人独自完成。在电影里，当潜艇艇长需要发动核鱼雷炸毁敌人，拯救文明的时候，正如我们所知道的一样，发射通常需要 3 个代码，这 3 个代码是由 3 个不同的高级船员订立的启动机制。这是职责分离的一个例子，它确保了艇长无法全部由自己一个人完成这样一个重要而可怕的任务。

职责分离是一种预防性的管理控制，落实到位，可以减少潜在的欺诈。例如，雇员不能自己完成关键的金融交易。在交易完成前，需要有上司的书面批准。

在一个实行职责分离的组织中，欺诈行为必会有合谋。合谋意味着，至少要有两个人一起工

作，才会造成某种类型的破坏或欺诈。在我们的例子中，雇员和她的主管必须参与欺诈活动才能做到这一点。

职责分离概念可演变为知识分割和双重控制两种类型。在这两种情况下，两个或两个以上的人被授权去执行义务或任务。在知识分割的情况下，没有一个人知道或拥有执行任务所需要的所有细节。例如，管理人员可能需要打开银行的金库，但每个人只知道组合密码的一部分。在双重控制的情况下，两个人再次被授权执行任务，但在他们的参与中，两人都必须是可用的和积极的，才能完成任务或使命。例如，两名人员必须在核导弹潜艇中依次输入各自的密钥来发射导弹，而两个密钥相互隔离。此处的控制可实现没有一个人有能力单独发射导弹，因为他们不能同时接触到这两个密钥并打开他们。

岗位轮换(Rotation of duties)是管理检测控制，落实到位则可以发现欺诈活动。没有什么人应该长时间呆在同一个岗位，因为那样他们最后对某个业务模块可能有太多的控制权。这种全权控制，往往会导致欺诈或资源的滥用。根据岗位轮换原则，员工应该被调遣到不同的职位，这样他们可能会检测到之前在这个岗位上的雇员进行的任何活动。这种类型的控制在金融机构中普遍采用。

在敏感领域工作的员工被强迫去度假，这被称为是强制休假。当他们休假时，其他的人填补了他们的职位，因此通常可以检测到欺诈性的错误或活动。众多检测欺诈和不恰当活动的方法中，有两种最为常见：一种是在确认他们已经去休假后，检测他们的个人账号发现问题；另一种是在某人离开或没有在网络上活动时，一个特定问题停止了。这些异常现象都值得调查。进行欺诈活动的员工通常不休假，因为他们不希望任何人可以找出自己在幕后做的事情。这就是为什么他们必须被迫离开组织一段时间，时间通常是两个星期。

关键术语

- **数据所有者**　负责特定数据集的保护和分类的人。
- **数据看管员**　负责实施和维护安全控制，以满足数据所有者列出的安全需求的人。
- **职责分离**　预防性的管理控制，用于确保一个人不能单独开展的一项重要任务。
- **合谋**　两个或两个以上的人一起工作，联合开展欺诈活动。
- **岗位轮换**　检测性的管理控制，用来发现潜在的欺诈活动。
- **强制休假**　检测性的管理控制，要求一个人离开组织一段时间以发现其潜在的欺诈活动。

2.11.18　招聘实践

——我喜欢你的帽子，你被录用了！

根据需要招聘的职位，人力资源部门应当进行人员选拔，以保证公司雇用合适的人才。人事部门应对应聘人员的技能进行测试与评估，并考查他们的品质与性格。Joe 也许是本州最优秀的编程人员，但调查他的经历会发现其曾因侵入银行系统偷钱而入狱，因此招聘经理对雇用 Joe 可能就不会太热心。

公司需要制订保密协议，并要求新员工签订此协议，以保护公司及其敏感信息。该协议必须解决所有利益冲突，同时应该对临时员工与合同工采用不同的协议和防范措施。

人事部门应当查实应聘人员的介绍材料，审查其军事档案，核实其教育经历，在必要时还应进行药检。很多时候，应聘人员往往会隐瞒其重要的个人行为，因此现在的招聘实践一般包括情景提问、个性测试和个人观察，而不是仅仅考查一个人的工作经历。当一名员工被雇用时，他不仅带来自己的业务技能，也带来与其有关的一切方面。通过首先执行有效且仔细规划的招聘实践，公司能够减少与人员有关的麻烦。

目标是 聘用“合适的人才”，而不是 “即刻”人才，对于组织机构而言，员工代表着一种投资，通过花费时间雇用合适的人才，组织机构才能获得最大的投资回报。

更详细的背景调查能够揭示一些有趣的信息。雇用历史中无法解释的空档、职业证明的合法性与实际状况、犯罪记录、驾驶记录、虚假的工作头衔、信用记录、不友好的解雇、出现在可疑恐怖分子监控名单上、甚至是失去前一份工作的真实原因，所有这些事情都可以通过背景调查来核实。这样做对雇主和组织机构都有很大帮助，因为它可以成为防止组织机构遭受内部攻击的第一道防线。在上述领域中查明的任何负面信息都表示待聘员工可能会在以后给公司带来潜在的问题。以信用记录为例。表面上，组织机构似乎不需要了解这方面的信息。但是，如果信用记录表明可能招聘的员工信用记录不佳，而且以前还出现过财务问题，那么你也许不希望他管理组织机构的账目，甚至是小额现金。

进行背景调查的最终目的是同时做到以下几点：减少风险，减少招聘成本，降低员工的流动率。如果你努力防范现有的客户和员工可能实施的恶意和欺骗性行为，并防止对你、你的员工、你的客户和普通公众造成伤害的人员被组织机构雇用，那么就可以同时实现上述目的。在很多情况下，如果某人已经被聘用且已开始工作，那么就很难再回过头来对他进行背景调查。这是因为，此时你需要特定的理由或原因才能进行背景调查。如果某名员工被调到一个安全敏感度更高或潜在风险更大的职位，那么就应考虑对其进行后续背景调查。

可能的背景调查准则包括：

- 社会安全号追踪
- 国家/州犯罪调查
- 联邦犯罪调查
- 性侵犯注册调查
- 就业记录核查
- 教育记录核查
- 职业介绍材料核查
- 移民调查
- 职业许可证/认证核查
- 信用报告
- 药物筛查

2.11.19 解雇

——我不再喜欢你的帽子了，你被解雇了！

由于有多种原因会引起解雇，而且解雇员工也会造成各种后果，因此公司应当制订一组特定的措施来管理每种解雇事件。例如：

- 被解聘员工必须在一名经理或保安的监督下立即离开公司。
- 被解聘员工必须上交所有身份徽章或钥匙，完成离职谈话，并返还公司的供应品。
- 公司应立即禁用或修改被解聘员工的账户和密码。

这些措施执行起来似乎相当严厉且冷漠。但是，当员工因为某些原因被解聘后，他们的报复行为会给公司造成损失。如果一名员工表现出不满情绪，或者解聘过程进行不顺利，那么公司应当立即禁用该员工的账户并修改所有系统的所有密码。

2.11.20　安全意识培训

——我们CEO 说我们的组织很安全。

——他比任何人都需要进行安全意识培训。

组织机构的安全计划要取得预期的效果，就必须同雇员交流与安全相关的问题，如执行哪些安全计划、执行方式以及执行这些计划的原因。安全意识培训应专门为特定团体特别设计，内容广泛，并在整个组织机构内全面施行。它应该以不同形式重复最重要的信息，时刻更新，有趣味性，积极幽默，易于理解，最重要的是得到高层管理者的支持。管理层必须为这个活动配备资源，并强调员工的出勤率。

安全意识培训的目的是让每名雇员都了解安全对于整个公司和每个人的重要性。必须阐明期望的责任和可接受的行为，并在援引法规之前明确不服从规定所造成的后果，视程度轻重给予警告或开除工作。安全意识培训的执行是为了修正员工对安全的错误行为和态度。这种状态能够通过正式的安全意识培训过程得到实现。

因为安全是一个涉及组织机构许多不同方面的主题，所以可能很难向适当的人员传达正确的信息。使用正式的安全意识培训过程，你就可以确定一种提供最佳结果的方法，确保向组织机构中合适的人员传达安全策略和措施。这样，你就可以确保每个人都理解企业安全策略的内容、安全策略的重要性以及它如何与组织机构中个人的职责相适应。更高级别的员工接受的培训更加全面，针对的是更加广泛的概念和目标。如果针对特定的工作和任务，那么培训就会变得更加具体化，因为它直接适用于公司中的某些职位。

一个安全意识培训计划通常至少有 3 种受众：管理层、职员、技术人员。每种意识培训都必须针对一类受众，从而保证每个群体都了解自己特定的责任、义务和期望。对高级管理层进行技术安全培训时，如果向他们提及协议和防火墙，那么他们会目瞪口呆。另一方面，如果同 IT 员工讨论法律问题、与数据保护有关的公司责任问题以及股东的期望，那么他们就会自己玩手机，玩猜词游戏，上网或者给朋友发短信。

专门召集管理层成员召开一次简短的安全意识定位会议，讨论与安全相关的企业资产和金融损益，他们就会获益良多。他们需要了解安全危害对股价的负面影响、公司面临的可能威胁及其后果，以及安全为什么需要像其他业务过程一样集成到系统环境中。因为管理层成员必须领导公司其他员工支持安全工作，所以他们应当对安全的重要性有正确的认识。

详细说明策略、措施、标准和指南以及它们与中层管理人员各自管理的部门之间的关系，这会让中层管理人员从中受益。应使中层管理人员认识到他们的支持对自己所在部门的重要性，同时他们还有责任保证员工实施安全的计算活动。此外，还应向中层管理人员说明其下属的不服从行为对整个公司的影响，以及他们作为部门经理对此不当行为应承担的责任。

技术部门必须接受以其日常任务为重点的单独培训。公司应对他们进行更深入的培训，讨论技术配置、事故处理和各种安全威胁的迹象，以便在出现这些问题时正确识别它们。

通常，最好与每名雇员都签订一份文档，以表明他们已获知和了解所有相关的安全主题，而且明白不服从会造成的后果。这样做一方面可以向雇员强化策略的重要性；另一方面，如果雇员声称自己从未被告知这些期望，那么这份文档还可以作为证据。安全意识培训应该贯穿整个招聘过程，之后至少每年进行一次。培训的出勤率也应该载入员工绩效报告中。

组织机构应采用不同的方法来强化安全意识概念。横幅、员工手册甚至海报都可以用于向雇员提醒他们的责任及良好安全实践的必要性。

2.11.21 学位或证书

组织内的某些角色需要实践经验和技能，这意味着招聘经理应该寻找那种具有指定行业认证资格的人。有些职位需要更多的综合考虑，以及对基本概念的理解或商业背景，在这些情况下，则可能需要一定的学位。表 2-12 提供了更多关于意识、培训和教育之间差异性的信息。

表 2-12 意识、培训和教育比较

	意　识	培　训	教　育
属性	什么	如何	为什么
水平	信息	知识	洞察力
学习目标	辨认和保持	技能	理解
教学方法示例	媒体 ● 视频 ● 时事通信 ● 海报	实践性指导 ● 演讲和演示 ● 案例教学 ● 实践联系	理论性指导 ● 研讨会和讨论 ● 阅读学习 ● 研究
测试考核	是非题，多选(识别性学习)	解决问题，如识别和分辨(应用性学习)	论文(解释性学习)
影响时间	短期	中期	长期

2.12 安全治理

——我们要把所有这些都搞对？

一个组织可能会遵循本章所列出的很多事项：建立一个安全规划，将其集成到业务架构中，制定风险管理计划，记录安全规划的不同方面，执行数据保护并培训员工。但是我们如何知道都做对了，并能持续进行呢？这时候，安全治理就有用了。安全治理是一个框架，它允许组织的安全目标由高级管理人员设置并传达出来，通过在组织不同层面交流传达，授予需要实施和加强安全措施的实体权限，并且提供一种方法来验证这些必要的安全活动的执行。仅由高级管理人员需要设置安全的方向是不够的，还需要一种方法能够查看和了解他们的指示是如何得到满足或没有得到满足的。

如果董事会和 CEO 要求将安全恰当地集成到组织的各个层级中，他们怎么知道切实贯彻了呢？必须开发和集成监督机制，这样，那些最终负责组织的人才会自始至终不断地更新组织的整体健康和安全态势。只有通过正确定义的沟通渠道、标准化的报告方法以及基于性能的考核指标，才会实现这些。

比较一下两家公司。A 公司有一个有效的安全治理规划，而公司 B 没有。现在，对于未经训练的人而言，看起来似乎是公司 A 和公司 B 在安全做法上是相同的，因为他们都有安全策略、程序、标准和相同的安全技术控制(防火墙、入侵检测系统和身份管理等)，定义了安全角色，也进行了安全意识培训。你可能会认为，“伙计，这两家公司都很机警，他们的安全规划都十分先进。”但是如果走近些看，会发现两家公司有着巨大差异(如表 2-13 所列)。

表 2-13　公司 A 和公司 B 的比较

A 公司	B 公司
董事会成员明白信息安全对公司是至关重要的，要求每季度更新安全的执行情况和违规情况报告	董事会成员不理解信息安全是他们份内的事情，仅关注企业治理及利润
CEO、CFO、CIO 和业务部门经理必须加入风险管理委员会，且每个月召开一次会议，始终将信息安全列为会议议事日程之一，开展审核工作	CEO、CFO 和业务部门经理认为，信息安全是 CIO、CISO 和 IT 部门的责任，与自己无关
执行管理层设置一个可接受的风险等级，将它作为公司的安全策略和所有安全活动的基础	CISO 采用了一些安全策略样板，在里面写下了公司的名称并让 CEO 签字生效
执行管理层要求业务部经理负责对其特定的业务单元开展风险管理活动	所有的安全活动都发生在安全部门内部，因此，安全工作很独立，没有集成到整个组织
在业务流程的不同环节中，归档记录关键业务流程中固有的风险	不记录业务流程、不分析可能会影响运营、生产效率和盈利能力的潜在风险
涉及到任何员工的安全违规，无论是恶意的或者是意外的，都会被追究责任	策略和标准开发了，但没有设想或部署任何强制执行或问责的机制
根据行业惯例购买和部署安全产品、管理服务和顾问咨询服务。同时经常审核，以确保符合投资效益比	购买和部署安全产品、管理服务和顾问咨询时没有任何真正的调研，也没有性能指标来衡量投资回报率或有效性
组织以持续改进为目标，坚持不断地审核包括安全在内的流程	组织不分析它的成效改进，反而不断前进，类似的错误发生了一遍又一遍

请问你工作的组织看起来是像 A 公司还是 B 公司呢？今天，大多数组织都已实施了很多安全规划(策略、标准、防火墙、安全团队和 IDS 等)，但管理层却没有真正参与其中，安全也没有渗透到整个组织中。有些组织只是依靠技术和仅仅隔离了 IT 部门内部的所有安全职责。如果安全只是技术问题，安全团队也仅需要正确地安装、配置和维护产品，那么公司将会获得一枚金牌，并能出色地通过审计。但是，这并不是今天信息安全工作的方式。信息安全远不止技术解决方案。安全必须贯穿于整个组织，并且需要在多点设立职责说明和问责办法。安全治理是一个将安全集成到过程中的条理分明的系统，它有助于确保一致性的监督、问责制和合规性。应该将安全治理的结构落实到位，以确保我们的努力顺利、高效，并且不会有所遗漏。

度量

我们不能只建立安全规划，说句好了就万事大吉。我们需要一种方法来评估工作的有效性，找出不足之处，并优先考虑那些还需要处理的地方。需要有一种方式，在对必要信息收集、分析和整理后，能够便于决策、绩效改进和责任制加强。常言道，“你不能管理你无法度量的东西。”在安全方面，有许多事项需要衡量，以便可以正确理解安全工作效果。我们需要知道实施的安全控制在保护资产时的效果如何，还要知道财务资金投入上的回报率如何。

在开发安全考核指标时，可以遵循不同的方法论，但不管依据哪种模型，有些事情是务必考虑的。强有力的管理层支持是必须的，虽然开发计量方式看起来没有那么复杂，但实际执行和使用考核指标并对系统开展考核时却任重而道远。必须开发和采纳考核指标，并将其集成到很多不同的已有过程或新过程中，还要解释考核指标并将其应用于决策链中。这些过程必须有管理层介入方可成功。

另一个需求是，必须要建立策略、规程和标准才能再次度量。在没有策略的情况下，如何度

量策略的合规性呢？在对一个完整的安全规划的组成部件进行度量前，需要先开发出安全规划本身并且其已发展成熟。

度量活动需要由量化的基于性能的数据作输入支撑，这些数据必须是可重复的、可靠的，并且产生的结果也要是有意义的。度量需要在连续的背景下开展，所以用到的数据采集方法也必须是可重复的。相同类型的数据必须连续收集和比较，才能标识出度量结果“改进或倒退”。采集的数据可能来源于解析系统日志、事件响应报告、审计发现、调查或风险评估。度量结果对于目标受众必须是有意义的。例如，总裁希望数据的表现方式能让他阅读后立刻了解到组织安全的健康状况，并符合他的使用风格。度量结果可能是热度图、曲线图、饼状图或记分卡。如图 2-17 所示，平衡计分卡是一个传统的战略工具，用于在商业界的绩效考核。目标是快速、轻松地呈现最相关的信息。度量结果和目标值进行对比时，如果成效偏离了期望值，那么它们可以以一种简单和直接的方式呈现出来。

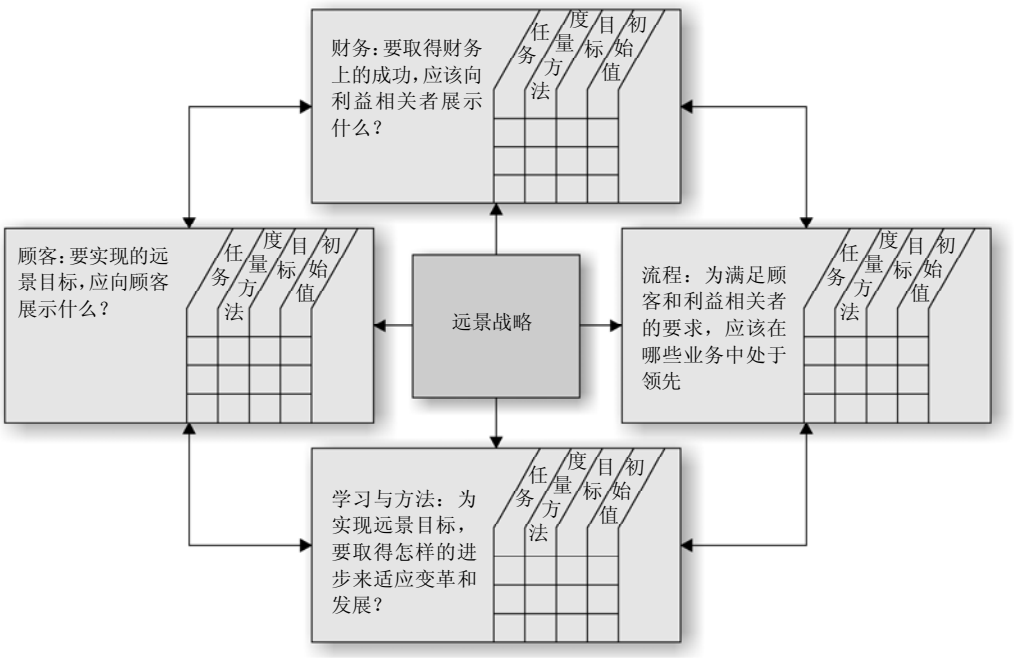

图 2-17　平衡计分卡

如果度量值的受众不是执行者，而是安全管理员，那么度量结果应以一种对他们来说最容易理解和使用的方式显示。

注意：

本书作者已经看过很多记分卡，如饼图、曲线图和仪表图，它们都不能实际映射环境中发生的事。除非收集的数据是真实的、正确的，否则饼图显示的结果可能与实际完全不同。有些人花更多的时间在制图颜色上，使图的外观颜色看起来赏心悦目，而不是把时间用来完善原始数据收集技术上。这可能会导致一种安全错觉和极大破坏。

有行业最佳实践可以用来指导安全度量标准和测量系统的开发。国际标准 ISO/IEC 27004:2009

用于评估信息安全管理体系和控制措施的有效性，它形成了 ISO/IEC 27001 中列出的安全规划。因此，ISO/IEC 27001 告诉你如何建立安全规划，而紧接着 ISO / IEC 27004 指明如何来度量它。NIST800-55 标准也涉及了安全的性能度量，但是它有美国政府的倾向。ISO 标准和 NIST 对度量开发的方法相似，但有一定的差异。ISO 标准打破了单一指标做法，推出了基本测量法、衍生测量法和指标值法。NIST 的方法如图 2-18 所示，它将指标分为执行过程测量、效果和效率测量以及业务影响测量。

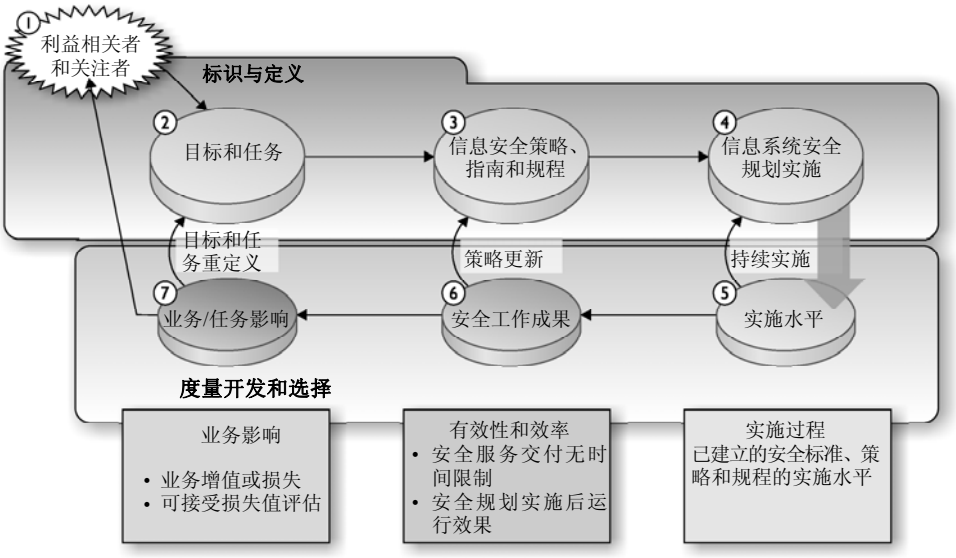

图 2-18　安全测量过程

如果组织有获得 ISO/IEC 27000 认证的目标，则应该遵循 ISO/IEC 27004:2009。如果组织是政府或政府签约的公司，那么遵循 NIST 标准会更有意义。度量工作最为重要的是一致性。要想很成功地开展度量工作，必须使度量标准化，同时每个度量项之间保持直接关系。例如，一个组织使用 1～10 的评级系统度量事件响应流程，而又使用高、中、低评级系统来度量恶意软件感染的保护机制效果，这两种度量指标不能轻松地被整合在一起。一个组需要建立它自己将使用的度量值类型，然后在整个企业中以标准化方法实现。在尝试实施度量之前，度量过程必须细致斟酌。表 2-14 描述了一个度量模板，可以用它来跟踪事件响应的成效水平。

表 2-14　事件响应测量模板

字　　段	数　　据
测量 ID	事件响应测量 1
目标	战略目标：在组织的程序上提供精准和及时的信息，同时保证服务可用。 信息安全目标：跟踪、记录并及时向对应的组织管理人员和主管部门报告
测量	在规定的时间内按照每种对应的事件类别报告事件的比例
测量类型	有效性
公式	对于每个事件类别(及时报告的事件数量/报告事件的总数量)×100
目标	85%

(续表)

字　段	数　据
实施证据	在 12 个月内有多少事件被报告？ 类别 1.非授权访问？_____ 类别 2.拒绝服务？_____ 类别 3.恶意代码？_____ 类别 4.滥用？_____ 类别 5.试图访问？_____ 有多少事件涉及人员身份信息(PII) 在已报告的事件中，有多少是在规定的时间内按照对应的类别上报的？ 类别 1.非授权访问？_____ 类别 2.拒绝服务？_____ 类别 3.恶意代码？_____ 类别 4.滥用？_____ 类别 5.试图访问？_____ 在涉及人员身份信息的事件中，有多少是在规定时间内按照类别上报的？
频率	采集频率：每月 报告频率：每年
响应团队	CIO，CISO
数据源	事件日志、事件跟踪数据库
报告格式	说明每个事件类型的线性图表

开发这种类型的度量指标，需要映射到安全规划的成熟度级别。最初，测量简单的项(例如已开发的策略数量)，然后随着安全规划日益成熟、度量指标也逐渐成熟，这时可以增加复杂性的度量(如漏洞数量的减少)。

度量指标的使用，使企业能够真正了解组织安全规划的健康程度，其原因在于每一项活动和初始状态都能以量化的方式来度量。度量指标可用于治理活动，因为借助它，可以做出最好的战略决策。度量指标的使用便于组织遵照前面描述的能力成熟度模型开展工作。成熟度模型用来进行持续改进，度量结果则指示出什么需要改进以及需要改进到什么级别。度量机制也可以用在过程改进模型中，如用在六西格玛模型和 ITIL 服务水平目标的测量中。我们不仅需要知道做什么(如实施控制，建立一个安全规划)，还需要知道我们如何做，以及如何持续改进。

2.13　小结

安全计划应当从战略、战术、操作角度来解决各种问题，如图 2-19 所示。安全计划应集成到企业结构中的每个层次。安全管理也应该体现必要的管理和行政活动，以支持并保护信息和整个公司的资产。它包括了安全策略及其支持机制(措施、标准、基准和指南)的开发和实施，涵盖了企业安全开发、风险管理、合理的对策选择与实现、治理和绩效考核。

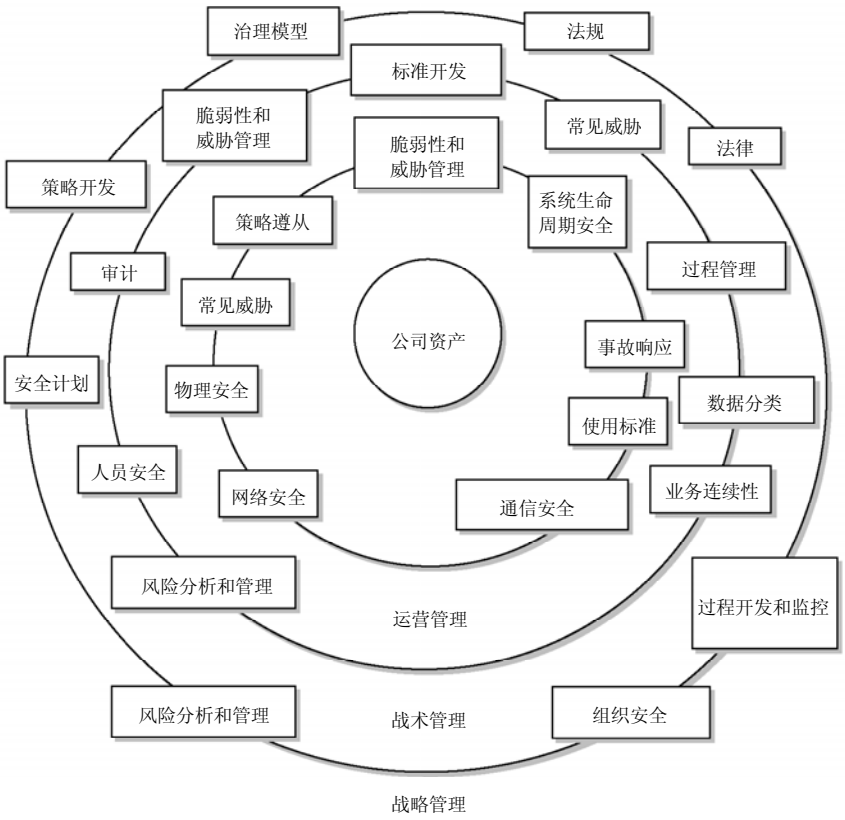

图 2-19　一个包含许多项的完整安全计划

安全是一个业务问题，因此应当被正确地对待。因为安全问题会对公司依赖的资源产生负面影响，所以安全必须被合理地融入公司的整体业务目标和目的。越来越多的公司都因为没有对安全问题给予正确的重视、支持和投资而付出惨痛的代价。生活在这个世界中是令人愉快的，但是会发生一些糟糕的事情。意识到这一点的人不但能够生存下去，而且会茁壮成长。

2.14　快速提示

- 安全的目标是对数据和资源提供可用性、完整性和机密性保护。
- 脆弱性指的是缺少防护措施或防护措施存在能够被利用的缺陷。
- 威胁是某人或某物有意或无意地利用某种脆弱性并导致资产损失的可能性。
- 风险是威胁主体利用脆弱性的可能性以及相应的潜在损失。
- 对策，也叫防护措施或者控制措施，能够缓解风险。
- 控制可以是行政性的、技术性的或物理性的，能够提供威慑性、防御性、检测性、纠正性或恢复性保护。
- 补偿控制是由于经济或业务功能性原因而采用的备选控制。
- CobiT 是控制目标架构，允许 IT 治理。
- ISO/IEC 27001 是建立、实施、控制和改进信息安全管理体系的标准。
- ISO/IEC 27000 系列源自 BS 7799，是国际上有关如何开发和维护安全计划的最佳实践。

- 企业架构框架用来为特定开发架构和呈现视图信息。
- 信息安全管理体系(ISMS)是一套策略、流程和系统的集合，用来管理 ISO/IEC 27001 中列出的信息资产所面临的风险。
- 企业安全架构是企业结构的子集，描述当前和未来的安全过程、体系和子单元，以确保战略一致性。
- 蓝图是把技术集成进入业务流程的功能性定义。
- 企业架构框架用来构建最符合组织需求和业务驱动力的单一架构。
- Zachman 是企业架构框架，SABSA 是安全企业架构框架。
- COSO 是治理模型，用来防止公司环境内出现欺诈。
- ITIL 是一套 IF 服务管理的最佳实践。
- 六西格玛用来识别进程中的缺陷，从而对进程进行改进。
- CMMI 是一个成熟度模型，使进程逐渐以标准化方式改进。
- 企业安全架构应该配合战略调整、业务启用、流程改进和安全有效性等。
- NIST 800-53 的控制类别分为：技术性的、管理性的和操作性的。
- OCTAVE 是团队型的、通过研讨会而管理风险的方法，通常用于商业部门。
- 安全管理应该由顶而下进行(从高级管理层向下至普通职员)。
- 风险可以转移、规避、缓解或接受。
- 威胁×脆弱性×资产价值=总风险。
- (威胁×脆弱性×资产价值)×控制间隙=剩余风险。
- 风险分析有下列 4 个主要目标：确定资产及其价值，识别脆弱性和威胁，量化潜在威胁的可能性与业务影响，在威胁的影响和对策的成本之间达到预算的平衡。
- 失效模式及影响分析(Failure Modes and Effect Analysis，FMEA)是一种确定功能、标识功能失效以及通过结构化过程评估失效原因和失效影响的方法。
- 故障树分析是一种有用的方法，用于检测复杂环境和系统中可能发生的故障。
- 定量风险分析会尝试为分析中的各个组件指派货币价值。
- 纯粹的定量风险分析是不可能的，因为定性项无法被精确量化。
- 在执行风险分析时，了解不确定性程度非常重要，因为它表明团队和管理层对于分析数据的信任程度。
- 自动化风险分析工具可以减少风险分析中的手动工作量。这些工具用于估计将来的预期损失，并计算各种不同安全措施的好处。
- 单一损失期望×年发生比率=年度损失期望(SLE×ARO=ALE)。
- 定性风险分析使用判断和直觉，而不是数字。
- 定性风险分析使富有经验的、接受过相关教育的人基于个人经验来评估威胁场景并估计每种威胁的可能性、潜在损失和严重程度。
- Delphi 技术是一种群体决策方法，此时每位成员都可以进行匿名沟通。
- 选择正确的防护措施以减弱某个特定的风险时，必须对成本、功能和效用进行评估，并且需要执行成本/收益分析。
- 安全策略是高级管理层决定的一个全面声明，它规定安全在组织机构内所扮演的角色。
- 措施是为了达到特定目标而应当执行的详细的、分步骤的任务。
- 标准指定如何使用硬件和软件产品，并且是强制性的。
- 基准是最小的安全级别。

- 指南是一些推荐和一般性方法，它们提供建议和灵活性。
- 工作轮换是一种检测欺诈的控制方法。
- 强制性休假是一种有助于检测欺诈活动的控制方法。
- 责任分离确保没有人能够完全控制一项活动或任务。
- 知识分割与双重控制是责任分离的两种方式。
- 数据分类将为数据分配优先级，从而确保提供合理的保护级别。
- 数据所有者指定数据的分类。数据看官员实施和维护控制措施，以强化集分类层级。
- 安全具有功能需求，它定义一个产品或系统的期望行为；此外还具有保证要求，它确定已实现产品或整个系统的可靠性。
- 管理层必须定义安全管理的范围和目的，提供支持，指定安全团队，委托职责，以及查看安全团队发现的结果。
- 风险管理团队应当包括来自组织机构内不同部门的人员，而不应该只是技术人员。
- 社会工程是非技术性攻击，指操纵某人向未获授权的个人提供敏感数据。
- 个人身份信息(PII)是指身份数据的集合，可被用于身份偷窃和金融欺诈，因此必须高度保护。
- 安全治理是提供监督、问责和合规的框架。
- ISO/IE C27004:2009 是信息安全变量管理的国际化标准。
- NIST800-55 是信息安全绩效考核的标准。

2.14.1　问题

请记住，这些问题的格式与提问的方式都是有原因的。必须记住的是，CISSP 考试在概念层次上提出问题。这些问题可能没有绝对正确的答案。我们建议考生不要总是寻求绝对正确的答案。相反，考生应当寻找最合适的答案。

1. Who has the primary responsibility of determining the classification level for information?

A. The functional manager

B. Senior management

C. The owner

D. The user

2. If different user groups with different security access levels need to access the same information, which of the following actions should management take?

A. Decrease the security level on the information to ensure accessibility and usability of the information.

B. Require specific written approval each time an individual needs to access the information.

C. Increase the security controls on the information.

D. Decrease the classification label on the information.

3. What should management consider the most when classifying data?

A. The type of employees, contractors, and customers who will be accessing the data

B. Availability, integrity, and confidentiality

C. Assessing the risk level and disabling countermeasures

D. The access controls that will be protecting the data

4. Who is ultimately responsible for making sure data is classified and protected?

A. Data owners

B. Users

C. Administrators

D. Management

5. Which factor is the most important item when it comes to ensuring security is successful in an organization?

A. Senior management support

B. Effective controls and implementation methods

C. Updated and relevant security policies and procedures

D. Security awareness by all employees

6. When is it acceptable to not take action on an identified risk?

A. Never. Good security addresses and reduces all risks

B. When political issues prevent this type of risk from being addressed

C. When the necessary countermeasure is complex

D. When the cost of the countermeasure outweighs the value of the asset and potential loss

7. Which is the most valuable technique when determining if a specific security control should be implemented?

A. Risk analysis

B. Cost/benefit analysis

C. ALE results

D. Identifying the vulnerabilities and threats causing the risk

8. Which best describes the purpose of the ALE calculation?

A. Quantifies the security level of the environment

B. Estimates the loss possible for a countermeasure

C. Quantifies the cost/benefit result

D. Estimates the loss potential of a threat in a span of a year

9. The security functionality defines the expected activities of a security mechanism, and assurance defines which of the following?

A. The controls the security mechanism will enforce

B. The data classification after the security mechanism has been implemented

C. The confidence of the security the mechanism is providing

D. The cost/benefit relationship

10. How do you calculate residual risk?

A. Threats×risks×asset value

B. (Threats×asset value×vulnerability)×risks

C. SLE×frequency = ALE

D. (Threats×vulnerability×asset value)×controls gap

11. Why should the team that will perform and review the risk analysis information be made up of people in different departments?

A. To make sure the process is fair and that no one is left out

B. It shouldn't. It should be a small group brought in from outside the organization because otherwise the analysis is biased and unusable

C. Because people in different departments understand the risks of their department. Thus, it ensures the data going into the analysis is as close to reality as possible

D. Because the people in the different departments are the ones causing the risks, so they should be the ones held accountable.

12. Which best describes a quantitative risk analysis?

A. A scenario-based analysis to research different security threats

B. A method used to apply severity levels to potential loss, probability of loss,and risks

C. A method that assigns monetary values to components in the risk assessment

D. A method that is based on gut feelings and opinions

13. Why is a truly quantitative risk analysis not possible to achieve?

A. It is possible, which is why it is used

B. It assigns severity levels. Thus, it is hard to translate into monetary values

C. It is dealing with purely quantitative elements

D. Quantitative measures must be applied to qualitative elements

14. What is CobiT and where does it fit into the development of information security systems and security programs?

A. Lists of standards, procedures, and policies for security program development

B. Current version of ISO 17799

C. A framework that was developed to deter organizational internal fraud

D. Open standards for control objectives

15. What are the four domains that make up CobiT?

A. Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate

B. Plan and Organize, Maintain and Implement, Deliver and Support, and Monitor and Evaluate

C.Plan and Organize, Acquire and Implement, Support and Purchase, and Monitor and Evaluate

D. Acquire and Implement, Deliver and Support, and Monitor and Evaluate

16. What is the ISO/IEC 27799 standard?

A. A standard on how to protect personal health information

B. The new version of BS 17799

C. Definitions for the new ISO 27000 series

D. The new version of NIST 800-60

17. CobiT was developed from the COSO framework. What are COSO's main objectives and purpose?

A. COSO is a risk management approach that pertains to control objectives and IT business processes

B. Prevention of a corporate environment that allows for and promotes financial fraud

C. COSO addresses corporate culture and policy development

D. COSO is risk management system used for the protection of federal systems

18. OCTAVE, NIST 800-30, and AS/NZS 4360 are different approaches to carrying out risk management within companies and organizations. What are the differences between these methods?

A. NIST 800-30 and OCTAVE are corporate based, while AS/NZS is international

B. NIST 800-30 and OCTAVE are IT based, while OCTAVE and AS/NZS 4360 are corporate based

C. AS/NZS is IT based, and OCTAVE and NIST 800-30 are assurance based

D. NIST 800-30 and AS/NZS are corporate based, while OCTAVE is international

Use the following scenario to answer Questions 19–21. A server that houses sensitive data has been stored in an unlocked room for the last few years at Company A. The door to the room has a sign on the door that reads "Room 1." This sign was placed on the door with the hope that people would not look for important servers in this room. Realizing this is not optimum security, the company has decided to install a reinforced lock and server cage for the server and remove the sign. They have also hardened the server's configuration and employed strict operating system access controls.

19. The fact that the server has been in an unlocked room marked "Room 1" for the last few years means the company was practicing which of the following?

A. Logical security

B. Risk management

C. Risk transference

D. Security through obscurity

20. The new reinforced lock and cage serve as which of the following?

A. Logical controls

B. Physical controls

C. Administrative controls

D. Compensating controls

21. The operating system access controls comprise which of the following?

A. Logical controls

B. Physical controls

C. Administrative controls

D. Compensating controls

Use the following scenario to answer Questions 22–24. A company has an e-commerce website that carries out 60 percent of its annual revenue. Under the current circumstances, the annualized loss expectancy for a website against the threat of attack is $92,000. After implementing a new application-layer firewall, the new annualized loss expectancy would be $30,000. The firewall costs $65,000 per year to implement and maintain.

22. How much does the firewall save the company in loss expenses?

A. $62,000

B. $3,000

C. $65,000

D. $30,000

23. What is the value of the firewall to the company?

A. $62,000

B. $3,000

C. –$62,000

D. –$3,000

24. Which of the following describes the company's approach to risk management?

A. Risk transference

B. Risk avoidance

C. Risk acceptance

D. Risk mitigation

Use the following scenario to answer Questions 25–27. A small remote office for a company is valued at $800,000. It is estimated, based on historical data, that a fire is likely to occur once every ten years at a facility in this area. It is estimated that such a fire would destroy 60 percent of the facility under the current circumstances and with the current detective and preventative controls in place.

25. What is the Single Loss Expectancy (SLE) for the facility suffering from a fire?

A. $80,000

B. $480,000

C. $320,000

D. 60%

26. What is the Annualized Rate of Occurrence (ARO)?

A. 1

B. 10

C. .1

D. .01

27. What is the Annualized Loss Expectancy (ALE)?

A. $480,000

B. $32,000

C. $48,000

D. .6

28. The international standards bodies ISO and IEC developed a series of standards that are used in organizations around the world to implement and maintain information security management systems. The standards were derived from the British Standard 7799, which was broken down into two main pieces. Organizations can use this series of standards as guidelines, but can also be certified against them by accredited third parties. Which of the following are incorrect mappings pertaining to the individual standards that make up the ISO/IEC 27000 series?

i. ISO/IEC 27001 outlines ISMS implementation guidelines, and ISO/IEC 27003 outlines the ISMS program's requirements

ii. ISO/IEC 27005 outlines the audit and certification guidance, and ISO/IEC 27002 outlines the metrics framework

iii. ISO/IEC 27006 outlines the program implementation guidelines, and ISO/IEC 27005 outlines risk management guidelines

iv. ISO/IEC 27001 outlines the code of practice, and ISO/IEC 27004 outlines the implementation framework

A. i, iii

B. i, ii

C. ii, iii, iv

D. i, ii, iii, iv

29. The information security industry is made up of various best practices, standards, models, and frameworks. Some were not developed first with security in mind, but can be integrated into an organizational security program to help in its effectiveness and efficiency. It is important to know of all of these different approaches so that an organization can choose the ones that best fit its business needs and culture. Which of the following best describes the approach(es) that should be put into place if an organization wants to integrate a way to improve its security processes over a period of time?

i. Information Technology Infrastructure Library should be integrated because it allows for the mapping of IT service process management, business drivers, and security improvement

ii. Six Sigma should be integrated because it allows for the defects of security processes to be identified and improved upon

iii. Capability Maturity Model should be integrated because it provides distinct maturity levels

iv. The Open Group Architecture Framework should be integrated because it provides a structure for process improvement

A. i, iii

B. ii, iii, iv

C. ii, iii

D. ii, iv

Use the following scenario to answer Questions 30–32. Todd is a new security manager and has the responsibility of implementing personnel security controls within the financial institution where he works. Todd knows that many employees do not fully understand how their actions can put the institution at risk; thus, an awareness program needs to be developed. He has determined that the bank tellers need to get a supervisory override when customers have checks over $3,500 that need to be cashed. He has also uncovered that some employees have stayed in their specific positions within the company for over three years. Todd would like to be able to investigate some of the bank's personnel activities to see if any fraudulent activities have taken place. Todd is already ensuring that two people must use separate keys at the same time to open the bank vault.

30. Todd documents several fraud opportunities that the employees have at the financial institution so that management understands these risks and allocates the funds and resources for his suggested solutions. Which of the following best describes the control Todd should put into place to be able to carry out fraudulent investigation activity?

A. Separation of duties

B. Rotation of duties

C. Mandatory vacations

D. Split knowledge

31. If the financial institution wants to force collusion to take place for fraud to happen successfully in this situation, what should Todd put into place?

A. Separation of duties

B. Rotation of duties

C. Social engineering

D. Split knowledge

32. Todd wants to be able to prevent fraud from taking place, but he knows that some people may get around the types of controls he puts into place. In those situations he wants to be able to identify when an employee is doing something suspicious. Which of the following incorrectly describes what Todd is implementing in this scenario and what those specific controls provide?

A. Separation of duties by ensuring that a supervisor must approve the cashing of a check over $3,500. This is an administrative control that provides preventative protection for Todd's organization

B. Rotation of duties by ensuring that one employee only stays in one position for up to three months of a time. This is an administrative control that provides detective capabilities

C. Security awareness training, which is a preventive administrative control that can also emphasize enforcement

D. Dual control, which is an administrative detective control that can ensure that two employees must carry out a task simultaneously

Use the following scenario to answer Questions 33–35. Sam has just been hired as the new security officer for a pharmaceutical company. The company has experienced many data breaches and has charged Sam with ensuring that the company is better protected. The company currently has the following classifications in place: public, confidential, and secret. There is a data classification policy that outlines the classification scheme and the definitions for each classification, but there is no supporting documentation that the technical staff can follow to know how to meet these goals. The company has no data loss prevention controls in place and only conducts basic security awareness training once a year. Talking to the business unit managers, he finds out that only half of them even know where the company's policies are located and none of them know their responsibilities pertaining to classifying data.

33. Which of the following best describes what Sam should address first in this situation?

A. Integrate data protection roles and responsibilities within the security awareness training and require everyone to attend it within the next 15 days

B. Review the current classification policies to ensure that they properly address the company's risks

C. Meet with senior management and get permission to enforce data owner tasks for each business unit manager

D. Audit all of the current data protection controls in place to get a firm understanding of what vulnerabilities reside in the environment

34. Sam needs to get senior management to assign the responsibility of protecting specific data sets to the individual business unit managers, thus making them data owners. Which of the following would be the most important in the criteria the managers would follow in the process

of actually classifying data once this responsibility has been assigned to them?

A. Usefulness of the data

B. Age of the data

C. Value of the data

D. Compliance requirements of the data

35. From this scenario, what has the company accomplished so far?

A. Implementation of administrative controls

B. Implementation of operational controls

C. Implementation of physical controls

D. Implementation of logical controls

Use the following scenario to answer Questions 36–38. Susan has been told by her boss that she will be replacing the current security manager within her company. Her boss explained to her that operational security measures have not been carried out in a standard fashion, so some systems have proper security configurations and some do not. Her boss needs to understand how dangerous it is to have some of the systems misconfigured along with what to do in this situation.

36. Which of the following best describes what Susan needs to ensure the operations staff creates for proper configuration standardization?

A. Dual control

B. Redundancy

C. Training

D. Baselines

37. Which of the following is the best way to illustrate to her boss the dangers of the current configuration issues?

A. Map the configurations to the compliancy requirements

B. Compromise a system to illustrate its vulnerability

C. Audit the systems

D. Carry out a risk assessment

38. Which of the following is one of the most likely solutions that Susan will come up with and present to her boss?

A. Development of standards

B. Development of training

C. Development of monitoring

D. Development of testing

2.14.2 答案

1. C。一个公司既可能只有一个指定的数据所有者，也可能由不同的数据所有者分别负责保护不同的数据。负责保护信息的人最应该对这些信息进行分类。

2. C。如果大批用户需要使用同一数据，那么就应当实现更细粒度的安全防护，以保证只有必要的人员才能访问这些数据，并且能够控制他们执行的操作。实现的安全措施包括身份验证和授权技术、加密以及特定的访问控制机制。

3. B。这个问题的最佳答案是 B。为了对数据进行适当的分类，数据所有者必须评估数据的

可用性、完整性和机密性要求。评估工作完成之后，哪些雇员、承包商和用户可以访问该数据自然也就清楚了，答案 A 表达了这个意思。这一评估还有助于确定应当实施哪些控制。

4. D。这个问题的关键在于“ultimately(最终)”这个单词。尽管管理层能够将具体的任务委托给其他人完成，但是公司内发生的任何事情最终还是需要他们负责。因此，必须长期确保数据和资源得到适当的保护。

5. A。没有高级管理层的支持，安全计划就无法得到必要的重视、资金、资源和实施能力。

6. D。如果消除风险所付出的代价有可能超过实际威胁所造成的潜在损失，那么公司就很可能决定对它们面临的特定风险不采取任何措施。对策总是很复杂，而且不同的风险总是有一些政治上的考虑，但是这些因素都不能成为不实现对策的理由。

7. B。尽管其他答案看起来也是对的，但 B 是最佳答案。这是因为，执行风险分析是为了识别风险并提供建议的对策。ALE 告诉公司实际发生特定威胁时可能造成的损失。ALE 的值可以用于成本/收益分析，但是 ALE 的目的并不是计算对策的成本和收益。答案 A、C 和 D 中的所有数据都可以用于成本/收益分析。

8. D。ALE 计算可以估计某一资产面对特定威胁时在一年内可能造成的损失。这个值用于计算为保护该资产远离特定威胁而应当投入的资金。

9. C。功能描述了一种安全机制的工作方式及其行为，与它实际提供的保护无关。保证是一种机制提供的保护级别的信任程度。在评估系统或机制时，它们的功能和保证应当分别查看和测试。

10. D。这个公式是概念性的，实际操作起来可能十分困难，因为很难对每个脆弱性和威胁进行量化并赋值。这个公式意味着，对于特定的资产，要查看潜在损失以及控制间隙(指的是具体对策不能提供的保护)。剩余风险是指实现安全对策之后仍然存在的风险。

11. C。一次风险分析结果的好坏取决于它所依赖的数据。公司使用的风险数据应当从最理解公司业务功能和环境的人那里获得。每个部门都理解他们自己的威胁和资源，并且可能已经知道对应特定威胁的解决方案。

12. C。定量风险分析为评估中的各个组件指派具体的金额和百分比。定性分析使用不同的个人观点对系统威胁的严重级别和对策的收益进行排序，并给出不同的等级。

13. D。在风险分析过程中，分析团队尝试正确地预测所有可能发生的风险。在某种程度上，它是一种主观的演习，必须使用有根据的猜测。有些风险很难预测，比如 10 年一遇的洪水给公司带来 4 万美元的损失，不过这正是定量分析试图完成的工作。

14. D。信息及相关技术控制目标 CobiT 是信息系统审计和控制协会(ISACA)与 IT 治理研究院(ITGI)共同开发的一个架构，它定义了应该用于正确管理 IT 并确保 IT 满足业务需求的控制措施的目标。

15. A。CobiT 分为 4 个领域：计划与组织，获取与实现，交付与支持，监控与评估。每个类别又细分为若干子类别。例如，“获取与实现”类别包括下列子类别：

- 获取和维护应用软件
- 获取和维护技术基础设施
- 开发和维护措施
- 安装和鉴定系统
- 管理变更

16. A。ISO/IEC 27799 标准针对健康信息学，其目的是指导保健机构和其他个人健康信息持有者如何通过实现 ISO/IEC 27002 来保护这些信息。

17. B。COSO 更多面向战略层面，CobiT 则更为关注操作层面。你可以将 CobiT 视为满足许

多 COSO 目标的一种方法，但是只能从 IT 角度来看。COSO 还处理非 IT 因素，如公司文化、财务会计原则、董事会职责以及内部通信结构。COSO 的主要目标是确保组织机构中不会出现虚假财务报告。

18. B。虽然 NIST 和 OCTAVE 方法都关注 IT 威胁和信息安全风险，不过 AS/NZS 4360 采取了一种更广泛的方法来进行风险管理。这种方法能够用于了解公司的财政、资本、人员安全和业务决策风险。尽管它能够用于分析安全风险，但是并非专门针对这个目标而创建的。

19. D。通过隐匿实现安全并没有实施真正的安全控制，而是通过试图隐藏资产脆弱的事实寄希望于攻击者不会注意。通过隐匿实现安全是试图欺骗潜在攻击者的方法，这是实践安全的糟糕方法。脆弱性应该被识别和修补，而不是被隐藏。

20. B。物理控制是物理世界的安全机制，如锁、篱笆、门、计算机笼等。有 3 种主要控制类型，它们是管理、技术和物理控制。

21. A。逻辑控制(或者技术控制)是安全机制，如防火墙、加密、软件权限和身份验证设备。它们常常和物理及管理控制联合使用来提供深度安全方法。

22. A。62 000 美元是正确答案。防火墙将年度损失期望(ALE)从 92 000 美元降至 30 000 美元。计算 ALE 的公式是单一损失期望(SLE)×年发生比率=ALE。从防火墙安装之前的值中减去安装了之后的 ALE 值，结果便是这类控制所节省的损失。

23. D。－3000 美元是正确答案。防火墙节省了 62 000，但是每年的成本是 65 000 美元，62000－65000=－3000。防火墙的实际成本高于它能带来的收益，因此结果是负数。其计算公式是(控制实施之前的 ALE)－(控制实施之后的 ALE)－(年控制成本)=控制值。

24. D。降低风险指使用控制措施试图降低事件发生的可能性或者事件带来的损失或者二者兼有。处理风险的 4 种方法为接受风险、规避风险、转移风险和减少风险。安装防火墙是降低威胁带来的风险的举措。

25. B。480 000 美元是正确答案。单一损失期望(SLE)的计算公式是资产×暴露因子(EF)=SLE。即资产(800 000 美元)×暴露因子(60%)=480 000 美元。这意味着公司因为这类威胁可能会造成资产(设施)潜在损失达 480 000 美元。

26. C。年发生率(annualized rate occurrence，ARO)指威胁在 12 个月内最有可能出现的频率。它是用于 ALE 公式中的一个值，即 SLE×ARO=ALE。

27. C。48 000 美元是正确答案。用年度损失期望的公式(SLE×ARO=ALE)来计算一项资产在一年 12 个月内经受威胁所造成的损失。得到的 ALE 值有助于确定为保护资产所花费的合理成本。在这个题中，公司为保护这个资产免受大火威胁所花费的代价不应该超过 48 000 美元。ALE 值有助于组织对所面临的风险的严重程度进行排序，从而知道应该首先应对哪些威胁、每种威胁应该花费多少来应对。

28. D。CISSP 考试总是有这样容易混淆的题目出现，需要做好准备。ISO/IEC 标准的正确搭配如下：

- ISO/IEC 27001　ISMS 需求
- ISO/IEC 27002　信息安全管理的实践准则
- ISO/IEC 27003　ISMS 实现指南
- ISO/IEC 27004　信息安全管理的度量及度量指标框架指南
- ISO/IEC 27005　信息安全风险管理指南
- ISO/IEC 27006　提供信息安全管理系统审计和认证的实体指南

29. C。这个列表当中提供的最佳流程改进方法是六西格玛和能力成熟度模型。下面是这个题

目中所提到的各项目的定义：

- TOGAF　The Open Group(开放小组)开发的企业架构开发模型和方法。
- ITIL　英国政府商务办公室指定的 IT 服务管理流程。
- 六西格玛　用来进行流程改进的业务管理战略。
- 能力成熟度模型(CMMI)　卡耐基・梅隆开发的组织流程改进开发模型。

30. C。强制休假是管理检测控制方法，指组织调查员工的日常业务活动从而发现可能正在发生的隐藏和潜在欺诈行为。员工应该被强制调离开组织两个星期的时间，然后另外一个人代替他。从而希望被轮换过来的人能够检测到可疑活动。

31. A。职责分离是一种管理控制，确保关键任务不是由一个人来执行。如果一个人能够单独执行一项关键任务，这会使组织处于风险之中。两人或多人一起进行欺诈称为共谋。所以，如果一个任务由两个人承担，他们必须共谋才能完成任务并进行欺诈。

32. D。相互控制是一种行政管理预防控制。它确保两个人必须同时执行一项任务，就好比开金库时需要两个人分别用钥匙打开。这不是检测控制。注意这个问题问的是 Todd 不做什么。记住，在考试中需要选出最佳答案。许多情况下，都会不喜欢 CISSP 考试中的问题或相应答案，要有思想准备。问题可能很绕，这也是这个考试难的一个原因。

33. B。对于 Sam 来说每个答案都是好事，但最先需要做的是确保策略能恰当解决公司对于数据分类和保护的需求。策略提供方向，所有其他的文档(标准、程序和指南)和安全控制都派生自这些策略并对策略提供支持。

34. C。数据对于任何组织来说都是最关键的资产之一。必须了解资产的价值，这样组织才能知道哪项资产需要最大的保护。计算一项资产的价值有许多组件：替换成本、资产产生的收入、对手为这项资产付费的多少、开发这项资产的成本、如果资产没了或被破坏后的生产成本以及没有适当保护资产的责任成本。所以数据所有者需要能够判断数据对于组织的价值，从而进行适当分类。

35. A。公司制定了一项数据分类策略，这是行政管理控制。

36. D。操作人员需要知道网络内每个系统所需要的最低安全水平。最低安全水平是一个底线。一旦为每个系统设定了安全底线，那么工作人员就有了参照来比较系统的情况，知道如果变化不正常，哪个会使系统变得脆弱。

37. D。Susan 需要向老板说明这些脆弱性(错误配置系统)的风险情况。这意味着她需要识别具体的脆弱性，这些脆弱性会带来的相关威胁，并计算风险。这会使其老板了解这些问题是多么关键，也就知道需要采取什么措施了。

38. A。需要开发一个标准，列明适当的配置管理流程和核准的基本配置设置。一旦开发且应用了这些标准，就得对员工就这些问题和如何实施与维护标准中所规定的事宜进行培训。根据这些标准测试系统，也可以根据这些标准来监控系统，检测系统是否有不符合标准中所列需求的配置。会发现 CISSP 问题有些似乎很主观，答案很难敲定。像问什么“最好”或者“最有可能”的问题很常见。