ISO27000系列标准相关知识

产品名称	ISO27000系列标准相关知识
公司名称	武汉账易通会计服务有限公司
价格	.00/件
规格参数	
公司地址	武汉东湖新技术开发区高新大道以南
联系电话	13871214012 13871214012

产品详情

信息是组织的血液，存在的方式各异。可以是打印，手写，也可以是电子，演示和口述的。当今商业竞争日趋激烈，来源于不同渠道的信息，威胁到信息的一致性。它们来自内部，外部，意外的，还可能是恶意的。随着信息储存，发送新技术的广泛使用，我们面临的各种风险也在增高。信息安全越来越重要！信息安全不是有一个终端防火墙，或找一个24小时提供信息安全服务的公司就可以达到的。它需要全面的综合管理。信息安全管理体系的引入，可以协调各个方面信息管理，使管理更为有效。信息安全管理体系是系统的对组织敏感信息及信息资产进行管理，涉及到人，程序和信息科技(IT)系统。需要建立广泛的信息安全方针。保证安全性，公正性。适用组织内部和客户。信息安全管理体系ISMS正成为世界上管理体系标准销售增长量最大的产品。

信息安全管理体系（Information security management systems，简称ISMS）（即ISO/IEC 27000系列）是目前国际信息安全管理标准研究的重点。

ISO27000 系列共包括10个标准，当前已经发布和在研究的有6个，分别为：

1、ISO/IEC 27000《信息安全管理体系 基础和词汇》；

2、ISO/IEC 27001：2005《信息安全管理体系 要求》；

3、ISO/IEC 17799：2005《信息安全管理实用规则》（2007年4月后，编号将改为27002）；

4、ISO/IEC 27003《信息安全管理体系实施指南》；

5、ISO/IEC 27004《信息安全管理测量》；

6、ISO/IEC 27005《信息安全风险管理》。

一、什么是信息安全？像其他重要业务资产一样，信息也是对组织业务至关重要的一种资产，因此需要加以适当地保护。在业务环境互连日益增加的情况下这一点显得尤为重要。这种互连性的增加导致信息暴露于日益增多的、范围越来越广的威胁和脆弱性当中（也可参考关于信息系统和网络的安全的OECD

指南）。信息可以以多种形式存在。它可以打印或写在纸上、以电子方式存储、用邮寄或电子手段传送、呈现在胶片上或用语言表达。无论信息以什么形式存在，用哪种方法存储或共享，都应对它进行适当地保护。信息安全是保护信息免受各种威胁的损害，以确保业务连续性，业务风险最小化，投资回报和商业机遇最大化。信息安全是通过实施一组合适的控制措施而达到的，包括策略、过程、规程、组织结构以及软件和硬件功能。在需要时需建立、实施、监视、评审和改进这些控制措施，以确保满足该组织的特定安全和业务目标。这个过程应与其他业务管理过程联合进行。

二、为什么需要信息安全？信息及其支持过程、系统和网络都是重要的业务资产。定义、实现、保持和改进信息安全对保持竞争优势、现金周转、赢利、守法和商业形象可能是至关重要的。各组织及其信息系统和网络面临来自各个方面的安全威胁，包括计算机辅助欺诈、间谍活动、恶意破坏、毁坏行为、火灾或洪水。诸如恶意代码、计算机黑客捣乱和拒绝服务攻击等导致破坏的安全威胁，已经变得更加普遍、更有野心和日益复杂。信息安全对于公共和专用两部分的业务以及保护关键基础设施是非常重要的。在这两部分中信息安全都将作为一个使动者，例如实现电子政务或电子商务，避免或减少相关风险。公共网络和专用网络的互连、信息资源的共享都增加了实现访问控制的难度。分布式计算的趋势也削弱了集中的、专门控制的有效性。许多信息系统并没有被设计成是安全的。通过技术手段可获得的安全性是有限的，应该通过适当的管理和规程给予支持。确定哪些控制措施要实施到位需要仔细规划并注意细节。信息安全管理至少需要该组织内的所有员工参与，还可能要求利益相关人、供应商、第三方、顾客或其他外部团体的参与。外部组织的顾问、专家建议可能也是需要的。

三、 如何建立安全要求组织识别出其安全要求是非常重要的，安全要求有三个主要来源：

1、一个来源是在考虑组织整体业务战略和目标的情况下，评估该组织的风险所获得的。通过风险评估，识别资产受到的威胁，评价易受威胁利用的脆弱性和威胁发生的可能性，估计潜在的影响。

2、另一个来源是组织、贸易伙伴、合同方和服务提供者必须满足的法律、法规、规章和合同要求，以及他们的社会文化环境。

3、第三个来源是组织开发的支持其运行的信息处理的原则、目标和业务要求的特定集合。

四、评估安全风险安全要求是通过对安全风险的系统评估予以识别的。用于控制措施的支出需要针对可能由安全故障导致的业务损害加以平衡。风险评估的结果将帮助指导和决定适当的管理行动、管理信息安全风险的优先级以及实现所选择的用以防范这些风险的控制措施。风险评估应定期进行，以应对可能影响风险评估结果的任何变化。

五、选择控制措施一旦安全要求和风险已被识别并已做出风险处理决定，则应选择并实现合适的控制措施，以确保风险降低到可接受的级别。控制措施可以从《信息安全管理适用规则》或其他控制措施集合中选择，或者当合适时设计新的控制措施以满足特定需求。安全控制措施的选择依赖于组织所做出的决定，该决定是基于组织所应用的风险接受准则、风险处理选项和通用的风险管理方法，同时还要遵守所有相关的国家和国际法律法规。《信息安全管理适用规则》中的某些控制措施可被当作信息安全管理的指导原则，并且可用于大多数组织。

六、信息安全起点，许多控制措施被认为是实现信息安全的良好起点。它们或者是基于重要的法律要求，或者被认为是信息安全的常用惯例。