

INFORMATION SAFETY

信息安全管理体系认证 ISO 27001

随着信息化水平的不断发展，信息安全逐渐成为人们关注的焦点，世界范围内的各个机构、组织、个人都在探寻如何保障信息安全的问题。英国、美国、挪威、瑞典、芬兰、澳大利亚等国均制定了有关信息安全的本国标准，国际标准化组织(ISO)也发布了信息安全相关的国际标准及技术报告。在信息安全管理方面，ISO 27001:2005已经成为国际上广泛应用的典型的信息安全管理标准，它是在BSI/DISC的BDD/2信息安全委员会指导下制定完成，目前最新版本为ISO 27001:2013。

IS 27001是一个信息安全管理体系实施规范，并可使用该规范对组织的信息安全管理体系进行审核与认证，以保证组织能摆脱信息安全遭破坏。ISO 27001:2013标准，是建立信息安全管理体系(ISMS)的一套规范，其中详细说明了建立、实施和维护信息安全管理体系的要求，指出实施机构应该遵循的风险评估标准。作为一套管理标准，ISO 27001指导相关人员如何去应用ISMS，其最终目的在于建立适合企业需要的信息安全管理体系。

信息安全管理体系标准是国际上具有代表性的信息安全管理体系标准。信息安全管理体系对每个企业或组织来说都是需要的，所以信息安全管理体系认证具有普遍的适用性，不受地域、产业类别和公司规模限制。

信息技术服务管理体系认证 ISO 20000

建立IT服务管理体系(ITSMS)已成为各种组织，特别是金融机构、电信、高科技产业等组织用于管理运营风险的重要机制。ISO 20000是面向组织的IT服务管理标准，目的是提供建立、实施、运作、监控、评审、维护和改进IT服务管理体系(ITSMS)的模型。ISO 20000让IT管理者有一个参考框架用来管理IT服务。

ISO 20000是一个针对管理流程系统的标准，ISO 20000的认证适用于IT服务的提供者，可以是外部的服务提供商，也可以是内部的IT部门。ISO 20000标准注重通过“IT服务标准化”来管理IT问题，即将IT问题归类，识别问题的内在联系，依据服务水准协议进行计划、推行和监控，并强调与客户的沟通。同时关注体系的能力，体系变更时所要求的管理水平、财务预算、软件控制和分配。

ISO 20000标准是为向内部或外部顾客提供IT服务的企业提供一个共同的参考标准。基于服务管理中沟通的重要性，在标准中为服务提供商及其供应商和他们的顾客中建立一套共同术语。通过ISO 20000 认证帮助组织更有效及高效地整合和利用信息、基础架构、应用及人员等IT资源。