**解读标准ISO27000**

2012/12/20    来源：万方数据    作者：[陈文利](http://www.e-works.net.cn/commsearch.aspx?author=%e9%99%88%e6%96%87%e5%88%a9)        
关键字：[解读ISO27000标准](http://tag.e-works.net.cn/tagsearch.aspx?tag=%bd%e2%b6%c1ISO27000%b1%ea%d7%bc)  [信息安全管理](http://tag.e-works.net.cn/tagsearch.aspx?tag=%d0%c5%cf%a2%b0%b2%c8%ab%b9%dc%c0%ed)  [ISO/IEC 27000](http://tag.e-works.net.cn/tagsearch.aspx?tag=ISO%2fIEC+27000)

ISO/IEC 27000标准是国际标准化组织专门为信息安全管理体系建立的一系列相关标准的总称，已经预留了ISO/IEC 27000到 ISO/IEC 27059共60个标准号，到目前为止，正式发布的信息安全管理体系(ISMS)标准有8个，其中两个已经转化成国家标准。全部标准从ISO/IEC 27000到ISO/IEC 27037，以及ISO 27799和其他，基本可以分为以下四部分。本文向大家介绍一下ISO/IEC27000族主要标准。

    ISO/IEC 27000标准是国际标准化组织专门为[信息安全](http://articles.e-works.net.cn/Security/)管理体系建立的一系列相关标准的总称,已经预留了ISO/IEC 27000到ISO/IEC 27059共60个标准号,到目前为止,正式发布的信息安全管理体系(ISMS)标准有8个,其中两个已经转化成国家标准.全部标准从ISO/IEC 27000到ISO/IEC 27037,以及ISO 27799和其他,基本可以分为以下四部分。

    ISO/IEC 27000标准是国际标准化组织专门为信息安全管理体系建立的一系列相关标准的总称，已经预留了ISO/IEC 27000到 ISO/IEC 27059共60个标准号，到目前为止，正式发布的信息安全管理体系(ISMS)标准有8个，其中两个已经转化成国家标准。全部标准从ISO/IEC 27000到ISO/IEC 27037，以及ISO 27799和其他，基本可以分为以下四部分。

**第一部分是要求和支持性指南，**包括ISO/IEC 27000到ISO/IEC 27005，是信息安全管理体系的基础和基本要求；**第二部分是有关认证认可和审核的指南，**包括ISO/IEC27006到ISO/IEC 27008，面向认证机构和审核人员；**第三部分是面向专门行业的信息安全管理要求，**如金融业、电信业，或者专门应用于某个具体的安全域，如数字证据、业务连续性方面；**第四部分是由ISO技术委员会TC215单独制定的**（而非和IEC共同制定）应用于健康行业的标准ISO 27799，以及一些处于研究阶段并以新项目提案方式体现的成果，比如供应链安全、[存储](http://articles.e-works.net.cn/Storage/)安全等。部分标准见附表。本文向大家介绍一下ISO/IEC27000族主要标准。

    ISO/IEC 270000是信息安全管理的概述和术语，是最基础的标准之一。它提供了ISMS标准族中所涉及的通用术语和基本原则，由于ISMS每个标准都有自己的术语和定义，以及使用环境和行业的差别，不同标准的术语间往往会有一些细微的差异，致使在使用过程中相对缺乏协调，而ISO/IEC 27000就是用于实现这种一致性。ISO/IEC 27000标准有三个章节，第一章是标准的范围说明；第二章对IS0 27000系列的各个标准进行介绍，说明了各个标准之间的关系；第三章给出了共63个与IS0 27000系列标准相关的术语和定义。

附表 ISO/IEC 27000标准族



**ISO/IEC 27001:** 2005是《信息技术安全技术信息安全管理体系要求》，等同转化为中国国家标准GB/T 22080-2008/ISO/IEC27001：2005，于200 8年6月19发布，同年11月1日正式实施。同ISO 9001标准的性质一样，它是ISMS的规范性标准，也是ISO/IEC27000系列最核心的两个标准之一，适用于所有类型的组织。它着眼于组织的整体业务风险，通过对业务进行风险评估来建立、实施、运行、监视、评审、保持和改进其信息安全管理体系，确保其信息资产的保密性、可用性和完整性。它还规定了为适应不同组织或部门的需求而制定的安全控制措施的实施要求，也是独立第三方认证及实施审核的依据。

**ISO/IEC 27002：**2005是《信息技术安全技术信息安全管理实用规则》，等同转化为中国国家标准GB/T 22081-2008/ISO/IEC27002:2005，也是ISO/IEC 27000系列最核心的两个标准之一。它从11个方面提出39个控制目标和133个控制措施，这些控制目标和措施是信息安全管理的最佳实践。从应用角度看，该标准具有专用和通用的二重性。作为ISO27000标准族系列的成员之一，它是配合ISO/IEC 27001标准来使用的，体现其专用性；同时，它提出的信息安全控制目标和控制措施又是从信息安全工作实践中总结出来的，不管组织是否建立和实施ISMS，均可从中选择适合自己的思路、方法和手段来实现目标，这又体现其通用性。

    ISO/IEC 27003是《信息安全管理体系实施指南》，该标准适用于所有类型、所有规模和所有业务形式的组织，为建立、实施、运行、监视、评审、保持和改进符合ISO/IEC 27001的信息安全管理体系提供实施指南。它给出了ISMS实施的关键成功因素，按照PDCA的模型，明确了计划、实施、检查、纠正每个阶段的活动内容和详细指南。

    ISO/IEC 27004是《信息安全管理测量》，该标准阐述信息安全管理的测量和指标，用于测量信息安全管理的实施效果，为组织测量信息安全控制措施和ISMS过程的有效性提供指南。它分为信息安全测量概述、管理责任、测量和测量改进、测量操作、数据分析和测量结果报告、信息安全管理项目的评估和改进共6个关键部分，该标准还详细描述了测量过程机制，分析了如何收集基准测量单位，以及如何利用分析技术和决策准则来生成信息安全的临界指标等。

    ISO/IEC 27005是《信息安全风险管理》，该标准描述了信息安全风险管理的要求，可以用于风险评估，识别安全需求，支撑信息安全管理体系的建立和维持。作为信息安全风险管理的指南，该标准还介绍了一般性的风险管理过程，重点阐述风险评估的重要环节。在附录中它给出了资产，影响、脆弱性以及风险评估的方法，即列出了常见的威胁和脆弱性，最后给出了根据不同通讯系统、不同安全威胁选择控制措施的方法。

    ISO/IEC 27006是《信息安全管理对认证机构的认可要求》，该标准主要是对从事ISMS认证的机构提出了要求和规范，即一个机构具备了怎样的条件才能从事ISMS认证业务，所有提供ISMS认证服务的机构需要按照该标准的要求证明其能力和可靠性。

    ISO/IEC 27007是《信息安全管理的审核指南》，该标准对提供ISMS认证的第三方认证机构的审核员的工作提供支持，内部审核员也可以参考本标准完成内部审核活动，还可为任何依据ISO/IEC27002标准来管理信息安全风险、审查组织措施有效性的人员提供指导和支持。

    ISO/IEC 27008是《信息安全管理的控制措施审核员指南》，该标准是对所有审核员在考察组织基于业务风险而采取信息安全控制措施方面提供工作指导，它通过比较信息安全风险管理过程中内部、外部、第三方的所有管理体系要求与控制措施之间的关系来判定其有效性，也判别其控制措施的有效程度，满足信息安全治理的要求。

    ISO/IEC 27010是《部门间通信的信息安全管理》，该标准提供了如何针对信息安全风险、控制措施约束以及如何在不同物理场地跨组织通信的情况下进行数据共享的方法，尤其是对跨重要设施进行通信时所产生的问题和影响提供了有效支持。通过对同一物理场地通信、不同物理场地通信、危机时与政府机构间的通信、常规商务环境下为满足正常合同要求而进行双向业务通信的一系列分析，该标准明确了不同组织之间安全信息交换的方法、模型、过程、协议、控制措施和工作机制。