高等学校网络空间安全专业“十三五”规划教材

信息安全管理与风险评估

毕方明　编著

西安电子科技大学出版社
http://www.xduph.com

高等学校 网络空间安全专业“十三五”规划教材

信息安全管理与风险评估

毕方明 编著

西安电子科技大学出版社

内 容 简 介

本书通过对信息安全风险评估领域的研究，在汲取国内外研究成果的基础上，总结信息安全风险评估的发展趋势与研究要点，对常用风险评估方法进行分析，提出几种改进的信息安全风险评估方法，详细介绍了所提出的改进评估方法的评估流程与特点，并通过评估实例与代码实现，加深读者对所介绍的评估方法的认识。

本书可供信息安全专业及相关专业本科生、技术人员、研究人员参考，方便此类人员抓住风险评估的要点，掌握风险评估方法与使用步骤，为进一步的风险评估研究与使用打下坚实的基础。

图书在版编目(CIP)数据

信息安全管理与风险评估/毕方明编著. —西安：西安电子科技大学出版社，2018.8
ISBN 978-7-5606-4985-6

Ⅰ.① 信… Ⅱ.① 毕… Ⅲ.① 信息安全—安全管理—研究 ② 信息安全—安全评价—研究 Ⅳ.① TP309

中国版本图书馆 CIP 数据核字(2018)第 153681 号

策划编辑 高 樱
责任编辑 宁晓青 阎 彬
出版发行 西安电子科技大学出版社(西安市太白南路 2 号)
电 话 (029)88242885 88201467 邮 编 710071
网 址 www.xduph.com 电子邮箱 xdupfxb001@163.com
经 销 新华书店
印刷单位 陕西天意印务有限责任公司
版 次 2018 年 8 月第 1 版 2018 年 8 月第 1 次印刷
开 本 787 毫米×1092 毫米 1/16 印张 11
字 数 252 千字
印 数 1～3000 册
定 价 25.00 元
ISBN 978-7-5606-4985-6/TP

XDUP 5287001-1

高等学校 网络空间安全专业“十三五”规划教材
编审专家委员会名单

前　言

伴随着信息技术的飞速发展，信息安全问题也变得日益严峻。信息安全风险评估作为预防和控制信息安全风险的重要手段，对解决信息安全问题起着至关重要的作用。本书以信息安全风险评估方法和现代化的分析模型为研究对象，对现有的风险评估方法进行深入研究，以期对现有的风险评估方法与模型进行改进，寻求更加高效的、准确的信息安全风险评估与控制手段。

本书共8章。

第1章对风险评估所涉及的基本概念进行了简单介绍，概括性地介绍了信息安全与信息安全风险评估的相关概念，还介绍了国内外风险评估的研究现状，总结了信息安全风险评估的发展趋势。

第2章主要介绍风险评估的评估流程与方法。首先介绍了风险评估的基本分类；之后简单概括了风险评估的流程；最后对常见的风险评估方法进行了介绍并比较了不同方法的特点。

第3章介绍风险分析的相关技术标准与评估工具。在评估标准方面，主要介绍了BS 7799/ISO 17799/ISO 27002、ISO/IEC TR 13335、OCTAVE 2.0、CC/ISO 15408/GB/T 18336等标准和风险评估等级保护；评估工具方面，详细介绍了几种常见的风险评估和管理工具，以及相应的辅助工具。

第4章是基于层次分析法的信息安全风险评估。首先对层次分析法的基本概念进行了相关介绍，然后通过评估模型与案例详细介绍了该方法的使用过程，并在章节末尾介绍总结了案例的实现过程以及相关代码。

第5章是对基于网络层次分析法的信息安全风险评估方法的研究。首先介绍了该方法的原理与基本流程，之后基于该方法建立了相应的风险评估模型，并将建立的评估模型用于某公司保密系统的风险评估，通过分析评估结果可以发现，基于网络层次分析法的风险评估方法可以有效地改善传统层次分析法难以反映风险因素间相互影响关系的缺陷，且该方法在实际应用中有着良好的使用效果。

第6章介绍了一种基于风险因子的信息安全风险评估方法，通过引入风险因子的概念来衡量风险因素之间的关系，并通过相应的风险评估案例对整个方法的流程进行了详细介绍。

第 7 章是对另一种基于三角模糊数的信息安全分析方法的研究。该方法结合常用的信息安全风险分析方法，通过引入三角模糊数减少评估过程中的主观性，使风险评估的结果更加客观公正。本章详细介绍了该方法的原理与评估模型，并通过仿真实例证明该模型的实用性。

第 8 章主要介绍基于灰关联分析方法的风险评估，通过灰色关联分析来获取不同风险因素之间的数值关系，并以此为依据对整个系统进行风险评估。本章通过介绍基于灰关联的风险评估方法，并结合代码与案例分析使读者对该方法有更清晰的认识。

本书详细介绍了几种风险评估的改进方法，并通过具体的风险评估实例与代码实现，使读者能够清晰地认识到风险评估方法的流程与特点，把握信息安全风险评估的研究方向，为进一步理解、研究和使用信息安全风险评估方法打下基础。

本书可供信息安全专业及相关专业本科生、技术人员、研究人员参考，有助于加深读者对信息安全风险评估的基本认识，把握信息安全风险评估方法的研究方向。

由于时间仓促，编者水平有限，书中不足与疏漏之处在所难免，恳请读者批评指正。

作　者

2018 年 3 月

目　录

传输、处理和存储的对象，如技术文档、存储介质、各种信息等；二是指使用的各种软件；三是安全管理手段的密钥和口令等信息。

目前使用最广泛的网络通信协议是 TCP/IP 协议。由于存在许多安全设计缺陷，网络信息常常面临许多威胁。网络管理软件是安全管理的重要组成部分，常用的有 HP 公司的 OpenView、IBM 公司的 NetView、SUN 公司的 NetManager 等，当然也需要额外的安全措施。

(1) 存储介质的安全管理。存储介质包括纸介质、磁盘、光盘、磁带、录音/录像带等，它们的安全对信息系统的恢复、信息的保密、防病毒起着十分关键的作用。对不同类别的存储介质，安全管理要求也不尽相同。对存储介质的安全管理主要考虑存储管理、使用管理、复制和销毁管理、涉密介质的安全管理。

(2) 技术文档的安全管理。技术文档是系统或网络在设计、开发、运行和维护中所有技术问题的文字描述。技术文档按其内容的涉密程度进行分级管理，一般分为绝密级、机密级、秘密级和公开级。对技术文档的安全管理主要考虑文档的使用、备份、借阅、销毁等方面，需要建立严格的管理制度并指定相关负责人。

(3) 软件设施的安全管理。对软件设施的安全管理主要考虑配置管理、使用和维护管理、开发管理和病毒管理。软件设施主要包括操作系统、数据库系统、应用软件、网络管理软件以及网络协议等。操作系统是整个计算机系统的基石，由于它的安全等级不高，需要提供不同安全等级的保护。对数据库系统，需要加强数据库的安全性，并采用加密技术对数据库中的敏感数据加密。

(4) 密钥和口令的安全管理。密钥是加密解密算法的关键，密钥管理就是对密钥的生成、检验、分配、保存、使用、注入、更换和销毁等过程所进行的管理。口令是进行设备管理的一种有效手段，对口令的产生、传送、使用、存储、更换均需要进行有效的管理和控制。

4. 运行的安全管理

信息系统和网络在运行中的安全状态也是需要考虑的问题，目前常常关注安全审计和安全恢复两个安全管理问题。

(1) 安全审计。安全审计是指对系统或网络运行中有关安全的情况和事件进行记录、分析并采取相应措施的管理活动。目前主要对操作系统及各种关键应用软件进行审计。安全审计工作应该由各级安全机构负责实施管理，安全审计可以采用人工审计、半自动审计或自动智能审计三种方式。人工审计一般通过审计员查看、分析、处理审计记录；半自动审计一般由计算机自动分析处理，再由审计员作出决策和处理；自动智能审计一般由计算机完成分析处理，并借助专家系统作出判断，更能满足不同应用环境的需求。

(2) 安全恢复。安全恢复是指网络和信息系统在受到灾难性打击或破坏时，为使网络和信息系统迅速恢复正常，并使损失降低到最小而进行的一系列活动。安全恢复的管理主要包括安全恢复策略的确立、安全恢复计划的制订、安全恢复计划的测试和维护及安全恢复计划的执行。

1.2 信息安全风险评估的概念

信息安全风险评估是从风险管理的角度，运用科学的手段，系统地分析网络与信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，为防范和化解信息安全风险，或者将风险控制在可以接受的水平，制订有针对性的抵御威胁的防护对策和整改措施，以最大限度地保障网络和信息安全提供科学依据。

1.2.1 信息安全风险的相关概念

信息系统是用于采集信息、组织信息、存储信息、传输信息的有组织的系统。更具体地说，它是研究人员和组织用于收集、过滤、处理、创建和分发数据的互补网络。

信息安全即保护组织的数据免遭未经授权的访问或修改，以确保其保密性、完整性和可用性。保密性意味着系统上可用的信息对于未经授权的人员应该是安全的，比如客户的信用卡、医保卡中的信息等；完整性则意味着可用的信息应该是完整的，任何未经授权的人都不能够改变它，如果信息由于某种攻击而受到严重损害，那么这个信息将由于完整性受损而变得不可靠；可用性同前两种属性一样重要，即授权用户请求或要求的信息应该始终可用。除此之外，信息安全可能还涉及保护和保存信息的真实性与可靠性，并确保实体可以追究责任。

信息安全风险评估是发现、纠正和预防安全问题的持续过程。风险评估作为风险管理流程的一个组成部分，旨在为信息系统提供适当级别的安全性，帮助机构确定可接受的风险水平以及由此产生的每个系统的安全性要求。

1.2.2 信息安全风险的基本要素

从信息安全的角度来讲，风险评估是对信息资产所面临的威胁、存在的弱点、造成的影响，以及三者的综合作用在当前安全措施控制下所带来的与安全需求不符合的风险的可能性进行评估。作为风险管理的基础，风险评估是组织进一步确定信息安全需求和改进信息安全策略的重要途径，属于组织信息安全管理体系策划的过程。

信息系统是信息安全风险评估的对象，信息系统中的资产、信息系统面临的可能威胁、系统中存在的脆弱性、安全风险、安全风险对业务的影响，以及系统中已有的安全控制措施和系统的安全需求等构成了信息安全风险评估的基本要素。

1. 资产(Asset)

资产是指对组织具有价值的信息或资源，是安全策略保护的对象。资产能够以多种形式存在，包括有形的或无形的、硬件或软件、文档或代码，以及服务或形象等诸多表现形式。

在信息安全体系范围内为资产编制清单是一项重要工作，每项资产都应该清晰地定

义、合理地估价，并明确资产所有权关系，进行安全分类，记录在案。根据资产的表现形式，可将资产分为软件、硬件、服务、流程、数据、文档、人员等，如表 1-1 所示。

表 1-1　资产分类

分　类	说　明
软件	系统软件：操作系统、语言包、开发系统、各种库/类等 应用软件：办公软件、数据库软件、工具软件等 源程序：各种共享源代码、可执行程序、开发的各种代码等
硬件	系统和外围设备：包括各种计算机设备 、网络设备、存储设备、传输及保障设备等 安全设备：防火墙、IDS(Intrusion Detection System，入侵检测系统)、指纹识别系统等 其他技术设备：打印机、复印机、扫描仪、供电设备、空调设备等
服务	信息服务：对外依赖该系统开展业务而取得业务收入的服务 网络通信服务：各种网络设备、设施提供的网络连接服务 办公服务：各种 MIS(Management Information System，管理信息系统)提供的为提高工作效率的服务 其他技术服务：照明、电力、空调、供热等
流程	包括 IT 和业务标准流程、IT 和业务敏感流程，其中敏感流程具有给组织带来攻击或引入风险的潜在可能，如电信公司在新开通线路时可能会引入特殊风险
数据	在传输、处理和存储状态的各种信息资料，包括源代码、数据库数据、系统文档、运行管理规程、计划、报告、用户手册、各类纸质上的信息等
文档	纸质的各种文件、传真、财务报告、发展计划、合同等
人员	除了掌握重要信息和核心业务的人员之外，如主机维护主管、网络维护主管、应用项目经理、网络研发人员等，还包括其他可以访问信息资产的组织外用户
其他	企业形象与声誉、客户关系等

2. 威胁(Threat)

威胁是指可能对组织或资产造成损害的潜在原因，即威胁有可能导致不期望发生的安全事件发生，从而对系统、组织、资产造成损害。这种损害可能是偶然性事件，但更多的可能是蓄意的对信息系统和服务所处理信息的直接或间接的攻击行为，例如非授权的泄露、修改、停机等。威胁主要来源于环境因素和人为因素，其中人为因素包括恶意攻击和非恶意攻击。

(1) 环境因素：指地震、火灾、水灾、电磁干扰、静电、灰尘、潮湿等环境危害，以及软件、硬件、数据、通信线路等方面的故障。

(2) 恶意攻击：对组织不满的或有目的的人员对信息系统进行恶意破坏，会对信息的机密性、完整性和可用性等造成损害。

(3) 非恶意攻击：由于缺乏责任心、安全意识或专业技能不足等原因而导致信息系统故障、被破坏或被攻击，本身无恶意企图。

根据威胁来源，可对威胁进行分类，如表 1-2 所示。

表 1-2　威胁分类

分　类	说　明
软硬件故障	对业务实施或系统运行产业影响的设备硬件故障、存储介质故障、通信链路中断、系统本身或软件缺陷等
物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然灾害，如地震、火灾、电磁干扰、静电、灰尘、潮湿、鼠蚁虫害等
物理攻击	通过物理的接触造成对软件、硬件或数据的破坏，如物理接触性损害、物理性破坏、盗窃等
恶意代码	在计算机系统上能执行恶意任务的程序代码，如病毒、特洛伊术马、蠕虫、间谍软件、窃听软件等
越权或滥用	对信息、信息系统、网络和网络服务的非授权访问，或滥用自己的权限，做出破坏信息系统的行为，如非正常修改系统配置或数据、滥用权限泄密等
网络攻击	利用工具和技术通过网络对信息系统进行攻击和入侵，如网络探测和信息采集、漏洞扫描、口令嗅探、用户身份伪造和欺骗等
泄密	信息泄露给不应了解的人，这包括内部信息泄露和外部信息泄露等
篡改	非法修改信息，破坏信息的完整性，使系统的安全性降低或信息不可用，如篡改网络配置信息、篡改用户身份信息或业务数据信息等
抵赖	否认收到的信息或所进行过的操作和交易等
管理不到位	安全管理无法落实或不到位，从而破坏信息系统的正常有序运行，如管理制度不完善、监督机制不健全等
无作为性失误	应该执行而没有执行相应的操作，或无意执行了错误的操作等

3. 脆弱性(Vulnerability)

脆弱性是指可能被威胁所利用的资产或若干资产的薄弱环节，例如操作系统存在漏洞、对数据库的访问没有访问控制机制、系统机房没有门禁系统等。

脆弱性是资产本身存在的，如果没有相应的威胁，单纯的脆弱性本身不会对资产造成损害，而且如果系统足够强健，则再严重的威胁也不会导致安全事件发生，从而造成损失。这说明，威胁总是要利用资产的脆弱性来产生危害。

资产的脆弱性具有隐蔽性，有些脆弱性只在一定条件和环境下才能显现，这也是脆弱性识别中最为困难的部分。要注意的是，不正确的、起不到应有作用的或没有正确实施的安全控制措施本身就可能是一种脆弱性。

脆弱性主要表现在技术和管理两个方面，如表 1-3 所示。其中技术脆弱性是指信

息系统在设计、实现和运行时，涉及的物理层、网络层、系统层、应用层等各个层面在技术上存在的缺陷或弱点；管理脆弱性则是指组织管理制度、流程等方面存在的缺陷或不足。

表 1-3　资产脆弱性分类

分　类	示　例	说　明
技术脆弱性	未安装杀病毒软件	能发生系统信息被病毒侵害
	使用口令不当	能导致系统信息的非授权访问
	无保护的外网连接	能破坏联网系统中存储与处理信息的安全性
管理脆弱性	安全培训不足	能造成用户缺乏足够的安全意识，或产生用户错误
	机房钥匙管理不严	能形成资产的直接丢失或物理损害等
	离职人员权限未撤销	能引起泄密或业务活动受到损害

1.3　信息安全风险管理体系

信息安全管理体系(Information Security Management System，ISMS)是 1998 年前后从英国发展起来的信息安全领域中的一个新概念，是管理体系(Management System，MS)思想和方法在信息安全领域的应用。近年来，伴随着 ISMS 国际标准的修订，ISMS 迅速被全球接受和认可，成为世界各国、各种类型、各种规模的组织解决信息安全问题的一个有效方法。ISMS 认证随之成为组织向社会及其相关方证明其信息安全水平和能力的一种有效途径。

信息安全管理体系是组织机构单位按照信息安全管理体系相关标准的要求，制定信息安全管理方针和策略，采用风险管理的方法进行信息安全管理计划、实施、评审检查、改进的信息安全管理执行的工作体系。信息安全管理体系是按照 ISO/IEC 27001 标准《信息技术　安全技术　信息安全管理体系要求》建立的，ISO/IEC 27001 标准是由 BS7799-2 标准发展而来的。

信息安全管理体系 ISMS 是建立和维持信息安全管理体系的标准，标准要求组织通过确定信息安全管理体系范围、制定信息安全方针、明确管理职责、以风险评估为基础选择控制目标与控制方式等活动建立信息安全管理体系；体系一旦建立组织应按体系规定的要求进行运作，保持体系运作的有效性；信息安全管理体系应形成一定的文件，即组织应建立并保持一个文件化的信息安全管理体系，其中应阐述被保护的资产、组织风险管理的方法、控制目标及控制方式和需要的保证程度。

1.3.1 ISMS 的范围

ISMS 的范围可以根据整个组织或者组织的一部分进行定义，包括相关资产、系统、应用、服务、网络和用于过程中的技术、存储以及通信的信息等，ISMS 的范围包括：

(1) 组织所有的信息系统；

(2) 组织的部分信息系统；

(3) 特定的信息系统。

此外，为了保证不同的业务利益，组织需要为业务的不同方面定义不同的 ISMS。例如，可以为组织和其他公司之间特定的贸易关系定义 ISMS，也可以为组织结构定义 ISMS，不同的情境可以由一个或者多个 ISMS 表述。

组织内部成功实施信息安全管理的关键因素在于：

(1) 反映业务目标的安全方针、目标和活动；

(2) 与组织文化一致的实施安全的方法；

(3) 来自管理层的有形支持与承诺；

(4) 对安全要求、风险评估和风险管理的良好理解；

(5) 向所有管理者及雇员推行安全意识；

(6) 向所有雇员和承包商分发有关信息安全方针和准则的导则；

(7) 提供适当的培训与教育；

(8) 用于评价信息安全管理绩效及反馈改进建议，并有利于综合平衡的测量系统。

1.3.2 信息安全管理体系的作用

信息安全管理体系是一个系统化、程序化和文件化的管理体系。该体系具有以下特点：

(1) 体系的建立基于系统、全面、科学的安全风险评估，体现以预防控制为主的思想，强调遵守国家有关信息安全的法律法规及其他合同方的要求；

(2) 强调全过程和动态控制，本着控制费用与风险平衡的原则合理选择安全控制方式；

(3) 强调保护组织所拥有的关键性信息资产，而不是全部信息资产，确保信息的机密性、完整性和可用性，保持组织的竞争优势和商务运作的持续性。

组织建立、实施与保持信息安全管理体系将会产生如下作用：

(1) 强化员工的信息安全意识，规范组织信息安全行为；

(2) 对组织的关键信息资产进行全面系统的保护，维持竞争优势；

(3) 在信息系统受到侵袭时，确保业务持续开展并将损失降到最低程度；

(4) 使组织的生意伙伴和客户对组织充满信心；

(5) 如果通过体系认证，表明体系符合标准，证明组织有能力保证重要信息，提高组织的知名度与信任度；

(6) 促使管理层贯彻信息安全保障体系；

(7) 组织可以参照信息安全管理模型，按照先进的信息安全管理标准 BS7799 建立组织完整的信息安全管理体系并实施与保持，达到动态的、系统的、全员参与、制度化的、以预防为主的信息安全管理方式，用最低的成本，达到可接受的信息安全水平，从根本上保证业务的连续性。

1.3.3　PDCA 原则

PDCA 循环的概念最早是由美国质量管理专家戴明提出来的，所以又称为“戴明环”，它在质量管理中应用广泛。PDCA 代表的含义如下：

P(Plan)：计划，确定方针和目标，确定活动计划；

D(Do)：实施，实际去做，实现计划中的内容；

C(Check)：检查，总结执行计划的结果，注意效果，找出问题；

A(Action)：行动，对总结检查的结果进行处理，成功的经验加以肯定并适当推广、标准化；失败的教训加以总结，以免重现；未解决的问题放到下一个 PDCA 循环。

PDCA 循环的四个阶段具体内容如下：

(1) 计划阶段：制订具体工作计划，提出总的目标。具体来讲又分为以下四个步骤。

① 分析目前现状，找出存在的问题；

② 分析产生问题的各种原因以及影响因素；

③ 分析并找出管理中的主要问题；

④ 制订管理计划，确定管理要点。

根据管理体制中出现的主要问题，制订管理的措施、方案，明确管理的重点。制定管理方案时要注意整体的详尽性、多选性、全面性。

(2) 实施阶段：指按照制订的方案去执行。

在管理工作中全面执行制订的方案。制订的管理方案在管理工作中执行的情况，直接影响全过程。所以在实施阶段要坚持按照制订的方案去执行。

(3) 检查阶段：检查实施计划的结果。

检查工作这一阶段是比较重要的一个阶段，它是对实施方案是否合理，是否可行有何不妥的检查，是为下一个阶段工作提供条件，是检验上一阶段工作好坏的检验期。

(4) 行动阶段：根据调查效果进行处理。

对已解决的问题，加以标准化，即把已成功的可行的条文进行标准化，将这些纳入制度、规定中，防止以后再发生类似问题。

找出尚未解决的问题，转入下一个循环中，以便解决。

PDCA 循环实际上是有效进行任何一项工作的合乎逻辑的工作程序。在质量管理中，PDCA 循环得到了广泛的应用，并取得了很好的效果，有人也称其为质量管理的基本方法。之所以叫 PDCA 循环，是因为这四个过程不是运行一次就完结，而是周而复始地进行，其特点是“大环套小环，一环扣一环，小环保大环，推动大循环”。每个循环系统包括 PDCA 四个阶段螺旋式上升和发展，每循环一次要求提高一步。

建立和管理一个信息安全管理体系需要像其他任何管理体系一样的方法。这里描述的过程模型遵循一个连续的活动循环：计划、实施、检查和处置。之所以可以描述为一个有效的循环，是因为它的目的是保证组织的最好实践文件化、加强并随时间改进。信息安全管理体系的 PDCA 过程如图 1-1 所示。

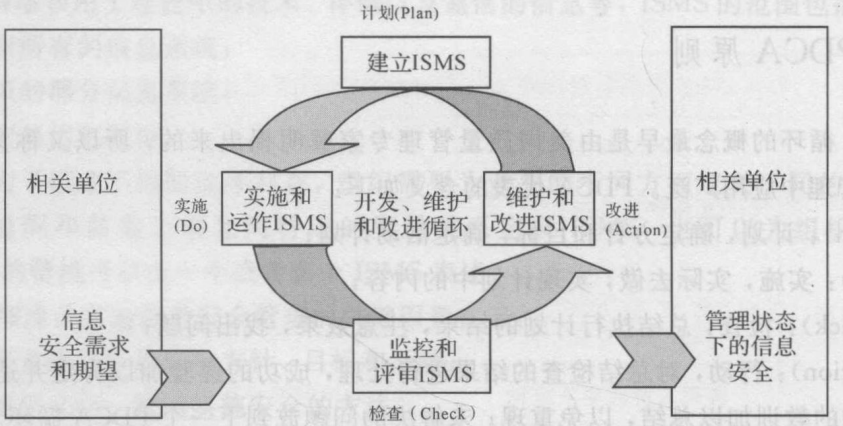

图 1-1　PDCA 模型与信息安全管理体系过程

1.3.4　ISMS 的 PDCA

1. 计划阶段

计划阶段的主要任务在于确定控制目标与控制方式，目的是保证正确地建立 ISMS 的内容和范围、识别和评估所有的信息安全风险，开发合适的风险处理计划。该阶段的要点在于：

1）确定信息安全方针

安全方针是在一个组织内，指导如何对信息资产进行管理、保护和分配的规则、指示，是组织信息安全管理体系的基本法。组织的信息安全方针，描述信息安全在组织内的重要性，表明管理层的承诺，提出组织管理信息安全的方法，为组织的信息安全管理提供方向和支持。

2）确定信息安全管理体系的范围

信息安全管理体系可以覆盖组织的全部或者部分。无论是全部还是部分，组织都必须明确界定体系的范围，如果体系仅涵盖组织的一部分这就变得更重要了。组织需要文件化信息安全管理体系的范围。

3）制定风险识别和评估计划

确定信息安全风险评估方法，并确定风险等级准则。评估方法应该和组织既定的信息安全管理体系范围、信息安全需求、法律法规要求相适应，兼顾效果和效率。组织需要建立风险评估文件，解释所选择的风险评估方法、说明为什么该方法适合组织的安全要求和业务环境，介绍所采用的技术和工具，以及使用这些技术和工具的原因。

4）制定风险控制计划

根据资产保密性、完整性和可用性丢失的潜在影响，评估由于安全失败(failure)可能