

数字图书馆 信息安全管理

数字图书馆信息安全管理 ● 黄水清 著



南京大学出版社

数字图书馆 信息安全管理

● 黄水清 著



南京大学出版社

图书在版编目(CIP)数据

数字图书馆信息安全管理 / 黄水清著. — 南京 :
南京大学出版社, 2011. 8

ISBN 978 - 7 - 305 - 08761 - 5

I. ①数… II. ①黄… III. ①数字图书馆—信息系统
—安全管理 IV. ①G250.76

中国版本图书馆 CIP 数据核字(2011)第 171833 号

出版发行 南京大学出版社
社 址 南京市汉口路 22 号 邮 编 210093
网 址 <http://www.NjupCo.com>
出 版 人 左 健
书 名 数字图书馆信息安全管理
著 者 黄水清
责任编辑 胥橙庭 编辑热线 025 - 83686308
照 排 南京南琳图文制作有限公司
印 刷 赣榆县赣中印刷有限公司
开 本 787×960 1/16 印张 25.75 字数 490 千
版 次 2011 年 8 月第 1 版 2011 年 8 月第 1 次印刷
ISBN 978 - 7 - 305 - 08761 - 5
定 价 60.00 元
发行热线 025 - 83594756 83686452
电子邮箱 Press@NjupCo.com
Sales@NjupCo.com(市场部)

* 版权所有, 侵权必究

* 凡购买南大版图书, 如有印装质量问题, 请与所购
图书销售部门联系调换

前 言

发端于 20 世纪 90 年代的数字图书馆的研究及实践在全球蓬勃发展,伴随着数字资源的积累与网络存取的开放性,数字图书馆的信息安全问题成为数字图书馆实践与研究中的热点和前沿问题。

国外的统计表明,70%的信息安全事件产生的原因并不是来自外界的病毒和黑客,而是来自内部的未授权访问,许多信息安全问题仅仅依靠产品和技术根本无法解决,而应依靠技术与管理的结合,所谓“三分技术七分管理”。因此,国外学者提出了信息安全管理与信息安全技术并举的观点,并在实践上加以贯彻执行,制定了一系列信息安全管理的规范与标准,如美国卡内基·梅隆大学的 OCTAVE、美国审计总署的 GAO/AIMD—98—68 和 GAO/AIMD—99—139、澳大利亚和新西兰的 AS/NZS 4360、美国国家标准和技术学会的 NIST 风险管理框架、国际标准 ISO27000 系列等。特别是 ISO27000 系列国际信息安全管理标准的发布,得到多个国家的认可与接受,在各个行业得到应用,中国国家质量监督检验检疫局、国家标准化委员会已接受并转化为对应的中国国家标准。

数字图书馆的信息安全管理是数字图书馆管理的组成部分,数字图书馆信息安全管理体系的建设是数字图书馆各项业务与服务功能正常开展的前提与保证。数字图书馆信息安全管理的必要性自不待言,但在当前数字图书馆信息安全管理的理论研究与具体实践过程中普遍存在重概念轻实施、重技术轻管理的倾向。同时,由于信息安全问题专业性强,牵涉面广,信息安全管理体系建设工作量巨大,数字图书馆在实施过程中常有无所适从之感或畏难情绪。

本书试图将在企业和政府机构得到广泛应用的信息安全管理标准引入数字图书馆领域,从规范管理行为入手提升数字图书馆信息安全水平,为数字图书馆的信息安全问题提供理论上完备、现实中具操作性、实施过程简便易行的解决方案,改变数字图书馆信息安全过于依赖防火墙、反病毒、用户访问控制的状况,在不提升技术条件的前提下解决数字图书馆信息安全管理的现实问题,并为数字图书馆信息安全的风险评估与风险控制提供模板,降低数字图书馆信息安全管理体系建立与实施的难度,减少工作量。以上工作在数字图书馆领域尚属首次。

本书的目标是希望从理论和操作层面上解决信息安全管理标准应用于数字图书馆信息安全管理可能存在的障碍。理论层面上,将在国际上得到广泛认同的信

息安全管理标准引入数字图书馆信息安全管理,确定数字图书馆信息安全管理体系建立和实施的原则、方法和流程;操作层面上,提炼数字图书馆风险评估与风险控制的模板,降低数字图书馆信息安全管理操作难度,减少数字图书馆信息安全管理体系建立与实施的工作量。

归纳起来,本书主要解决了以下三个方面的问题:

将在世界范围内得到广泛认同的信息安全管理标准引入数字图书馆领域,在对国内数字图书馆的信息安全现状进行调查的基础上,结合数字图书馆信息安全管理实际需要,确定了 ISO27000 系列标准为数字图书馆信息安全的依从标准。这是本书解决的第一个主要问题。

在数据调查的基础上,根据数字图书馆信息安全的现实情况,设计了基于模糊数学的资产价值评估模型、基于“构建威胁场景”的威胁等级评估模型、基于 CVSS 的脆弱性评价模型、数字图书馆风险值计算模型、基于投资约束和风险防范策略的数字图书馆风险控制决策模型、风险评估与风险控制间的联动关系三维坐标系(含已施加控制措施的风险值计算模型)。这是本书解决的第二个主要问题。

以数字图书馆业务流程、资产、威胁、脆弱性的调查数据为基础,建立了数字图书馆业务流程与资产关联表、数字图书馆资产—威胁—脆弱性对照表,提出了数字图书馆信息安全风险等级的划分方法,构建了数字图书馆风险评估的模板。可将数字图书馆信息安全风险评估过程很大程度上简化为查表过程,降低了数字图书馆信息安全风险评估的难度,减少了工作量。在分析、提炼数字图书馆核心控制要素的基础上,确定了数字图书馆的风险控制目标和组织控制措施与技术控制措施的实施方法,构建了数字图书馆风险控制模板。这是本书解决的第三个主要问题。

本书是在国家社科基金项目“数字图书馆信息安全管理与评价”(项目编号 07BTQ005)最终研究报告的基础上修改而成。作者指导的研究生任妮、熊健、陈双喜参与了项目的全部研究工作,深圳大学图书馆赵洗尘、南京图书馆吴政、南京农业大学图书馆查贵庭、对外经济贸易大学图书馆邱小红和范利群、东莞图书馆李东来和叶少青、大连理工大学图书馆金玉玲、浙江省图书馆范沈姍、浙江工商大学图书馆朱小玲等参与了项目的数据调查或专家咨询工作,在此一并致谢!

由于时间与作者水平的关系,书中存在许多不足甚至是错误。如,书中对某大学的数字图书馆信息安全的风险评估与风险控制,既没有得到长时间运行的有效性验证,也没有得到第三方认证机构的确认(即获得认证证书),作者的研究团队目前还未能开发出完整的数字图书馆信息安全风险管理软件系统,对于数字图书馆信息安全管理工作的具体实施会带来不便。作者希望专家和读者对书中的不足和错误给予批评指正。

目 录

第一章 绪论	1
第二章 数字图书馆与数字图书馆信息安全	6
2.1 数字图书馆	6
2.1.1 数字图书馆的定义	6
2.1.2 数字图书馆在本书中的涵义	8
2.2 数字图书馆建设	8
2.2.1 国内外数字图书馆建设概况	8
2.2.2 国内数字图书馆建设的调查与总结	10
2.3 信息安全的概念及其发展	12
2.3.1 信息安全的概念	13
2.3.2 信息安全的几个发展阶段	14
2.3.3 信息安全技术与信息安全管理	15
2.4 数字图书馆信息安全	17
2.4.1 数字图书馆信息安全的概念	17
2.4.2 数字图书馆信息安全的技术措施	19
2.4.3 国外对数字图书馆信息安全的研究	22
2.4.4 国内对数字图书馆信息安全的研究	26
2.4.5 数字图书馆信息安全现状调查	28
2.4.6 数字图书馆信息安全管理学解决方案	34
第三章 数字图书馆信息安全管理标准	36
3.1 信息安全管理标准及其发展	36
3.1.1 信息安全管理标准的概念与主要内容	36
3.1.2 信息安全管理标准的起源	37
3.1.3 信息安全管理标准的发展	38
3.2 国外的信息安全管理标准	39
3.2.1 GAO/AIMD—99—139 风险评估指南	39
3.2.2 NIST 风险管理框架	40
3.2.3 OCTAVE 方法	42

3.2.4 AS/NZS 4360 风险管理指南	44
3.2.5 ISO27000 系列标准	45
3.2.6 国外的其他信息安全管理标准	47
3.3 国内的信息安全管理标准	51
3.3.1 信息技术安全性评估准则(GB/T18336)	52
3.3.2 计算机信息系统安全保护等级划分准则(GB17859—1999)	53
3.3.3 信息安全等级保护管理办法	53
3.3.4 ISO27000 在国内的转化	54
3.4 数字图书馆信息安全管理依从标准的选定	55
3.4.1 数字图书馆信息安全管理标准遴选的原则	55
3.4.2 ISO27000 对数字图书馆信息安全管理的适用性	56
3.4.3 ISO27000 应用于数字图书馆信息安全管理的基本思路	59
第四章 数字图书馆信息安全管理的方法	61
4.1 术语与概念	61
4.1.1 与风险评估有关的概念	61
4.1.2 与风险控制有关的概念	64
4.1.3 概念之间的关系	66
4.2 数字图书馆信息安全管理的过程模式	67
4.2.1 过程与过程方法	67
4.2.2 ISO27001 中的 PDCA 过程模式	69
4.2.3 PDCA 模式在数字图书馆信息安全管理中的应用	70
4.3 风险评估	72
4.3.1 风险评估的步骤	72
4.3.2 资产、威胁与脆弱性的识别与估值	73
4.3.3 风险值的计算	74
4.3.4 资产、威胁、脆弱性三维坐标	74
4.4 风险控制	76
4.4.1 风险控制的步骤	76
4.4.2 ISO27002 中的控制措施	77
4.4.3 资产、业务、控制措施三维坐标	78
第五章 数字图书馆风险评估与风险控制的模型	80
5.1 风险评估的方法与模型	80
5.1.1 风险评估的基本方法	80
5.1.2 几种典型的风险评估模型	81



5.1.3 数字图书馆信息安全风险评估模型的框架	85
5.2 数字图书馆的资产、威胁及脆弱性评估模型	86
5.2.1 基于模糊数学的资产价值评估模型	87
5.2.2 基于“构建威胁场景”的威胁等级评估模型	87
5.2.3 基于 CVSS 的脆弱性评价模型	88
5.3 数字图书馆已有控制措施确认与风险值计算	92
5.4 数字图书馆风险控制模型	93
5.4.1 数字图书馆风险控制决策的流程	93
5.4.2 数字图书馆风险控制决策模型的建立	94
第六章 数字图书馆业务流程	98
6.1 数字图书馆的功能框架	98
6.1.1 数字图书馆功能框架研究综述	98
6.1.2 文献中与数字图书馆功能有关的关键词的统计	100
6.1.3 现实中的数字图书馆功能框架	102
6.1.4 数字图书馆功能框架总结	106
6.2 数字图书馆业务流程的调查与分析	106
6.2.1 调查方案设计	107
6.2.2 调查结果分析	112
6.3 数字图书馆业务流程总结	120
第七章 数字图书馆信息安全风险评估	124
7.1 数字图书馆资产、威胁与脆弱性调查	124
7.2 数字图书馆资产识别与估值	125
7.2.1 资产识别	126
7.2.2 资产估值	129
7.3 数字图书馆威胁识别与估值	135
7.3.1 威胁识别	135
7.3.2 威胁估值	136
7.4 数字图书馆脆弱性识别与估值	138
7.4.1 脆弱性识别	138
7.4.2 脆弱性估值	139
7.5 数字图书馆信息安全风险分析	140
7.5.1 风险计算方法	140
7.5.2 风险等级划分	141
7.5.3 数字图书馆资产—威胁—脆弱性对照分析	142



第八章 数字图书馆信息安全风险控制	144
8.1 ISO27002 控制要素对数字图书馆的作用调查	144
8.1.1 调查方案与调查过程	145
8.1.2 调查结果分析	145
8.2 数字图书馆信息安全控制要素的筛选	149
8.2.1 筛选的目标与方法	150
8.2.2 控制要素分析与筛选	151
8.2.3 筛选的结果	167
8.3 数字图书馆信息安全风险控制的实施	168
8.3.1 数字图书馆的信息安全风险控制目标	168
8.3.2 数字图书馆信息安全组织控制的实施	170
8.3.3 数字图书馆信息安全技术控制的实施	173
第九章 数字图书馆信息安全管理体系的实施	176
9.1 数字图书馆信息安全管理体系的实施流程	176
9.1.1 前期准备	176
9.1.2 风险评估与风险处置计划	178
9.1.3 信息安全管理体系文件的编写与审核	179
9.1.4 信息安全管理体系文件发布与运行	179
9.2 数字图书馆信息安全管理体系的软件支持	180
9.2.1 风险评估软件的类别	180
9.2.2 数字图书馆信息安全风险管理软件的设计目标	182
9.2.3 数字图书馆信息安全风险管理软件的功能结构	183
9.2.4 数字图书馆信息安全风险管理软件的开发	184
9.3 数字图书馆信息安全管理体系的认证	185
第十章 数字图书馆信息安全管理实证	187
10.1 实证研究对象简介	187
10.2 风险管理方案制定阶段	188
10.2.1 风险管理的目的	188
10.2.2 风险管理的原则	188
10.2.3 风险管理组织构建	189
10.2.4 评估及控制的模型、方法	189
10.2.5 所需数据内容及采集方法	189
10.3 数据调研采集阶段	189
10.3.1 资产识别	190

10.3.2	威胁识别及相关赋值	191
10.3.3	脆弱性识别及相关赋值	193
10.3.4	现有控制措施识别及实施程度调查	196
10.3.5	单位风险指数的资产损失值调查	198
10.3.6	控制措施的实施成本及有效性调查	201
10.4	风险评价与分析阶段	202
10.4.1	资产价值等级计算	202
10.4.2	威胁等级计算	205
10.4.3	脆弱性等级计算	207
10.4.4	风险等级计算	208
10.4.5	风险评价结果分析	209
10.5	风险控制方案的制定与实施阶段	212
10.5.1	风险控制的目标确定	212
10.5.2	控制措施的筛选与推荐	212
附录 A	数字图书馆信息安全管理备查数据	217
附录 A-1	安全类别及控制要素、控制措施列表	217
附录 A-2	数字图书馆业务流程与资产关联表	226
附录 A-3	数字图书馆威胁与脆弱性对照表	228
附录 A-4	数字图书馆现存的威胁与脆弱性对照表	236
附录 A-5	数字图书馆资产—威胁—脆弱性对照表	244
附录 A-6	数字图书馆信息安全控制要素表	368
附录 A-7	数字图书馆信息安全组织控制、技术控制与核心控制要素对照表	373
附录 B	N 大学数字图书馆信息安全管理实证数据	374
附录 B-1	脆弱性等级评价表	374
附录 B-2	控制措施的实施成本及有效性列表	375
附录 B-3	风险值计算列表	380
附录 B-4	高风险项具体情况列表	384
附录 B-5	不可接受风险的控制措施计算结果列表	389

图 目 录

图 3-1	风险管理循环	40
图 3-2	PDCA 循环的基本模式	58
图 4-1	风险评估与风险控制概念关系图	67
图 4-2	适用于 ISMS 过程的 PDCA 模式	69
图 4-3	单项资产与威胁、脆弱性对应关系图	75
图 4-4	资产、威胁、脆弱性三维坐标系	75
图 4-5	资产、业务、控制措施三维坐标系	78
图 5-1	数字图书馆信息安全风险评估模型框架图	85
图 5-2	CVSS 各要素及相互关系图	89
图 5-3	风险控制决策的流程	94
图 5-4	软件资产-控制措施对应表	95
图 6-1	数字图书馆功能结构图	99
图 6-2	中国数字图书馆功能结构图	103
图 6-3	中数创新数字图书馆功能结构图	104
图 6-4	北京国图数字图书馆功能结构图	104
图 6-5	CADLIS 数字图书馆总体架构图	105
图 6-6	CADLIS 高校数字图书馆功能框架图	105
图 6-7	数字图书馆功能框架图	106
图 10-1	N 大学数字图书馆各等级风险项分布情况图	211

表 目 录

表 2-1	图书馆管理系统使用年限分布表	11
表 2-2	数字图书馆技术人员数量分布表	11
表 2-3	数字图书馆电子资源 2008 年采购经费分布表	11
表 2-4	数字图书馆设备 2008 年采购和维护经费分布表	12
表 2-5	2001—2009 年数字图书馆信息安全发文数量统计表	27
表 2-6	数字图书馆信息安全事件发生情况统计表	29
表 2-7	信息安全事件发生原因统计表	30
表 2-8	数字图书馆信息安全事件发现方式统计表	31
表 2-9	数字图书馆信息安全风险处理的方式统计表	31
表 2-10	数字图书馆信息安全组织建设情况表	32
表 2-11	数字图书馆信息安全制度建设概况表	32
表 2-12	数字图书馆机房环境指标控制情况表	32
表 2-13	数字图书馆备份/恢复方案建设概况统计表	33
表 3-1	TCSEC 的等级划分	49
表 5-1	风险价值矩阵表	82
表 5-2	威胁分级法的风险计算示例	83
表 5-3	威胁发生的频率值表	83
表 5-4	可接受与不可接受风险矩阵	84
表 5-5	实际评估所用的风险矩阵表	84
表 5-6	CVSS 各要素及取值范围表	89
表 5-7	数字图书馆 CVSS 度量指标取值表	91
表 6-1	数字图书馆功能分类表	100
表 6-2	印本资源处理业务及说明表	108
表 6-3	网络电子资源加工业务及说明表	108
表 6-4	元数据标引业务及说明表	109
表 6-5	异构资源整合业务及说明表	109
表 6-6	数字资源管理业务及说明表	109
表 6-7	硬件设备业务及说明表	110



表 6-8	系统和软件的开发业务及说明表	110
表 6-9	维护业务及说明表	111
表 6-10	用户服务业务及说明表	111
表 6-11	各馆开展业务比例分配表	113
表 6-12	数字图书馆业务开展情况排名表	113
表 6-13	部门名称及其他称谓对照表	115
表 6-14	业务与部门对照表	117
表 6-15	各类型图书馆开展业务比例列表	120
表 6-16	数字图书馆业务流程表	121
表 7-1	ISO27001 资产分类表	126
表 7-2	数字图书馆资产分类表	126
表 7-3	数字图书馆资产类别列表	128
表 7-4	资产保密性赋值表	130
表 7-5	资产完整性赋值表	130
表 7-6	资产可用性赋值表	130
表 7-7	资产价值赋值表	131
表 7-8	数字图书馆资产估值情况详表	132
表 7-9	数字图书馆威胁列表	136
表 7-10	数字图书馆威胁赋值表	136
表 7-11	数字图书馆的威胁等级列表	137
表 7-12	图书馆威胁与脆弱性存在比例的分布情况列表	139
表 7-13	脆弱性严重性赋值表	140
表 7-14	信息安全风险计算示例	141
表 7-15	数字图书馆安全风险等级表	142
表 8-1	ISO27002 各控制要素对数字图书馆的作用排序表	146
表 10-1	N 大学数字图书馆资产类别列表	190
表 10-2	N 大学数字图书馆面临的威胁分类表	191
表 10-3	N 大学数字图书馆面临的威胁相关数据列表	191
表 10-4	N 大学数字图书馆威胁与脆弱性识别对照表	193
表 10-5	N 大学数字图书馆现有控制措施识别及实施程度调查表	196
表 10-6	单位风险指数的资产损失值调查结果列表	199
表 10-7	N 大学数字图书馆所有资产的资产价值列表	202
表 10-8	N 大学数字图书馆所面临的威胁等级计算表	206

表 10 - 9	“拒绝服务攻击”威胁对应的“操作系统存在漏洞”脆弱性计算列表	207
表 10 - 10	N 大学数字图书馆数据库平台风险值计算表	208
表 10 - 11	N 大学数字图书馆风险等级定义表	209
表 10 - 12	N 大学数字图书馆所有资产的风险值及风险等级分布情况统计表	209
表 10 - 13	数据文档类“很高”风险威胁—脆弱性—控制措施对照表	213
表 10 - 14	数据文档类“很高”风险的控制措施计算结果列表	214

第一章 绪 论

从 20 世纪 90 年代起,数字图书馆的研究及实践在全球蓬勃发展。从美国的数字图书馆先导计划、美利坚记忆和 NSDL 计划,到欧盟的“欧洲图书馆”以及中国的多项数字图书馆工程项目,在新技术的开发与应用、资源的积累、相关标准的制订、服务环境的建设等各方面都已经取得了很大的成就。伴随着数字资源的积累与网络存取的开放性,数字图书馆的信息安全问题成为数字图书馆实践与研究中的热点和前沿问题。

在当前的实际工作中,数字图书馆信息安全问题有重概念轻实施、重技术轻管理的倾向。同时,由于信息安全问题专业性强,牵涉面广,信息安全管理体系建设工作量巨大,数字图书馆在实施过程中常有无所适从之感或畏难情绪。研究数字图书馆信息安全风险评估与风险控制,目的是为数字图书馆的信息安全问题提供理论上完备、现实中具操作性、实施过程简便易行的解决方案,改变数字图书馆信息安全管理过于依赖防火墙、反病毒、入侵检测的现状,在不提升技术条件的前提下解决数字图书馆信息安全管理的现实问题,促进数字图书馆事业的发展。

目前,国内外数字图书馆界对信息安全的概念与重要性已有了较清楚的认识。近年来,国内外对数字图书馆信息安全的研究主要集中在技术、管理与法律法规三个方面。目前国内的绝大部分研究都着重于技术,即计算机与网络安全技术在数字图书馆的应用。如:数据备份与软件更新、密码技术、杀毒软件、身份认证与访问控制、防火墙技术、漏洞扫描与检测等。管理方面,国内有研究者在分析管理的重要性的基础上,从人员管理、设备管理、灾难恢复制度、用户与员工的培训和监督方面提出了某些一般性的管理措施。国内也有学者强调了法律法规建设的重要性,并提出要加强执行力度。法律法规在国外的研究中被纳入管理的范畴,即管理措施应符合法律法规的要求、安全风险控制在法律法规许可范围内。总的来看,国内有关数字图书馆信息安全管理方面研究缺乏系统性,研究内容显得比较空泛,没有可操作的解决方案。

国外统计表明,70%的信息安全事件产生的原因并不是来自外界的病毒和黑客,而是来自内部的未授权访问,许多信息安全问题仅仅依靠产品和技术根本无法解决,而应依靠技术与管理的结合,所谓“三分技术七分管理”。因此,国外学者提出了信息安全管理与信息安全技术并举的观点,并在实践上加以贯彻执行,制定了



一系列的信息安全管理的规范与标准。如:美国卡内基·梅隆大学的 OCTAVE、美国审计总署的 GAO/AIMD—98—68 和 GAO/AIMD—99—139、澳大利亚和新西兰的 AS/NZS 4360、美国国家标准和技术学会的 NIST 风险管理框架、国际标准 ISO27000 系列等。特别是 ISO27000 系列国际信息安全管理标准的发布,得到多个国家的认可与接受,在各个行业得到应用,中国国家质量监督检验检疫局、国家标准化委员会已接受并转化为对应的中国国家标准。

数字图书馆的信息安全管理是数字图书馆管理的组成部分,数字图书馆信息安全管理体的建设是数字图书馆各项业务与服务功能正常开展的前提与保证。数字图书馆信息安全管理的必要性自不待言,但在理论研究与具体实践过程中应既牢记其他行业“三分技术七分管理”的宝贵经验,又遵循国际国内强制性及得到广泛认可的各项推荐标准与规范。

基于其他行业信息安全领域的研究成果与实践经验,可以得出这样的结论:解决信息安全管理问题的主要出路在于管理体系,数字图书馆也是如此。数字图书馆可以在不提升技术水平的前提下依靠管理的改进大幅提高数字图书馆信息安全的层级、降低安全风险,并且针对数字图书馆这一特定类型的信息系统,可以制定出操作性很强的风险评估与风险控制模型,供数字图书馆使用。

将在企业和政府机构得到广泛应用的信息安全管理标准引入数字图书馆领域,从规范管理行为入手提升数字图书馆信息安全状况,改变数字图书馆信息安全过于依赖防火墙、反病毒的状况,并强调安全管理的操作性,为数字图书馆信息安全的风险评估与风险控制提供模板,降低数字图书馆信息安全管理体建立与实施的难度,减少工作量。这就是本书的目标。为了实现这一目标,须将信息安全领域的标准和规范应用于数字图书馆这一业务趋同性很强的特定组织类型,设计数字图书馆信息安全风险计算和风险控制数学模型,在数据调查的基础上总结出数字图书馆风险评估与风险控制的模板,制定数字图书馆信息安全管理的步骤,并用实际数字图书馆的信息安全管理实践验证模型、模板和方法的可行性。

为了从现实的数字图书馆信息安全管理工作中总结带普遍性的原则与规范,需要以国内建设情况较好的有典型性与代表性的数字图书馆为调查对象,针对数字图书馆建设现状,信息安全管理现状,数字图书馆业务流程,数字图书馆资产及估值、威胁及估值、脆弱性及估值、风险控制措施等方面进行数据调查。整个数据调查过程比较复杂,涉及的因素较多,某种意义上相当于对所有被调查的数字图书馆做一遍粗略的风险评估与风险控制措施筛选。

本书将数字图书馆定位于建立在传统的实体图书馆之上的数字图书馆部分。参与调查的数字图书馆应该属于某个已开展传统的图书馆服务的实体图书馆,在此前提下,该馆的服务理念和建设规划应该遵循数字图书馆的要求,拥有一定的数

字资源,并且已经开展相关的数字图书馆业务,这是数字图书馆信息安全管理调查对象的基本要求。

最终参与调查的数字图书馆为全国三十家已经建设有数字图书馆部分的公共图书馆和高校图书馆。其中,公共图书馆有省级馆、地市级馆和县级馆三种,高校图书馆有综合类、理工类、经济类、农林类、医药类等多种。数字图书馆建设需要大量的资金支持,因此调查对象选定为在数字图书馆建设方面有一定基础的发达地区的图书馆。调查范围覆盖了江苏、浙江、广东、辽宁、北京、上海四省和两直辖市,所处的城市包括南京、北京、上海、杭州、苏州、常熟、张家港、常州、广州、深圳、东莞、大连等,均为经济发达地区。

所有参与调研的图书馆除了保留有传统的采编、流通等图书馆业务外,都不同程度地开发建设有数字图书馆,并且开展了文献传递、特色数据库建设、参考咨询、馆际合作、个性化服务等活动和服务,工作重心逐渐向网络化、数字化方向转移。这些图书馆有各自自成体系的常规业务和特色业务,符合数字图书馆信息安全管理调查的基本要求。

参与调研的公共图书馆有 10 家,比例为 33.3%,高校图书馆有 20 家,比例为 66.7%。其中公共图书馆中,省级馆有 2 家,占全部参与调研的公共图书馆的 20%,地市级图书馆有 6 家,占全部参与调研的公共图书馆的 60%,县级市馆有 2 家,占全部参与调研的公共图书馆的 20%。

从地区分布来看,全部参与调研的图书馆中,来自辽宁的图书馆占 3.3%,来自浙江、上海的图书馆各占 6.7%,来自北京的图书馆占 13.3%,来自广东的图书馆占 20%,来自南京的图书馆占 30%,来自除南京以外的江苏其他地区的图书馆占 20%。

由于需要调查掌握的数据繁多,且许多数据即使数字图书馆的工作人员也没有现成答案,需要调查人员与被调查对象经过长时间的沟通、交流与探讨才能得出一个基本满意的答案,因此,数据调查过程不能采用简单的问卷发放、填写与回收的办法,而是多种调查方法的结合。具体来说,整个调查过程用到了走访与面谈、利用现代通信工具进行沟通、网站调查、现场考察、专家访谈、问卷填报等多种调查方法。

本书主要包括七个方面的内容:

(1) 对国内数字图书馆建设与信息安全管理现状的调研。

在梳理数字图书馆与信息安全管理相关概念及国内外研究现状的基础上,本书以经济发达、数字图书馆建设基础较好的北京、上海、广州、深圳、杭州、大连、南京及苏南地区的数字图书馆的调查数据为依据,对国内数字图书馆建设与信息安全管理的现状进行了阐述,统计了数字图书馆出现的安全事件与应对措施,分析了