ISMS 审核案例

准确识别信息风险，保证高速公路收费的安全

摘要：现场审核京开分公司于 2016.8.1 对体系文件进行修订，包括四标整合-B-01《管理手册》，版本 B-01 版；SOA-C-01《信息安全适用性声明》，版本 C-01；程序文件 56 个，以及三级文件、记录模板。体系文件主要是适应 ISO/IEC 27001：2013 标准的需要进行的转版。京开公司的《信息安全风险评估程序》、《信息安全风险管理程序》规定，先对信息资产按 6 类进行识别，重要资产判别方法是通过资产安全属性 CIA 识别后，CIA 赋值分别为 1、3、5、7、9. 资产价值=保密性赋值＋完整性赋值＋可用性赋值，等级分成 4 级，其中 3、4 级是重要资产。再对重要资产进行风险评估，风险计算方法：风险值=资产等级＋威胁性赋值＋脆弱性赋值，一级为高等级风险不可接受。

2016 年 8 月京开分公司按照 ISO/IEC 27001:2013 标准要求，重新确认、识别业务中的信息资产和存在的风险。全公司按照 6 类资产分类提供了每类资产的统计表，提供了信息资产清单，京开分公司共有信息资产 4937 个，其中 2359 个属于重要信息资产。提供《信息安全风险评估表》，识别出风险 6467 项，其中不可接受风险 2013 项。

现场审核发现《信息安全风险评估表》，对 1-4 级所有的信息资产进行风险评估，评估发现存在 2013 个高等级风险，4274 个中等级风险，180 个低等级风险。造成《重要资产清单》的编制没有意义。

查《风险处理计划》，对 2013 项高等级风险风险制定了处理计划后，直接判定都是剩余风险可接受，缺少二次风险评估的证据。并且与《残余风险评价报告》中剩余 3 级风险 63 个相矛盾。

针对该审核发现，审核组开出了 ISO/IEC 27001:2013 标准 8.2/8.3 条款的一般不符合项。

现场审核资产物业管理部，该部门负责固定资产的申购、报废等工作，监督周期内，分公司共报废一台笔记本电脑、一台电脑、一台照相机等；查电脑信息处置单，电脑报废时间：2016.06.02；记录了电脑编号、所属部门、销毁原因等；电脑已经格式化，信息销毁人签字：张辉；但是未提供对相机报废前进行处理的证据。

针对该审核发现，审核组开出了 ISO/IEC 27001:2013 标准 A.8.3 条款的一般不符合项。

现场审核杜家坎监控中心，检查发现 NIP 入侵检测设备，型号：华为 NIP2000，网络安全设备。系统安装在服务器上，服务器安装 Macfee、SQL server2005。用途包括：邮件监控、网络监控、FTP 监控。

查到 NIP 入侵检测设备厂家出具的《前十位入侵检测统计》，有 Netbios 释放漏洞、TCP 异步状态攻击，未对发现问题进行处理。

针对该审核发现，审核组开出了 ISO/IEC 27001:2013 标准 A.12.6.1 条款的一般不符合项。

受审核方改进成效及验证情况：现场审核后，公司信息安全管理小组针对第一个不符合项，组织修订了《信息安全风险评估程序》，对京开分公司各机关和各收费所重新进行了信息资产识别和风险评估工作。

针对第二个不符合项，组织资产物业管理部学习了《京开分公司信息资产管理规定》，对可移动介质的处置过程进行了规定。

针对第三个不符合项，组织杜家坎监控中心学习了《京开分公司入侵检测系统事件处理规范》，对各收费所发现攻击入侵检测系统的事件处理过程进行了规定。

通过本次审核，企业高度认可审核组的专业能力，认识到了在介质管理和运行安全管理方面存在的安全漏洞，以及对公司在信息资产识别和风险评估方法上存在的缺陷，提高了信息安全管理方面的意识和能力。

推荐机构：北京新世纪检验认证股份有限公司

受审核方：北京市首都公路发展集团有限公司京开高速公路管理分公司

认证类型：信息安全管理体系

审核组长：雷峥

审核组员：寇素敏、胡倩、赵峰（实习）

一、案例发生背景

1、 认证范围：与高速公路收费服务（不包括 ETC）相关的信息安全管理；
适用性声明：SOA-C-01 版本：C-01

2、 审核类型：监督审核

3、 审核场所：北京市大兴区京开高速公路西红门收费站内

4、 审核时间：监督审核时间：2016.9.5-9.8 上午

二、企业背景

北京市首都公路发展集团有限公司京开高速公路管理分公司是北京市国有大型企业首发集团下属分公司，是从事高速公路收费运营管理的专业化公司。京开分公司实行区域化管理，现负责京港澳高速（北京段）、京开高速公路（北京段）、六环路（马驹桥－阎村西）、京津高速（北京段）、京昆高速（北京段）的收费运营工作，管辖高速公路里程 227.83 公里。设置杜家坎、窦店、琉璃河、西红门、榆垡、狼垡、台湖、永乐、青龙湖、镇江营十个收费管理所。

三、审核发现和审核沟通过程

现场审核京开分公司于 2016.8.1 对体系文件进行修订，包括四标整合-B-01《管理手册》，版本 B-01 版；SOA-C-01《信息安全适用性声明》，版本 C-01；程序文件 56 个，以及三级文件、记录模板。体系文件主要是适应 ISO27001：2013 标准的需要进行的转版。

京开分公司执行《信息安全风险评估程序》、《信息安全风险管理程序》的规定。

2016 年 8 月监控中心主管京开分公司按照 ISO27001:2013 标准要求，重新确认、识别业务中的资产和存在的风险。查见《信息安全风险评估表》，其中监控中心识别了以下资产：

硬件：办公电脑、服务器、机房网络设备、数据存储设备、监控设备等。

软件：电脑操作系统、360 杀毒软件、WPS 办公软件、收费系统结账软件、数字视频监控软件、全程监控系统、集团 OA 系统、集团 NC 系统；

文档：监控管理工作手册、管理手册、部门公章、合同；

数据：顾客投诉记录、无卡车辆申请表、特种车队通行情况记录、自检自查、设备维修记录、电子收费退款单、监控中心培训记录、离职人员变更表、机房外来人员登记、报损清单、砸车报告、UPS 室巡查记录、办公网络拓扑图、IP 与 MAC 地址绑定对照表、软件管理台账表；

人员：主任、副主任、机电设备管理员、网络管理员、统计分析员等；
服务：京开高速公路机电设备维护维修、京港澳高速公路机电设备维护维修、南六环高速公路机电设备维护维修、京津高速公路机电设备维护维修技术服务合同、京开分公司手机视频监控系统维护维修、现金传输、征费综合管理系统维护维修技术服务、2×100M 互联网专线业务接入服务、供电。

全公司按照 6 类资产分类提供了每类资产的统计表，资产清单中每项资产识别了所有者，资产清单由武文捷负责管理，经询问自上次审核到目前，资产包括人员未发生变化，查见《信息处理设施管理程序》，对资产的归还作出规定；由资产负责人负责管理和使用。

重要资产识别：

重要资产判别方法是通过资产安全属性 CIA 后，CIA 赋值分别为 1、3、5、7、9. 资产价值= 保密性赋值＋完整性赋值＋可用性赋值，将资产等级分为 4 级，取最大值作为资产重要性等级，等级分成 4 级，其中 3、4 级是重要资产；

提供了重要资产清单，京开分公司共有信息资产 2359 个。

信息资产风险评估：

风险评估方法：针对重要资产进行风险评估

风险计算方法：风险值=资产等级＋威胁性赋值＋脆弱性赋值

在控制程序文件中提供了威胁值、脆弱值二个参数赋值范围：1-5；

可能性=威胁值*脆弱值，损失=重要性等级*脆弱值，风险值=平均值（可能性，损失）

风险级别分为，依据风险值划分 3 个等级：

风险接受准则：风险的 3 级为不可接受风险，1、2 级风险属于可以接受的风险。查见 2016 年 8 月 6 日风险评估报告，识别出风险 6467 项，其中不可接受风险 2013 项，主要是：病毒入侵导致数据损失或系统瘫痪，硬件故障和失窃等，不可接受风险资产在监控中心。

2016.8.7 针对不可接受风险制定了《风险处置计划》，要求 2016.8.7 之前完成。

二次风险评估与残余风险批准：

查见 2016 年 8 月 18 日《残余风险评价报告》，本公司存在 2013 个高等级风险，4274 个中等级风险，180 个低等级风险，根据风险接受准则，确定 3 级风险不可接受，必须立即采取控制措施降低风险，2 级风险可以接受，但需要采取进一步措施降低风险或在威胁发生时采取处理措施，1 级风险可以接受，可以保持目前的控制措施。经过各部门负责人对 3 级风险进行处理，大部分风险已经降到 1、2 级，还剩余 3 级风险 63 个,最终评价结果是对剩余的 3 级风险予以接受；武文捷起草了残余风险报告，部门负责人杨勇于 2016 年 8 月 20 日批准。

现场审核发现《重要资产清单》，识别出 3 级、4 级重要信息资产 4937 个。

查《信息安全风险评估表》，对 1-4 级所有的信息资产进行风险评估，评估发现存在 2013 个高等级风险，4274 个中等级风险，180 个低等级风险。造成《重要资产清单》的编制没有意义。

查《风险处理计划》，对 2013 项高等级风险风险制定了处理计划后，直接判定都是剩余风险可接受，缺少二次风险评估的证据。并且与《残余风险评价报告》中剩余 3 级风险 63 个相矛盾。。

针对该审核发现，审核组开出了 ISO27001-2013 标准 8.2/8.3 条款的一般不符合项。

现场审核资产物业管理部，该部门负责固定资产的申购、报废等工作，监督周期内，分公司共报废一台笔记本电脑、一台电脑、一台照相机等；查电脑信息处置单，电脑报废时间：2016.06.02；记录了电脑编号、所属部门、销毁原因等；电脑已经格式化，信息销毁人签字：张辉；但是未提供对相机报废前进行处理的证据。

针对该审核发现，审核组开出了 ISO27001-2013 标准 A.8.3 条款的一般不符合项。

现场审核杜家坎监控中心，机房位于办公楼三楼监控室内，独立区域，每天有专人负责巡检。温度 21.6 度，湿度 45%。有气体灭火器，在有效期内，机柜数量 8，设备包括交换机、路由器、防火墙、数字视频监控系统服务器、高速公路信息综合管理系统服务器等。网络分为内网和外网，内网由云星宇负责维护，内网由京沈负责维护。监控中心、机房，均为物理锁，钥匙保存在监控中心管理员售中，监控中心，24 小时均有人值班；进入监控室、机房，外来人员需要登记；楼道内有视频监控探头，对机房及监控设室进行监视；支持性设备：机房内一组 UPS，供机房设备使用；监控系统及车道设备通过发电机进行备用电源提供，UPS 能提供 2 小时的备用电源；

现场检查发现 NIP 入侵检测设备，型号：华为 NIP2000，网络安全设备。系统安装在服务器上，win server 2003。

权限：2 个用户账户，云星宇和西红门监控中心，各使用一个账户。

策略包括：邮件监控、网络监控、FTP 监控。

容量：CPU0%，内寸：648M。实时事件：引擎名称：磁各庄，检测时间：016-9-7 11:20:40，事件类型：扫描，事件名称：***，服务：netbios，源 IP：**137，目的 IP：**137，，内外部区分：外部到外部。

服务器安装 Macfee、SQL server2005。病毒库更新时间 2016-9-6。服务器不能访问外网。

查到 NIP 入侵检测设备厂家出具的《前十位入侵检测统计》，有 Netbios 释放漏洞、TCP 异步状态攻击，未对发现问题进行处理。

针对该审核发现，审核组开出了 ISO27001-2013 标准 A.12.6.1 条款的一般不符合项。

四、受审核方改进成效及验证情况

现场审核后，公司信息安全管理小组针对第一个不符合项，组织修订了《信息安全风险评估程序》，对京开分公司各机关和各收费所重新进行了信息资产识别和风险评估工作。

针对第二个不符合项，组织资产物业管理部学习了《京开分公司信息资产管理规定》，对可移动介质的处置过程进行了规定。

针对第三个不符合项，组织杜家坎监控中心学习了《京开分公司入侵检测系统事件处理规范》，对各收费所发现攻击入侵检测系统的事件处理过程进行了规定。

通过本次审核，企业高度认可审核组的专业能力，认识到了在介质管理和运行安全管理方面存在的安全漏洞，以及对公司在信息资产识别和风险评估方法上存在的缺陷，提高了信息安全管理方面的意识和能力。