Digital Library Forum 数字图书馆论坛
http: // www.dlf.net.cn

从管理角度探求数字图书馆信息安全的解决之道
——《数字图书馆信息安全管理》书评

□ 李广建 / 北京大学信息管理系 北京 100871

摘要：随着数字图书馆的发展，数字图书馆的信息安全问题日益凸显，如何“在不提升技术条件的前提下通过管理手段解决数字图书馆信息安全的现实问题”，《数字图书馆信息安全管理》一书对此给出了解决方案，提出了数字图书馆信息安全管理的依从标准，构建了数字图书馆信息安全风险评估和风险控制的数学模型，提炼出了数字图书馆信息安全风险评估和风险控制的模板。该书是近年来数字图书馆领域中一部理论和实践相结合的优秀专著。

关键词：书评，数字图书馆，信息安全
DOI：10.3772/j.issn.1673—2286.2012.03.014

数字图书馆是新时代图书馆的发展方向，也是全球文化科技竞争的焦点和一个国家信息事业发展水平的重要标志。随着资源管理和服务的深化，数字图书馆在给人们便利的同时，其安全问题也日益凸显，如数据丢失、信息泄密、系统瘫痪、网络堵塞等，都会直接影响数字图书馆的服务水平和声誉。因此，加强数字图书馆信息安全的研究和防范出现各类安全问题，营造和谐的运行环境和服务氛围，已经成为数字图书馆理论与实践的重要内容。

从当前的研究和实践上看，数字图书馆的信息安全更多地依赖于计算机技术、网络技术和数据通信技术等专业技术，目前数字图书馆建设中也比较普遍地关注合理的网络拓扑结构、防火墙、系统加固技术。利用高质量的产品和技术解决数字图书馆的信息安全问题，固然没有错误。然而，有资料表明，70%的信息安全事件并非来自系统外部的网络攻击和病毒，而是来自系统内部的未授权访问。对于数字图书馆这种不仅要经由网络对外提供信息服务，而且内部各种业务全面依赖ICT技术的系统而言，情况更是如此。针对数字图书馆的这一特点，南京农业大学信息学院黄水清教授的新作《数字图书馆信息安全管理》（2011年由南京大学出版社出版），从管理角度给出了数字图书馆信息安全问题的解决之道。正如作者所说的那样，在数字图书馆中，“如果说技术是保障信息安全的手段，管理则是选择、使用、维护、审查包括技术措施在内的安全手段的整个过程。技术是点，管理是面，它将各种散乱的点组织在一起，形成一个坚实的整体”。

《数字图书馆信息安全管理》一书共计10章，49万余字，重点探讨并解决了以下三大问题：

（1）选定ISO27000系列标准为数字图书馆信息安全管理的依从标准

信息安全管理标准是一个组织建立并实施信息安全管理体系的指导性准则，它提供了有效的安全管理措施建议，并规范了信息安全管理的方法和程序，是一个组织进行信息安全管理不可或缺的一部分。目前，国内外的信息安全管理

标准数量繁多，作者从保护对象、管理过程、行业特点和国家地域特点等角度进行比较分析，最终确定ISO27000系列标准是最适用于数字图书馆信息安全管理的依从标准。该标准能够满足数字图书馆在组织类型、风险评估和风险控制过程、风险评估方法等诸多方面对于数字图书馆信息安全风险管理的要求，能够用于指导数字图书馆信息安全管理的实践活动。

（2）构建了数字图书馆信息安全风险评估和风险控制的数学模型

ISO27000中给出了用于信息安全管理的PDCA过程模式以及风险评估的通用模型框架，作者以此为基础，进一步研究探讨了适用于数字图书馆信息安全管理的风险评估和风险控制的具体步骤和模型。根据数字图书馆信息安全管理的现实情况，作者确定了从数字图书馆业务流程入手，识别和计算资产、威胁和脆弱性的风险评估过程，以及以资产、业务流程和控制措施为主要因素的风险控制操作过程。同时，根据充分的数据调研，构建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的联动关系模型。这些模型不仅可以具体计算数字图书馆的风险值，而且能够在平衡风险和投资利弊关系的基础上提出恰当的控制措施，为数字图书馆信息安全风险管理的实践活动提供恰当的方法论和实践指南。

（3）提炼出了数字图书馆信息安全风险评估和风险控制的模板

作者从数字图书馆的业务流程入手，对数字图书馆的资产、威胁和脆弱性进行识别和估值，建立了数字图书馆业务流程与资产的关联表以及数字图书馆资产—威胁—脆弱性的对照表，并根据风险评估模型计算得到数字图书馆的信息安全风险等级划分方法，构建了数字图书馆风险评估的模板。然后，在分析筛选得到数字图书馆信息安全管理的核心控制要素的基础上，确定了数字图书馆信息安全风险控制的目标，构建了数字图书馆风险控制模板。在数字图书馆信息安全管理的实际操作中，利用作者给出的模板，可以最大限度地降低数字图书馆信息安全管理体系建立与实施的难度，增强了数字图书馆信息安全风险评估和风险控制全过程的可操作性。数字图书馆信息安全风险评估和风险控制中需要的许多重要数据，都可以在作者提供的模板中获得。

总的来看，本书的最大特色是将数字图书馆信息安全问题的重心从技术转移到了管理上，提出了“在不提升技术条件的前提下通过管理手段解决数字图书馆信息安全的现实问题”这样一种创新性理念，对我国数字图书馆的信息安全管理极具启迪。同时，作者在数字图书馆风险评估和风险控制方法、模型、模板等方面的研究成果，可以直接应用到数字图书馆信息安全管理的实践中。这样一部理论和实践相结合的专著，非常值得我们关注和学习。

作者简介

李广建（1963-），北京大学信息管理系教授、博士生导师，研究方向为信息管理与信息系统。E-mail: ligj@pku.edu.cn

To Explore Information Security Solution for Digital Libraries from a Management Perspective
– Book Review of *Information Security Management of Digital Library*

Li Guangjian / Department of Information Management, Peking University, Beijing, 100871

Abstract: With the development of digital libraries, information security of digital libraries becomes an increasingly outstanding issue. The monograph "*Information Security Management of Digital Library*" answers the question of how to "solve the information security problems of digital libraries by means of management on the premise that the technical conditions are not enhanced", through the determination of compliant standard, the construction of mathematical models and the building of evaluation templates. The book is an excellent monograph with a combination of theory and practice in the field of digital libraries in recent years.

Keywords: Book review, Digital libraries, Information security

（收稿日期：2011-12-06）