文档编号	shangyilong-001
版 本 号	V1.0
密　　级	内部公开

企业为什么要实施 ISO 27001 信息安全管理体系

文档信息

发布版本：V1.0
最后发布时间：2013-04-19 编写人：shangyilong 审核人：
文档编写目的
本文件的目标是增强员工的信息安全意识，提高员工的信息安全素质，规范信息安全管理，并为信息安全考核工作提供考核依据。
文档主要内容
文档适用范围

版本控制

编号	修订人	修订时间	版本号	修订内容说明
1	shangyilong	2013-4-16	V1.0	创建初稿
2				
3				

目录

实例

某公司曾遇到这样的难题：

A．某项目经理面对客户时，客户问：“你们如何保障我的信息在你们公司是安全的？你们如何保证我的信息不会泄露给第三方？”

B.当项目经理为此客户解决了所有问题，双方的合作仅差一步时，项目经理却遇到这样的问题：“下个月就需要交付使用了，本来工期就比较紧，该死的病毒将我上周的数据资料全删掉了，我该怎么办？”

C．另一个经理也很无奈地说：“怎么有很多的公司机密信息被传播出去了!”

D．最后事情到了总经理那里，总经理却感到：“客户在抱怨；项目不能如期交付；对客户的承诺要食言，公司的机密在外传；公司的生存出现严重危机，我该怎么办？”

这是一个已经通过 CMMI 认证、ISO 9001 认证公司的无奈。想必在你公司中，这类问题也是存在的，在面临这类问题时也束手无策。

俗话说“三分技术、七分管理”，目前很多公司采用计算机技术来构建公司的信息系统。但对信息资产所面临的威胁的严重性认识不足，缺乏明确的信息安全方针、缺乏完整的信息安全管理制度、相应的管理措施不到位。导致信息安全事件的发生及公司内部资料的泄漏等等问题。这些问题会给公司的经营管理、生存及安全都带来了严重的影响。

一、ISO 27001 的介绍

业务信息给公司能够带来竞争力，但同时也带来了更多的风险。为了化解这种风险可能造成的恶劣结果，信息安全的重要性得到了全体高层管理者们的一致认可。

我们谈到信息安全，应从 20 世纪说起，当时人们把信息安全的希望寄托在加密技术上面，认为一经加密，什么安全问题都可以解决，然而，失败了。随着互联网络的发展，一段时期我们又常听到“防火墙决定一切”的论调。在防火墙的神话也破灭之后，入侵检测，PKI，VPN 和 UTM 等新的技术应用又被接二连三地提了出来，信息安全的技术创新从未停止。

然而，公司在采购安全设备，采用安全技术之后，仍然不能走出信息安全问题的阴影，原因何在？

实际上，对安全技术和产品的选择运用，只是信息安全实践活动中的一部分，只是实现安全需求的手段而已。信息安全更广泛的内容，还包括制定完备的安全策略，通过风险评估来确定需求，根据需求选择安全技术和产品，并按照既定的安全策略和流程规范来实施、维护和审查安全控制措施。Gartner 曾经在一份安全报告中指出：“各类令公司损失惨重的安全违规事件归根到底都是人所造成的，并且发展成为物理安全和人员的问题。IT 安全部门试图用技术方法来解决这些安全问题，但这是行不通的。”

归根到底，信息安全并不是技术过程，而是管理过程。

信息安全管理提供管理程序，技术和保证措施，是商业管理者确信商业交易的可信性，确保信息技术服务的可用性，能适当地抵抗不正当操作、蓄意攻击或者自然灾害，并从这些故障中恢复；确保拒绝没有经过授权地访问重要的机密信息。

关于信息安全管理的标准和规范也没有安全技术那么众多，最有代表性的，就是 ISO 27001。

二、ISO 27001 的重要性

接着案例讲：

上述公司认为达到了 CMMI、ISO 9001 认证就足以应付信息安全问题，可事实上 CMMI、ISO 9001 认证无法使其摆脱这些问题所带来的困扰。

ISO 27001 起源是英国标准协会（British Standards Institution, BSI）针对信息安全管理方面而制定的英国标准 BS7799，经过十年的不断改版，终于在 2005 年被国际标准化组织（ISO）发布为正式的国际标准，用于组织的信息安全管理体系的建立，保障组织的信息安全，采用相关指定方法，基于风险评估的管理理念，全面系统地持续改进组织的信息安全管理。**它是目前世界上公认的、唯一的信息安全管理标准，已被全球五千多家政府机构和知名公司所采用。是否通过 ISO 27001 在某些行业中，已经成为一些客户的要求条件之一。**目前除英国外，还有荷兰、丹麦、澳大利亚、巴西等发达国家已使用该标准，我国的台湾、香港地区也在执行该标准。

许多国家的政府机构、银行、证券、保险公司、电信运营商、网络公司及许多跨国公司都采用了此标准对自己的信息安全进行系统的管理。这套标准注重体系的完整性，强调对法律法规的符合性，并且可与 ISO 9000 标准有很强的兼容性。

接着案例讲：

在经过一段时间探试和研究后，最后该公司采用了 ISO 27001 标准。该公司通过 ISO 27001 体系建设和实施，建立了完备的信息安全管理体系，为公司各项安全相关活动提供了明确的目标和操作指南。同时，通过系统的方法建立起组织保障体系，具备了信息安全风险驾驭能力，保证了公司核心业务的可持续运行。通过把 ISO 27001 的要求引入业务流程，使现有的业务运作更加安全规范，全面提升了公司本身和客户信息资产的安全度，尤其是加强了对客户知识产权和商业秘密的保护，提高了对客户信息安全的保障水平。不仅如此，在公司通过 ISO 27001 标准认证过程中，强化了员工的信息安全意识，规范了组织信息安全行为，在信息系统受到侵袭时，仍然可以确保业务持续开展并将损失降到最低程度。

三、ISO 27001 的认证

信息安全对每个公司或组织来说都是必要的，从目前获得认证的公司情况看，较多的是涉及电信、保险、银行、数据处理中心、IC 制造和软件外包等行业。通过一个独立的第三方的评审，公司的管理体系或产品可以成功通过某种标准的认证，为公司提供了一个向客户

表明其体系或产品符合国家或国际标准，其过程会有所不同。

ISO 27001 信息安全管理体系建设步骤如下：

一、仔细阅读标准并理解各项条款

实施该标准对公司来说非常有意义。充分了解标准，有相当多的已公布的信息可以用来帮助我们了解和实施一个标准。当然，采用信息安全管理体系应该是公司的一个战略性的决定，除了指派一个专门的团队具体负责体系的开发与实施外，所有高层管理者的积极参与往往是成功的关键。

二、人员培训

负责实施与维护管理体系的人员需要了解标准的全部细节，有一些专门的培训正好提供了这方面的帮助。ISO 27001 所要求建立的信息安全管理体系，较之纯粹的信息安全技术又更显得“务虚”和“高端”，是和公司的整体经营紧密相关的。

三、对高级管理层和关键岗位人员进行访谈，经过和高层领导磋商，明确公司信息安全工作愿景和目标，包括资金和人力资源的投入。

四、进行“信息安全风险评估”。

五、根据风险评估结果、法律法规要求、需要制定信息安全控制目标与措施。

六、实施所选的安全控制措施。

七、依据策略、程序、标准和法律法规，对安全措施的实施情况进行符合性检查。

八、针对检查结果采取应对措施，改进安全状况，使之符合 ISO

27001 标准要求。

九、再次进行第四步，一直循环。**（高层管理者必须明白：信息安全不是一蹴而就的。）**

十、当具备条件时，公司联系国际标准化认证部门指定的第三方审计机构进行现场审计。审计机构审计完成时，会向公司反馈审计报告：如果审计通过，公司或审计机构将向国际标准化认证组织提交公司的审计报告；如果审计不通过，审计机构将通知公司在它指定的时间内整改，并再次申请现场检测。如果公司未在规定的时间内整改通过，则被认为不通过本次审计。只能下一次向审计机构申请重新现场审计。

十一、审计通过后，公司就可以向国际标准化认证组织申请获得《ISO 27001 信息安全管理体系认证证书》。

十二、**在获得《ISO 27001 信息安全管理体系认证证书》之后，公司要继续按照 ISO 27001 信息安全管理体系标准执行，并不是获得证书就项目完成。国际标准化认证组织会委托第三方机构对公司进行抽查和年度审计：如果通过，保持证书有效；如果不通过，注销证书。**

十三、**特别强调：ISO 27001 信息安全管理体系只是公司进行信息安全建设的一个基础，一个阶段，一个过程，不是企业的信息安全终极目标。**