<<信息安全管理>>

图书基本信息

书名：<<信息安全管理>>

13位ISBN编号：9787563516711

10位ISBN编号：7563516719

出版时间：2008-6

出版时间：北京邮电大学出版社

作者：徐国爱，彭俊好，张淼 编著

页数：307

<<信息安全管理>>

内容概要

本书作为信息安全系列教材之一，在汇总作者及所在团队多年来信息安全管理相关工作的基础上，还提炼了国内和国际上信息安全管理方面的最新成果。
本书在保证知识点讲解精炼的基础上，全面吸纳了最新国内外信息安全管理相关标准和指南的内容，能够反映出信息安全管理理及与方法的研究和应用现状。
本书内容共9章。
第1章是绪论。
第2章是信息安全控制规范。
第3章是信息系统安全审计。
第4章是信息安全事件管理。
第5章是信息安全风险评估。
第6章是信息安全管理体系实施。
第7章是信息安全测评认证。
第8章是信息安全工程管理。
第9章是信息安全法规标准。
本书适用于高等院校通信专业本科教材，也可作为相关专业技术人员的参考书目。

<<信息安全管理>>

书籍目录

第1章 绪论　1.1 信息安全管理　1.2 信息安全技术体系　1.3 信息安全管理方法　1.4 信息安全保障体系　1.5 本书的内容安排　习题第2章 信息安全控制规范　2.1 概述　2.2 信息安全策略　2.3 信息安全组织　2.4 资产分类和管理　2.5 人员安全　2.6 物理和环境的安全　2.7 通信和运营管理　2.8 访问控制　2.9 系统的开发与维护　2.10 业务连续性管理　2.11 符合性　本章小结　习题第3章 信息系统安全审计　3.1 概述　3.2 安全审计系统的体系结构　3.3 安全审计的一般流程　3.4 安全审计的分析方法　3.5 安全审计的数据源　3.6 信息安全审计与标准　3.7 计算机取证　本章小结　习题第4章 信息安全事件管理　4.1 概述　4.2 信息安全事件管理过程　4.3 信息安全事件分类分级　4.4 应急响应　4.5 信息安全灾难恢复　本章小结　习题第5章 信息安全风险评估　5.1 概述　5.2 信息安全风险评估策略　5.3 信息安全风险评估流程　5.4 信息安全风险评估方法　5.5 风险评估案例　本章小结　习题第6章 信息安全管理体系实施　6.1 概述　6.2 ISMS实施模型　6.3 ISMS实施过程　6.4 ISMS文件要求　6.5 ISMS审核　6.6 ISMS持续改进　6.7 ISMS实施案例　6.8 信息安全管理工具　本章小结　习题第7章 信息安全测评认证　7.1 概述　7.2 测评认证有关规范　7.3 测评技术　7.4 信息安全测评实施案例　本章小结　习题第8章 信息安全工程管理　8.1 概述　8.2 MM概念　8.3 模型体系结构　8.4 能力级别概述　8.5 安全性工程过程区　8.6 SSE-CMM的使用　本章小结　习题第9章 信息安全法规标准　9.1 概述　9.2 国外信息安全法规　9.3 我国信息安全法规　9.4 国外信息安全标准　9.5 我国信息安全标准　本章小结　习题参考文献

章节摘录

第2章　信息安全控制规范信息安全管理是保障信息系统安全的有力手段，是当今世界各国都在努力推广与应用的重点课题。
它涉及的内容非常广泛，包括安全组织架构、安全管理制度、人员安全、物理安全、通信安全、访问控制、业务连续性和法律法规符合性等多方面内容。
本章的主要内容取材于国际上著名的信息安全管理体系标准BS7799，并结合我国的国情和最新的技术发展，为读者详细介绍信息安全管理所涉及的各项安全控制目标和控制措施。
2.1　概述在全球迈入信息时代的今天，各国的企业都驰骋在信息高速公路上。
现代企业对信息的依赖越来越强，没有各种信息的支持，企业就不能发展。
事实上，信息已成为现代企业的重要资产，成为企业成功的关键所在。
这种资产，需要加以妥善保护，否则，可能由于黑客攻击、人员疏忽和自然灾害等原因，在一瞬间被毁灭、损坏、盗窃或贬值，给企业带来致命的打击。
企业将如何提高信息安全水平，防范信息资产毁损和泄密风险，保证信息的机密性、完整性和可用性就显得越发重要。
BS7799信息安全管理体系标准便是这样一套为规范企业信息安全管理，提高信息安全管理能力水平的标准。
BS7799标准是由英国标准协会（BSI）制定，是目前国际上具有代表性的信息安全管理体系标准。
BS7799标准于1993年由英国贸易工业部立项，1995年首次发布BS7799-1：1995《信息安全管理实施细则》，它提供了一套综合的、由信息安全最佳惯例组成的实施规则，其目的是作为确定工商业信息系统在大多数情况所需控制范围的参考基准，并且适用于大、中、小组织。
1998年英国公布标准的第二部分BS7799-2《信息安全管理体系规范》，它规定信息安全管理体系要求与信息安全控制要求，它是一个组织的全面或部分信息安全管理体系评估的基础，它可以作为一个正式认证方案的根据。
BS7799-1与BS7799-2经过修订于1999年重新予以发布，1999版考虑了信息处理技术，尤其是在网络和通信领域应用的近期发展，同时还非常强调了商务涉及的信息安全及信息安全的责任。
2000年12月，BS7799-1：1999（（信息安全管理实施细则》得到了国际标准化组织（ISO）的认可，正式成为国际标准ISO／IEC17799：2000（（信息技术信息安全管理实施细则》，并于2005年进行了修订。
2002年9月5日，BS7799-2：2002草案经过广泛的讨论之后，终于发布成为正式标准，同时BS7799-2：1999被废止。
2005年10月15Et，BS7799-2：2002正式被国际标准化组织采纳，成为ISO／IEC27001：2005。
新标准的正式标题为ISO／IEC27001：2005（（信息技术安全技术信息安全管理系统要求》。
BS7799标准包括如下两部分：BS7799-1：1999《信息安全管理实施细则》BS7799-2：2002《信息安全管理体系规范》。
BS7799-1：1999《信息安全管理实施细则》是组织建立并实施信息安全管理体系的一个指导性的准则，主要为组织制定其信息安全策略和进行有效的信息安全控制提供的一个大众化的最佳惯例。
BS7799-2：2002《信息安全管理体系规范》规定了建立、实施和文件化信息安全管理体系（ISMS）的要求，规定了根据独立组织的需要应实施安全控制的要求。
BS7799标准第二部分明确提出安全控制要求，标准第一部分对应给出了通用的控制方法，因此可以说，标准第一部分为第二部分的具体实施提供了指南。
但标准中的控制目标，控制方式的要求并非信息安全管理的全部，组织可以根据需要考虑另外的控制目标和控制方式。
BS7799汇集了优秀企业最佳实践，规范了10个安全控制区域，36个安全控制目标和127个安全控制措施。
它以风险评估为基础，采用自顶向下的管理方法，对组织、人员、流程、技术、法律法规、连续性等实施全方位安全管理。

BS7799的控制细则包括10个安全控制区域。
（1）安全策略：为信息安全提供管理指导和支持，通过在组织内发布和维护信息安全策略来表明管理层对信息安全的支持和承诺。
（2）组织的安全：建立信息安全架构，保证组织的内部管理；并在第三方访问或外协时，保障组织的信息安全。
（3）资产的分类和管理：明确资产责任，保持对组织资产的适当保护；将信息进行归类，确保信息资产受到适当程度的保护。
（4）人员安全：在工作说明和资源方面，减少因人为错误、盗窃、欺诈和设施误用造成的风险；加强用户培训，确保用户清楚地知道信息安全的危险性和相关事项，以便在他们的日常工作中支持组织的安全方针。
（5）物理与环境安全：确定安全区域，防止非授权访问、破坏、干扰信息；通过保障设备安全，防止资产的丢失、破坏、资产危害及商务活葫的中断；采用通用的控制方式，防止信息或信息处理设施损坏或失窃。
（6）通信和运营管理：明确操作程序及其责任，确保信息处理设施的正确，安全操作；加强系统策划与验收，减少系统失效风险；防范恶意软件以保持软件和信息的完整性；加强网络管理确保网络中的信息安全及其辅助设施受到保护；通过保护媒体处理的安全，防止资产损坏和商务活动的中断；加强信息和软件交换的管理；防止组织间在交换信息时发生丢失，更改和误用。
（7）访问控制：按照访问控制的要求，控制信息访问；加强用户访问管理，防止非授权访问信息系统；明确用户职责，防止非授权的用户访问；加强网络访问控制，保护网络服务程序；力Ⅱ强操作系统访问控制，防止非授权的计算机访问；加强应用访问控制，防止非授权访问系统中的信息；通过监控系统的访问与使用，监测非授权行为；在移动式计算和电传工作方面，确保使用移动式计算工作设施的信息安全。
（8）系统开发与维护：明确系统安全要求，确保安全性已构成信息系统的一部分；加强应用系统的安全，防止应用系统用户数据的丢失、被修改或误用；加强密码技术控制，保护信息的保密性，可靠性或完整性；加强系统文件的安全，确保IT方案及其支持活动以安全的方式进行；加强开发和支持过程的安全，确保应用系统软件和信息的安全。
（9）业务连续性管理：防止业务活动的中断及保护关键业务过程不受重大失误或灾难事故的影响。
（10）符合性：使信息安全活动符合法律法规要求，避免与刑法、民法、有关法令法规或合同约定事宜及其他安全要求的规定相抵触；加强安全方针和技术符合性评审，确保体系按照组织的安全方针及标准执行。
现在，BS7799标准已得到了很多国家的认可，是国际上具有代表性的信息安全管理体系标准，依据BS7799建立信息安全管理体系并获得认证已经成为世界潮流。
组织可以参照信息安全管理模型，按照BS7799标准建立组织完整的信息安全管理体系并进行实施与保持，达到动态的、系统的、全员参与的、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，提高企业的社会形象和市场竞争力。
. 2005年修订后的IS0／IEC17799较BS7799-1有一些变更，主要表现在增加了“信息安全事件管理”这一安全控制区域，基于本书有专门一章内容讨论信息安全事件管理，因而本章为读者介绍修订前的BS7799-1的10个安全控制区域的详细内容，而不讨论信息安全事件管理。
2.2 信息安全策略信息安全策略的目标是为信息安全提供管理指导和支持。
一个组织的管理层应当提出一套清晰的策略指导，并且通过在组织内发布和维护信息安全策略来表明对信息安全的支持和承诺。
落实信息安全策略的基本措施包括：信息安全策略文档的建立，信息安全策略文档的复查和评价。
1. 信息安全策略文档信息安全策略文档应当声明管理者的承诺，阐明一个组织实现信息安全的途径。
该策略文档至少应当包括以下指导性内容：（1）信息安全的定义，它的总体目标和范围以及安全保密性作为信息共享的许可机制的重要性。
（2）对管理意图、总体信息安全的目标和原理的简单说明。

（3）简短的说明安全策略、原理、标准和对该组织具有特殊重要意义的符合性要求，例如：符合法律规定和合同要求；安全教育的需求；病毒和其他恶意软件的阻止及检测；业务连续性管理；违反安全管理策略的后果。
（4）定义信息安全管理包括报告安全事故的一般性责任和特殊性责任。
（5）参考可能支持该策略的文献资料，例如，针对特殊的信息系统或者用户应当遵守的安全规则以及更为详尽的安全策略和程序。
信息安全策略文档需要以一种容易理解的和易于接受的方式在整个组织中公开。
2. 信息安全策略文档复查和评价信息安全策略文档需要专人依据确定的程序进行检查。
程序能够确保出现重大安全事故、发现新的易损性、组织基本机构变更或新的技术引入时，检查工作能够被触发，同时，程序还包括指定内容的定期检查，比如：策略的效率，由所记录的安全事故的性质、次数和影响来表示；对业务效率管理的成本和影响；技术变革的影响。
2.3 信息安全组织2.3.1 信息安全的基本架构组织为启动和控制信息安全的实施，需要建立适当的信息安全管理架构。
管理层要建立适当的管理问题论坛，以便确认信息安全策略、指派安全角色并在组织中协调安全措施的实施。
为跟上技术发展趋势、监控安全标准和测评方法并在处理意外安全事故时提供适当的联络点，组织应当加强与外部的信息安全专家的联系。
组织要鼓励发展综合信息安全解决方案，这类综合解决方案可能涉及经理、用户、管理员、应用程序设计人员、审计人员和安全人员的协调和合作，以及在一些领域的专门技术，比如保险和风险管理。
1. 管理信息安全论坛信息安全是一项由所有管理层成员共同承担的运营责任。
因此组织要考虑建立一个管理论坛，以确保从管理上对安全进行支持，并且使这种支持有一个清晰的方向。
该论坛应当通过适当的承诺责任和足够的资源配置来提高组织内部的安全性。
此论坛可以是现有管理机构的一部分。
通常情况下，论坛承担以下责任：（1）检查并批准信息安全策略和总的责任。
（2）当信息资产暴露在大多数威胁之下时，检测所发生的重要变动。
（3）复查并监测信息安全事故。
（4）支持重要的创新，以加强信息安全。
2. 信息安全协作在一个大型组织中，管理层代表的多功能论坛对于协调处理信息安全策略的执行是十分必要的。
这些管理层的代表都来自于组织的相关部门。
一般而言，这样的论坛能够：（1）批准整个组织内安全管理的特殊角色和责任。
（2）批准信息安全的特殊方法和程序，例如，风险评估，安全分级系统。
（3）批准并支持整个组织范围内的信息安全能动性，例如，安全意识计划。
（4）确保安全性是信息规划过程的一部分。
（5）评价适当性并协调对新系统或者服务的特殊安全管理措施的实施。
（6）应对信息安全事故。
（7）提高在整个组织内对信息安全业务支持的可见性。
3. 信息安全责任的分配保护个人资产的责任和执行特殊安全程序的责任应当清楚地定义。
信息安全策略应当提供在组织中确定安全角色和分配安全责任的一般性指导。
如果需要的话，这些指导还应当针对特殊的地点、系统或者范围补充上更为详细的指导。
对个人生命财产和信息资产所承担的局部责任应当清晰界定，对安全程序比如业务连续性规划所承担的局部责任也应当明确定义。
很多的组织会指定一个信息安全负责人，由其总体负责信息安全的发展和实现并管理措施的确定。
然而，资源配置和实现管理措施的责任常常留给单独的管理者。
通常的做法是为每项信息资产指派一个所有权人来负责其日常安全。
信息资产的所有权人可以把他们的安全责任委派给单独的管理者或者服务提供商。

尽管如此，所有权人仍然对此资产的安全负有最终的责任，并且所有权人应当能够确定任何责任错误分配的情况。
每一个管理者所负责的领域要清晰地阐明，这一点非常重要，特别是在下述情况发生时：（1）对于不同种类资产的安全程序和与各自系统相关的安全程序，都应当进行识别并清楚地定义。
（2）负责每项资产或者安全过程的管理者都应当得到批准，而且应当把此项责任的细节记录在案。
（3）授权等级应当清楚地定义并记录。
4. 信息处理方法的授权过程对新的信息处理方法应当建立管理授权过程：（1）新的信息处理方法应当有相应的客户授权，赞同其目的和用途，还应当获得负责维护当地信息系统安全环境的管理人员的同意，以确保满足所有相关策略和需要。
（2）在需要的时候，检测硬件和软件以确保它们和系统的其他组成部分互相兼容。
（3）对处理业务信息的个人信息处理程序的使用和任何必须的控制手段都应当经过授权。
（4）在工作场所中使用个人信息处理程序可能导致新的危险，因此需要进行评估和授权。
上述这些管理措施在网络化的环境中尤其重要。
5. 信息安全专家的建议许多组织可能都需要安全专家的建议。
理想的状况是，一位有经验的内部信息安全专家可以提供这些建议。
并不是所有的组织都愿意雇用一位咨询专家。
在这种情况下，建议确定一位专门人员来协调内部的安全知识和安全经验，以确保处理问题时的连续性并协助做出安全决策。
他们还应当能够找到适当的外部咨询专家来提供超出他们经验范围的专业建议。
信息安全建议者或者具有相同作用的联系人应当担负就信息安全的所有方面提供建议的任务。
他们要么自己提出建议，要么利用来自外部的建议。
他们对安全威胁所做评估的质量和对管理措施的意见决定了该组织的信息安全的效果。
为了达到最大的效用、产生最好影响，应当允许他们直接接触整个组织的管理。
6. 组织间的合作组织要与执法部门、管理机构、信息服务提供商和电信运营商保持适当联络，以确保在发生安全事故时能够及时采取适当的措施并能够及时通知。
类似的，也应当考虑到与安全组成员和行业协会进行合作。
7. 信息安全的独立检查信息安全策略明确了信息安全的策略和责任。
为确保组织的实践恰当地反映了这一策略，应当独立地检查其执行情况，并证明该策略是可行的和有效的。
这样的检查可以由内部的审查功能执行。
此外，独立的经理或者在此种检测方面有特殊专长的第三方人员也可以做这种检查。
这些候选人要具有检查所必备的技能和经验。
2.3.2 第三方访问的安全为保护组织信息处理程序的安全和被第三方访问的信息资产的安全，应当控制第三方对组织信息处理程序的访问。
如果有这样的第三方访问的业务需要，应当进行风险评估以确定安全隐患和管理对策，所要采取的管理措施应当得到第三方的同意，并在与之签订的合同中加以定义。
第三方访问还可能包括其他的参与者。
授予第三方访问权限的协议应当包括准许指定其他具备资格的参与者和相应访问的条件。
1. 判断第三方访问的风险允许第三方使用的访问类型非常重要。
例如，通过网络连接进行访问的风险不同于物理访问的风险。
访问类型包括：（1）物理访问：例如，访问办公室、计算机机房和档案柜。
（2）逻辑访问：例如，访问组织的数据库和信息系统。
（3）可能出于多种原因授予第三方访问权限。
例如，向组织提供访问的第三方并不在现场，但是可以给以物理访问和逻辑访问的权利，比如：①硬件和软件支持人员，他们需要访问系统层次或者低层次的应用程序功能。
②贸易合作伙伴或者联合经营方，他们可能交换信息、访问信息系统或者共享数据库。
如果缺乏足够的安全管理，则第三方访问信息时就会将其置于危险的境地。

若是有与第三方地点建立联络的业务需要，就要进行风险评估，以确定任何特殊管理措施的要求。
组织应当考虑到所需的访问类型、信息的价值、第三方采取的管理措施和这种访问对组织信息的安全所造成的影响。
第三方人员可能按照合同规定在现场驻扎一段时间，这会增加信息系统安全隐患。
现场承包方的例子包括：（1）硬件和软件维护以及支持人员。
（2）保洁、看护、安全警卫和其他外包的服务项目承包方。
（3）学生安置和其他临时的短期安排。
（4）咨询人员。
究竟要采取什么措施来管理第三方对信息处理设备的访问，理解这一点十分重要。
一般说来，所有的由于第三方访问或者内部管理措施导致的安全要求，都应当反映在组织与第三方签订的合同中。
例如，如果对信息的保密性有特殊要求，就应采用保密协议。
在采取了适当的管理措施和签署了定义有连接或者访问相关条款的合同之前，组织不应当向第三方提供对信息和信息处理设备的访问。
2. 第三方合同的安全要求涉及第三方访问组织信息和信息处理设备的有关安排应当建立在一份正式的合同基础上，这一合同应当包括或者涉及所有的安全要求，以求符合组织的安全策略和安全标准。
该合同应当保证在组织和第三方之间没有误解。
组织应当对供应商做满意的补偿，并考虑把以下各项条款写入合同中：（1）总的信息管理策略。
（2）资产保护，包括：①保护组织资产的措施方法，包括对信息和软件的保护。
②确定资产是否受到什么损害的方法手段，比如确定数据是否丢失或者被修改。
③在合同期结束或者合同期中某个协商同意的时间，确保信息或者资产被返回或者销毁。
④完整性和有效性。
⑤对于信息复制和信息披露的限制。
（3）对所要采用的每项访问的一个详细描述。
（4）服务的目标水平和无法接受的服务水平。
（5）适当的人员调任的规定。
（6）合同各方各自所应承担的义务。
（7）对相关法律问题所承担的责任，例如，数据保护立法。
特别是如果该合同涉及与其他国家中组织的合作，就要考虑不同国家法律体系。
（8）知识产权（IPR）和产权责任以及对所有合作项目的保护。
（9）服务控制协议，包括：①许可的访问方法、对唯一标识，比如用户ID和密码的管理和使用。
②对用户访问和特权的授权程序。
③要求保留一份列表，记录得到授权可以使用现有服务的个人、他们的权限与这种使用的关系。
（10）定义可以验证的业绩标准，以及对它们的监测和报告。
（11）监测和废除用户活动的权力。
（12）审查合同责任的权利，或者由第三方执行审查。
（13）为问题解决建立一个扩大程序；在适当的地方也应当考虑对偶然性事件的处置。
（14）有关硬件和软件的安装与维护的责任。
（15）清晰的报告结构和协商一致的报告格式。
（16）一个清晰的和专门化的变更管理程序。
（17）任何要求的物理保护措施和机制，确保那些管理措施得到落实。
（18）对客户和管理员的培训，包括方式方法、处理程序和安全性。
（19）确保能够防范恶意软件的管理措施。
（20）有关安全事故和安全漏洞的报告、通知和调查的安排。
（21）分包合同第三方的参与。

<<信息安全管理>>

编辑推荐

《普通高等教育"十一五"国家级规划教材·信息安全专业系列教材·信息安全管理》由北京邮电大学出版社出版。

版权说明