附件

# 江苏省邮电规划设计院有限责任公司审核案例

撰写者：李治纲

**【案例摘要】**

企业对网络及其设备安全隐患和漏洞的治理，能有效防止企业信息外泄，抵御外部攻击，降低国家、企业信息安全风险。

## 一、案例背景介绍

**推荐机构：方圆标志认证集团有限公司**

**案例类型：管理体系认证**

**认证类型：信息安全管理体系**

**受审核方名称： 江苏省邮电规划设计院有限责任公司**

**审核依据：** GB/T22080-2016 ISO/IEC 27001:2013

**审核时间：** 2017 年 10 月 25~27 日

**审核范围：**位于江苏省南京市建邺区楠溪江东街 58 号邮电设计大厦-1 层、1 层、3 层、4 层、7 层、8 层、13 层、14 层、15 层、18 层、19 层、20 层、22 层江苏省邮电规划设计院有限责任公司的通信工程的设计、咨询；计算机信息系统集成；安全防范系统集成；计算机通信软件的设计与开发；通信建设项目招标代理；建筑智能化工程的设计与施工相关的信息安全管理活动。信息安全适用性声明：A/0

**审核组长：李治纲** **审核组员：吴荣华**

## 二、受审核方基本情况

受审核方为一家有着悠久历史从事基础电信设施的咨询、规划、设计、施工国有企业，主要客户为：移动、电信、联通，以及各地地方政府。其主要承接国内外各种规模的技术咨询、管理咨询、通信工程勘察设计、建筑工程勘察设计、网络优化、系统集成、网络规划与研究、应用软件开发与标准及规范制订。属于通信行业顶层架构规划、设计单位，在江苏通信行业处于“龙头”地位，且承接的项目一般涉及城市基础设施，属于国计民生范畴，很多信息需要保密、防止篡

改，如规划方案、设计方案、图纸等。为此企业 2016 年按 ISO/IEC 27001：2013 标准建立信息安全管理体系，不但加固了本身信息安全这个“堤坝”，还倡导本行业各类企业使用 ISO/IEC 27001：2013 管理企业各类信息资产。

**三、主要审核发现、沟通过程**

名称解释：

- 端口：TCP/IP 协议集成到操作系统的内核中，这就相当于在操作系统中引入了一种新的输入/输出接口技术，因为在 TCP/IP 协议中引入了一种称之为"Socket（套接字）"应用程序接口。有了这样一种接口技术，一台计算机就可以通过软件的方式与任何一台具有 Socket 接口的计算机进行通信。端口在计算机编程上也就是"Socket 接口。目前端口数量为：65535 个，分为公认端口、注册端口、动态和/或私有端口。
- 公认端口：这类端口的端口号从 0 到 1023，它们紧密绑定于一些特定的服务。通常这些端口的通信明确表明了某种服务的协议，这种端口是不可再重新定义它的作用对象。例如：80 端口、445 端口，445 此端口是各种共享文件夹或共享打印机。
- 注册端口：端口号从 1024 到 49151。它们松散地绑定于一些服务。例如：1433 端口、4000 端口，1433 此端口是 Microsoft 的 SQL 服务开放的端口，4000 此端口是 QQ 客户端通信。
- 动态和/或私有端口：端口号从 49152 到 65535。理论上，不应把常用服务分配在这些端口上。
- 上网行为管理软件：它一般用于管理员工的上网行为，提高员工的工作效率，所以又被称为员工上网管理软件。它能帮助企业有选择的禁止、监控 BT，炒股，聊天，管理 QQ，监控邮件，带宽流量等，减少病毒，对员工的上网行为进行正确的引导。
- URL：全球资源定位器，即通常说的网络地址；URL 库就是存放这些地址信息仓库。

2017 年 10 月 25~27 日上午受方圆标志认证集团有限公司的委托李治纲、吴荣华等 2 人，对江苏省邮电规划设计院有限责任公司进行信息安全管理体系第

1 次监督现场审核，审核组组长编制审核计划，确定监督主要审核工程技术部、人力资源部、综合办公室、移动院、咨询院、西南院、市场经营部、采购部、计划财务部、通信院、城市信息工程院及项目部，以及相应的资产识别、风险评估和风险控制措施。

监督现场审核，审核组现场取证发现：

第一：2017 年 6 月公司内部进行一次网络安全隐患、漏洞扫描，发现部分服务器 44*端未关闭，审核组调阅该次扫描形成检测报告，已经给出存在隐患的具体服务器编号及其处置建议，但现场核实仍然存在，没有处置，询问管理人员，答复是：大概服务器拥有者需要用吧。

开具不符合原因：44*端口是用于共享文件或打印机的，同时也是病毒传播的主要途径（如勒索病毒），如不能正常管理和控制，对整个网络重大安全隐患，极易造成网络、设备瘫痪，数据掉失、损坏和外泄。故开具第一份不符合报告

不符合：GB/T22080-2016 ISO/IEC27001:2013　8.3 组织应实现信息安全风险处置计划，组织应保留信息安全风险处置结果的文件化信息。

第二：审核员查看上网行为管理软件，发现 URL 库、应用识别库、审计库，版本是 2017 年 1/2 月份的，系统已自动提示有更新需要升级。同时 OA 服务器有 25 个重要系统补丁未更新。询问管理人员，答复：没有交钱，所以没有及时升级。

开具不符合原因：没有交钱不是理由，病从口入，如果不及时升级上网行为管理软件这些库，如何应对瞬息万变的互联网有害地址和信息，无法最大程度隔离、拒绝网络访问，带来后果就是降低公司整体网络安全等级，也无法有效控制内部人员网络访问行为，有染病毒和泄密的可能。故开具第二份不符合报告。

不符合：GB/T22080-2016 ISO/IEC27001:2013 A.12.6.1 应及时获取在用信息系统的技术方面的脆弱性信息，评价组织对这些脆弱性的暴露状况并采取适当的措施来应对相关风险。

经与受审核方确认了上述两项目不符合，为一般不符合报告，给 30 天整改，需要采取纠正和纠正措施，审核组采取异地验证方式。

## 四、不符合报告整改和验证

受审核方对不符合报告采取纠正和纠正措施进行整改，分别是：

第一份：

原因分析：管理人员管理意识淡薄，未意识该安全隐患可能带来的严重性。

纠正：立即向服务器使用部门口头下达整改要求，使用部门书面答复，由于工作需要保留此端口申请保留，经主管领导批准后，不关闭。

纠正措施：举一反三对检测报告提及安全隐患再次进行检查，并补充一份“处置单”，除上述 2 个服务器端口未处理外，其余均已处理。编制了一份《安全漏洞管理制度》，明确安全漏洞识别范围、风险等级、处置流程、责任人、处置时间等

验证：提供 1 份服务器端口开启说明，1 份隐患“处置单”，1 份《安全漏洞管理制度》，经异地书面验证，基本接受。

第二份：

原因分析：管理工作懈怠，未能及时升级。

纠正：立即对深信服上网行为管理系统进行升级，确保版本最新。在中午休息期间对 OA 服务器进行系统升级，确保没有重要补丁遗漏。

纠正措施：编制一份《服务器、病毒库更新管理制度》，明确机房内服务器和网络设备病毒库更新、升级的程序、要求和应急处置等内容。

验证：提供 1 份升级后深信服版本截图，1 份 OA 服务器重要更新后截图，1 份《服务器、病毒库更新管理制度》。经异地书面验证，审核组基本接受。

## 五、受审核组织主要的改进方法及其成效

通过上述二份不符合报告内容，我们看到部分企业负责人对信息安全不重视、无所谓，只知道企业要实现信息化，为此投入大笔资金，但信息化后的信息安全风险往往不特别关注，除非发生一次重大信息安全事件后，才后悔。通过对不符合整改，看似给受审核方没有带来什么现实经济效益，但消除或降低受审核方存在信息安全风险，是无形的，是管控信息风险效益。

审核组在后续对该企业进行信息技术服务管理体系（也有信息安全条款）

监督审核时，特别关注不符合整改的情况及其绩效，通过对网络管理员、业务部门人员、管理者代表口头交流，发现人们对端口安全管理有了更深刻理解，如谈到了“勒索”病毒利用端口漏洞对企业和个人危害。该企业还下属部门中成立信息安全处理小组，专门负责本公司网络内信息安全事件处理和漏洞扫描，不定期向管理层提供网络安全报告。抽查几台服务器的高危端口均进行关闭处理；查看网行为管理器均已是最新版，同时打开同步更新功能；查看 OA 服务器、业务服务主要系统补丁均已安装；查看系统更新日志，符合《服务器、病毒库更新管理制度》要求。审核组认为通过这份不符合报告开具基本达到目的，使企业人员提高了信息安全意识，信息安全管理得到管理层重视，愿意主动投入了一定的人力和物力管理和防范信息安全隐患，制定相关措施和制度得到有力执行，目前该企业尚未出现明显网络安全事件。

习近平总书记在二次国家层面会议中强调：

2014 年 02 月 27 日在中央网络安全和信息化领导小组第一次会议的讲话：“没有网络安全就没有国家安全，没有信息化就没有现代化”

2016 年 4 月 19 日在在网络安全和信息化工作座谈会上的讲话:“维护网络安全，首先要知道风险在哪里，是什么样的风险，什么时候发生风险，正所谓“聪者听于无声，明者见于未形”。感知网络安全态势是最基本最基础的工作。要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改。……。网上信息管理，网站应负主体责任，政府行政管理部门要加强监管。”

## 五、总结

信息安全管理没有永远没有结束，永远在路上。