DOI:CNKI:11-2746/G2.20111117.0930.001

对《数字图书馆安全管理指南》及其“解读”的辨析

黄水清　任　妮

摘　要　《数字图书馆安全管理指南》及《〈数字图书馆安全管理指南〉解读》存在不当之处,尤其是对于 ISO 27000 以及风险管理相关定义和流程的理解存在偏差。本文结合 ISO 27000 系列标准以及数字图书馆信息安全领域的调查数据,针对存在的问题依次从数字图书馆安全管理的相关概念、依从标准选择、实施流程、控制要素四个角度进行辨析,旨在梳理 ISO 27000 系列的各个标准之间以及信息安全相关概念及要素之间的相互关系,以利于将其合理准确地运用在数字图书馆领域。表 1。参考文献 22。

关键词　数字图书馆安全管理指南　信息安全管理　ISO 27000

分类号　G251

The Analysis of *A Guide to Digital Library Security Management* and Its Interpretation

Huang Shuiqing & Ren Ni

ABSTRACT　This paper conducted a comprehensive review of the ISO27000 series of standards and related research on information security management in digital libraries. In particular, we pointed out the flaws and misunderstandings in A Guide to Digital Library Security Management and The Interpretation of A Guide to Digital Library Security Management from four perspectives including related concepts, selection of standards, implementation processes, and control measurements. We then suggested approaches to improve information security management in digital libraries, which has useful practical implications for the development of digital libraries. 1 tab. 22 refs.

KEY WORDS　*A Guide to Digital library Security Management.*　Lnformation security management.　ISO 27000.

1　问题的提出

2010 年在全国数字图书馆建设和服务联席会议第十次会议上发布了由上海图书馆主持编写的《数字图书馆安全管理指南》(以下简称《指南》)。《指南》阐述了数字图书馆安全管理的含义及目的,强调了从安全政策、过程管理、访问控制、信息资源安全、备份与容灾、环境安全、应急响应与安全公告等角度关注安全管理的操作实施[1]。2011 年 1 月,赵亮等人发表了《〈数字图书馆安全管理指南〉解读》一文(以下简称《解读》),介绍了《指南》制定的原则与思路,并对其中的条款进行了分析说明[2]。《指南》的制定对于指导和规范数字图书馆安全管理的操作模式和实施方法有现实意义,但《指南》及《解读》也存在诸多不恰当之处,尤其是对于 ISO 27000 以及风险管理相关定义和流程的理解存在偏差。本文将结合 ISO 27000 系列标准以及数字图书馆信息安全领域的调查数据,针对《指南》及《解读》中存在的问题依次从数字图书馆安全管理的相关概念、依从标准选择、实施流程、控制要素四个角度进行辨析,意在梳理 ISO 27000 系列各个标准之间以及信息安全相关概念及要素之

通讯作者:黄水清,Email: sqhuang@njau.edu.cn

间的相互关系,以利于将其合理准确地运用在数字图书馆领域。

2 概念辨析

定义是对研究对象的界定和规范,也是进行科学研究的前提。《指南》中最重要的一个条款是对数字图书馆信息安全的定义[2]:"数字图书馆信息安全是指保护数字图书馆中的信息系统相关资产免受任何可能的威胁和损失,保持其中信息资源完整性和可用性并保障其实现所设定信息服务和其它功能的行为。数字图书馆中的信息系统相关资产可包含物理资源、软件资源与信息资源等。其中信息资源是指以数字形式发布、存取和利用的信息资源总和"[1]。同时,《指南》侧重于风险控制,基本未涉及风险评估。然而,且不论作为一种行业指南而言,《指南》对数字图书馆信息安全的定义是否具备代表性和权威性,单从准确性而言,指南存在三大问题:否认了数字图书馆信息安全的"保密性";信息资产定位不准确;使信息安全管理等同于风险控制,忽视了作为风险控制前提与管理基础的风险评估环节。

2.1 数字图书馆安全管理

诚如《解读》所分析,数字图书馆安全问题的本质就是数字图书馆的信息安全问题,数字图书馆安全管理与数字图书馆信息安全管理的概念之间可以划等号。因此,探讨"数字图书馆安全管理"的概念,应该从信息安全入手。《指南》认为信息安全即保持信息资源的完整性和可用性。

国际标准化组织 ISO/IEC 在"IT 安全管理指南(GMITS)"中对信息(Information)一词给出的解释得到国际社会的公认:信息是通过施加于数据上的某些约定,当前赋予这些数据的特定含义。ISO 27001 中指出"信息是一种资产,对于组织的业务不可或缺"。而"安全"一词的基本含义为"远离危险的状态或特性"或"客观上不存在威胁,主观上不存在恐惧"。因此,"信息安全"可以直观解释为"让信息远离危险"或"保证信息的安全性"。ISO 27001 强调信息安全就是要保护信息免受威胁的影响,从而确保业务的连续性,缩减业务风险,最大化投资收益并充分把握业务机会。同时给出了一个定义:信息安全即保持信息的保密性、完整性、可用性及其他属性,如真实性、可核查性、抗抵赖和可靠性[3]。

由此可见,保密性、完整性和可用性是验证信息安全与否的三大基本属性。其中,保密性意指信息不被任何未授权的人、实体或技术手段获取;完整性是指保护信息的准确和完整;可用性含义为授权人可以获取和使用所需要的信息。保密性是指信息源头的安全性,完整性是指信息传输过程的安全,可用性是针对信息用户而言,是指准确的信息内容为授权人所用。保密性、完整性和可用性贯穿于信息传输的全部过程,三大基本属性相互作用、相互影响、缺一不可。而《解读》认为"《指南》没有强调保密性,因为从字面意义上讲,保密性更容易使人联想起加密、解密与相关安全技术",因此数字图书馆信息安全不需要保密性,这是说不通的。首先,知识产权保护是数字图书馆建设需要解决的首要问题,数据加密技术、信息伪装技术、数字水印技术恰恰是国内外数字图书馆信息安全相关技术研究的重点和热点[4-8]。其次,保密不等于加密,任何信息都是有密级的,只是密级不等而已,如数字图书馆的用户信息不对外公开、数字资源被限定在一定的 IP 地址范围内访问都是保密措施。因此,单从对数字图书馆的作用而言,保密性更是必不可少,而现实中的数字图书馆在业务开展过程中多多少少都对信息资产进行了一定程度的保密。《指南》忽略信息资产的保密性没有依据可言,是不准确的。

对于数字图书馆信息安全,王东波[9]、黎平国[10]、郭建峰[11]、王召龙[12]等学者分别给出过自己的定义,但这些定义对数字图书馆信息安全的内容及特点进行的阐述都稍显单薄。而《指南》中数字图书馆信息安全的定义是从作用和目标的角度定义,除忽略了保密性这一重要属性外,也同样只是从某一角度进行定义,若作为研究探讨无分可厚非,作为一种行业指南,则

没有依据。

数字图书馆信息安全就是信息安全在数字图书馆领域的运用,因此,完全可以将 ISO 27000 对信息安全的定义与数字图书馆的特点相结合,从而得到数字图书馆信息安全的定义。即,保持数字图书馆各项信息的保密性、完整性和可用性,使得数字图书馆传递给用户的信息具有真实性、可核查性、抗抵赖和可靠性。其中,保密性、完整性和可用性是数字图书馆信息安全的完整体系和内核,真实性、可核查性、抗抵赖和可靠性是数字图书馆提供给用户的信息服务的质量标准[13]。数字图书馆信息安全的保密性指避免非授权者伪装授权用户的身份获得信息资源,也指保证攻击者不能够获得管理员的权限。数字图书馆信息安全的完整性是指在数字化信息存储和传输过程中,防止被未经授权的用户篡改,保证数字图书馆系统上的数据和信息的绝对真实和可靠。数字图书馆信息安全的可用性是指保证数据的获取途径始终畅通,保证数字图书馆的信息内容与相应功能可随时提供给授权用户[14-15]。

"管理"即组织中的管理者通过实施计划、组织、人员配备、领导、控制、创新等职能来配置组织资源和活动,进而更有效地实现组织目标的过程[16]。管理是计划、组织、领导、控制的总和,其本身是一个活动过程。ISO 27000 强调信息安全管理采用过程方法,即 PDCA 过程,这与"管理"本身定义是相符的。因此,"数字图书馆信息安全管理"可以简单地定义为:保持数字图书馆各项信息的保密性、完整性和可用性,使得数字图书馆传递给用户的信息具有真实性、可核查性、抗抵赖和可靠性的全部过程。

2.2　数字图书馆的资产

在 ISO 27000 中,资产定义为"任何对组织有价值的事物"。这个定义直接引用了 ISO/IEC 13335-1:2004 中的定义。并且,ISO 27001 中给出了一个资产分类的示例[3](见表 1)。

表 1　ISO 27001 资产分类

分　类	示　例
信息	数据库和数据文件、合同和协议、系统文件、研究信息、用户手册、培训材料、操作或支持程序、连续性计划、应急安排、审核记录、归档信息
软件资产	应用软件、系统软件、开发工具和实用程序
实物资产	计算机设备,通信设备,可移动介质,其他设备
服务	计算和通信服务、公共服务,例如供暖、照明、供电、空气调节
人员	人员的资格、技能和经验
无形资产	组织的名誉和形象

由此可见,组织的资产除了应该包括信息、软件和物理设备等这些可见的有形资产外,服务、名誉、形象等无形资产以及人力资源也应认定为组织必不可少的重要资产。

在数字图书馆中,资产即指数字图书馆所拥有或者能控制的一切能为数字图书馆带来社会与经济利益(即对数字图书馆有价值)的事物或资源,包括信息本身、信息处理设施、参与信息处理过程的人员以及服务等。《指南》中对资产的定义仅从物理资源、软件资源与信息资产等实物资产考虑,是有狭隘和局限性的。笔者通过对数字图书馆业务流程和部门设置等相关因素的分析调研,以 ISO 27001 提出的分类示例为基本依据,将数字图书馆的资产分为电子资源、数据文档、实物资产、软件资产、服务、人员等六大类,并在每个大类下设置二级类目[17]。

2.3　信息安全管理、风险评估与风险控制

ISO 27000 将信息安全风险管理定义为:指导和控制一个组织风险的协调活动,包括风险

评估、风险处置、风险接受和风险沟通四个过程。信息安全风险管理从信息安全风险评估开始,然后对风险评估中不可接受的风险选择并且执行措施来更改风险(风险处置),使全部风险处于可接受的范围内(风险接受),再就决策者与其他内部人员及用户心中存在的与信息安全有关的担忧及有争议的问题以科学为基础进行有效的信息交换与共享(即风险沟通)。而风险控制,在 ISO 27000 中并没有定义,多数情况下指风险处置与风险接受,有时也等同于风险处置。因此,信息安全风险管理两个最主要的过程即为风险评估和风险控制。

风险评估是"风险分析和风险评价的全过程"。风险分析指的是系统地使用信息以识别来源和估计风险;风险评价是依据给定的风险准则比较已估计的风险,从而确定风险严重程度的过程。风险控制是指风险管理者依据风险评估的结果,选择并实施控制措施,以将风险控制在组织可接受的范围内[18]。风险评估是风险控制的前提和基础,是确定组织信息安全要求的途径之一。在信息安全管理体系的 PDCA 循环中,风险评估主要属于策划阶段,风险评估的结果将为选择控制措施来防范风险提供指导,并且用于确定适当的管理措施和优先级。在数字图书馆中,风险评估用于识别数字图书馆所面临的安全风险,并计算具体风险的等级值,作为实施风险控制的依据。

风险控制是风险评估的后续工作,是信息安全风险管理目标的具体实现,也是保障组织信息安全的关键环节。通过风险控制降低风险程度,确保风险在安全要求可接受的范围内。风险控制过程分为控制措施的识别与选择、控制措施的实施、风险接受三个阶段。在信息安全管理体系的 PDCA 循环中,控制措施的识别与选择属于策划环节,控制措施的实施与风险接受属于实施环节。

在数字图书馆的信息安全管理过程中,风险评估和风险控制是同样必不可少的两个部分,它们是两个并列的概念,在实施顺序上有先后之分,却无重要程度的大小之分。如果一定要区分两者之间的重要性,风险评估反而应在风险控制之上,因为没有风险评估作为基础,风险控制便是无源之水、无本之木。《指南》脱离风险评估而实施风险控制有无的放矢之嫌。

3 标准选择

《指南》指出选择恰当的依从标准是一个行业进行信息安全管理的关键所在,但在标准的内容及相互关系方面却对 ISO 27000、ISO 27001 和 ISO 27002 出现了误读,仅因为 ISO 27001 的复杂而否定了它在 ISO 27000 系列中的主导地位和重要作用,割裂了它与 ISO 27002 的关系、忽视了它在 ISO 27000 系列标准中的支撑性地位,是不可取的。《指南》仅"选择了 ISO 27002(即 GB /T 22081 – 2008)的内容作为指南文本的主要参照"[2],还带来了在《指南》中只重视风险控制,基本没有涉及风险评估的缺陷。

3.1 ISO 27000、ISO 27001 与 ISO 27002 简介

ISO 27000 系列标准起源于在世界范围已被广泛采用的信息安全管理体系标准 BS7799。BS7799 标准于 1993 年由英国贸易工业部立项,由两部分构成:BS7799 – 1《信息安全管理实施细则》(1995 年发布);BS7799 – 2《信息安全管理体系规范》(1998 年发布)。

2000 年 12 月,BS7799 – 1 通过国际标准组织 ISO 和国际电工委员会 IEC 的认可,正式成为国际标准 ISO/IEC 17799。2005 年,ISO 决定用新的标准号 27000 命名信息安全管理系列标准。2005 年 5 月,ISO 17799 进行了修订改版,成为 ISO 17799:2005,并于 2005 年 6 月以更改后的新标准编号 ISO/IEC 27002:2005 出版,ISO/IEC 27002 正式诞生。2005 年 10 月,BS7799 – 2:2005 出版,并正式转化为国际标准 ISO/IEC 27001:2005。至此,ISO 27000 系列标准的框架基本形成。

在 ISO 27000 系列标准中,ISO 27001 从组织整体业务风险的角度,为建立、实施、运行、监视、评审、保持和改进文件化的信息安全管理体系(ISMS)规定了要求并提供了方法。内容共分 8 章和 3 个附录,其中附录 A 的内容直接引用并与

ISO 27002 第5—15 章一致[3]。ISO 27002 详细规定了适用于各类组织、不同应用程序、系统及技术平台的控制措施,并保证组织在标准化过程中不损失任何利益,共包含 11 个控制域、39 个控制类、133 个控制点、500 个左右的子控制点[19]。

目前,ISO 27000 系列标准中已开发和规划中的标准有 22 个。除 ISO 27001 与 ISO 27002 外,已开发的标准还有:ISO/IEC 27000:2009,概况与术语;ISO/IEC 27003:2010,信息安全管理体系实施指南;ISO/IEC 27004:2009,信息安全管理度量和改进;ISO/IEC 27005:2008,信息安全风险管理指南;ISO/IEC 27006:2007,信息安全管理体系审核认证机构要求;ISO/IEC 27011:2008,电信机构基于 ISO/IEC 27002 的信息安全管理指南;ISO/IEC 27799:2008,使用 ISO/IEC 27002 的医疗信息安全管理。

3.2　ISO 27000、ISO 27001、ISO 27002 的关系

ISO 27000 有两个含义:ISO/IEC 27000:2009 和 ISO 27000 系列标准。本文中的 ISO 27000 大多数情况下并非指 ISO/IEC 27000:2009,而是指 ISO 27000 系列标准,它由多个标准组成,共同指导信息安全管理体系建设活动。其中,ISO 27001 是 ISO 27000 系列的主标准,类似于 ISO 9000 系列中的 ISO 9001,是认证机构实施认证审核过程的主要审核依据,各类组织可以按照 ISO 27001 的要求建立自己的信息安全管理体系,并通过认证。ISO 27002 是实施 ISO 27001 的支撑标准,它给出了组织建立 ISMS 时应选择实施的控制目标和控制措施集,可以作为开发组织安全标准和安全管理的实践指南。而 ISO 27000 系列的其他标准都是对 ISO 27001 和 ISO 27002 的补充说明或者在不同行业的应用。

因此,ISO 27001 与 ISO 27002 是 ISO 27000 系列标准的核心,它们分别描述了组织的信息安全风险评估与风险控制的方法与流程。ISO 27001 采用"策划、实施、检查、改进"(PDCA)模式构建信息安全管理体系,从而确定组织的风险所在。ISO 27002 为了满足风险评估的需要而列出了详细的风险控制措施以供选择。如同风险控制不能脱离风险评估而独立存在一样,ISO 27001 和 ISO 27002 应用于信息安全管理过程的不同阶段,两个标准密不可分,同等重要,不能舍弃任何一个。

虽然,以 ISO 27001 为依据建立信息安全管理体系进行风险评估所需要的方法复杂、时间跨度长、耗费经费多、操作难度大,相比之下,仅仅选用 ISO 27002 进行风险控制似乎更容易理解也更容易操作。但是如上分析,《指南》将 ISO 27002 脱离于 ISO 27001,从而代替 ISO 27000 系列标准作为信息安全管理依从标准的作法是不可取的。ISO 27001 与 ISO 27002 综合起来才是数字图书馆信息安全管理最适合的依从标准[3,19-20]。

4　过程方法

"过程方法"对信息安全管理的实践有指导意义,是任何安全管理标准体系不可或缺的重要内容。《指南》的"过程管理"与"过程方法"类似,但是地位不突出,内容不具备操作的可行性。

4.1　过程方法的重要性

过程方法是质量管理体系中行之有效的方法。2004 年 5 月 13 日,国际标准化组织质量管理和质量保证技术委员会(ISO/TC 176)的 SC2 制定了对"过程方法"的理解和应用指南文件《管理体系过程方法的概念和使用指南》,即 ISO/TC 176/SC 2/N 544R2(r)。ISO/TC 176/SC 2/N 544R2(r)将过程方法解释为一种对活动进行管理使之能为客户和其他相关方创造价值的有效方式[21],组织内诸过程的系统应用及这些过程的识别、相互作用与管理可称为"过程方法"[3]。

"过程方法"是信息安全管理实施的框架和指南,可以清晰有条理地阐述信息安全管理的操作步骤。总揽国际著名的信息安全管理标准(指南),GAO/AIMD-99-139 的评估风险与确定需求、实施方针与控制、提高意识、监控与评价

的循环过程，NIST 信息安全保障框架中的信息系统、选择安全控制、补充安全控制、文档化安全控制、实现安全控制、评估安全控制、认可信息系统、监控和改进安全控制八个步骤，OCTAVE 的三阶段（不含准备阶段）八过程的实施方法，AS/NZS 4360：1999 的建立环境、风险识别、风险分析、风险评价、风险处理、风险监控与回顾、通信和咨询风险管理七个步骤，都有明确的“过程方法”作为实施的基本路线。

过程方法在应用于信息安全管理时应着重强调以下方面：了解组织的信息安全要求及建立信息安全策略和目标的需求；在组织的整体业务风险框架内，通过实施和运行控制以管理组织的信息安全风险；监视和评审信息安全管理体系的业绩和有效性；基于客观测量的持续改进。因此，“过程方法”不可简化，更不能缺乏。

《指南》中提出“数字图书馆安全主要应关注以下相关要素，包括安全政策、过程管理、访问控制、信息资源安全、备份与容灾、环境安全、应急响应与安全公告等内容。”根据 ISO 27002，安全策略、访问控制、信息资源安全、备份与容灾、环境安全、应急响应与安全公告等与 ISO 27002 中的某些控制域（或控制类别、控制措施）基本对应。《指南》中对“过程管理”的表述虽然不尽完善，但是其本意应该是指信息安全管理的“过程方法”，对应于 GAO/AIMD-99-139 的四阶段循环 、NIST 的八个步骤、OCTAVE 的三阶段八过程、AS/NZS 4360：1999 的七步骤、ISO 27000 的 PDCA 。“过程方法”应是《指南》的方法论与实施路线，跟“目的、定义及相关说明”一样，应居于具体的控制措施之上，与控制措施并非并列关系，更不属于控制措施之一。

4.2 数字图书馆安全管理的过程方法

《指南》认为“过程管理是确立数字图书馆安全目标，建立组织架构，明确职责，进行角色分配、风险评估、安全审计、系统分类、制订预案、事故处理、回顾检查和改进的过程”，虽然其中确立目标、建立组织、风险评估、事故处理等源自于 ISO 27000 过程方法的部分内容，但是总体看来，这些内容之间没有时间先后顺序，不具备连贯性，甚至内容之间存在重复包含关系（如明确职责、进行角色分配都属于建立组织架构的内容），因此不能作为数字图书馆信息安全管理的实施依据。

《指南》中“过程管理”的第 2 条似在讲述风险评估和风险控制的做法，但是对于风险评估的三大要素“资产、威胁、脆弱性”，《指南》中只提到威胁和脆弱性。根据 ISO 27000，在风险评估中，资产、威胁和脆弱性是多对多的关系，其中，资产的识别可以通过研究组织的业务流程得到，而威胁和薄弱点依附于资产之上，它们的识别需要依赖于资产的确认。因此，脱离了资产，威胁和薄弱点也无从谈起。

ISO 27001 明确指出，信息安全管理体系采用的“策划—实施—检查—改进”（PDCA）过程方法适用于信息安全管理体系的所有过程[3]。该过程方法同样适用于数字图书馆信息安全管理[15]。依照 ISO 27000 系列标准的要求，数字图书馆信息安全管理体系建立与实施也应该采用 PDCA 的过程方法。

（1）P（策划）——建立信息安全管理体系环境，进行风险评估。策划阶段是为了确保正确建立数字图书馆信息安全管理体系的范围和详略程度，识别并评估所有的信息安全风险，为这些风险制定适当的处理计划。其中，所有重要活动都要被文档化，以备将来追溯和控制更改情况。其流程和内容包括：确定数字图书馆信息安全管理的范围和方针；定义数字图书馆风险评估的系统性方法；识别并评估数字图书馆的风险；识别并评价数字图书馆风险处理的方法；为数字图书馆风险的处理选择控制目标与控制方式；获得数字图书馆最高管理者的授权批准。

（2）D（实施）——实施并运行信息安全管理体系。实施阶段的任务是以适当的优先权进行管理运作，执行所选择的控制，以管理策划阶段所识别的信息安全风险。对于那些被评估认为是可接受的风险，不需要采取进一步的措施；对于不可接受风险，需要实施所选择的控制。实施阶段涉及人员、时间和资金的分配，将资源

有效合理地配置,以运行信息安全管理体系。

(3)C(检查)——监视并评审信息安全管理体系。检查阶段,又叫学习阶段,是 PDCA 循环的关键阶段。该阶段须分析运行效果,寻求改进机会。如果发现控制措施不合理、不充分,就要采取纠正措施,以防止数字图书馆处于不可接受风险状态。具体过程有:快速识别并检测风险控制措施的有效性,总结经验,预测结果,确定措施;定期对信息安全管理体系有效性进行评审,收集各方反应;评审剩余风险和可接受风险的等级;审核执行管理程序,确定规定的安全程序的恰当性和可行性;对数字图书馆信息安全管理体系进行定期的正式的评审(最少一年一次);记录并报告能影响信息安全管理体系有效性或业绩的所有活动、事件。

(4)A(措施)——改进信息安全管理体系。经过策划、实施、检查之后,数字图书馆在措施阶段必须对所策划的方案给出结论,是应该继续执行,还是放弃重新进行新的策划。这样,就可以开始新一轮的 PDCA 循环。

5　控制措施

恰当地选择控制措施可以指导一个行业在节约成本、减少工作量的基础上实现信息安全管理。《指南》的主体所阐述的"安全政策、过程管理、访问控制、信息资源安全、备份与容灾、环境安全、应急响应与安全公告"等安全要素(ISO 27002 中称为控制域),除了过程管理外,其余七项均可在 ISO 27002 中找到根据。但这些安全要素在 ISO 27002 中有很大程度的删减和改动,删减和改动的理由是什么?《指南》与《解读》未给出具体的解释。

5.1　ISO 27002 中控制措施的内容及运用

ISO 27002 包含 11 个控制域、39 个安全类别、133 个控制点(或称控制要素、控制措施),这些共同构成了 ISO 27000 的控制措施,又称为信息安全的通用惯例。其中 11 个控制域和 39 个安全类别分布情况如下[19]:

①安全方针,包含 1 个控制类:信息安全方针;②信息安全组织,包含 2 个控制类:内部组织、外部组织;③资产管理,包含 2 个控制类:资产责任、信息分类;④人力资源安全,包含 3 个控制类:雇佣前、雇佣中、雇佣的终止或变更;⑤物理和环境安全,包含 2 个控制类:安全区域、设备安全;⑥通信和操作管理,包含 10 个控制类:操作程序和职责、第三方服务交付管理、系统策划与验收、防范恶意和移动代码、备份、网络安全管理、介质处理、信息交换、电子商务服务、监视;⑦访问控制,包含 7 个控制类:访问控制的业务要求、用户访问管理、用户责任、网络访问控制、操作系统访问控制、应用系统和信息访问控制、移动计算和远程工作;⑧信息系统的获取、开发和保持,包含 6 个控制类:信息系统的安全要求、应用系统的正确处理、加密控制、系统文件安全、开发和支持过程安全、技术薄弱点管理;⑨信息安全事故管理,包含 2 个控制类:报告信息安全事故和弱点、信息安全事故管理和改进;⑩业务连续性管理,包含 1 个控制类:业务连续性管理的信息安全问题; ⑪符合性,包含 3 个控制类:与法律法规要求的符合性、与安全策略和标准的符合性以及技术符合性、信息系统审计考虑因素。

完善的控制措施集合是实时信息安全的一个良好起点,组织一旦确定了安全要求并作出风险处置的决策,就应该选择并实施控制措施以确保将风险降低到可接受的程度。ISO 27002 的控制措施尽可能地覆盖了各种组织类型的风险控制行为,其最大特点是周全。但在具体应用于某个或某一特定类型的组织时,周全往往成为繁琐、工作量巨大的代名词。ISO 27002 也强调部分控制措施可能并不适用于每一个信息系统或环境,或每一个组织。因此,选择合适的信息安全控制措施是对组织或系统进行信息安全保护的前提。缺乏恰当、完备的控制措施,可能会导致组织或系统额外的成本支出,也可能会削减控制措施的有效性,更甚者可能无法实现充分的信息安全。

5.2　适用于数字图书馆安全管理的控制措施

ISO 27002 指出,控制措施没有重要性的区

别,根据实际需要,所有控制措施可能都是重要的。所以,每个组织在使用 ISO 27002 时都需要识别出适用的控制措施,其重要性取决于组织的业务过程。因此,在数字图书馆信息安全风险控制过程中,需要识别出适用于数字图书馆的控制措施。然而,数字图书馆是一个集纸质、数字、人员、系统为一体的信息系统集合,实施信息安全风险控制的必要性毋庸置疑,但是如何选择合适的控制措施以保证其安全,在数字图书馆的研究领域尚为空白。在此情况下,数据调查是一种非常必要且可行的方法。笔者曾针对 ISO 27002 的所有控制措施对数字图书馆信息安全的适应性进行过详细的调查,调查目的是为数字图书馆核心控制措施的筛选提供数据支持。

通过调查统计,黄金分割法划定初筛结果及核心控制措施大致数量、专家访谈结果、数字图书馆业务及安全要求与 ISO 27002 标准比对分析,最终筛选得到的数字图书馆信息安全风险控制的核心控制措施 87 项,参考控制措施 34 项。其中,核心控制措施分布于 11 个控制域的 33 个控制类,参考控制措施分布于 10 个控制域的 22 个安全类别[22]。《指南》的七项控制措施虽来源于 ISO 27002,却作了大幅度的删改,其理由与依据不足。

6 结语

《解读》的末尾指出对于复杂的数字图书馆安全管理工作而言,《指南》只能算是一个起步,编写本身需要不断完善的过程,这一点毋庸置疑。但是,《指南》的制定需要以恰当的选择依从标准为前提,以充分的行业调研和分析为依据,以完善的实施方法和流程为主要内容,有针对性的控制措施为实施依据,而这些工作需要建立在对国内外信息安全管理标准(尤其是 ISO 27000 系列标准)充分认识理解和对国内数字图书馆信息安全管理广泛调研的基础上,也恰恰是在这两个方面,《指南》有所欠缺。对于数字图书馆信息安全管理,需要更多的学者在全面理解并遵守国际国内标准的基础上,以调研和实践为依据,寻求适合我国国情和数字图书馆行业特点的信息安全管理指南。

参考文献:

[1] 上海图书馆. 数字图书馆安全管理指南[EB/OL]. [2011-05-05]. http://www.lsc.org.cn/Attachment/Doc/1300959839.doc. (Shanghai Library. A guide to digital library security management[EB/OL]. [2011-05-05]. http://www.lsc.org.cn/Attachment/Doc/1300959 839.doc.)

[2] 赵亮,刘炜,徐强.《数字图书馆安全管理指南》解读[J]. 中国图书馆学报,2011(1):47-58. (Zhao Liang, Liu Wei, Xu Qiang. Interpretation of *a guide to digital library security management* [J]. Journal of Library Science in China, 2011(1):47-58.)

[3] ISO/IEC 27001:2005. Information technology—Security techniques—Information security management systems—Requirements[S]. Genevan: International Organization for Standardization, 2005.

[4] 黄宇. 图书馆网络安全技术的研究[J]. 黑龙江科技信息,2008(6):114-116. (Huang Yu. The study of library web security technology[J]. Heilongjiang Science and Technology Information, 2008(6):114-116.)

[5] 黄永跃. 数字图书馆的安全防护技术[J]. 现代情报,2005(3):97-99. (Huang Yongyue. The security protection technology of digital library [J]. Modern Information, 2005(3):97-99.)

[6] 李书宁,马明霞. 数字水印技术在数字图书馆安全性问题中的应用[J]. 现代图书情报技术,2002(1): 17-19. (Li Shuning, Ma Mingxia. The applying of digital watermark in digital library security[J]. New Technology of Library and Information Service,2002(1):17-19.)

[7] Gladney H M, Gantu, Arthur. Authorzation management for digital librarys[J]. Communications of the ACM, 2001(5):63-65.

[8] Drake, Miriam A. Safeguarding patrons' privacy [J]. Information Today, 2003(20):35.

[9] 王东波. 数字图书馆信息安全策略研究[J]. 江西图书馆学刊,2004(3):76-77. (Wang Dongbo. Policy study of information security of digital library[J]. The Journal of the Library Science in

Jiangxi, 2004(3):76 - 77.)

[10] 黎平国,钟守机. 数字图书馆的信息安全问题与相关对策的探讨[J]. 现代情报,2005(9):73 - 74. (Li Pingguo, Zhong Shouji. The problems and related countermeasures of digital library information security[J]. Modern Information, 2005(9):73 - 74.)

[11] 郭建峰. 数字图书馆安全体系探析[J]. 科技情报开发与经济,2007(18):7 - 9. (Guo Jianfeng. Probe into the security system of digital library[J]. Sci-Tech Information Development & Economy,2007(18):7 - 9.)

[12] 王召龙,许军振. 数字图书馆的信息安全[J]. 济南职业学院学报,2005(4):69. (Wang Zhaolong, Xu Junzhen. The security of digital library[J]. Journal of Jinan Education College, 2005(4):69.)

[13] 郑德俊,任妮,熊健,等. 我国数字图书馆信息安全管理现状[J]. 现代图书情报技术,2009(7/8):27 - 32. (Zheng Dejun, Ren Ni, Xiong Jian, et al. Current situation of information security management in digital libraries[J]. New Technology of Library and Information Service, 2009 (7/8):27 - 32.)

[14] 徐宽,刘万国,房玉琦. 数字图书馆安全特点及影响因素研究[J]. 现代情报,2008 (11):84 - 86. (Xu Kuan, Liu Wanguo, Fang Yuqi. The study on digital library security features and its influence fectors[J]. Modern Information, 2008(11):84 - 86.)

[15] 秦浩. 浅谈数字图书馆的信息安全管理[J]. 科技情报开发与经济,2008(4):49 - 50. (Qin Hao. Talking about the information security management of digital library[J]. Sci-Tech Information Development & Economy,2008(4):49 - 50.)

[16] 刘金芳. 现代管理学[M]. 成都:电子科技大学出版社,2010:1. (Liu Jinfang. Modern Management Science[M]. ChengDu: Press of Electronic Science and Technology University,2010:1.)

[17] 黄水清,茆意宏,熊健. 数字图书馆信息安全风险评估[J]. 现代图书情报技术,2009(7/8):33 - 38. (Huang Shuiqing, Mao Yihong, Xiong Jian. Assessment of information security risk in digital libraries[J]. New Technology of Library and Information Service,2009(7/8):33 - 38.)

[18] 王桢珍,谢永强,武晓悦,等. 信息安全风险管理研究[J]. 信息安全与通信保密,2007(8):164. (Wang Zhenzhen, Xie Yongqiang, Wu Xiaoyue, et al. A survey of information security risk evaluation[J]. Information Security and Communications Privacy,2007(8):164.)

[19] ISO/IEC 27002:2005. Information Technology - Security Techniques - Code of practice for information security management[S]. Genevan: International Organization for Standardization, 2005.

[20] 茆意宏,黄水清. 数字图书馆信息安全管理依从标准的选择[J]. 中国图书馆学报,2010(4):54 - 59. (Mao Yihong, Huang Shuiqing. On the choice of standards for information security management of digital library[J]. Journal of Library Science in China,2010 (4):54 - 59.)

[21] ISO/TC 176/SC 2/N 544R2(r):2004. Introduction and support package guidance on the concept and use of the process approach for management systems document. Genevan: International Organization for Standardization, 2004.

[22] 黄水清,任妮. 数字图书馆信息安全风险控制[J]. 现代图书情报技术,2009 (7/8):39 - 44. (Huang Shuiqing, Ren Ni. Control of information security risk in digital libraries[J]. New Technology of Library and Information Service,2009 (7/8):39 - 44.)

黄水清　南京农业大学信息科学技术学院教授。通讯地址:江苏南京卫岗1号。邮编:210095。

任　妮　南京陆军指挥学院图书馆助理馆员。通讯地址:江苏南京浦口龙盘路1号。邮编:210045。

(收稿日期:2011-08-17;修回日期:2011-09-09)