CIO 知识（1）：信息系统安全管理的国际标准

信息系统在当今的企业运营中发挥着极其重要的作用，信息系统的安全性（完整性、保密性、可用性等）问题也越来越突出。信息系统安全成为企业信息化建设和运维的重要组成部分。企业需要通过引进和参考国际信息系统安全标准体系，建立符合企业发展战略的信息系统安全管理的目标、方针、组织、流程、制度和技术措施，实现物理安全、系统安全、网络安全、应用安全，从而有效指导企业信息安全管理工作。

在信息安全管理体系方面，英国标准协会制定的信息安全管理标准 BS7799 已经成为世界上应用最广泛与典型的信息安全管理标准。BS7799 分两个部分，其第一部分于 2000 年被 ISO 组织采纳，成为 ISO/IEC 17799 标准。该标准 2005 年经过最新改版，发展成为 ISO/IEC 17799:2005 标准。BS7799 标准的第二部分也于 2005 年成为 ISO 标准，即 ISO/IEC 27001:2005。

ISO17799:2005 标准（即 BS7799 第一部分），是信息安全管理实施细则(Code of Practice for Information Security Management)，其中包含 11 个主题，定义了 133 个安全控制。ISO17799:2005 中的 11 个主题分别是：

安全方针（Security policy）；

依据业务要求和相关法律法规提供管理指导并支持信息安全

信息安全组织（Organization of information security）；

包括内部组织和外部各方。

资产管理（Asset management）；

包括对资产负责和信息分类。

人力资源安全 （Human resource security）；

包括员工任用前、任用中和任用的终止或变化的管理。

物理和环境安全（Physical and environmental security）；

包括安全区域、设备安全等内容。

通信和操作管理(Communication and operation management)；

包括操作程序和职责、第三方服务交付管理、系统规划和验收、防范恶意和移动代码、备份、网络安全管理、介质处置、信息的交换、电子商务服务、监视等内容。

访问控制（Access control）；

包括访问控制的业务要求、用户访问管理、用户职责、网络访问控制、操作系统访问控制、移动计算和远程工作等内容。

信息系统获取、开发和维护（Information systems acquisition, development and maintenance）；

包括信息系统的安全要求、应用中的正确处理、密码控制、系统文件的安全、开发和支持过程中的安全、技术脆弱性管理等内容。

信息安全事件管理（Information security incident management）；

包括报告信息安全事态和弱点、信息安全事件和改进的管理等内容

业务连续性管理（Business continuity management）；

防止业务活动中断，保护关键业务过程免受信息系统重大失误或灾难的影响，并确保它们的及时恢复。

符合性（Compliance）。

包括符合法律要求、符合安全策略和标准以及技术符合性、信息系统审核考虑等内容。

ISO27001:2005 标准，是建立信息安全管理体系（ISMS）的一套规范（Specification for Information Security Management Systems），基于规划(Plan)-实施(Do)-检查(Check)-处置(Act)”

的（PDCA）模型，来建立、实施、运行、监视、评审、保持和改进一个组织信息安全管理体系，指出实施机构应该遵循的风险评估标准。

规划（建立 ISMS）	建立与管理风险和改进信息安全有关的 ISMS 方针、目标、过程和程序，以提供与组织总方针和总目标相一致的结果。
实施（实施和运行 ISMS）	实施和运行 ISMS 方针、控制措施、过程和程序。
检查（监视和评审 ISMS）	对照 ISMS 方针、目标和实践经验，评估并在适当时，测量过程的执行情况，并将结果报告管理者以供评审。
处置（保持和改进 ISMS）	基于 ISMS 内部审核和管理评审的结果或者其他相关信息，采取纠正和预防措施，以持续改进 ISMS。

ISO27001:2005 标准包括范围、规范性引用文件、术语和定义、信息安全管理体系（ISMS）、管理职责、内部 ISMS 审核、ISMS 的管理评审和 ISMS 改进等内容。