智锐达仪器科技南通有限公司ISMS审核案例

推荐机构：北京新世纪检验认证有限公司

受审核方：智锐达仪器科技南通有限公司

审核类型：信息安全管理体系认证

审核员：戎林（组长）、段跃峰（组员）、 沈向阳（组员）

一、 案例发生背景：

1、 认证领域：信息安全管理体系。

2、 受审核组织：智锐达仪器科技南通有限公司

3、 认证范围：与食品成分检测信息化管理系统以及检测仪器的开发和技术服务相关的信息安全管理，适用性声明：ZRD-IM-002-V1.0 版本：V1.0

4、 认证标准：GB/T22080-2008《信息安全管理体系 要求》

5、 审核场所：办公及经营地点—江苏省南通市经济技术开发区通盛大道188号E座1601室

6、 审核时间：一阶段审核时间：2014.8.3上午；二阶段审核时间：2014.8.4-5

二、 案例发生的主要过程：

智锐达仪器科技南通有限公司是一家致力于国内食品安全快速检测仪器及食品安全检测信息化管理软件的研发、生产、销售和技术服务的现代化科技型企业。公司2014年3月刚刚成立，

为了打好管理基础，同时建立了 QMS 和 ISMS，但公司规模较小，信息安全管理基础比较薄弱，审核组需要通过审核过程，在企业管理的各个方面寻找信息安全管理的薄弱环节，从而达到本次认证审核的目的；

企业的产品核心是软硬件开发，之前已获取了多个软件产品的著作权，知识产权实际上是本公司的核心竞争力；审核组成员能够关注这项重要信息资产在不同部门、不同管理环节的管理情况，按照审核计划的安排，分头进行各部门的审核，审核过程中始终围绕公司产品设计成果的信息安全管理，从细节入手，系统性发现企业管理中的问题，通过企业及时整改，规避了管理中的漏洞，达到审核目的；

三、 审核过程及主要的审核发现、受审核方的整改：

企业的产品核心是软硬件开发，而产品生产并不是企业的强项，暂时不具备生产能力，必须将产品生产过程外包，与外包生产方签署了外包加工合同，审核员在审核外包加工合同时发现双方未就产品知识产权及技术保密作出文字表述与责任确定，可能存在公司产品核心技术的泄密，提出了该问题得到受审核方认可；开出了第一项不符合项：

查到公司委托**斯普锐汽车部件有限公司生产检测仪整机-A 型和检测仪整机-B 型的《整机采购合同》，公司提供设计图纸、技术参数等产品重要数据，但该合同中没有保密条款和知识产权所属关系等内容。不符合标准 A.6.2.3“在第三方协议中强调安

全”的要求；

受审核方非常认可该不符合项的开具，及时进行了原因分析，认为是体系运行初期，销售部人员未能按照第三方服务管理程序和知识产权管理程序的流程要求执行，签订合同时，未能考虑到此项目涉及的保密和知识产权保护的需求，体系的运行还需要继续深入；

纠正：与外包加工方协商保密需求，形成保密协议和知识产权声明，界定知识产权的所属关系，作为合同附件进行补签，从而避免了可能的知识产权纠纷的发生；提供了补签的合同和知识产权声明书截图作为证据；

纠正措施：对公司销售人员进行相关管理程序的再培训，强调与第三方组织业务过程中涉及组织信息应得到妥善保护；

2014.8.8 管理者代表确认了上述纠正与纠正措施实施完成；

在审核研发部设计文件管理的过程中，发现了对设计输出文件的管理漏洞，不同的设计人员分别进行了软硬件设计，设计输出文档均保存在设计人员的电脑中，而公司成立初期，设计人员少，经常携带笔记本电脑外出，可能造成设计输出文件的丢失和泄露，公司虽然配备了一台备份服务器用于存储设计文件，但由于管理水平薄弱，相关人员未系统归档设计文件、严格执行定期备份制度，所以在审核过程中发现某个产品型号的设计图纸和设

计文档分别保存在设计人员和管理者代表的笔记本电脑中，未及时备份；开出了不符合项3：

公司正在进行开发的智能金标分析仪图纸、文件资料散存在开发人员、管理者代表的电脑中，未上传公司文件服务器进行定期备份；不符合A.10.5“信息备份”的要求；

受审核方进行了原因分析：IT人员只负责文件服务器的定期备份，对于各部门的资料备份要求培训不到位。研发部对于部门数据的定期备份情况缺乏必要的监控措施，无法确保信息备份的完成度；

纠正：对未备份的智能金标分析仪图纸、文件资料等信息立即备份到文件服务器；各部门重新检查各自部门人员数据备份情况，防止出现数据漏备的情况；提供了备份截图作为证据；

纠正措施：要求相关人员严格按照重要信息备份管理程序文件执行，部门负责人负责进行监督备份情况，防止类似事件的再发生；对相关人员进行了再培训，讲解备份的重要性以及数据丢失造成的危害，提高信息安全管理意识；提供了再培训记录证据；

管理者代表验证了此项不符合的纠正与纠正措施实施完成；

在审核文件服务器的管理中又发现所有登陆文件服务器的用户都使用administrator管理员帐号，文件未区分密级对所有

人员都开了共享，可能造成存储在服务器上的数据被恶意拷贝或误操作删除，存在较大风险；开出了第四项不符合项：

登录文件服务器的用户都使用 administrator 管理员帐号，服务器上的各部门文件均开了共享，但未进行用户权限的划分。不符合 A.11.2 “用户访问管理”的要求；

受审核方进行了原因分析：IT 人员对用户访问管理理解不够充分；公司的权限管理人员缺乏相应的信息安全意识；

采取的纠正：在文件服务器的用户帐号管理中建立了各部门对应的帐号，并在对应部门的共享文件夹上设置该帐户的读写权限；修改文件服务器的 administrator 管理员帐号口令，收回管理员帐号的使用权限；提供了相关更改截图作为实施证据；

纠正措施：对 IT 人员进行了相关程序文件要求培训，讲解了权限管理的方法和必要性，避免问题的再发生；将新增的文件服务器的用户权限更新至系统访问权限说明书中，并定期进行评审；分别提供了培训记录和系统访问权限说明书，作为实施证据；

管理者代表进行了上述纠正和纠正措施实施的验证；

本次审核还发现公司员工电脑转移过程中的一项不符合，同样进行了整改；审核员均验证关闭；

在本项目审核过程中，审核组通过对受审核组织的现状及管理特点分析，始终关注组织重要信息资产的管理风险，在多个部

门的多个管理环节查找管理漏洞，为组织信息安全管理状态提供了有效的证据，达到本次审核的目的，得到受审核组织的好评。

2015.5.20 进行了受审核方回访，体系持续运行，公司有了一定的发展，上年发现的不符合项已整改，并已落实到日常工作中，对公司的发展有很大的帮助；