信息安全管理体系审核实践

-----引导企业逐步全方位加强信息安全管理

推荐机构：北京新世纪检验认证有限公司
案例交流人：宋鹏

一、 受审核方背景

1、 **受审核组织：**北京国双科技有限公司

2、 **认证领域及审核性质：**信息安全管理体系 初次审核

3、 **现场审核时间：**2018 年 3 月 28-30 日

4、 **审核人员：**宋鹏（组长） 罗海鹰（组员） 李孟显（组员） 文艺杰（组员） 汪莹（一部）（实习组员）

5、 **组织主要产品服务：**北京国双科技有限公司经过一阶段审核后，确认经营地址位于北京市海淀区双榆树小区知春路 76 号翠宫饭店写字楼 8 层、9 层 A 区、10 层、11 层、12 层和 14 层，其主要业务过程是云计算企业级大数据分析和人工智能解决方案提供商，主要为司法，新媒体（如网络电视台,OTT 视频点播）主要做节目播出效果检测，同时也为政府部门提供相应产品，同时公司的所有业务都在信息安全管理体系范围内；此次认证范围是：**与基于大数据与人工智能技术的软件开发、技术运维、技术咨询、系统集成服务相关的信息安全管理；适用性声明：Q/ISMS-A-03 版本：A/0；SOA 文件中只删减了 A14.2.7 一条控制措施；**

二、 审核过程

1、 审核准则与目的

此次审核是应我公司的委派实施的第三方审核，审核过程依据国标 GB/T22080-2016/ISO/IEC27001:2013，公司的信息安全管理体系文件以及适应的法律法规（参见受审核组织收集的法律法规清单）；审核的主要目的是评价组织信息安全管理体系的建立、运行的符合性及有效性，以确定能否推荐认证注册。

2、 受审核组织结构与信息安全职责

公司由领导层、技术部、运营管理部、财务部、商业事业群、政企业务部组成，在此基础上成立信息安全小组，统一组织领导公司的信息安全体系的实施，由管代任组长定期向最高管理者汇报 ISMS 运行情况；其中：

1） 领导层/信息安全小组

负责组织实施管理体系的策划、实施、运行、检测和改进，具体体现在 ISMS 职责分配、文件

的审批、信息安全风险管控、内审和管理评审实施等;

2） 技术部

负责软件开发与技术运维过程，公司 IT 网络（含机房和 IDC 机房）以及计算机设备管理过程的信息安全管理;

3） 运营管理部

运营管理部主要负责公司运营支持过程，分别由行政部、人力资源部、法务部、合同部、知识产权部、公关部和市场部组成。负责公司的人事、行政、法律法规合规评价、合同管理、对外公关以及市场品牌宣传过程管理等;

4） 财务部

负责公司财务预决算、财务报表、报税等工作，并保证财务数据的可用、准确和安全;

5） 商业事业群

领完成公司下达的区域销售任务指标，在市场部门配合下制定产品、解决方案的销售计划和方法；保证客户信息安全；

6） 政企业务部

负责承接系统集成、咨询服务项目，售前方案部门将所有材料，包括完整的设计(或施工)方案、设备订购详单交给该系统集成项目的项目经理；并且在项目实施过程中保证相关方的信息安全；

3、 受审核组织的管理特点与审核方式

受审核组织人员相对较多有近 200 人，组织结构分工明确，特别是管理过程的信息化程度较高。使用 gitlab 系统、OA 系统、邮箱系统、HR 系统、客服信息管理系统、合同管理系统和用友财务系统等分别管理着软件开发、办公过程、人事管理等过程中的信息安全管理；

公司有上级公司的隶属关系，和上级公司在一起办公；上级公司有独立的办公区域；公司在识别相关方以及相关方的信息安全要求时给予识别；

公司的组织结构中的各个部门工作职责相对独立，工作过程中的职责交叉较少，技术部和商业事业群直接保持灵活的人员随着项目进程流动的现状;

此次审核过程中审核组成员坚持采用问、看、查三种方式实施有效审核:

问: 采用与部门领导或信息安全员进行座谈，了解部门的主要职责和工作流程以及责任人；同时了解部门的信息资产情况，即在工作过程中使用哪些信息资产、责任人是谁？以及信息资产的领用、使用、带出、回换、报废等事宜;

看：不但通过座谈了解情况，还要查阅信息安全管理相关证据；例如:

1) 查阅信息资产识别表，确认所审核的部门管辖的信息资产是否识别的齐全?
2) 查阅计算机操作: 账户、口令、清屏、杀毒、高危漏洞等管理是否满足标准要求?
3) 查阅本部门关键数据备份证据，是否满足备份策略的要求?

等等

注: 对信息化管理程度较高的受审核方，在查阅证据过程中尽量采信信息系统的记录;

查：通过“问“了解到的情况和”看“获知的证据，经过分析后与审核准则对比，形成审核发现最终得出审核结论；

对各个部门的审核都是通过了解部门职责与工作流程基础上，从巡查本部门所管辖的信息资产入手，对各项信息资产的信息安全风险管理实施有效审核。

4、 ISMS 具体实施

1) ISMS 建立与运行

基于市场以及内部管理的需要，受审核组织引进了 ISMS 管理体系，并于 2017.9.1 建立了一套独立的信息安全管理体系文件，现场审核时企业提供了对组织内部、外部信息安全需要的识别，提供了识别证据；在文件中制定的信息安全方针、目标通过多种渠道进行了有效宣传；在公司的走廊中粘贴有信息安全宣传画（方针、目标、注意事项等）；按照文件规定进行了内审、管理评审；公司领导对ISMS建立与运行较为重视，成立了一个近20人的信息安全小组，由各部门领导或安全员组成，主要负责规划、监督、检查公司的 ISMS 运行，定期向总经理汇报 ISMS 运行情况。

按照 ISMS 文件要求每个部门进行了信息资产的识别以及风险评价，信息安全小组统一制定风险处置计划并实施后进行了二次评价；形成残余风险报告交予总经理批准；

2) 现场审核重点和领域，以及审核中关注到的信息安全风险管控的特点

公司信息安全管理体系文件中的 SOA 文件只删除了 A14.2.7 一个控制措施，标准中其余的 113 条信息安全风险控制措施都已选择；在审核过程发现受审核方结合实际针对不同的信息安全风险采取了有效的管控措施：

物理安全：

企业每个楼层的入口都有门禁，在两个楼层的电梯间设有前台和保安；关键的办公区内部也有门禁系统，同时安装有覆盖全域的视频监控系统；整个楼宇安装了消防系统，办公环境内和机房内同时放置了大量的灭火设备，但机房内不是气体灭火器。审核组就该监控系统的时钟与企业进行了询问，同时关注到门禁卡和门禁系统权限的管理，现场进入机房查看相关信息安全的物理环境的管理，并进行了实际查看和取证。

虽然受审核组织与上级单位在一起办公，内部的物理空间进行了有效隔离，物理边界清晰可辨；审核组在一阶段审核后将经营地址进行了重新定义；将 9 层办公区区分为 A/B 两个区，以及没有包含 13 层办公区；

网络安全：

组织的网络分成办公网络和产品服务网络，办公网络和产品服务网络分别部署在公司的内部和 IDC 机房，从而实现办公网络与服务网络物理分离。

两个网络都设有网络安全设备：防火墙、核心交换机等，办公网络设有上网行为管理器等；

办公网络中设有 Vlan，将部门之间进行了逻辑隔离；上级组织的网络是独立的办公网络，不与受审核组织共用；基于与部门领导和工作人员的沟通，了解到以上情况后，审核组从网络资产的识别、网络拓扑图的规划、网络设备的策略设置等多方面进行了详细的审核和取证。

设备操作安全：

公司的信息处理设备都是从运营管理部领出，同时包括所有设备在进行采购、发放、回收、报废等操作后在系统中的录入，设备在发放之前由网络管理员进行必要设置；离职人员进行交接后将设备归还运营管理部，网络管理员按规定将数据清除；审核组在审核现场大量提取了各类设备的处置的证据，并与设备管理人员进行了处置结果是否有效的确认，通过设备管理人员，在公司的办公系统中进行了抽样。

在设备管理过程的审核中，审核组通过现场抽查计算机操作（账户、口令、屏保、清屏、杀毒、漏洞补丁等）都满足组织的信息安全管理要求，没有发现异常；

公司对设备带出进行了风险评估，制定了管理制度，配置笔记本电脑的岗位设备可以带出公司无需审批，配置台式机的岗位不得带出设备；

由于公司使用信息系统管理比较普及，办公过程较少使用移动介质交换信息；从审核过程抽查结果来看，抽查的移动介质没有发现公司数据信息；

信息系统安全：

公司在办公过程中使用 gitlab、OA、邮箱系统、门禁系统、HR 系统、客服信息管理系统、合同管理系统和用友财务系统；现场按照相关策略要求，分别检查了上述系统账户设置、权限分配、特权账户管理、数据备份和定期复查等控制措施；审核组对上述系统的权限做了全方位的审核。

通过审核，发现对信息系统的管理分成两级：网络管理员负责服务器操作系统和网络可用，各个信息系统责任部门指定专人承担系统管理员职责，系统管理员负责账户、权限、口令、备份等管理事项；

软件开发安全：

受审核组织制定了软件开发管理流程，并在流程中强化了信息安全要求；从现场审核确认软件开发流程基本采用瀑布模型，现场抽查了两个软件研发项目，基本满足审核准则要求；

数据信息安全：

公司的数据信息基本都是采用信息系统管理，对数据访问通过系统的账户、权限进行分配管理，强化了数据备份机制，对关键数据实现本地和异地双备份；

数据进行交换传输时要求使用企业邮箱，保持一定的可追溯性；

公司的纸质文档（例如合同）由运营管理部专人管理，保存在带锁的文件柜中，交接、借阅等有记录可查；审核组针对备份过程、备份后的管理、备份操作的日志管理等方面进行了审核和抽样。

供应商安全：

公司对供应商在合同中提出了信息安全要求，并定期进行了评价，没有发现违规事项；

人员安全：

组织对人员的信息安全管理主要采用签署保密协议；在审核中发现部分人员的保密协议签署的主体是上级单位，现场提示企业可能存在法律风险，第三方人员进入现场时也存在管理上的不足，有接触公司敏感信息的风险，就以上可能存在的问题在末次会议上与最高领导进行了交流；

三、 审核发现

经过审核组内部交流一致认为，基于现场与受审核方交流以机收集到的相关证据，受审核方的信息安全管理体系运行满足审核准则的要求；此次审核除上述发现的受审核方做得满足审核准测要求的地方，还发现了有待改进的地方，共开出 4 个书面不符合项，还有一些可能存在信息安全风险或对风险控制措施有漏洞的地方在末次会议中进行口头交流，并未开出书面的观察项;

1、不符合项:

1) **查阅办公机房没有发现适用的灭火器，不符合标准 A11.1.4 要求；**

主要是管理人员缺少对消防知识和必要的检查；企业购置了新的气体灭火器，并请厂家进行了必要的培训，制定了定期巡查制度;

2) **检查公司各个楼层的视频监控系统相互之间的时间不一致，相差约 10 多分钟；不符合标准 A12.4.4 要求**

通过末次会议现场交流，受审核方提高了信息安全认识，懂得视频监控系统是事件追溯的主要技术手段，追溯过程通常是以时间为依据，因此时间同步对视频监控系统至关重要;设置每个楼层的监控主机的 NTP 自动同步时间服务器修正所有楼层的监控时钟;企业更新《物理环境安全控制程序》，将对视频监控管理要求内容进行添加，将对视频监控的时间检查列为日常检查内容;

3) **现场查看离职人员焦本然的门禁卡，已丢失，进一步查看门禁管理系统权限控制，未能删除。不符合标准 A9.2.6 要求**

企业及时删除焦本然的门禁卡，并认真分析了原因，列出下列整改措施:

a) 由知识产权部组织行政部人员对条款 A9.2.6 条款进行学习;

b) 由专人每天汇总当天离职人员门禁卡，并发邮件给门禁管理员，管理员据此解除离职人员的门禁权限，同时每周五对所有相关邮件进行复查，以防止遗漏

c) 门禁卡有效期同劳动合同时效,由专人登记有效期时间,在到期前及时进行相应延期;

d) 门禁卡领用开卡需制作《开卡记录表》，并以邮件形式通知前台;

e) 如遇重启门禁卡，需记录重启前的使用人及其停止使用此卡的日期;

f) 离职人员的门禁卡按照月份单独存放，由专人保管，封存期 1 年。

注释：不符合 2 和不符合 3 分开看起来都是很简单的风险，但是当两个风险同时出现时，企业的物理环境管理就等同于失控，意味着不仅可以任由任何非法享有进出权限或持卡的人出入，该入侵者还能够创造不在现场的时间差。这一问题的提出，立刻引起了企业的警觉和高度重视，并就此进行了整改，提供了大量的整改证据。

4) **现场通过行政人员于芳登录办公 OA 系统，查看报废设备的敏感信息处置记录，未能提供有效证据，相关内容为空。不符合标准 A11.2.7 要求**

企业及时补充了必要记录，并认真分析了原因，列出下列整改措施:

a） 修改 OA 系统填写资料报废过程中，“敏感信息处理”设置为必填项，确保敏感信息处置记录的完整性，可追溯性。

b） 加强信息安全重要性的培训。

注释：审核组就此不符合项与企业沟通，企业意识到报废设备中如果携带了大量的代码、财务信息、合同等敏感信息，不做处置就放行，这些密级较高的信息就会通过多个渠道被泄露，对企业造成不可预估的风险。因此企业积极地进行了整改，规定在设备报废前必须有相关备份和敏感信息的处理，同时在信息系统中做详细的记录，才能报废，并且对相关人员加强了培训。之后，向审核组提供了大量的整改证据。

2、 交流事项：

在末次会议上审核组成员（除文艺杰外）都对审核过程中审核发现进行了积极评价，充分肯定了企业对贯彻执行 ISMS 的积极性和认真态度，以及公司领导的大力支持。对公司的信息安全风险的识别、评价、处置和管控是有效的，除了开出上述的 4 个书面不符合项以外，审核组重点与企业交流了以下可能的风险点：

1） 备份过程的容错能力有待提高

在检查源代码管理系统 gitlab 备份策略时，每天 0 点备份，异地全备，保留一周的备份数据；现场按照备份策略检查本地和异地服务器，备份结果一切正常，均满足备份策略要求；进一步检查本地服务器异地备份脚本执行的日志（backup.log）时,发现 7 天前的某一天 0 点至 2 点之间连续异地备份三次失败，第二天的 0 点备份成功。审核组考虑到数据本地备份正常，异地备份偶发一次对数据安全影响不大；但需要加强对日志的分析从而强化备份过程的容错管理能力；

2） 第三方人员保密制度加强

受审核方与上级集团公司共用运营管理人员，而这些人员的保密协议都是与上级集团签署，协议中的内容未明确员工与受审核方的责任与义务，考虑到受审核方与上级集团是两个独立的法人主体，考虑到双方协议对第三方不具有约束力，要求受审核方关注必要时进行针对性风险评价；第三方服务人员进入现场提供服务过程的时候如何进行管理，要求受审核方根据不同情况制定出可行的策略，进行必要的风险评估和管控。

3） 各类信息系统权限的时效管理

审核组就信息系统权限的时效问题提出了意见：应考虑信息系统、门禁系统、临时访客权限、网络授权的时效管理，这也是满足信息安全标准权限定期检查要求的有效技术措施。必要时进行全方位的安全检查和对密码等关键环节的修改，要求受审核方加强对授权过程和授权时间单元的风险评估，必要时制定相应的管理制度并予以实施，减少不必要的意外带来的信息安全事件。

四、 审核结束后的增值服务

审核发现为组织指出了信息安全管理体系薄弱的环节，指出了组织深入理解信息安全标准要求与实际工作过程的结合，全面管理好组织信息安全风险的切入点；在众多信息安全风险领域中重点突出

了较为好理解的物理安全和设备安全信息安全风险管理；3 个不符合项涉及物理安全风险管理，1 个不符合项涉及设备安全风险管理或理解为体系运行记录必要性;通过审核过程和不符合项的开具，引导企业由浅入深的持续改进，逐步实现组织全方位信息安全管理。

企业在整改不符合项过程中，多次积极与审核组进行沟通，企业在理解基础上认真整改，查找原因制定纠正措施；举一反三，多部门配合在公司内部进行筛查，企业各部门领导均表示此次审核提高了信息安全风险控制的有效性，对审核结果予以肯定，通过审核组的审核，帮助企业深刻理解信息安全风险控制要求，实现企业提高信息安全风险的识别、评价、监测和控制水平，引导企业实现自我保护企业信息安全。

针对审核组提出的交流事项，进行了认真分析，以及风险评估，改进了原有处置措施::

1) 针对异地备份程序进行分析，当异地备份失败时每隔 15 分钟尝试一次，连续三次都失败就终止异地备份，未考虑其他补救措施；通过风险评估，本地已经有备份数据风险可控；当异地备份失败时邮件通知管理员，早上上班时手动异地备份；综合多种情况修改备份策略，增加了备份恢复测试频次,改进各类日志管理的方法,公司增设了日志服务器并定期进行分析。

2) 基于部分员工的保密协议签署的主体是组织的上级单位，经过风险评估，企业决定在原保密协议中增加下属控股企业内容，使得保密协议在法律上可以覆盖集团的下属各个企业；对于不同的第三方人员进入公司，制定了不同的管理策略，同时指定了相关负责部门和人员。

3) 整体筛查所有信息系统内的权限时效，增加了对于权限开通时时效的申请策略和使用策略；例如：门禁系统的权限都是半年有效期，到期复查重新设置。

五、 总结

通过审核组认真专业的审核服务，在审核过程中，与受审核方 充分沟通、解决分歧、达到共识、提高 ISMS 管理，为企业有效运行、持续改进自身的信息安全管理体系提供了帮助。特别是审核中开出的不符合项和交流项，没有采用遍地开花的策略，而是以点带面、突出此次审核重点地帮助企业深入理解 ISMS 标准的要求，从而使得企业逐步提高信息安全管理的能力，实现为企业的正常业务顺利开展保驾护航;

利用持续改进机制去评价受审核组织的 ISMS 管理体系，可以控制审核风险，又能得到了企业的认可和好评；实现真正的双赢!