中电力咨询

质量/环境/职业健康安全/信息安全

四标整合管理体系教程

北京中电力企业管理咨询有限责任公司 组编

光耀华 主 编

谢宗晓
程瑜琦 副主编

虞旭清 主 审

中国标准出版社

质量/环境/职业健康安全/信息安全

四标整合管理体系教程

主　编：光耀华
副主编：谢宗晓　　程瑜琦
主　审：虞旭清

中国标准出版社
北京

图书在版编目（CIP）数据

质量、环境、职业健康安全、信息安全四标整合管理体系教程/光耀华主编．—北京：中国标准出版社，2009
ISBN 978-7-5066-5428-9

Ⅰ.质… Ⅱ.光… Ⅲ.①质量管理体系-国家标准-中国-教材②环境管理-体系-国家标准-中国-教材
③劳动保护-劳动管理-体系-国家标准-中国-教材
④劳动卫生-卫生管理-体系-国家标准-中国-教材
⑤信息系统-安全管理-体系-国家标准-中国-教材
Ⅳ.F273.2-65 X-65 R132.2 TP309-65

中国版本图书馆 CIP 数据核字（2009）第 159471 号

中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码：100045
网址 www.spc.net.cn
电话：68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 787×1092 1/16 印张 26.5 字数 642 千字
2009 年 9 月第一版 2009 年 9 月第一次印刷
*
定价 58.00 元

前言

中华人民共和国国家质量监督检验检疫总局于2008年6月19日发布GB/T 22080—2008《信息技术　安全技术　信息安全管理体系　要求》(等同采用ISO/IEC 27001:2005,以下简称“信息安全管理体系标准”),为在我国开展信息安全管理体系建设提供准则。众所周知,近年来,信息安全问题日益突出,逐渐成为影响企业生存和发展的重要因素。信息安全管理体系(ISMS)和质量管理体系(QMS)、环境管理体系(EMS)、职业健康安全管理体系(SMS)具有许多共同的要求,其原理、方法、过程和体系结构也基本一致。所以,将上述四个管理体系进行整合就成为可能。

ISO/IEC 27001在其“范围”中指出:“如果一个组织已经有一个运转着的业务过程管理体系(例如,与ISO 9001或者ISO 14001相关的),那么在大多数情况下,更可取的是在这个现有的管理体系内满足本标准的要求。”也就是说,如果组织已经建立并运行着质量、环境、职业健康安全三标一体化管理体系,那么,无需从头做起,在现有管理体系的基础上将信息安全管理体系要求整合到三标一体化管

理体系中去，就可以成为“四标”整合管理体系。对于一个组织来说，这无疑是经济、快捷的强化管理之道。

多年来，我国广大企业积极贯彻 ISO 9001、ISO 14001、OHSAS 18001 三个国际标准，建立具有中国特色的质量、环境、职业健康安全三标一体化管理体系，无论是规范企业管理、提高经营管理水平，还是与国际接轨等方面，都取得了显著的成效。随着经济和科学技术的发展，信息安全问题被提出来了。国际标准化组织(ISO)于 2005 年推出了 ISO/IEC 27001 信息安全管理标准，用于建立信息安全管理体系，要求组织制定信息安全控制措施。事实上，信息安全问题寓于质量、环境、职业健康安全以及其他所有活动和服务之中。把信息当作资产，识别信息方面的风险，评价风险，采取相应的控制目标和控制措施，将有助于推进质量、环境、职业健康安全管理体系持续有效地运行。所以，把信息安全管理体系纳入“三标”管理体系，整合成“四标”管理体系就是势在必行之事了。而且，ISO/IEC 27001:2005 标准在制定过程中就已经考虑了与 ISO 9001、ISO 14001 的相容性，其基本思想、体系要素、标准结构都非常接近 ISO 14001。ISO/IEC 27001:2005 也要求体系文件化，规定管理职责，提供资源，进行内部审核和管理评审。对这些要求的满足在建立、运行“三标”一体化管理体系时，已经积累了成熟的经验。如果纳入信息安全管理标准中特有的要求，进行有机地整合，就成为“四标”整合管理体系了。所以，建立“四标”整合管理体系并不是一件很困难的事情。

经验证明，目前国际上通用的 ISO 9001、ISO 14001、OHSAS 18001、ISO/IEC 27001 四个管理标准具有鲜明的科学性、系统性和兼容性，内容上有许多共同点，四个标准都遵循相同的管理原理，采用相同的运行模式，提出可兼容的公共管理要求，而且，在我国已积累了不少成功的运行经验。所以，企业完全有条件结合自己的实际情况将质量、环境、职业健康安全、信息安全管理整合成一体化管理体系。这有利于优化资源配置，协调运作过程，局部服从整体，提高整体有效性，从而实现组织总的目标。

本书共分四篇。第一篇是整合管理体系概论，分述质量、环境、职业健康安全、信息安全四个管理体系的基本思想、原则以及标准的发展过程。在此基础上，论述管理体系整合的方法、特点、意义和建立“四标”整合管理体系的可行性。第二篇是四个标准内涵的释义，按照标准条文顺序逐条阐释条文要点，并辅以实例，为有意建立“四标”整合管理体系的组织提供实施指南。第三篇是管理体系专论，对在建立整合管理体系过程中经常遇到的一些问题作了深入的探讨，对包括体系策划、运行、监视、评价、文件编写、风险因素分析评价、法律法规知识、内部审核、管理评审和体系认证等在内的有关事项，进行了详细评述，具有较强的适用性和可操作性。第四篇是实施案例，介绍一些行业在最近几年贯彻质量、环境、职业健康安全、信息安全管理标准，建立整合管理体系的做法和经验。

本书内容广泛，理论明晰，结构严谨，文字简明。书中还配插了大量图表和案例，具有较高的理论水平和较强的实用性。

本书适用于各行各业贯彻“四标”或“三标”之用，可供广大企、事业单位管理人员，咨询机构咨询师，认证机构审核员使用，也可作为各类组织的内审员培训教材。

本书由北京中电力企业管理咨询有限责任公司主持编写。主编是教授级高级工程师、国家注册高级审核员、国家注册高级咨询师光耀华，他负责编写第一篇第1、2、3、4章，第二篇第6、7、8章，第三篇第10、11、12章和第13.1节～13.3节、14.1节～14.3节，以及第15、16、17章。程瑜琦、谢宗晓编写第一篇第5章，第二篇第9章，第三篇第13.4节、14.4节。第四篇为光耀华、谢宗晓合写。在编写过程中，湖北省电力勘测设计院、中国水电建设集团国际工程有限公司、国家电网公司宁波供电局等给予了大力支持，在此一并表示感谢。

编　著　者

2009年5月10日于北京

目录

第一篇 “四标”整合管理体系

第二篇　标准释义

第一篇

“四标”整合管理体系

第 1 章 “四标”整合管理体系概论

1.1 整合管理体系的提出

什么是“四标”整合管理体系？首先，“四标”是国际标准化组织(ISO)历年发布的三个国际标准(ISO 9001、ISO 14001、ISO/IEC 27001)和欧洲 13 个国家推出的 OHSAS 18001 标准。根据这些标准的要求各自建立起来的管理体系，是单标管理体系，即质量管理体系，环境管理体系，职业健康安全管理体系，信息安全管理体系，如果把四个单标管理体系加以有机的整合成为单一要素的管理体系，就称之为“四标”整合管理体系。

整合管理体系的提出，缘于企业的经营管理活动涉及方方面面，它包括质量管理、环境管理、职业健康安全管理、信息管理、人力资源管理、财务管理、物资管理、经营管理，以至于企业战略策划管理、党群管理、行政管理等。这些不同的管理类型为了完成各自的任务，都有自己的目标，都需要建立各自的体系(有时称之为“分体系”)，这些分体系之间，无论是组织结构、职责分配、资源配置，还是过程运作，客观上都可能发生职责交叉、重叠、脱节等不协调现象，影响工作效率，制约着企业目标的实现。如果一个企业一次次地进行不同体系的认证，就会带来许多重复工作，造成资源浪费，贯标效果也不一定理想。上述情况促使人们考虑管理体系一体化的问题，把分散的、多头的管理变为集中的、系统的、分类的管理。同时，也考虑多体系认证审核的联合实施问题。

所谓“管理体系”，在标准中有明确的阐述。ISO 9000:2005 给出的定义是：“建立方针和目标并实现这些目标的体系”。ISO 14000:2004 指出，管理体系是用来建立方针和目标，并进而实现这些目标的一系列相互关联的要素的集合。管理体系包括组织结构、策划活动、惯例、程序、过程和资源。

所谓“整合管理体系”，就是组织将两个或两个以上的管理体系经过有机的整合成为一个管理体系运行。如 ISO 9001 与 ISO 14001 整合、ISO 14001 与 OHSAS 18001 整合，或者 ISO 9001 与 ISO 14001、OHSAS 18001、ISO/IEC 27001 四者整合成为质量、环境、职业健康安全、信息安全一体化管理体系。这样的体系不是多个管理体系的简单叠加，而是按照系统化的原则形成统一而又相互协调、相互兼容、相互补充的有机整体。

任何管理都是对系统的管理。系统具有集合性、层次性和相关性特征。系统管理就是对系统内的组织结构、策划、职责、程序、过程和资源各要素之间的相互关系以整体为主进行协调、有序的管理，局部服从整体，达到整体效果最优。

如前所述，组织内有众多的管理类型所形成的管理体系，而按照 ISO 9001、ISO 14001、OHSAS 18001 和 ISO/IEC 27001 标准所建立起来的体系，有严谨的标准导引，且已被广泛应用，具有较成熟的运行经验，如果以科学的方式将它们进行整合，在共同的管理原则及可兼容的各标准条款的基础上，兼顾各分系统的特殊要求，就可以建立一个完整、有机、全新的整合管理体系。

所需的组织结构、策划、职责、程序、过程和资源，经过有机地整合，形成共有要素的单一管理体系”。采用质量管理体系(Quality Management Systems，简称 QMS)、环境管理体系(Environmental Management Systems，简称 EMS)、职业健康安全管理体系(Occupational

Health Safety Management Systems，简称 SMS）、信息安全管理体系（Information Security Management Systems，简称 ISMS）的第一个英文字母的集合，则“四标”整合管理体系可简称为 QESI。

应当指出，本书所称的“整合管理体系”虽然只包括质量、环境、职业健康安全和信息安全管理，但是，由于整合管理体系的扩张性能较强，它可为组织的其他管理体系提供导入的管理平台（见图 1-1）。通过这个平台，企业的各项管理最终都要纳入标准化的轨道，建立企业统一的标准化体系，即符合现代企业所要求的科学管理体系。

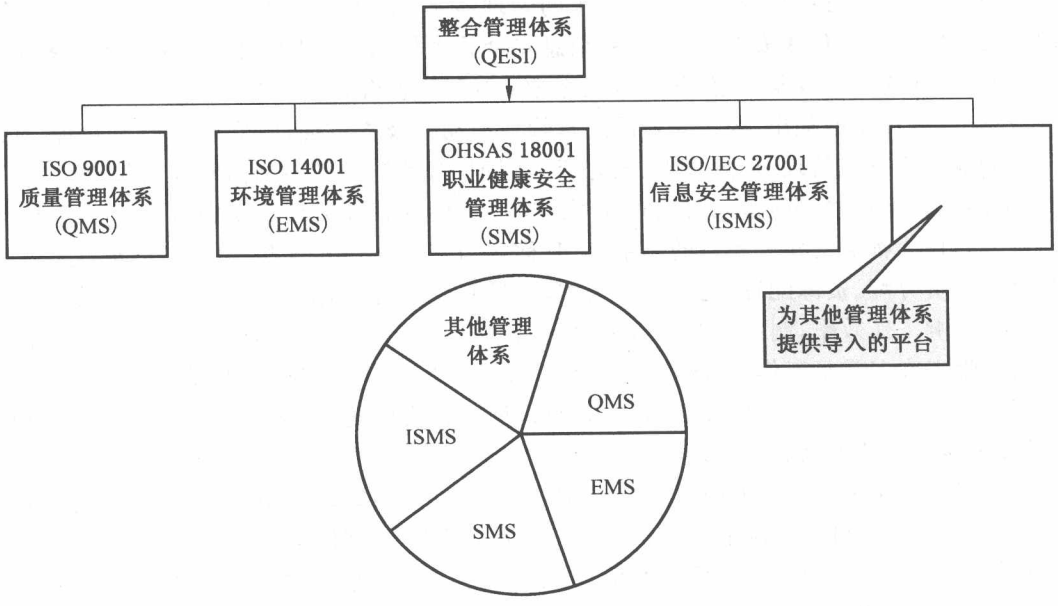

图 1-1 整合管理体系

整合管理体系是基于系统论、控制论、信息论的基本思想，采用先进的管理技术，如目标管理、过程方法、系统的管理方法、精益化管理、标准化管理、优化技术、信息技术等。它的优势在于既能合理配置资源，优化过程，协调目标，规范管理，还讲究效率，具有远见，追求系统整体有效性，以实现组织总的方针目标（见图 1-2）。

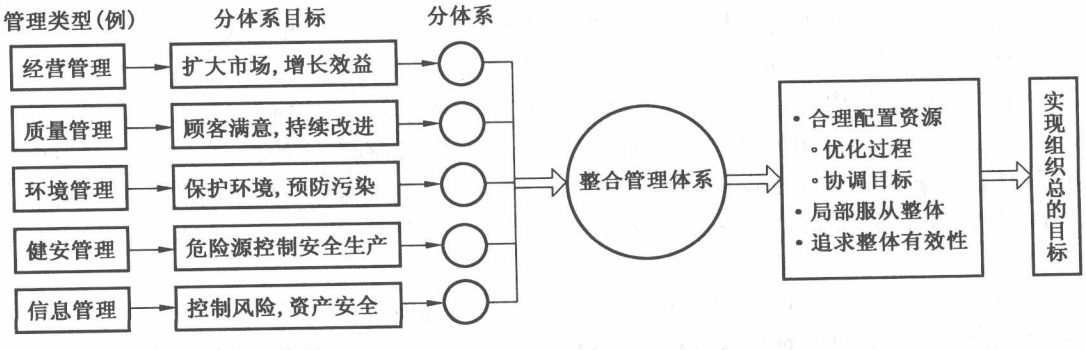

图 1-2 整合管理体系的优势

1.2 整合管理体系的来源

早在 20 世纪 90 年代初期，ISO/IEC 就将环境与安全问题列为标准化的紧迫任务，并与已成熟的质量管理体系标准协同研究。

联合国环境计划署于 1996 年在其发表的《环境管理》一书中，就论述了质量、环境、职业健康安全管理体系一体化问题。书中分析了三个体系相同、相似和相异之处，提出了一体化的理论模型，同时也指出促进和妨碍一体化的因素。

该理论模型由方针、信息提供、改进、保证、评价、人员和组织 6 个要素构成。理论模型各要素包含的内容，如表 1-1 所列。

表 1-1 理论模型整合管理体系要素详解

要素	详 细 内 容
方针和策划	寻找相关方的领域，与已有体系的接口，整理相关团体的需求，制定方针和目标，确定活动方案并制定计划，确定资源
提供信息	确定所需信息，测量与具体参数，收集信息；文件控制，信息交流
改进	识别改进的过程和活动，确定改进方案，制定并执行改进计划
保证	识别需求和保证的活动，制定并实施保证措施
评价	比较信息与需求，确认并评审反馈结果，确定并实施纠正措施
人员和组织	激励并支持职工；保持竞争能力，安排工作任务；明确职责和权限，保持资源的获得

ISO 于 2000 年发布 ISO 9000 系列标准时，就明确阐述了质量管理体系与其他管理体系的关注点，即体系一体化和相容性的问题。ISO 9000:2005 中 2.11 指出：“质量管理体系是组织的管理体系的一部分，它致力于实现与质量目标有关的结果。适当时，满足相关方的需求、期望和要求。组织的质量目标补充其他目标，如增长、筹资、收益性、环境及职业健康与安全等目标。一个组织的若干管理体系，可以与质量管理体系整合成一个使用通用要素的综合管理体系。这将有利于策划、资源配置、确定互补的目标以及评价组织的整体有效性”。

ISO 于 2008 年 11 月 15 日发布 ISO 9001:2008 标准，在其“引言”中指出：“本标准不包括针对其他管理体系的特定要求，如环境管理、职业健康与安全管理、财务管理或风险管理的特定要求。然而，本标准使组织能够将自身的质量管理体系与相关的管理体系要求相协调或整合。”

ISO 14001:1996 标准的“引言”指出：“本标准与 ISO 9000 系列质量体系标准遵循共同的管理体系原则，组织可选取一个与 ISO 9000 系列相符的现行管理体系，作为其环境管理体系的基础。”

OHSAS 18001:2007 与 ISO 14001:2004 在要素上存在一一对应关系，表明 OHSAS 18001吸取了 ISO 14001 的思想和管理方法。

ISO/IEC 27001:2005 在其“引言”中指出：“本标准与 ISO 9001:2000 及 ISO 14001:2004 相结合，以支持与相关管理标准一致的、整合的实施和运行。”

由此可见，国际标准化组织一直都在努力促进相关管理体系的整合，对管理体系标准的制定作了许多相关阐述，奠定了整合管理体系的理论基础。

现在世界上流行的趋势，不是只做一个 ISO 9000 质量管理体系，而是将 ISO 9000 质量