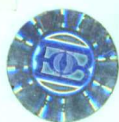


科飞管理咨询公司 编著

信息安全
管理丛书

BS 7799和 ISO/IEC 17799 信息安全管理体系 及其认证认可 相关知识问答

9-65



中国标准出版社



信息安全管理丛书

**BS7799和ISO/IEC17799
信息安全管理体系及其认证认可
相关知识问答**

科飞管理咨询公司 编著

中国标准出版社

内 容 简 介

本书涉及到 BS 7799 和 ISO/IEC 17799 几乎全部的要点,也包括两个标准在发展中的一些问题。全书共分为五章,其中包括:BS 7799 的术语和定义,BS 7799-2 标准的适用范围、PDCA 过程模式、信息安全管理体系统文件编写,风险评估方面的问题,在应用 ISO/IEC 17799 过程中可能遇到的问题及认证、认可相关的疑问等。

本书适合企事业单位信息化管理者、电子政务管理者、信息安全管理者、信息安全服务提供者以及信息安全管理研究人员、爱好者参考使用。

图书在版编目(CIP)数据

BS 7799 和 ISO/IEC 17799 信息管理体系及其认证认可相关知识问答/科飞管理咨询公司编著. —北京:中国标准出版社,2003

ISBN 7-5066-3249-7

I. B… II. 科… III. ①信息系统—安全管理—国家标准,BS 7799—英国—问答②信息系统—安全管理—国际标准,ISO/IEC 17799—问答 IV. TP309-65

中国版本图书馆 CIP 数据核字(2003)第 071448 号

版权专有 侵权必究 举报电话:(010)68533533

中国标准出版社出版(北京复兴门外三里河北街 16 号) 邮政编码:100045 电 话:68523946

68517548

中国标准出版社秦皇岛印刷厂印刷

新华书店北京发行所发行

各地新华书店经售

网址 www.bzchs.com

开本 880×1230 1/32 印张 8% 字数 205 千字

2003 年 9 月第一版 2003 年 9 月第一次印刷

印数 1—4 000

定价:25.00 元

本书编写组名单

组长 门洪利

主编 于海霞 吴昌伦

编委 俎全胜 孙洪涛 王毅刚



· 前 言

当今世界,信息对企业生存和发展的作用越来越大,已经成为关系企业核心竞争力的重要资源,如何保障信息安全这个课题也备受瞩目。近几年,在众多的信息安全标准中,信息安全管理标准 BS 7799 脱颖而出,从管理和技术的角度,通过建立、实施、保持并持续改进信息安全管理体系来保障组织的信息安全。BS 7799 已在全球范围内得到广泛的应用,被翻译成多种语言版本,甚至还被许多国家转化为国家标准。

组织在进行信息化建设,尤其是在进行信息安全规划、安全建设和验收的时候,或者在按照 BS 7799 标准建立信息安全管理体系的时候,经常对一些问题存在理解上的差异。为了减少理解分歧,帮助组织更好地把信息安全工作做好,我们编写了本书。

本书涉及到 BS 7799 和 ISO/IEC 17799 几乎全部的要点,也包括两个标准在发展中的一些问题。问题主要来源包括:ISMS 国际用户组织(IUG)注册用户普遍关注的问题、科飞公司与国际知名认证机构在信息安全管理领域广泛探讨的问题、读者对《信息安全管理概论——BS 7799 理解与实施》的反馈信息、我们在进行信息安全管理咨询过程中遇到的典型问题等。

全书共分为五章。第一章:BS 7799 和 ISO/IEC 17799 概括性问题,主要涵盖了 BS 7799 的术语和定义、组成、发展、相关的信息安全管理标准,BS 7799-1 国际

化进程以及 ISO/IEC 17799 相关的问题;第二章:BS 7799-2 涉及的问题,主要涵盖了 BS 7799-2 标准的适用范围、PDCA 过程模式、信息安全管理体系文件编写,以及 BS 7799-2 修订的相关内容;第三章:风险评估涉及的问题,主要解答了风险评估相关的术语和定义、风险评估方法的分类和定义,以及评估方法的选择等方面的问题;第四章:ISO/IEC 17799(BS 7799-1) 涉及的问题,主要解答了在应用 ISO/IEC 17799 过程中可能遇到的问题,按照标准的结构,分节予以解释;第五章:有关认证、认可的问题,主要解答了认证、认可相关的疑问和信息安全管理体系认证认可的发展状况,以及与信息安全管理体系审核员相关的问题。

本书面向的读者群包括企事业单位的信息化管理者、电子政务管理者、信息安全管理者、信息安全服务提供者以及信息安全管理研究人员、爱好者。随着人们对信息安全管理重视程度的提高,将会有越来越多的人想对 BS 7799 有更深层、更全面、更准确的理解,我们希望本书能够加强您对 BS 7799 和 ISO/IEC 17799 标准的理解,推动企业的信息安全管理工作更好地开展。

由于信息安全管理是一个新兴的行业,也是一门新兴的学问,在我国的应用还刚刚起步,加之编者对信息安全的了解和认识毕竟有限,书中难免有不当之处,敬请广大读者批评指正。

编 者

2003 年 7 月

· 目 录

第一章 BS 7799 和 ISO/IEC 17799 概括性问题

- 1 1. 什么是信息?
- 1 2. 什么是信息安全?
- 2 3. 为什么需要信息安全?
- 4 4. 我国的信息安全管理现状如何?
- 6 5. 针对我国的信息安全管理现状,我国的信息安全管理
工作应如何开展?
- 6 6. 如何保障信息安全?
- 7 7. 什么是信息安全管理体系(ISMS)?
- 8 8. 组织内建立信息安全管理体系(ISMS)的作用有哪些?
- 9 9. 对组织内部成功实施 ISMS 至关重要的因素有哪些?
- 9 10. 本书中关于 BS 7799 和 ISO/IEC 17799 的各种版本
分别是怎么区别的?
- 10 11. BS 7799 由哪几部分组成?
- 10 12. BS 7799 的发展历程是怎样的?
- 11 13. BS 7799 是否仅适用于英国?
- 12 14. BS 7799 是否包含对英国法律体系的特殊要求?
- 12 15. BS 7799 是否是一个国际标准?
- 12 16. 目前有多少国家接受 BS 7799 为其国家标准?
- 13 17. 为什么只有 BS 7799 第一部分被提议成为 ISO/IEC
标准?
- 13 18. 什么是 ISO,它与 IEC 有什么关系?

- 14 19. BS 7799 中是否规定了具体的风险评估方法?
- 14 20. 本书中为什么将 BS 7799 标准中的“Policy”译为“方针”?
- 15 21. ISO/IEC 17799:2000 的目的是什么?
- 15 22. ISO/IEC 17799:2000 和 BS 7799 的关系是怎样的?
- 15 23. ISO/IEC 17799:2000 包括哪些内容?
- 17 24. ISO/IEC 17799:2000 不涉及哪些内容?
- 17 25. ISO/IEC 17799:2000 是由谁制定的?
- 18 26. ISO/IEC 17799:2000 是否也像 BS 7799 一样有第二部分?
- 18 27. ISO/IEC 17799:2000 是否可以用作信息安全管理体系的认证标准?
- 19 28. ISO/IEC 17799 是否可以被组织独立应用?
- 19 29. 什么是 CC 标准,其发展历程如何?
- 21 30. CC 标准与 BS 7799 有什么异同?
- 21 31. 什么是 ISO/IEC TR 13335,它与 ISO/IEC 17799 有什么关系?
- 23 32. 如何确定组织的信息安全要求?
- 23 33. 信息安全管理标准化有什么意义?
- 24 34. 我国信息安全管理标准化工作应如何开展?
- 25 35. 我国为信息安全标准化做了哪些工作?

第二章 BS 7799-2 涉及的问题

- 28 36. BS 7799-2 适用于哪些类型的组织?
- 28 37. BS 7799-2 于 2002 年重新修订的主要原因是什么?
- 29 38. BS 7799-2:2002 主要修订内容是什么?
- 29 39. BS 7799-2:2002 引入了新的审核和认证要求吗?
- 29 40. BS 7799-2:2002 颁布后按 BS 7799-2:1999 颁发的证

书还有效吗?

- 30

41. BS 7799-2:2002 引用了哪些标准?
- 30

42. BS 7799-2:2002 引入了新的控制方式吗?
- 30

43. BS 7799-2:2002 有利于各种管理体系的整合认证吗?
- 32

44. BS 7799-2:2002 是由谁修订的?
- 33

45. 什么是 ISMS IUG?
- 33

46. 风险评估在 BS 7799-2:2002 中是否仍然是建立信息安全管理体系的关键步骤?
- 33

47. 什么是过程方法?
- 34

48. 过程方法鼓励用户关注哪些信息安全内容?
- 34

49. 什么是 PDCA 过程模式?
- 35

50. 按照 BS 7799-2:2002 要求 PDCA 四个阶段的工作是如何分布的?
- 36

51. BS 7799-2:2002 中给出哪些术语和定义?
- 36

52. 是否可以考虑对标准进行删减,删减的原则是什么?
- 37

53. 信息安全管理体系的总要求是什么?
- 37

54. 信息安全管理体系的设计和实施受哪些因素影响?
- 37

55. 组织应该将信息安全管理体系放在一个什么高度?
- 38

56. 建立 ISMS 的具体步骤是怎样的?
- 39

57. ISMS 策划与准备阶段涉及的工作有哪些?
- 40

58. ISMS 建立过程中培训教育工作如何开展?
- 40

59. 如何准确描述 ISMS 的范围?
- 41

60. ISMS 建立过程中现状调查与风险评估的主要工作有哪些?
- 41

61. 现状调查与风险评估的工作流程是怎样的?
- 42

62. ISMS 策划的具体工作有哪些?
- 43

63. 什么是信息安全管理体系文件?
- 43

64. ISMS 至少应该包括哪些文件?

- 43 65. 信息安全管理体系文件编写要求有哪些?
- 44 66. 编写信息安全管理体系文件的主要依据有哪些?
- 45 67. ISMS 是如何控制体系文件的?
- 45 68. 各组织的 ISMS 文件是否可以不同?
- 45 69. 什么是信息安全管理手册?
- 46 70. 信息安全管理手册包括哪些内容?
- 46 71. 程序文件应该包括哪些内容?
- 46 72. 编写信息安全管理体系程序文件应遵循哪些原则?
- 47 73. 信息安全管理体系程序文件的内容与格式有哪些要求?
- 48 74. 编写信息安全管理体系程序文件时应注意哪些事项?
- 48 75. 程序文件与作业指导性文件有何区别和联系?
- 49 76. 什么是记录?
- 49 77. 组织为什么要保留记录?
- 50 78. ISMS 如何控制记录?
- 50 79. ISMS 运行过程中,组织应注意哪些方面?
- 51 80. 组织在提高员工能力方面应该做哪些工作?
- 52 81. 最高管理者如何支持信息安全管理体系?
- 52 82. 信息安全管理体系建立文件化的程序的目的是什么?
- 52 83. 什么是管理评审?
- 53 84. 管理评审的输入有哪些?
- 53 85. 管理评审的输出有哪些?
- 54 86. 信息安全管理体系评审的步骤是怎样的?
- 54 87. 通过哪些方法持续改进信息安全管理体系?
- 56 88. ISMS 的内部审核周期多长?
- 56 89. 什么是纠正措施?
- 56 90. 纠正措施的具体步骤是怎样的?
- 56 91. 什么是预防措施?

- 56 92. 预防措施的具体步骤是怎样的?
- 57 93. 什么是控制概要?
- 57 94. 控制概要(SoC)和适用性声明(SoA)在 BS 7799-2:
2002 中有何关系?
- 57 95. ISMS 如何处理与上级 ISMS 或者下级 ISMS 的
关系?
- 58 96. 什么是风险处理计划?

第三章 风险评估涉及的问题

- 59 97. 什么是威胁?
- 60 98. 评估威胁发生的可能性需要考虑哪些方面?
- 60 99. 什么是薄弱点?
- 61 100. 什么是风险?
- 61 101. 什么是风险评估?
- 61 102. 什么是安全控制?
- 62 103. 什么是剩余风险?
- 62 104. 什么是适用性声明?
- 62 105. 为什么要进行风险评估?
- 62 106. 什么是风险管理?
- 63 107. 风险评估与 ISO/IEC 17799 和 BS 7799-2 的关系?
- 63 108. 风险评估时应考虑哪些因素?
- 63 109. 风险评估过程中哪些内容应该被文件化?
- 64 110. 怎样才能确保识别全部重要信息资产?
- 64 111. 对于已识别的风险组织应如何进行处理?
- 65 112. 风险评估的基本步骤有哪些?
- 65 113. 影响威胁发生的可能性的因素有哪些?
- 66 114. 安全控制可分为哪几类,每一类的作用是什么?
- 66 115. 风险控制过程涉及的活动有哪些?

- 67 116. 根据风险评估的深度,风险评估方法有哪几种?
- 67 117. 什么是基本的风险评估,此评估方法适用于何种组织?
- 68 118. 基本风险评估活动涉及的具体内容有哪些?
- 68 119. 基本风险评估的优点有哪些?
- 69 120. 基本风险评估的缺点有哪些?
- 69 121. 什么是详细的风险评估?
- 70 122. 详细风险评估活动涉及的具体内容有哪些?
- 71 123. 详细风险评估的优点有哪些?
- 71 124. 详细风险评估的缺点有哪些?
- 71 125. 什么是联合评估方法?
- 71 126. 联合评估方法的优点有哪些?
- 72 127. 联合评估方法的缺点有哪些?
- 72 128. 组织在选择风险评估方法时,应该考虑哪些方面的内容?
- 73 129. 信息安全风险评估应在何时进行?

第四章 ISO/IEC 17799(BS 7799-1)涉及的问题

- 74 第一节 信息安全方针(策略)中涉及的问题
- 74 130. 什么是信息安全方针?
- 74 131. 信息安全方针和标准、指南、程序、控制有什么区别?
- 75 132. 为什么需要信息安全方针?
- 76 133. 信息安全方针包括哪些信息?
- 78 134. 什么时候进行信息安全方针的评审?
- 78 135. 信息安全方针的评审包括哪些内容?
- 78 136. ISO/IEC 17799 中明确提出哪些信息安全方针?
- 79 137. 如何保证信息安全方针得到贯彻执行?

80 138. 如何衡量信息安全方针优劣?

81 第二节 安全组织中涉及的问题

81 139. 信息安全组织机构包括哪些内容?

83 140. 信息安全管理论坛的作用是什么?

83 141. 信息安全协调委员会的作用是什么?

84 142. 信息安全权责的分配应该遵循什么原则?

84 143. 信息处理设施的授权程序应考虑哪些方面?

85 144. 向谁咨询信息安全相关的问题?

86 145. 组织在信息安全事宜上可能需要哪些外部支持?

86 146. 如何能够保证在发生信息安全事件时能够迅速得到外部支持?

86 147. 什么是审核的独立性?

86 148. 信息安全审核为什么要坚持独立性?

87 149. 在信息安全管理体中哪些人员属于第三方?

87 150. 第三方访问的类型有哪几种?

87 151. 第三方访问的原因是什么?

88 152. 为什么要控制第三方访问?

88 153. 第三方访问的控制目标是什么?

88 154. 哪些第三方访问需要授权?

89 155. 第三方访问合同中的安全要求有哪些?

90 156. 怎样执行第三方访问授权程序?

91 157. 对第三方访问的控制措施有哪些?

91 158. 外包合同中应该包含哪些安全要求?

92 第三节 资产的分类和控制中涉及的问题

92 159. 为什么要进行信息资产盘点?

92 160. 为防止信息资产被盗与丢失,组织可采取哪些控制

措施？

- 93 161. 哪些资产在需要盘点之列？
- 93 162. 维护一份信息资产清单有什么好处？
- 94 163. 信息资产清单应包括哪些项目？
- 94 164. 为什么要对信息进行分级？
- 94 165. 组织应如何进行信息分级？
- 95 166. 信息分级应该坚持什么原则？
- 95 167. 谁来确定信息的级别？
- 95 168. 谁负责维护信息级别的适宜性？
- 96 169. 怎样对信息进行标识？
- 96 170. 信息标识应该注意哪些问题？
- 96 171. 不同分级的信息在管理的哪些方面存在区别？

97 第四节 人员安全中涉及的问题

- 97 172. 人员安全控制的目的是什么？
- 97 173. 为加强组织内部人员的安全控制，组织应采取何种措施？
- 98 174. 工作职责应该包括哪些信息安全职责？
- 98 175. 应对哪部分人员进行信息安全考察？
- 99 176. 信息安全的人员考察过程应在什么时候进行？
- 99 177. 在招聘长期雇员时应该考察哪些方面？
- 99 178. 为什么需要签订保密协议？
- 100 179. 什么时候需要保密协议？
- 100 180. 保密方面的约定可以突破组织的范围吗？
- 100 181. 保密方面的约定可能突破雇用合同期吗？
- 100 182. 雇用条款中应包括哪些方面的安全要求？
- 101 183. 用户培训的目的是什么？
- 101 184. 组织需要对哪些用户进行信息安全培训？

- 101 185. 组织的信息安全培训主要有哪些内容?
- 102 186. 用户培训时机怎么来确定?
- 102 187. 在安全事件与安全故障响应中组织应注意哪几方面?
- 103 188. 什么是安全事件?
- 103 189. 为什么需要信息安全报告与响应机制?
- 104 190. 谁来报告信息安全事件和可疑现象?
- 104 191. 安全事件与安全故障报告程序中应明确规定哪些内容?
- 104 192. 哪些内容需要报告?
- 105 193. 谁来响应信息安全报告?
- 105 194. 影响信息安全事件响应优先次序的因素有哪些?
- 105 195. 谁来确认信息安全薄弱点?
- 105 196. 如何来提高信息安全事件报告和响应的效率效果?
- 106 197. 发生软件故障时应采取何种措施?
- 106 198. 员工违背了信息安全方针和程序怎么办?

107 第五节 物理和环境安全中涉及的问题

- 107 199. 什么是安全区域(Security Areas)?
- 107 200. 为什么需要设立安全区域?
- 107 201. 如何确保安全区域安全?
- 108 202. 为安全区域建立安全周界时应考虑哪些因素?
- 109 203. 如何控制安全区域的物理进出?
- 109 204. 如何保证办公室、房间和设施的安全?
- 110 205. 组织应对在安全区域内的人员采取哪些控制?
- 111 206. 组织应如何对存储区域和传送区域加以控制?
- 111 207. 设备的定置需要考虑哪些因素?
- 113 208. 在安排供电方面需要考虑的因素有哪些?

- 113 209. 电缆可能有哪些威胁?
- 113 210. 需要对电缆采取哪些控制?
- 114 211. 对于敏感和重要系统的电缆需要采取哪些额外控制?
- 114 212. 设备维护应考虑哪些方面?
- 115 213. 设备要外出维修时候应注意哪些问题?
- 115 214. 什么是场所外设备?
- 116 215. 怎样管理和使用工作场所外的设备?
- 116 216. 如何保证设备的处置和再使用安全?
- 117 217. 清除桌面 (Clear Desk) 方针和清除屏幕 (Clear Screen) 方针包括哪些要求?
- 117 218. 为什么需要制定清除桌面方针和清除屏幕方针?
- 118 219. 如何控制资产迁移?

118 第六节 通信和运作管理中涉及的问题

- 118 220. 运作程序和职责控制包括哪些方面的内容?
- 120 221. 运作程序和职责控制的目的是什么?
- 120 222. 组织的运作程序 (Operating Procedures) 应该对哪些方面进行规范?
- 120 223. 如何控制信息处理设施和系统的更改?
- 121 224. 事件管理程序的目的是什么?
- 121 225. 事件管理程序应该涵盖哪些类型的安全事件?
- 121 226. 事件管理程序应该涵盖哪些行动?
- 122 227. 事件管理程序为什么要强调证据的收集?
- 122 228. 为什么要强调职责分离?
- 122 229. 职责分离应该考虑哪些因素?
- 123 230. 如果职责分离有困难怎么办?
- 123 231. 直接在运行系统进行开发会带来哪些风险?

- 123 232. 开发设施和运行设施隔离可采用哪些控制?
- 124 233. 外包设施控制需要考虑哪些因素?
- 124 234. 为什么需要对系统进行容量策划?
- 125 235. 系统容量策划需要考虑哪些因素?
- 125 236. 系统验收标准应考虑哪几方面?
- 125 237. 怎么能够保证系统满足验收标准?
- 125 238. 什么是“恶意软件”(Malicious Software)?
- 126 239. 恶意软件的控制应该考虑哪些因素?
- 127 240. 什么是“内务管理”?
- 128 241. 为什么需要信息备份?
- 128 242. 如何保证备份的有效性?
- 128 243. 操作者记录中应记录哪些内容?
- 129 244. 对操作日志的核查要求有哪些?
- 129 245. 处理故障报告应遵循哪些规则?
- 130 246. 什么是“网络管理”?
- 130 247. 网络所面临的典型威胁包括哪些?
- 130 248. 可采用的网络安全控制措施有哪些?
- 131 249. 可移动计算机媒体的管理要坚持什么原则?
- 131 250. 哪些媒体的处置需要考虑安全问题?
- 131 251. 信息媒体的处置应该坚持哪些原则?
- 132 252. 系统文档为什么重要?
- 132 253. 如何保证系统文档安全?
- 133 254. 信息和软件交换的协议应该考虑哪些因素?
- 133 255. 媒体传送过程中需要采取哪些控制?
- 134 256. 电子商务活动可分为哪几种?
- 135 257. 确保电子商务安全应该考虑哪些因素?
- 136 258. 电子邮件给组织带来哪些风险?