湖北企业如何落实ISO27000信息安全管理体系

产品名称	湖北企业如何落实ISO27000信息安全管理体系
公司名称	武汉搏今企业管理咨询有限公司
价格	.00/件
规格参数	
公司地址	武汉市东西湖区金山大道欧亚写字楼
联系电话	15623755573

产品详情

各行业许多企业都根据业务所需选择不同的国际、国内标准搭建了信息安全管理体系(ISMS)，无论是基于国际信息安全标准ISO27000，还是基于国家标准国家等级保护测评准则的要求，信息安全管理体系(ISMS)的建立并不是一蹴而就的。在建立信息安全管理体系(ISMS)过程中企业会投入很多资源进行资产收集、风险评估、采取种种控制措施降低风险、且制定相关的管理制度规范以降低企业风险，提升员工信息安全意识，从而达到提升企业整体信息安全管理水平。但如何可以真正的将信息安全管理体系落到实处，而不仅仅停留在一年一到两次的风险评估、突击性的控制措施实施和一套看似完备的信息安全管理制度，这可能是许多信息安全管理体系管理者经常思考且关注的话题。就此话题，我想简单总结一下在这方面的经验，希望籍此能启发您的更多灵感。 通知公告 通过信息安全相关公告通知发放的方式，在企业中渗透信息安全各方面的信息和知识，逐渐形成信息安全无处不在的工作氛围，提升全员信息安全意识。信息安全公告的内容可以包括行业在信息安全方面的新要求或指引的发布;企业内部信息安全相关要求的发布;近期信息安全相关新闻的以及发生的信息安全事件等信息。信息安全公告的发布周期和发布形式可以根据企业自身情况而定，通过企业内部使用的公共信息发布平台、电子邮件、电子期刊等形式均可。 帐号管理 建议企业对各类帐号进行严格管理，包括基本帐号(员工入职后默认都需开通的帐号，例如邮箱帐号，OA帐号，所在部门的公共文件夹等)、工作所需的各类应用系统帐号(通常根据岗位职责所需开通的帐号)、特殊权限的帐号(例如应用系统管理员的帐号，数据库管理员的帐号，域管理员的帐号等)，VPN等特殊应用的帐号。从管理角度，不同类别的帐号申请需要不同级别的管理人员授权，一方面企业需清晰识别各类账号并定义申请流程和授权方式;同时也需要保留必要的申请记录以便查证，及测量体系实施的有效性。从使用角度，需要加强对员工的培训并制定必要的规范(例如不允许帐号共享，密码定期修改等策略)，以确保帐号不被滥用误用，从而降低信息安全事件的发生。 人员安全 员工作为企业信息使用和传递的重要载体，员工变动可能会给企业的信息安全带来很大影响。在员工发生变动，即员工入职、转岗和离职几个关键点进行控制，可大大降低其对企业信息安全的影响。因此在入职前，许多企业会对关键岗位的员工进行背景调查并形成记录，签订保密协议等;发生内部职责变动时，要求员工填写工作交接单，删除其原有岗位账号等措;离职时，要求员工填写离职交接单，清理数据，归还物品。同样，在这些关键点，企业最好能制定明确的交接审批流程并妥善保留记录。

设备安全

通常企业在资产管理方面相对完善，但对设备自身的信息安全管理相对弱很多，IT设备承载大量的企业信息数据，在维护过程中无论是对设备自身进行的更换、更新，还是对其承造的系统、应用和数据进行

的配置调整、结构调整等变更均有可能对其中的信息数据造成不利影响，甚至有可能导致应用不能使用影响到企业的正常业务操作。因为对IT设备变更进行控制是至关重要的，在实施变更前，须根据变更的紧急程度和可能带来的影响程度进行变更分类和风险评估，制定详细的变更计划并得到相应级别的授权;变更实施后须对变更结果进行记录且进行回顾，以确保变更实施的成功和经验总结，具体实施方法可参照ITIL或ISO20000 IT服务管理的最佳实践和国际标准。 软件安全 自主研发软件的专利及外购软件的许可证管理均已成为企业不得不重视的问题，一旦疏忽就有可能给企业带来很大的经济和名誉损失。通过信息安全管理体系的建设，许多企业要求软件许可证也作为固定资产由专门部门管理，使用须进行登记，采购须申请，到期须提醒。人员变动、业务变动都有可能导致软件的变更，因此对软件许可证的管理并不是采购后进行登记一劳永逸的事情，在日常工作中需要保证一旦发生变化即更新许可证信息，且提前做好许可证过期的准备工作。 数据安全 数据对于企业是至关重要的，对其进行的安全管理措施更需加大力度。对存储数据的移动介质要做到登记并限制使用人群;对于大批量的数据清楚需要经授权才可执行;同时数据备份须落实到位，从业务角度识别数据备份需求，清晰定义数据备份策略(包括备份方式频率等)，的;数据备份需要进行记录，并定期进行恢复性测试保留记录，从而降低数据损失的风险。 物理安全 大多数企业都设立了门卫、保安、前台等岗位，通过信息安全管理体系的建立，也采用了访客登记，应用门禁系统等措施，对于敏感区域(例如财务、机房、研发中心等)进行了隔离或更高权限的物理访问控制。但访客登记进入后是否可以到处参观，是否有专人陪同并登记，进入和离开的时间是否进行了记录，必要时是否提交参观申请得到授权;员工门禁卡和钥匙的领取是否进行了登记，敏感区的访问是否提交了申请等这些方面均是物理安全的以保障的控制点。 安全检查 安全检查与年度或半年度的内审并不同，审核通常会基于行业要求、标准规定和内部规范进行能够检查，安全检查目的是排查各方面的安全隐患，降低安全事件发生的风险，可以是随机，也可是定期的。每次检查结果可保存，可作为日后改进和信息安全管理体系(ISMS)有效性测量的依据。 安全事件 信息安全事件一旦发生，就须快速响应妥善处理，否则可能会给企业带来更大损失。首先，企业须清晰定义什么是信息安全事件，使大家对信息安全事件形成相同的认识;第二，可根据信息安全事件的严重程度进行分级，定义不同级别的事件汇报途径、升级时间和处理要求;且在整个公司公布相关要求，做到发生安全事件即报告记录并快速响应处理。对于安全事件的管理可参照ITIL或ISO20000 IT服务管理的最佳实践和国际标准的事件管理章节。 安全培训 安全培训也是一项应持续的长期活动，安全培训可针对不同对象分成不同的培训，可以定期组织面向管理层的信息安全标准、法律法规解读的管理培训;面向全员的信息安全意识普及性培训;针对IT相关技术人员的信息安全技术知识的专业培训;面向信息安全运维和管理人员提供的信息安全相关(CISSP、CISP、ISO27001主任审核员等)。建议企业对培训过程、结果进行记录，可作为信息安全体系建设的记录和有效性测量的依据。(谷安天下拥有数名专业资深的信息安全培训讲师和顾问，可为您提供定制化的各种信息安全培训。) 由此可看出，信息安全管理体系的落地貌似简单，并非易事，贵在坚持，以上工作均需长期执行，才可起到效果，逐步提升企业的信息安全管理水平并将信息安全渗透到企业的各个角落中形成安全的工作环境。 从上文中可看出，基本每块内容都提及了记录保留相关信息等字眼，对这些长期工作的记录保留目前各个企业采取不同的形式，有的领域采用纸张记录，有些领域利用公司的一些操作平台进行记录(例如OA、IT服务管理系统等)，目前市面上协助信息安全管理体系落地的工具很稀缺，谷安天下数名信息安全领域的资深顾问共同总结多年信息安全管理方面经验结合各行业特点，开发了协助各行业企业建立并维护信息安全管理体系的一套工具(如下图所示)，涵盖了上文提及到的.