十六、北京 XX 数码科技有限公司 ISMS 审核案例

推荐机构：中国信息安全认证中心

认证类型：信息安全管理体系

审核人员：王崇斌 王雷

一、案例背景

北京 XX 数码科技有限公司是一家专门为政府行业客户提供业务应用系统开发、业务系统运营外包服务、系统集成的专业公司。为加强信息安全管理，保护客户信息及公司敏感信息，尤其是保护政府行业客户信息安全，北京 XX 数码科技有限公司依据 GB/T22080-2008 标准要求，建立覆盖全公司各业务部门的信息安全管理体系。

此次审核主要针对北京XX数码科技有限公司信息安全管理体系的建立、实施、运行和保持的情况进行审核，特别是信息安全控制措施的落实情况。

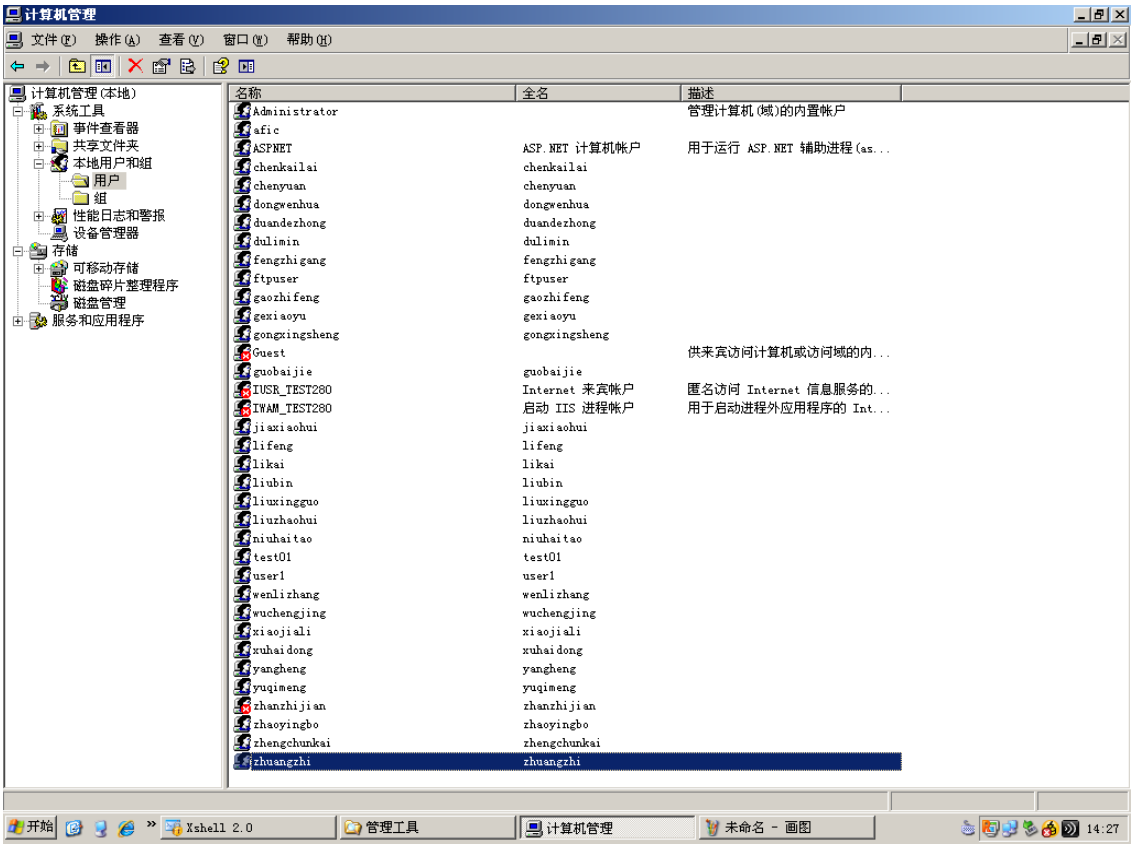
二、主要审核发现、沟通过程

围绕受审核方信息安全管理重点即保护政府行业客户信息和公司敏感信息，审核组对受审核方风险评估过程和结果进行充分评价，认为受审核方在没有采取技术手段的条件下对敏感信息(客户数据和公司具有自主知识产权的软件)的访问控制存在一定的安全风险，受审方在风险识别过程中也进行了识别，并采取了一定的管理手段，但审核组在查阅访问控制相关文件及访谈 IT 服务中心部门和行政部门时发现由于受审核方关于访问控制的相关要求覆盖范围不明确，相关人员对用户访问控制相关的要求理解不到位，导致对敏感信息系统的访问没有有效地管控。

受审核方的适应性声明（SOA）选择了A.11.2“用户访问管理”这一控制域下的所有四条控制措施，且控制措施引用文件均为《访问控制实施规范》。审核过程中首先查看《访问控制实施规范》关于用户访问管理相关内容的描述，发现文件对“A.11.2.1用户注册”和“A.11.2.4用户访问权限的复查”都提出了明确要求，但在访谈IT服务中心人员时发现该中心有自己的工作规范文件,即《业务系统维护规范》，相关人员对于“用户注册”和“用户访问权限的复查”的概念不清楚，《访问控制实施规范》的要求也不明确，访谈中了解到该部门日常工作中会登陆客户业务系统，接触敏感客户信息，且人

员岗位流动较大，审核组决定抽样该部门涉及的业务系统访问控制情况，查看是否符合标准和自身体系的管理要求。具体步骤如下：

1. 首先根据访谈行政部了解IT服务中心人员情况，并获得过去一年该部门离职、调岗人员名单及相关的交接清单并作记录。
2. 访谈IT服务中心相关人员，了解业务系统维护流程，获知维护人员通过地方局业务系统访问跳转机(10.98.156.**)可直接登陆客户业务系统,接触客户敏感数据。
3. 确认跳转机的访问人员数量(19人)并要求出示跳转机访问帐号的审批材料。
4. 登陆地方局业务系统访问跳转机(10.98.156.**)，发现用户帐号数量多于确认的数量，其中有一账号“zhuangzhi”确认是一离职员工账号；且有部分测试和临时帐号，如下图(一)。
5. 根据上述发现，审核组与体系负责人及IT服务中心相关人员沟通，受审核方一致认为针对A.11.2控制域的控制措施（具体为A.11.2.1和A.11.2.4）在实际操作中未落地，存在较大风险和安全隐患，审核组对此开具不符合项，受审核方无任何疑义。



图(一)

三、标准解读及问题分析

GB/T22080-2008附录A中条款“A.11.2用户访问管理”的目标为“确保授权用户访问信息系统，并防止未授权的访问”。其中“A.11.2.1用户注册”要求“有正式的用户注册及注销规程，来授权和撤销对所有信息系统及服务的访问”，组织应基于业务要求建立用户访问角色，对不同级别的信息系统访问管控要求不同，对于涉及组织敏感信息的系统访问控制应强化；其中“A.11.2.4用户访问权的复查”要求“宜定期使用正式过程对用户的访问权进行复查”，定期复查访问权限对于保持对数据和信息的有效控制，防止信息系统非预期访问非常必要。“用户访问管理”对于保护组织的信息安全，防止信息泄露起着至关重要的作用，业界比较有影响的信息泄密事件，例如三星家电部核心技术泄密事件和富士康IPAD2后壳泄密事件都是由于用户访问管理不到位引起。

由于标准对如何进行用户访问管理并未统一要求，组织可以根据自身实际情况制定具体实施措施。通常一个组织可以采用技术手段，也可以采用管理手段来进行用户访问管理。

通过访谈了解到受审核方出现该问题的原因：

1. 由于质量部门制定《访问控制实施规范》并负责监督落实情况，受技术水平限制，该部门对信息系统访问控制的实际情况的了解仅停留在各部门的报告上，所以对具体控制措施要求不明确、针对性不强，导致可操作性也不够。
2. 各部门对《访问控制实施规范》要求没有引起足够重视。
3. 相关人员对用户访问权限及时注销和复查理解不到位，尤其对涉及敏感信息的系统的访问控制没有上升到事关组织信息泄露风险的层面。
4. 控制措施实施后的有效性检查没有有效落实，导致上述控制措施较长一段时期没有落地。

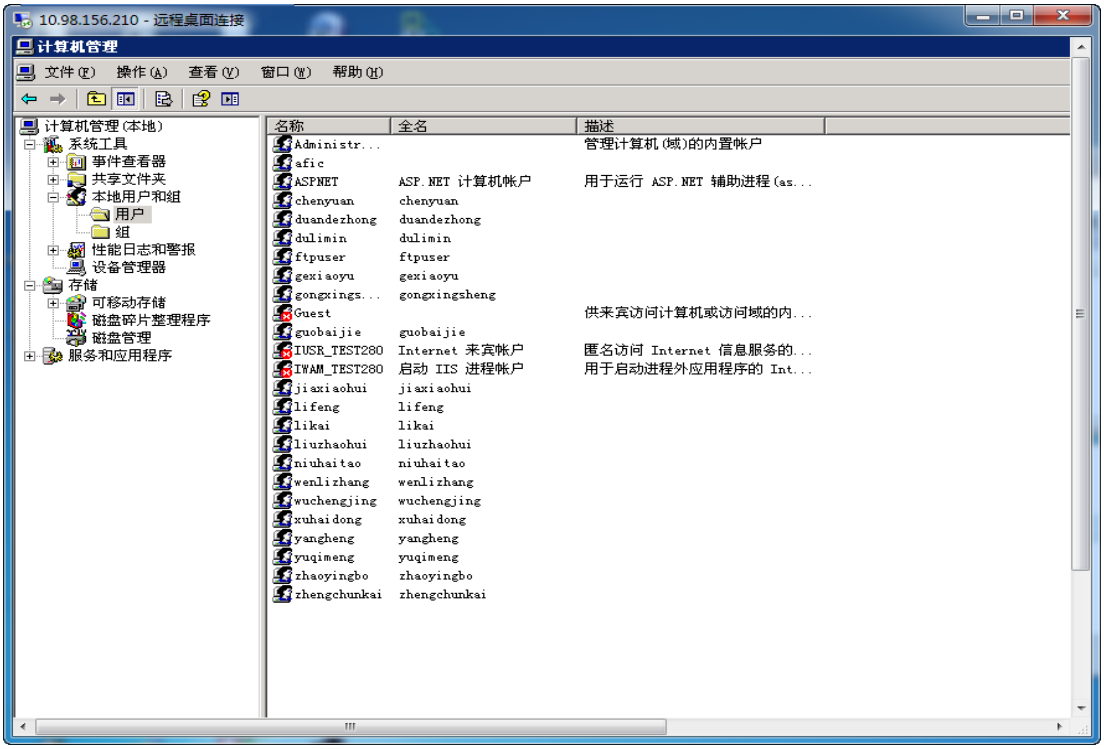
四、改进过程及取得的成效

基于以上事实和沟通，受审核组织领导对我们发现的问题欣然接受，并表示此次审核人员指出的问题工作中没有关注到，但却存在很大的安全隐患和风险，一定认真整改。现场审核后，受审核组织对提出的不符合项均进行原因分析并制定了纠正措施，并举一反三，排查所有信息系统，取得了良好的管理成效。

1. 整改要求：

1） 组织相关人员学习《访问控制规范》和标准关于“用户访问管理”的条款学习，明确“用户访问管理”的重要性；并组织人员修订《业务系统维护规范》，提供整改记录。

2） 立即对地方局业务系统访问跳转机(10.98.156.**)访问权限进行一次全面复查，清理多余账户（图(二)为整改后跳转机账户情况）。



图(二)

3） 举一反三，全面排查系统访问权限，并提供整改记录及检查记录。

2. 取得成效：

通过整改保证了能及时清理和检查应用系统的用户访问权限，降低了客户信息泄露的风险；对用户访问管理如何在组织内的落地实施和检查有了很深刻的理解；大大提高了全体员工对用户访问管理重要性的认识，提高了人员的安全意识。

3. 我们的体会：

ISMS审核时越是根据受审组织信息安全保护重点并结合其风险评估情况有针对性发现问题，给组织改进的效果越明显。