ISO27000 系列标准介绍

ISO 已为信息安全管理体系标准预留了 ISO/IEC 27000 系列编号，类似于质量管理体系的ISO 9000 系列和环境管理体系的ISO 14000 系列标准。规划的 ISO 27000 系列包含下列标准：

ISO27000，ISO27001，ISO27002，ISO27003，ISO27004，ISO27005，ISO27006，ISO27007

上述标准中,ISO 27001 是 ISO 27000 系列的主标准,类似于 ISO 9000 系列中的 ISO9001，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（ISMS），并通过认证。目前的有效版本是 ISO/IEC 27001：2005。

注：上述标准以 ISO 发布的为准。

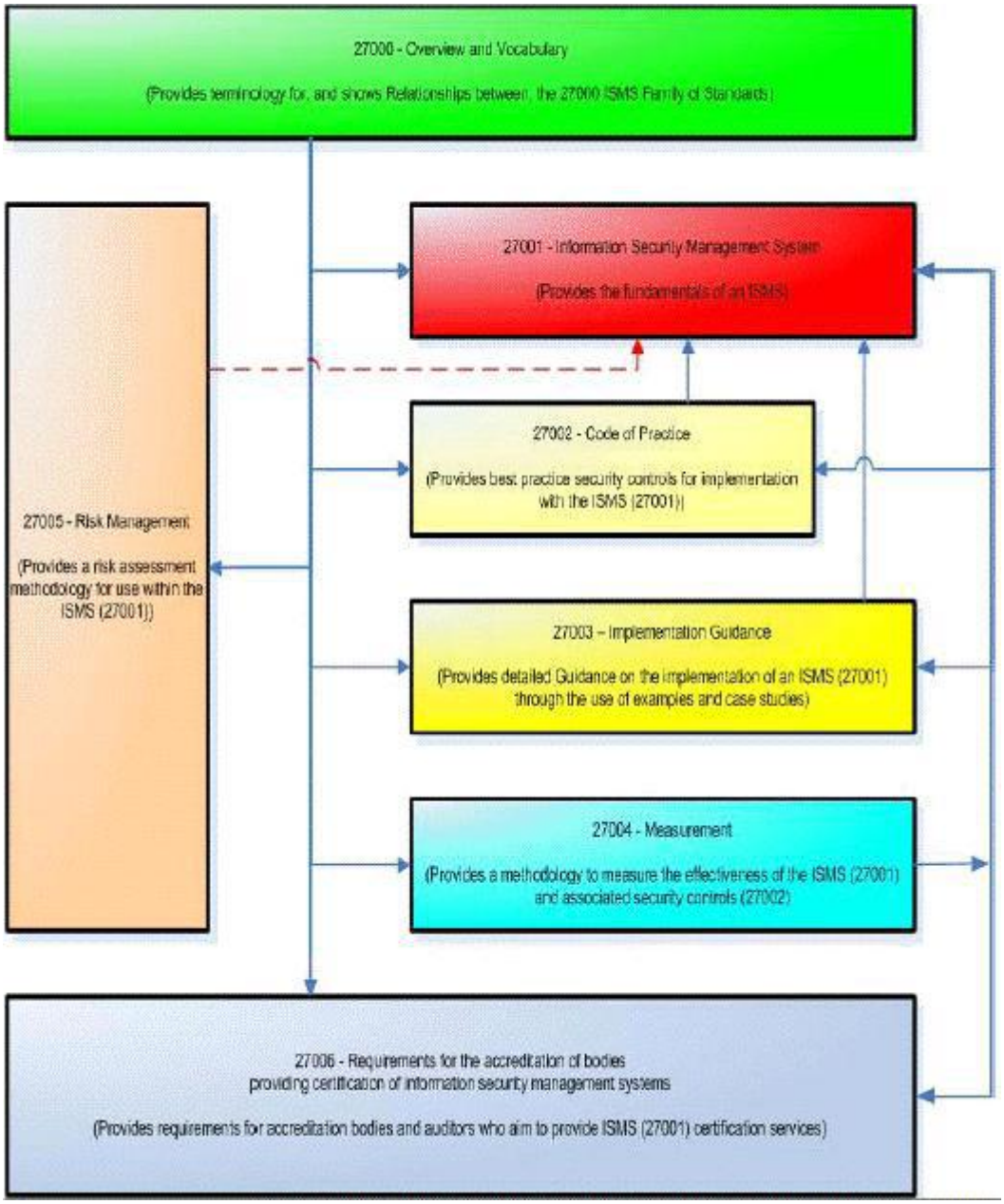
- ISO/IEC 27000

Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary

信息技术—安全技术—信息安全管理体系—概况与术语

该标准目前已完成委员会草案，计划 2007 年 11 月完成最终标准草案，2008 年 5 月发布。

标准介绍：该标准对应用于信息安全管理体系的 ISO/IEC 27000 系列标准的概况、状态和关系提供说明，并规定了与 ISO/IEC 27000 ISMS 系列标准相关的术语。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 ISO27000 系列的各个标准进行了介绍，说明了各个标准之间的关系,包 括:ISO27000,ISO27001,ISO27002,ISO27003,ISO27004,ISO27005,ISO27006。第三章给出了与 ISO27000 系列标准相关的术语和定义,共 63 个。



- ISO/IEC 27001

Information technology -- Security techniques -- Information security management systems -Requirements

信息技术—安全技术—信息安全管理体系—要求

该标准源于 BS7799-2，主要提出 ISMS 的基本要求，已于 2005 年 10 月正式发布。

标准介绍：ISO27001 用于为建立、实施、运行、监视、评审、保持和改进信息安全管理体系（Information Security Management System，简称 ISMS）提供模型。采用 ISMS 应当是一个组织的一项战略性决策。一个组

织的 ISMS 的设计和实施受业务需求和目标、安全需求、所采 用的过程以及组织的规模和结构的影响。上述因素及其支持过程会不断发生变化。期望信息安全管理体系可以根据组织的需求而测量，例如简单的情形可采用简单的 ISMS 解决方案。ISO27001 标准可以作为评估组织满足顾客、组织本身及法律法规的信息安全要求的能力的依据，无论是组织自我评估还是评估供方能力，都可以采用，也可以用作独立第三方认证的依据。

- ISO/IEC 27002

Information technology -- Security techniques -- Code of practice for information security management

信息技术—安全技术—信息安全管理实用规则

该标准将取代 ISO /IEC 27002：2005 ，直接由 ISO/IEC 27002：2005 更改标准编号为 ISO/IEC 27002，计划 2007 年 4 月实施。

标准介绍：本标准为在组织内启动、实施、保持和改进信息安全管理提供指南和通用的原则。本标准概述的目标提供了有关信息安全管理通常公认的目标的通用指 南。本标准的控制目标和控制措施预期被实施以满足由风险评估所识别的要求。本标准可以作为一个实践指南服务于开发组织的安全标准和有效的安全管理实践，帮 助构建组织间活动的信心。本标准包含的实施规则可以认为是开发组织具体指南的起点。本实施规则中的控制和指导并不全都是适用的。而且，可能需要本标准中未 包括的附加控制和指南。当开发包括附加控制和指南的文件时，包括对本标准适用的条款进行交叉引用可能是有用的，该交叉引用便于审核员和商业伙伴进行符合性 核查。

- ISO/IEC 27003

Information technology -- Security techniques -- Information security management systems implementation guidance

信息技术—安全技术—信息安全管理体系实施指南

目前还在开发中，处于工作组草案状态，计划 2008 年发布。

标准介绍：该标准为按照 ISO/IEC 27001 建立、实施、运作、监控、评审、维持和改进信息安全管理体系提供应用实施指南。该标准适用于所有类型、所有规模和所有业务形式的机构。各类组织 可以利用本标准，实施符合 ISO/IEC 27001 的信息安全管理体系。

- ISO/IEC 27004

Information technology -- Security techniques -- Information security management —Measurements

信息技术—安全技术—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，预计 2008 年 5 月发布。 该标准目前处于委员会草案状态。

标准介绍：本标准提供指南和建议，用于评估按照 ISO/IEC 27001 建立的 ISMS、控制目标以及控制措施的有效性。管理者可以使用本标准作为有效的测量方法，判断信息安全管理体系的有效性。测量结果可以作为评 审现有控制有效性的输入，以决定是否需要更改或改进。

- ISO/IEC 27005

Information technology -- Security techniques --Information security risk management

信息技术—安全技术—信息安全风险管理

该标准以 BS7799-3 和 ISO13335 为基础，已于 2008 年 6 月正式发布。

标准介绍：本标准描述了信息安全风险管理的要求，可以用于风险评估，识别安全要求，支撑信息安全管理体系的建立和维持。

- ISO/IEC 27006

Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems

信息技术—安全技术—信息安全管理体系审核认证机构要求

该标准已于 2007 年 2 月正式发布。

标准介绍：该标准对提供 ISMS 认证的机构提出要求，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

Information technology -- Security techniques - ISMS auditor guidelines

信息技术—安全技术—信息安全管理体系审核员指南

该标准目前处于工作组准备阶段。

标准介绍：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。