玉晶光电（厦门）有限公司 ISMS 审核案例

推荐机构：北京新世纪检验认证股份有限公司

受审核方：玉晶光电（厦门）有限公司

案例类型：信息安全管理体系认证

审核组成员：组长：宋鹏，组员：魏云鹏

一、 背景

审核类型：监督审核

审核时间：2015 年 12 月 8 日下午——2015 年 12 月 11 日下午

审核依据：GB/T22080-2008/ISO/IEC27001:2005

玉晶光电（厦门）有限公司是一家全资台企企业，隶属于玉晶光电股份有限公司（台湾），公司产品以传统相机镜头、数码相机镜头、影像传输镜头、手机及 PDA（掌上电脑）镜头、AF 模组、相机观景窗镜片、镭射指示器镜片/镜头以及客户委托的各式镜头的设计、加工为主。目前是苹果手机摄像头配件的第二大供应商。

本次案例背景审核体系和范围为:“ISMS：与光学透镜和手机、相机光学组件的设计和制造相关的信息安全管理”，审核类型为第一次监督审核。本案例针对的不是企业认证范围专业（光学设计）方面的信息安全管理，而是针对企业自身整体信息安全中通用的病毒防范方面管理进行举例。

因案例描述整体不涉及企业自身信息安全秘密，不做匿名处理。

二、 过程

本次审核笔者负责财务、行政、人资、资讯四个部门，案例部门为资讯部门。在本企业中，资讯部门就是传统意义上的信息部门。

审核过程中了解到，该企业使用了域控对整个集团公司进行了管控，所有计算机均纳入 AD 域进行管理控制，整体访问控制、软件安装、杀毒终端等均做了统一部署和控制。采用了 4 台防病

毒服务器进行统一的病毒防御查杀，以防护公司整体网络不受病毒攻击。审核员认为，在此环境下对于条款“A.10.4.1 对恶意代码的控制措施”的审核可从服务器端直接查看全体部署和控制情况，然后在部门审核时单独抽样验证即能全面和快捷的得到审核发现。

审核员查看了赛门铁克杀毒软件服务器端，该软件目前使用了防毒功能和上网访问控制（软件防火墙）。服务器更新调度为每日 12:00 调度更新，持续 1 小时尝试更新。再查看服务器端对客户端的管理策略，开启了防火墙策略、防病毒和防间谍软件策略、入侵防护策略、应用程序与设备控制策略、liveupdate 设置策略等总体管控策略;查看防火墙规则主要是禁止访问远端网盘、外部邮件网站、自定义网站（淘宝、娱乐方面）等；最后审核员通过该软件筛选功能查看杀毒方面的最新检测摘要，发现有部分终端未安装 sonar 功能模块（综合判断引擎），其中 Y400001368 等 13 台还未开启自动防护功能,与管理员沟通让他远程连上其中 Y400002230（192.168.***.***）电脑，发现病毒库为 2011.4.18，未进行更新，也未开启自动防护。证据已充分显示不符合标准条款“A.10.4.1 对恶意代码的控制措施”。

经过与防病毒服务器管理人员（网络管理员）沟通，认为主要的技术问题是终端电脑杀毒软件功能模块损坏，导致服务器端无法对其进行更新升级和开启防护功能。而管理方面，公司未制定相关的防病毒巡查制度要求，管理员也以为安装好了服务器端并设置好各种策略就全部自动运行，不需要查看，从而导致该问题一直存在。

经过与组长沟通，组内一致认为应开具不符合，企业方面也认可和接受此项不符合。在末次会议上，审核组就存在的问题及其可能导致的风险、后果进行了讲解，同时针对企业完备的技术设备情况，常见的依赖设备的问题进行了剖析，把“三分技术、七分管理”的思路与企业方进行了分享，企业方也认识到了己方的不足，愿意用心整改并对相关人员加以培训教育。

三、 结果

现场审核后，受审核组织对提出的不符合项进行原因分析并纠正，制定了纠正措施，进行了培训。

纠正：

1、对公司各终端进行清查；

2、对有异常的终端电脑开启自动防护功能；

2015.12.29 对全公司终端（包括域控下的、非认证范围的其他子公司）进行清查，发现 1177 个终端最新的病毒库和防护有 902 个，过时 16 个，脱机（截图时未开机）254 个，禁用了杀毒软件的 5 个。

2015.12.29 清查截图如下：

2016.1.5 清查处理后截图：

清查后做了纠正处理，于 2016.1.5 基本完成。 1177 个终端除了脱机状态以外的终端有 952 个升级到最新的病毒库和开启了防护，还有 1 个过时的终端也在处理当中。两图对比可明显看到“病毒和风险活动摘要”中清查前和清查后的 24 小时病毒活动程度和下载风险的不同。

纠正措施：

1、每月从服务器端核查计算机的病毒库状况，如发现异常及时改善，并纳入《ISP-02-13 信息安全事件管制程序》文件管理；

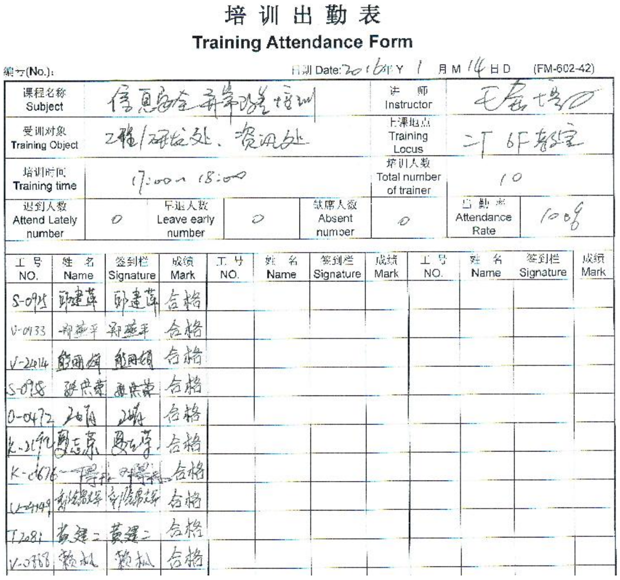
GSEO 玉晶光电	文件编号	ISP-02-13
	版本版次	B-2
信息安全事件管制程序 Information Security event Control Procedure	页　次	2/5
	发行日期	2016/01/07

5.执行方法：

5.1信息安全事件巡查：

5.1.1杀毒软件服务器端，需每月进行巡查，一旦发现用户端有功能异常，需立即进行排除并恢复正常功能运作，已确保用户端电脑保持在安全的保护之内。

2、针对更新的新要求对厂内相关人员培训



培 训 出 勤 表

Training Attendance Form

编号(No.)：　　　　日期 Date: 2016年Y 1 月M 14 日D　　(FM-602-42)

课程名称 Subject	信息安全弃常规培训	讲师 Instructor	[illegible]
受训对象 Training Object	工程/研发处、资讯处	上课地点 Training Locus	二丁 6F 教室
培训时间 Training time	17:00~18:00	培训人数 Total number of trainer	10

迟到人数 Attend Lately number	早退人数 Leave early number	缺席人数 Absent number	出勤率 Attendance Rate
0	0	0	100%

工号 NO.	姓名 Name	签到栏 Signature	成绩 Mark	工号 NO.	姓名 Name	签到栏 Signature	成绩 Mark	工号 NO.	姓名 Name	签到栏 Signature	成绩 Mark
S-0915	邱建萍	邱建萍	合格								
V-0133	郑燕平	郑燕平	合格								
V-2414	[illegible]	[illegible]	合格								
S-0958	[illegible]	[illegible]	合格								
O-0472	[illegible]	[illegible]	合格								
K-2170	[illegible]	[illegible]	合格								
K-0676	[illegible]	[illegible]	合格								
V-4149	[illegible]	[illegible]	合格								
T2081	黄建二	黄建二	合格								
V-0868	[illegible]	[illegible]	合格								

从纠正和纠正措施实施的结果来看，企业病毒防护确实有了很大的提升，而通过培训和明确每月巡查制度，也使企业后续的防病毒方面工作形成了长效机制。通过这次整改，对企业信息安全管理中“管理与技术结合”方面起到了启迪作用，从而提升了企业的信息安全管理能力。

四、　扩展

通过本次审核，笔者有两点体会：

1、审核过程在可行的条件下，应灵活运用专业知识，尽可能全面的为受审核组织进行“体检”。如本次审核在企业本身实行了域控的情况下，通过一个服务器端查看到整个企业的所有终端防病毒情况，以及密码策略、访问控制策略、桌面控制策略等（AD server 域控服务器），不会遗漏任何一个终端，这是抽样所不能比拟的全范围，杜绝了抽样的偶然性，从而得到完整的审核发现；

2、通过这样方式的审核，以及与受审核组织方面的沟通交流，引导企业，使企业更深切的感受到管理体系与技术、设备结合的必要性，对技术、设备方面的盲目信任降低，使企业信息安全工作效能提高、信息安全风险降低，使其从本次审核中得到实实在在的益处，从而使企业信息安全管理水平和信息安全防护能力进一步提升。