上海联众网络信息有限公司

ISO27001:2005 信息安全目标与控制检查表

编制：

审核：

批准：

二〇一三年三月十二日

A.5 安全方针

标准条款号	标 题	目标 /控制	控制 理 由	控 制 要 求	审核发现
A.5.1	**信息安全方针**	**目标**	**依据业务要求以及相关的法律法规为信息安全提供管理指导和支持。**		
A.5.1.1	信息安全方针文件	控制	根 据 Info-Riskmanager 风险评估的结果。	总经理是否确保制定与公司目标一致的清晰的信息安全方针，并且通过在组织内发布和维护信息安全方针来表明对信息安全的支持和承诺。信息安全方针在《信息安全管理手册》中描述，《信息安全管理手册》由总经理批准发布？	管理手册中有信息安全方针
A.5.1.2	信息安全方针评审	控制	根 据 Info-Riskmanager 风险评估的结果。	每年管理评审或发生重大变化时是否对信息安全方针的持续适宜性、充分性和有效性进行评价，必要时进行修订？	管理评审报告

A.6 信息安全组织

标准条款号	标 题	目标 /控制	控 制 理 由	控 制 要 求	审核发现
A.6.1	**信息安全组织**	**目标**	**管理组织内部信息安全。**		
A.6.1.1	信息安全管理承诺	控制	根 据 Info-Riskmanager 风险评估的结果。	总经理是否承诺建立、实施、运作、监视、评审、保持和改进 ISMS，并通过一系列的活动，提供证实。该承诺《信息安全管理手册》中进行相是否描述？	
A.6.1.2	信息安全的协作	控制	根 据 Info-Riskmanager 风险评估的结果。	公司是否成立以信息安全管理者代表、各部门信息安全负责人组成的跨部门的联席会议，协调信息安全管理工作，对体系运行中存在的问题进行解决。会议由人事行政部负责组织安排并做好会议记录？	
A.6.1.3	信息安全职责分配	控制	根 据 Info-Riskmanager 风险评估的结果。	公司是否清楚的确定所有的信息安全职责。最高管理者授权信息安全管理者代表，全面负责信息安全管理体系的建立、实施与保持工作？ 对每一项重要资产指定信息安全责任人。	

A.6.1.4	信息处理设备的授权过程	控制	根据 Info-Riskmanager 风险评估的结果。	软件部是否根据使用部门需求提出新的信息处理设施（包括软件）的配置要求，并组织验收与实施，确保与原有系统的兼容？	
A.6.1.5	保密协议	控制	根据 Info-Riskmanager 风险评估的结果。	本公司是否与正式录用员工在劳动合同中附加有关保密方面的内容条款或签订《保密协议》。员工聘用期满离开公司之前，是否提醒其对保密所作的承诺？	
A.6.1.6	与权威机构的联系	控制	根据 Info-Riskmanager 风险评估的结果。	人事行政部是否制定规定，详细说明由谁何时与权威机构联系，以及怎样识别是否该及时报告的可能会违背法律的信息安全事件？	
A.6.1.7	与专业小组的联系	控制	根据 Info-Riskmanager 风险评估的结果。	软件部是否就计算机信息及通信网络安全问题与服务提供部门保持联系，以确保和在出现安全事故时尽快采取适当的行动和取得建议？	

A.6.1.8	信息安全的独立评审	控制	根据 Info-Riskmanager 风险评估的结果。	人事行政部是否负责组织、策划内部审核，根据策划的时间间隔，或者当安全设施发生重大变化时，对组织管理信息安全的方法及其实施情况进行独立评审？	
A.6.2	**外部相关方**	**目标**	**识别外部相关方访问的风险，明确对外部相关方访问控制的要求，并控制外部相关方带来的风险，保持被外部相关方访问、处理、共享、管理的组织信息及信息处理设施的安全。**		
A.6.2.1	与外部相关方有关的风险识别	控制	根据 Info-Riskmanager 风险评估的结果。	公司是否识别外部相关方对信息资产和信息处理设施造成的风险，并在批准外部相关方访问信息资产和信息处理设施前实施适当的控制，并签署规定访问和工作安排条款和条件的《保密协议》？	
A.6.2.2	处理与顾客相关的安全问题	控制	根据 Info-Riskmanager 风险评估的结果。	外包责任部门是否是否识别外包活动的风险，明确外包活动的信息安全要求，在外包合同中明确规定信息安全要求。在批准顾客访问组织信息或资产前，是否该处理所有已识别的安全要求？	

A.7 资产管理

标准条款号	标 题	目标 /控制	控 制 理 由	控 制 要 求	审核发现
A.7.1	**资产责任**	**目标**	**对本公司资产（包括顾客要求保密的数据、软件及产品）进行有效保护。**		
A.7.1.1	资产清单	控制	根 据 Info-Riskmanager 风险评估的结果。	软件部是否组织各部门识别资产，并根据重要资产判断准则确定公司的重要资产，通过风险管理软件，建立《重要资产清单》？	
A.7.1.2	资产所有权	控制	根 据 Info-Riskmanager 风险评估的结果。	软件部是否组织相关部门识别资产并指定资产负责人？	
A.7.1.3	资产的合理使用	控制	根 据 Info-Riskmanager 风险评估的结果。	是否制定相是否的业务系统是否用管理制度，重要设备有使用说明书，规定了资产的合理使用规则？ 使用或访问组织资产的员工、合作方以及第三方用户是否了解与信息处理设施和资源相关的信息和资产方面的限制。并对信息资源的使用，以及发生在其责任下的使用负责？	

A.7.2	**信息分类**	**目标**	**本公司根据信息的敏感性对信息进行分类，明确保护要求、优先权和等级，以确保对资产采取适当的保护。**		
A.7.2.1	分类指南	控制	根 据 Info-Riskmanager 风险评估的结果。	本公司是否有信息密级规定划分秘级？	
A.7.2.2	信息的标识和处理	控制	根 据 Info-Riskmanager 风险评估的结果。	对于属于企业秘密、企业机密与国家秘密的文件，密级确定部门是否按要求进行适当的标注？	

A.8 人力资源安全

标准条款号	标 题	目标 /控制	控 制 理 由	控 制 要 求	审核发现
A.8.1	**聘用前**	**目标**	**对聘用过程进行管理，确保员工、合同方和第三方用户理解其责任，并且能胜任其任务，以降低设施被盗窃、欺诈或误用的风险。**		
A.8.1.1	角色和职责	控制	根 据 Info-Riskmanager 风险评估的结果。	与信息安全有关的部门的安全职责是否明确规定？	
A.8.1.2	筛选	控制	根 据 Info-Riskmanager 风险评估的结果。	人力资源部是否负责对初始录用员工进行能力、信用考察，每年对关键信息安全岗位进行年度考察，对于不符合安全要求的不得录用或进行岗位调整？	
A.8.1.3	雇佣条款和条件	控制	根 据 Info-Riskmanager 风险评估的结果。	公司是否规定了员工、合同方以及第三方的聘用条款和条件？	

A.8.2	**聘用期间**	**目标**	**确保所有的员工、合同方和第三方用户知道信息安全威胁和利害关系、他们的职责和义务、并准备好在其正常工作过程中支持组织的安全方针，并且减少人为错误的风险。**		审核发现
A.8.2.1	管理职责	控制	根据 Info-Riskmanager 风险评估的结果。	公司管理者是否要求员工、合作方以及第三方用户，加强信息安全意识，依据建立的方针和程序来应用安全？	
A.8.2.2	信息安全教育和培训	控制	根据 Info-Riskmanager 风险评估的结果。	与 ISMS 有关的所有员工，有关的第三方访问者，是否接受安全意识、方针、程序的培训。方针、程序变更后是否及时传达到全体员工。人力资源部通过组织实施培训，确保员工安全意识的提高与有能力胜任所承担的信息安全工作？	
A.8.2.3	惩戒过程	控制	根据 Info-Riskmanager 风险评估的结果。	违背组织安全方针和程序的员工公司是否将根据违反程度及造成的影响进行处罚，处罚在安全破坏经过证实地情况下进行？	

A.8.3	**聘用中止或变化**	**目标**	**确保员工、合作方以及第三方用户以一种有序的方式离开公司或变更聘用关系。**	
A.8.3.1	终止责任	控制	根 据 Info-Riskmanager 风险评估的结果。	在员工离职前和第三方用户完成合同时，是否进行明确终止责任的沟通？
A.8.3.2	资产归还	控制	根 据 Info-Riskmanager 风险评估的结果。	员工离职或工作变动前，是否办理资产归还手续，然后方能办理移交手续？
A.8.3.3	解除访问权限	控制	根 据 Info-Riskmanager 风险评估的结果。	员工离职或工作变动前，是否解除对信息和信息处理设施访问权限，或根据变化作相是否的调整？

A.9 物理与环境安全

标准条款号	标 题	目标/控制	控 制 理 由	控 制 要 求	审核发现
A.9.1	**安全区域**	**目标**	**防止对组织办公场所和信息的未授权访问、损坏和干扰。**		是
A.9.1.1	实物安全周界	控制	根 据 Info-Riskmanager 风险评估的结果。	本公司安全区域是否分为一般安全区域与特别安全区域，特别安全区域包括机房和监控机房、机要室？ 。	是
A.9.1.2	物理进入控制	控制	根 据 Info-Riskmanager 风险评估的结果。	进出公司大院是否有门卫保安控制？ 员工是否凭工作牌进入办公区。是否经过授权的长期访问第三方《出入证》进入被授权的工作区域？	是
A.9.1.3	办公室、房间和设施的安全	控制	根 据 Info-Riskmanager 风险评估的结果。	特别安全区域内的办公室、房间和设施是否进行必要的控制，以防止火灾、盗窃或其它形式的危害？	是

A.9.1.4	防范外部和环境威胁	控制	根据 Info-Riskmanager 风险评估的结果。	机房设备是否安装在距墙、门窗有一定距离的地方。并具有防范火灾、水灾、雷击等自然、人为灾害的安全控制措施？	是
A.9.1.5	在安全区域工作	控制	根据 Info-Riskmanager 风险评估的结果。	公司是否建立相关制度，明确规定员工、第三方人员在有关安全区域工作的基本安全要求，并要求员工、第三方人员严格遵守？	是
A.9.1.6	公共访问、交付和装载区	控制	根据 Info-Riskmanager 风险评估的结果。	公司是否设立设置前台接待处接待外来人员，前台与特别安全区域予以隔离？	是
A.9.2	**设备安全**	**目标**	**防止资产的损失、损坏或丢失及业务活动的中断。**		
A.9.2.1	设备的定位和保护	控制	根据 Info-Riskmanager 风险评估的结果。	设备使用部门是否负责对设备进行定置管理或保护好，采取措施以降低来自环境威胁和危害的风险以及未经授权访问的机会？	是
A.9.2.3	电缆的安全	控制	根据 Info-Riskmanager 风险评估的结果。	软件部是否按照相关标准对传输线路进行敷设、调配、维护，防止线路故障？	是

A.9.2.4	设备维护	控制	根 据 Info-Riskmanager 风险评估的结果。	信息系统设备及用户计算机终端是否由软件部进行维护？	是
A.9.2.5	场所外设备的安全	控制	根 据 Info-Riskmanager 风险评估的结果。	拥有笔记本的部门在其离开规定的区域时，是否经过部门领导授权并对其进行严格控制，防止其丢失和未经授权的访问？	是
A.9.2.6	设备的安全处置及再利用	控制	根 据 Info-Riskmanager 风险评估的结果。	含有敏感信息的设备在报废或改做他用时，是否由使用部门是否利用安全的处置方法将设备中存储的敏感信息清除并保存清除记录？	是
A.9.2.7	资产转移	控制	根 据 Info-Riskmanager 风险评估的结果。	未经授权之前，是否不将设备、信息或软件带到工作场所外？ 重要信息设备的迁移是否被授权，迁移活动是否被记录？	是

A.10 通信和操作管理

标准条款号	标 题	目标/控制	控 制 理 由	控 制 要 求	审核发现
A.10.1	**操作程序和职责**	**目标**	**确保信息处理设备的正确和安全使用。**		
A.10.1.1	作业程序文件化	控制	根 据 Info-Riskmanager 风险评估的结果。	本公司是否按照信息安全方针的要求，建立并实施文件化的作业程序？ 。	是
A.10.1.2	变更管理	控制	根 据 Info-Riskmanager 风险评估的结果。	对信息处理设施的变更是否按相关规定进行。是否用系统和软件等方面的更改实施严格控制，在更改前评估更改所带来的潜在影响，正式更改前履行更改审批手续，并采取必要的措施确保不成功更改的恢复？	是
A.10.1.3	职责分离	控制	根 据 Info-Riskmanager 风险评估的结果。	为防止非授权的更改或误用信息或服务的机会，是否按要求进行职责分配？	是

A.10.1.4	开发和运作设备的分离	控制	根据 Info-Riskmanager 风险评估的结果。	开发部门在进行软件和测试程序的开发时，是否有一个独立开发与测试环境，与作业设施分离？	是
A.10.2	**第三方服务交付管理**	**目标**	**执行并保持与第三方服务交付协议相一致的信息安全和服务交付等级。 检查协议的执行情况，监控其符合性并控制相是否的变化，以确保交付的服务满足第三方协议中的所有要求。**		
A.10.2.1	服务交付	控制	根据 Info-Riskmanager 风险评估的结果。	是否对第三方的服务的交付，包括协议规定的安全安排、服务定义以及服务管理等方面进行管理和验收。是否确保第三方保持充分的服务能力，并且具备有效的工作计划，即便发生重大的服务故障或灾难也能保持服务交付的连贯性？	是
A.10.2.2	第三方服务的监控和评审	控制	根据 Info-Riskmanager 风险评估的结果。	第三方关系的管理是否有专门的人员，确保第三方分配职责符合协议要求。是否对协议要求，特别是安全要求的符合性进行监控是否该有充分可用的技术技能和资源。是否当发现服务交付不足时是否该采取适当的措施？	是

A.10.2.3	管理第三方服务的更改	控制	根据 Info-Riskmanager 风险评估的结果。	对第三方服务更改的管理过程是否考虑： a) 组织的更改，包括加强当前提供的服务，开发新是否用程序和系统，修改和更新方针及程序，解决信息安全事件，提高安全性的新控制？ b) 第三方服务的更改，包括更改和加强网络，使用新技术，更改服务设施的物理位置，更改供是否商？	是
A.10.3	系统策划与验收	目标	使系统故障风险最小化。		
A.10.3.1	容量管理	控制	根据 Info-Riskmanager 风险评估的结果。	软件部是否对信息网络系统的容量需求进行监控，并对将来容量需求进行策划，适当时机进行容量扩充？	是

A.10.3.2	系统验收	控制	根据 Info-Riskmanager 风险评估的结果。	新系统、系统升级接收前，系统验收部门是否制定接收准则，经测试合格后方可正式运行，测试记录及验收报告是否予以保存/	是
A.10.4	**防范恶意软件**	**目标**	保护软件和信息的完整性。		
A.10.4.1	防范恶意代码	控制	根据 Info-Riskmanager 风险评估的结果。	软件部是否为控制恶意软件的主管部门，负责提供防范恶意软件的技术工具并对技术工具进行实时升级，各部门是否具体负责本部门的恶意软件预防控制工作？	是
A.10.4.2	防范可移动代码	控制	根据 Info-Riskmanager 风险评估的结果。	授权使用移动代码时，配置是否该确保已授权移动代码的运行符合明确定义的安全方针，未经授权的移动代码是否该被阻止执行。	是

A.10.5	**备份**	**目标**	**保持信息处理和通信服务的完整性和可用性。**		
A.10.5.1	信息备份	控制	根据 Info-Riskmanager 风险评估的结果。	本公是否司根据风险评估的结果对重要数据库、软件等进行备份软件部为全公司信息备份提供技术支持，各业务主管部门是否协同软件部制定备份策略？	是
A.10.6	**网络安全管理**	**目标**	**为保持对网络中的信息及支持性设施进行有效保护**		
A.10.6.1	网络控制	控制	根据 Info-Riskmanager 风险评估的结果。	本公司是否充分管理和控制网络，以防范威胁，维持系统和使用网络的是否用程序的安全，包括传输中的信息。实施网络安全控制以确保网络上信息的安全，并对接入服务进行保护，防止未经授权访问？	是

A.10.6.2	网络服务的安全	控制	根据 Info-Riskmanager 风险评估的结果。	软件部是否根据组织的安全策略，识别现有的网络服务，明确规定网络服务安全属性值，由授权的网络系统安全管理员进行参数配置与维护管理？	是
A.10.7	**介质的处理**	**目标**	**为防止资产损坏和业务活动中断，根据介质所储存的信息的敏感性或重要性进行适当的保护，安全处置，确保因介质不当造成信息泄露事故发生。**		
A.10.7.1	可移动介质的管理	控制	根据 Info-Riskmanager 风险评估的结果。	对可移动介质包括光盘、磁带、磁盘、盒式磁带和已经印刷好的报告，各部门是否按其管理权限并根据风险评估的结果对其实施有效的控制？	是
A.10.7.2	介质的处置	控制	根据 Info-Riskmanager 风险评估的结果。	对于含有敏感信息或重要信息的介质在不需要或再使用时，处置部门是否按照要求采取安全可靠处置的方法将其信息清除？	是
A.10.7.3	信息处置程序	控制	根据 Info-Riskmanager 风险评估的结果。	为保护敏感信息不会因未经授权处理而造成泄漏或滥用，本公司是否建立并实施管理制度？	是

A.10.7.4	系统文件的安全	控制	根据 Info-Riskmanager 风险评估的结果。	本公司是否采取措施，保护系统文件，防止未经授权的访问。各部门对所属的系统文件，无论以何种媒体形式存在，是否按要求予以控制？	
A.10.8	**信息和软件交换**	**目标**	**明确信息和软件交换的控制目标，确保在内部及任何外部机构之间所交换的信息和软件的安全。**		
A.10.8.1	信息交换方针和程序	控制	根据 Info-Riskmanager 风险评估的结果。	在与顾客进行数据与软件交换的过程中是否采用以下的安全控制措施： a)签订安全保密协议，明确双方的安全责任与安全交接方式？ b)如果有要求，采用加密方式传输数据？ c)由授权人员接受并登记？	是
A.10.8.2	交换协议	控制	根据 Info-Riskmanager 风险评估的结果。	是否建立并保持相应的方针，以保护被传输的信息和物理介质，并作为制定交换协议的参考？	是
A.10.8.3	物理介质的传送	控制	根据 Info-Riskmanager 风险评估的结果。	根据 Info-Riskmanager 风险评估的结果。为避免被传送的介质在传送（运输）过程中发生丢失、未经授权的访问或毁坏，造成信息的泄露、不完整或不可用，负责介质传送的部门是否采用以下方法进行控制： a) 选择适宜的安全传送方式；	是

				b) 保持传送活动记录？	
A.10.8.5	业务信息系统	控制	根据 Info-Riskmanager 风险评估的结果。	本公司通过是否用系统进行日常办公、生产经营管理，本公司建立并实施相是否系统的安全使用策略和是否用管理，以保护与业务信息系统互联相关的信息，减少系统造成的信息泄露？	是
A.10.9	**电子商务服务**	**目标**	确保电子商务服务的安全，及其安全使用。		
A.10.9.1	电子商务	控制		本公司无该项业务	
A.10.9.2	在线交易	控制		本公司无该项业务	
A.10.9.3	公共信息	控制	根据 Info-Riskmanager 风险评估的结果。	本公司通过公共可用网站使用电子方式公布的信息，是否按规定进行控制？	是

A.10.10	**监控**	**目标**	**探测未经授权的信息处理活动。**		
A.10.10.1	审核日志	控制	根据 Info-Riskmanager 风险评估的结果。	软件部是否建立并保存例外事件或其它安全相关事件的审核日志，以便对将来的调查和访问控制监测提供帮助。审核日志一般通过使用系统检测工具按照事先的设置自动生成？	是
A.10.10.2	监控系统的使用	控制	根据 Info-Riskmanager 风险评估的结果。	监控部门是否按照规定周期对对监控结果进行评审，确保用户只执行被明确授权的活动。发现异常事件是否采取必要的措施并实施？	是
A.10.10.3	日志信息的保护	控制	根据 Info-Riskmanager 风险评估的结果。	是否实施控制，防止对日志记录设施的未经授权的更改和出现操作问题？	是
A.10.10.4	管理员和操作员日志	控制	根据 Info-Riskmanager 风险评估的结果。	管理员和操作员的日志是否该包括： a) 事情（成功或失败）发生的时间； b) 事情的有关信息（如：操作的文件）或故障信息； c) 涉及哪一个账号以及哪一个管理员或操作员； d) 涉及哪一个过程？	是

A.10.10.5	故障日志	控制	根据 Info-Riskmanager 风险评估的结果。	是否规定了用户或系统程序报告的有关信息处理系统的问题如何记录，以及清楚的规定了如何处理报告的故障？	是
A.10.10.6	时钟同步	控制	根据 Info-Riskmanager 风险评估的结果。	公司中心路由器是否设置为时钟同步服务器，在网络系统的域控制器与时钟同步服务器进行对时，所有的计算机设备是否必须登陆域？	

A.11 访问控制

标准条款号	标 题	目标 /控制	控 制 理 由	控 制 要 求	审核发现
A.11.1	**访问控制的业务要求**	**目标**	**确保信息处理设备的正确和安全使用。**		
A.11.1.1	访问控制策略	控制	根 据 Info-Riskmanager 风险评估的结果。	本公司是否基于访问控制策略，明确规定访问控制的业务要求，规定访问控制规则和每个用户或用户组的访问权力？	是
A.11.2	**用户访问管理**	**目标**	**确保授权用户能够访问信息系统，防止对信息系统未经授权的访问。**		
A.11.2.1	用户注册	控制	根 据 Info-Riskmanager 风险评估的结果。	是否根据规定的访问控制策略及确定的访问规则，访问权限管理部门对用户进行书面访问授权？	是

A.11.2.2	特权管理	控制	根据 Info-Riskmanager 风险评估的结果。	特权分配是否以它们的功能角色的最低要求为据，有些特权在完成特定的任务后是否被收回，确保特权拥有者的特权是工作所需要的且不存在富裕的特权？	是
A.11.2.3	用户口令管理	控制	根据 Info-Riskmanager 风险评估的结果。	各系统管理员是否对被授权访问该系统的用户口令予以分配？	是

A.11.3	**用户责任**	**目标**	**明确用户责任,防止对信息和信息处理设施非授权用户的访问、破坏或盗窃。**		
A.11.3.1	口令的使用	控制	根据 Info-Riskmanager 风险评估的结果。	本公司是否在相应的是否用管理中明确规定了口令安全选择与使用要求，所有用户是否严格遵守？	是
A.11.3.2	无人值守的用户设备	控制	根据 Info-Riskmanager 风险评估的结果。	本公司是否在和相应的应用管理中规定所有用户保护无人值守设备的安全要求和程序，以及他们在实施此类保护方面的责任？	是

A.11.3.3	清洁桌面和清除屏幕策略	控制	根据 Info-Riskmanager 风险评估的结果。	本公司是否制定清除桌面、清除屏幕的策略并实施，各部门负责人是否负责监督本部门员工该策略的日常实施情况？	是
A.11.4	**网络访问控制**	**目标**	**保护网络服务，防止对网络服务的未授权访问。**		
A.11.4.1	网络服务使用策略	控制	根据 Info-Riskmanager 风险评估的结果。	本公司是否建立并网络服务安全策略，以确保网络服务安全与服务质量？	是
A.11.4.2	外部联接用户的验证	控制	根据 Info-Riskmanager 风险评估的结果。	外部连接的用户对本公司内部网络访问，是否用户的访问授权按规定实施授权；是否只有经过授权的用户才可以实施外部连接？	是
A.11.4.3	网络中设备的鉴别	控制	根据 Info-Riskmanager 风险评估的结果。	如果通讯仅能从特定的位置和设备发起是重要的，是否可以采用设备鉴别？设备中的标识符或附加的标识符是否可以用来显示该设备是否被允许连接到网络？如果存在多个网络，尤其是这些网络有不同的敏感程度，那么标识符是否该明确显示设备被允许接入的网络？是否需要考虑设备的物理保护，以保持设备标识符的安全？	是
A.11.4.4	远程诊断和配置端口的保护	控制	根据 Info-Riskmanager 风险评估的结果。	软件部是否与设备供是否商签订安全协议，口令等安全措施对远程诊断断口的保护，防止被非法使用？	是

A.11.4.5	网络分离	控制	根 据 Info-Riskmanager 风险评估的结果。	是否为确保本公司网络安全，采用物理和逻辑两种方式进行网络隔离？	是
A.11.4.6	网络连接控制	控制	根 据 Info-Riskmanager 风险评估的结果。	软件部是否根据访问控制策略的要求，来限制用户的连接能力。例如通过网络网关来控制，网关的安全设置是否与组织的访问控制策略保持一致？	是
A.11.4.7	网络路由控制	控制	根 据 Info-Riskmanager 风险评估的结果。	软件部是否根据访问控制方针和网络安全要求，采用硬件或软件的手段，基于源地址和目的地址的检查机制，对路由实施控制？	是
A.11.5	**操作系统的访问控制**	**目标**	**防止未经授权的计算机访问。**		
A.11.5.1	安全登录程序	控制	根 据 Info-Riskmanager 风险评估的结果。	本公司是否通过技术手段提供安全的操作系统系统安全登录程序？为减少非授权访问的机会，是否对信息服务系统访问采用安全登录过程实现？	是
A.11.5.2	用户标识与验证	控制	根 据 Info-Riskmanager 风险评估的结果。	用户是否有唯一的识别符，以便他们个人单独使用时，能查出活动的个人责任，用户 ID 由系统管理员根据授权的规定予以设置；如果多个用户共用一个识别符（USER ID）是否由访问授权主管部门授权？	是

A.11.5.3	口令管理系统	控制	根 据 Info-Riskmanager 风险评估的结果。	软件部是否加强口令管理，通过技术手段提供有效的、互动的设施以确保口令质量。除非一次口令系统，通过操作系统的强制措施要求用户定期变更口令？	是
A.11.5.4	系统实用程序的使用	控制	根 据 Info-Riskmanager 风险评估的结果。	软件部门是否对系统是否用程序的使用进行限制和严格控制，并规定授权的使用者。	是
A.11.5.5	会话超时	控制	根 据 Info-Riskmanager 风险评估的结果。	各系统管理员在其管理的终端处于不活动时，是否利用锁屏、清除屏幕以防止非授权的访问，但不关闭是否用或网络话路。 对于外部访问系统服务器的连接是否有时限控制？	是 是
A.11.5.6	联接时间的限制	控制		根据风险评估的结果，本条款不适用	NA
A.11.6	**是否用程序及信息访问控制**	**目标**	**防止未经授权访问信息系统内的信息。**		
A.11.6.1	信息访问限制	控制	根 据 Info-Riskmanager 风险评估的结果。	基于本公司生产经营管理是否用要求并遵从访问策略，向应用用户提供访问信息和是否用系统功能?	是

A.11.6.2	敏感系统隔离	控制	根据 Info-Riskmanager 风险评估的结果。	为确保含有敏感信息的系统不发生泄密事故，是否采取措施对敏感系统予以隔离？	是
A.11.7	**移动式计算和远程工作**	**目标**	**明确控制目标，确保移动式计算和远程工作设施的信息安全。**		
A.11.7.1	移动计算和通信	控制	根据 Info-Riskmanager 风险评估的结果。	本公司是否建立实施使用规定，对笔记本电脑的移动办公实施有效安全管理？	是
A.11.7.2	远程工作	控制	根据 Info-Riskmanager 风险评估的结果。	本公司是否建立远程工作安全策略，并对远程工作用户实施授权管理，采取必要的安全措施防止远程工作带来的安全风险？	是

A.12 系统获取、开发和维护

标准条款号	标 题	目标/控制	控 制 理 由	控 制 要 求	审核发现
A.12.1	**信息系统的安全要求**	**目标**	**确保安全性已构成信息系统的一部分。**		
A.12.1.1	安全需求分析和规范	控制	根据 Info-Riskmanager 风险评估的结果。	信息系统建设部门在进行新系统建设或系统更新时，是否对系统进行分析，根据业务功能要求及信息安全要求，明确规定控制要求？	是

				系统（软件）本身的功能及安全特性是否在设计开发输入时是否明确提出，并进行评审？ 是否用系统建设按照规定执行？	是 是
A.12.2	**是否用程序的正确处理**	**目标**	**防止是否用程序中错误的、用户数据丢失、未经授权的修改或滥用。**		
A.12.2.1	输入数据的验证	控制	根据 Info-Riskmanager 风险评估的结果。	系统建设是否明确是否用系统输入数据验证的要求，以确保输入数据正确和恰当？ 各部门是否用系统的操作人员是否对输入到系统内的数据进行认真核对，对于关键或重要输入数据的输入是否由相是否的作业流程所规定的人员进行确认？	是 是
A.12.2.2	内部处理控制	控制	根据 Info-Riskmanager 风险评估的结果。	系统建设是否考虑系统内部数据确认检查的要求，以查处数据处理过程的错误？	是
A.12.2.3	消息的完整性	控制	根据 Info-Riskmanager 风险评估的结果。	系统建设时是否识别消息的真实性和完整性需求，并识别和实施适当的控制？	是
A.12.2.4	输出数据的验证	控制	根据 Info-Riskmanager 风险评估的结果。	系统建设是否考虑应用系统输出数据确认的要求，以确保对贮存的信息处理的正确和	是

				环境相适是否？ 各部门是否用系统的操作人员是否对是否用系统输出的数据进行认真核对，对于关键或重要的输出数据是否由相是否的作业流程所规定的人员进行确认？	是
A.12.3	**加密控制**	**目标**	**通过加密方法确保信息的机密性、完整性和有效性。**		
A.12.3.1	使用密码控制策略	控制	根据 Info-Riskmanager 风险评估的结果。	本公司是否根据及保护本公司机密数据的要求，制定数据加密策略并实施？是否正确应用加密技术，确保是否用利益最大化，危险最小化，须避免不恰当或不正确的使用？	是
A.12.3.2	密钥管理	控制	根据 Info-Riskmanager 风险评估的结果。	本公司是否根据所采用的加密技术对密钥产生、安全分发、储存、安全使用等方面进行管理，以支持密码技术的是否用？是否防止密钥的任何损坏或丧失（包括泄密）都可以导致信息机密、真实性和/或完整性的损害？	是
A.12.4	**系统文件的安全**	**目标**	**控制对系统文件和程序源代码的访问，并确保系统文件的安全。**		

A.12.4.1	操作软件的控制	控制	根据 Info-Riskmanager 风险评估的结果。	规定软件部和系统应用主管部门是否对操作系统软件的版本管理、安装、使用和备份进行严格控制。规定在新软件安装或软件升级之前，是否经测试和审批后方可按规定程序进行？	是
A.12.4.2	系统测试数据的保护	控制	根据 Info-Riskmanager 风险评估的结果。	本公司是否规定不得使用包含个人信息和敏感信息以及运行数据库用于测试？	是
A.12.4.3	对程序源代码的访问控制	控制	根据 Info-Riskmanager 风险评估的结果。	为降低计算机程序被破坏的可能性，系统建设部门是否按规定的要求对程序源代码实施管理/	是
A.12.5	开发和支持过程的安全	**目标**	确保是否用系统软件和信息的安全。		
A.12.5.1	变更控制程序	控制	根据 Info-Riskmanager 风险评估的结果。	为使对信息系统的损害降至最小，系统的变更，在更改前是否进行适当的测试与评审，经开发软件负责人批准后予以实施？ 操作系统及是否用系统的升级是否经过系统主管部门测试、评审与批准后方可进行？	是 是
A.12.5.2	操作系统变更后对是否用程序的技术	控制	根据 Info-Riskmanager 风险评估的结果。	当操作系统发生更改时，操作系统更改对应用系统的影响是否由系统主管部门进行评	是

	复查			审，确保对作业或安全措施无不利影响？	
A.12.5.3	软件包的变更的限制	控制	根据 Info-Riskmanager 风险评估的结果。	本公司不鼓励修改软件包，如果有必要确需进行更改，更改提出部门是否在实施前进行风险评估，确定必须的控制措施，保留原始软件，并在完全一样的复制软件上进行更改，更改实施前是否得到软件部领导和系统是否用主管部门的授权？	是
A.12.5.4	信息泄漏	控制	根据 Info-Riskmanager 风险评估的结果。	是否对软件的采购、使用、变更及开发过程进行控制和检查以防止可能的隐藏通道和特洛伊码？	是
A.12.5.5	外包软件开发	控制	根据 Info-Riskmanager 风险评估的结果。	开发软件正式外包前，设计开发部门是否明确软件开发的安全技术要求，并与软件开发方签订技术协议在协议中明确规定安全技术要求（包括开发过程）；软件安装使用前，是否进行测试，以防止隐藏通道及特洛伊码的存在？	是
A.12.6	**技术薄弱点管理**	**目标**	**降低由已经公布的薄弱点所带来破坏的风险。**		
A.12.6.1	技术薄弱点的控制	控制	根据 Info-Riskmanager 风险评估的结果。	归口管理部门是否对技术薄弱点是否进行风险评估，进行专项分析，制订风险处理计划，根据风险处理计划采取对是否的技术和	是

				管理措施。	

A.13 信息安全事件管理

标准条款号	标 题	目标 /控制	控 制 理 由	控 制 要 求	审核发现
A.13.1	**报告信息安全事情和弱点**	**目标**	**保证与信息系统相关联的信息安全事情和弱点的沟通，沟通的方式是否允许采取及时纠正措施。**		

A.13.1.1	报告信息安全事情	控制	根据 Info-Riskmanager 风险评估的结果。	安全事情、事故一经发生，事情、事故发现者、事情、事故责任者是否立即向主管部门报告，主管部门和责任部门是否及时对事情、事故进行反是否处理。所有员工有报告安全事情、事故的义务？	是
A.13.1.2	报告安全弱点	控制	根据 Info-Riskmanager 风险评估的结果。	各部门及全体员工是否按照要求及时识别安全薄弱点及可能的安全威胁，一旦发现是否及时向有关人员或部门报告并记录，主管部门或安全管理负责人是否采取有效的预防措施，防止威胁的发生?	是
A.13.2	**信息安全事件和改进的管理**	**目标**	**保证是否用于信息安全事件管理的方法的一致和有效。**		
A.13.2.1	责任和程序	控制	根据 Info-Riskmanager 风险评估的结果。	事故主管部门接到报告以后，是否立即进行迅速、有效和有序的反应?	是
A.13.2.2	从事故中吸取教训	控制	根据 Info-Riskmanager 风险评估的结果。	事故发生后，主管部门是否对事故发生的原因、类型、损失进行鉴定，并提出防止此类事故再次发生的措施或建议，形成事故调查分析及处理报告，责成责任部门实施纠正措施？	是

A.13.2.3	证据的收集	控制	根据 Info-Riskmanager 风险评估的结果。	人事行政部是否负责发生法律纠纷与诉讼的证据收集，并确保证据收集是否符合以下要求： a) 所呈证据是否符合国家有关的证据法规； b) 符合用于提供可接受证据的任何已发布的标准或法规； c) 对已收集到的证据进行安全的保管，防止未经授权的更改或破坏； d) 收集到的证据符合法庭所要求的形式。	

A.14 业务持续性管理

标准条款号	标 题	目标 /控制	控 制 理 由	控 制 要 求	审核发现

A.14.1	**业务持续性管理的内容**	**目标**	**抵消业务活动受到干扰的影响，并防止关键业务处理受大的信息系统故障或者灾难的影响，确保能够及时恢复基本运行。**		
A.14.1.1	业务持续性管理过程中包含的信息安全	控制	根据 Info-Riskmanager 风险评估的结果。	公司是否建立并实施管理程序，在发生灾难或安全故障时，实施持续性管理计划，确保关键业务及时得到恢复？	是
A.14.1.2	业务持续性和风险分析	控制	根据 Info-Riskmanager 风险评估的结果。	为达到公司业务的持续性目标，软件部是否组织有关部门在适当的风险评估的基础上，进行灾难及系统中断影响分析，识别出造成关键业务中断的主要事件及其影响？	是
A.14.1.3	编制并实施包含信息安全在内的持续性业务计划	控制	根据 Info-Riskmanager 风险评估的结果。	有关部门是否编制《业务持续性管理计划》，由信息安全管理者代表批准，以便在重要系统发生中断或故障后，实施持续性管理计划，以保证系统或作业中断的及时恢复？	是 见《业务持续性管理计划》
A.14.1.4	业务持续性策划框架	控制	根据 Info-Riskmanager 风险评估的结果。	是否保持独立的业务持续性计划的框架，以确定各种计划的一致性并确定检测和维护的优先权？	是
A.14.1.5	业务持续性计划的测试、保持和重新评估	控制	根据 Info-Riskmanager 风险评估的结果。	每年软件部是否组织有关部门采取适宜的测试方法对《业务持续性管理计划》进行测试，并保持测试记录；每次测试后，软件部组织与计划有关的部门对计划的时效和有效性进行评审，必要时，对业务持续性计划	是

				进行修改？	

A.15 符合性

标准条款号	标 题	目标 /控制	控 制 理 由	控 制 要 求	审核发现

A.15.1	**符合法律要求**	**目标**	**避免违反任何民法、刑法、规章或契约义务以及任何安全要求。**		
A.15.1.1	适用法规的识别	控制	根 据 Info-Riskmanager 风险评估的结果。	人事行政部是否负责组织收集与信息安全有关的法律法规，并对适用性评价，确定其实用范围和具体适用条款，形成适用的法律法规清单，将法律法规一起通过网络传达给有关部门并予以执行？	是
A.15.1.2	知识产权	控制	根 据 Info-Riskmanager 风险评估的结果。	本公司是否严格执行国家有关知识产权方面的法律法规，保证使用合法的正版软件，并按规定进行控制？	是
A.15.1.3	保护组织记录	控制	根 据 Info-Riskmanager 风险评估的结果。	各部门是否按照要求，明确规定重要记录的保存期限并提供适当的保护，防止丢失、损坏和伪造？	是
A.15.1.4	数据保护和个人信息隐私	控制	根 据 Info-Riskmanager 风险评估的结果。	对处理与个人数据与信息有关的部门是否按照有关规定，对个人信息进行妥善管理与保护，防止丢失或泄露个人秘密？	是
A.15.1.5	防止信息处理设施的误用	控制	根 据 Info-Riskmanager 风险评估的结果。	信息处理设施是否按批准的使用目的和使用范围使用。如果将这些设备用于未经批准的非业务目的，或用于未经授权的目的，为设备使用不当。一经发现，将采取惩戒措施？	是

A.15.1.6	密码技术控制条例	控制	根 据 Info-Riskmanager 风险评估的结果。	根据保护本公司机密数据的要求，是否正确应用加密技术，确保是否用利益最大化，危险最小化，须避免不恰当或不正确的使用？	
A.15.2	符合安全策略和标准、技术	**目标**	**确保系统符合组织的安全策略和标准。**		
A.15.2.1	符合安全策略	控制	根 据 Info-Riskmanager 风险评估的结果。	每年人事行政部是否组织至少一次信息安全管理体系内部审核，每次审核的范围是否覆盖与信息安全管理体系有关的所有部门与安全区域，确保职责范围内的所有安全程序正确完成， 依从安全方针和标准？	是 见内部审核报告
A.15.2.2	技术符合性检查	控制	根 据 Info-Riskmanager 风险评估的结果。	软件部是否利用入侵检测、漏洞扫描等工具对网络系统进行定期技术性检查？ 内部审核活动是否包括对各信息系统的技术性审核，内部审核组至少拥有一名具有一定信息安全技术的内部专家；技术性审核是否在被监督的情况下进行？	是
A.15.3	**信息系统审核相关事宜**	**目标**	**将系统审核程序的有效性最大化并把对该程序的干扰降到最低限度。**		

A.15.3.1	信息系统审核控制	控制	根据 Info-Riskmanager 风险评估的结果。	正式审核之前，审核组是否明确技术性审核的项目与要求，防止审核活动本身造成不必要的安全风险？	是
A.15.3.2	信息系统审核工具的保护	控制	根据 Info-Riskmanager 风险评估的结果。	软件部是否对漏洞扫描工具进行管理，使用者是否被授权，检查工作是否在监督的情况进行，审核活动是否被记录？	是