# 审核案例

**案例简述：**

受审核企业名称：OPPO 广东移动通信有限公司

审核标准:GB/T22080-2016 idt ISO/IEC 27001：2013 信息技术 安全技术 信息安全管理体系

审核员：鲁立

认证范围：手机的设计、开发和生产（适用性声明版本：V1.1）

审核时间：2018 年 12 月 17 日~2018 年 12 月 21 日

审核类型：第二次监督审核

**案例背景**

OPPO 广东移动通信有限公司，位于广东省东莞市长安镇乌沙海滨路 18 号。公司集手机科研、制造和营销于一体的大型高科技企业，产品远销美国、俄罗斯、欧洲、日本、韩国、东南亚等市场，OPPO 致力于打造高品质时尚数码行业的国际一流品牌。

媒体曾曝光苹果公司员工 Paul Devine 向外传出苹果公司的机密信息，例如新产品的预测、计划蓝图、价格和产品特征造成苹果公司损失超过 240 万美金。随着手机市场的日趋成熟与饱和，手机品牌之间的竞争也日趋白热化。为了保持在市场竞争中的优势，OPPO 对研发年投入超 40 亿，如何保护研发成果是公司对信息安全管理的首要课题。本次审核的关注要点在于如何为公司识别改进机会和可能出现风险的领域。

**审核过程**

为了明确审核目的，审核员先与公司高层及信息安全管理部门主管沟通。OPPO 对信息安全管理的核心是新机型上市前信息的管控，在信息安全管理体系关注的可用性、保密性以及完整性三个属性中，保密性是最重要的。因为企业的产品面向终端消费者，一个机型上市之前如果硬件配置、特殊功能、外观为竞争对手了解，可能被竞争对手抢先上市，从而影响最终销量。

手机市场竞争激烈，手机产品的研发是复杂的合作过程（外观设计、结构设计、硬件设计等等同步开展），且生命周期非常短（一个机型研发周期不到半年）。为了提高研发效率，OPPO 导入了 PLM 系统管理整个开发周期。在 PLM（Product Lifecycle Management）System 中，新产品开发（NPI：New Product Introduction）大至分为 Planning（产品构想阶段），EVT（工程验证与测试阶段），DVT（设计验证与测试阶段），PVT（生产验证与测试阶段），MP（量产阶段）五个阶段。

审核员了解到为使 PLM 有效运行，OPPO 内部部门间的网络不存在物理隔离。另一方面，为了及时获取互联网上的最新信息，并与供应商保持及时沟通，企业内网与互联网在物理层面也是联通的，而如何在联通的大前题下进行管控，对企业的信息安全管理提出了复杂的要求。

审核员首先从 PLM 系统的访问权限入手，先了解 PLM 系统的身份认证机制。企业的 PLM 系统已实现与 AD（域控）集成，人员账号的开通、关闭均与人力资源系统集成，从而实现在人力资源系统离职流程完成时可自动关闭账户访问权限。其次，审核员向 PLM 系统管理员了解 PLM 系统的权限划分情况，比对企业提供的 EVT、DVT、PVT 等各开发阶段部门参与情况，未发现在开发过程中权限设置不当。

针对 PLM 系统未发现信息安全风险，审核员进一步关注企业的互联网边界。从企业的网络维护部门了解到，企业在网络出口部署了 Check Point 防火墙，Forcepoint DLP 设备，设置了基于文件类型、关键字等审计信息外发情况的管控策略，通过对策略的查阅，以及日志信息的抽样，了解到当前策略设置符合企业信息安全目标，日志记录的信息安全事件均已跟进。

针对网络边界的访问控制未发现信息安全风险，审核员进一步针对邮件外发管控进行审核。从企业的邮箱管理员处了解到，企业有自建的邮箱系统，邮箱账户与 AD（域控）集成，实现人员离职自动关闭，所有邮件外发都需要直属领导审批，且对邮件进行了归档审计。

针对邮箱的管控未发现信息安全风险，审核员进一步针对内部网络隔离进行审核。审核员专门与企业网络管理人员一起从行政办公网络、生产网络尝试通过 FTP、SMB 等文件共享协议访问研发网络，均以失败告终。

至此，企业的网络安全似乎万无一失，审核到此结束了吗？

审核员认为还没有结束，虽然通过审核可以认定无法通过入侵的手段窃取到企业的信息，但合法人员是否有办法将敏感信息摆渡出去呢？审核员与企业网络管理员一起在研发网络做了一项测试，通过 Windows 系统自带的远程桌面功能，在远程登陆办公网电脑的同时挂载研发网的本地磁盘。测试结果，磁盘被成功挂载，且通过此方法向远程电脑拷贝文件不会留下任何记录。

**重点同企业沟通内容**

（1） 企业从系统架构到系统维护都已经做了充分的信息安全风险应对，如 PLM 系统的权限划分和回收，但信息安全事件既可能源于外患，也可能源于内忧。通过 Windows 系统自带的远程桌面功能摆渡文件，实施成本低，且事后没有记录可被审计。

（2） 由于研发工作与日常办公的性质差异，企业对研发网的审计和访问控制远比办公网的审计和访问控制严格，敏感数据一旦从研发网被摆渡至办公网，则后续外泄的可能、无法审计的可能都将提高。

依据以上审核发现和问题分析，审核组开具了不符合项：“研发 5 楼未进行网络隔离，测试可通过远程桌面挂载共享盘向其它网段拷贝数据，不符合研发楼物理安防管理方案的相关要求。”不符合标准 A.13.1.3 网络中的隔离的相关要求。

**改进及取得的成效**

经以上分析，OPPO 公司领导对我们发现的问题欣然接受，对提出的不符合项进行原因了分析并采取了纠正和纠正措施。

改进过程：

（1） 针对五楼保密区域办公终端，使用域组策略限制远程复制及共享功能。

具体策略：组策略--计算机配置--管理模板--Windows 组件--远程桌面服务--远程桌面会话主机--设备和资源重定向

1）不允许剪贴板重定向，调整为已启用

2）不允许驱动器重定向，调整为已启用。

（2） 目前红区会议室资源不足，导致内部人员需在非保密区域进行会议远程红区电脑使用，故无法进行彻底的网络隔离，计划下半年扩展保密项目专区面积，配置充足会议室资源，区域内配备保密项目专用办公终端，限制个人办公终端带入，且保密项目办公区配置独立网段，以实现网络隔离。

取得的成效：

（1） 提高了网络管理人员的安全意识，补齐了网络管理内到外控制较松的短板。使网络管理人员的视野更开阔，不仅关注外到内的攻击、进一步关注内到外的摆渡。

（2） 企业认为本案例中的不符合项为其风险评估的全面性提供了参考，进一步在现有的威胁列表中增加内部人员摆渡资料这个评估维度，对企业以后的信息安全管理产生了有意义的影响。将在后续的风险评估工作中，不仅在网络控制层面，也在设备带出管控、人员进出管控等方面，关注由内主动出外的信息安全管理。

（3） 通过此次审核进一步完善企业研发信息的信息安全管控，增强了公司在市场上的竞争力，提高了公司的社会效益。