逻辑安全检查记录单
Logic Security Check List

检查人: Checker:		陪同人: Escorted by:		检查完成日期: Date of end of the Audit:		
评审人: Reviewer:				审核类型: Audit Type:	月检查 Monthly inspection	
控制要求 Control	方法和要求 How and References			日期和时间 Date and Time	结果 Result	备注（抽样样品ID） Comments (IDs of Samples being Checked)
数据室控制 Data Room Control						
测试Data Room的权限控制 Testing access right for Data Room	1. 对比Data Room室的进出清单与权限人员清单，确保没有非法人员进行 2. 检查Data Room机柜及Key Box的控制，不在使用时应是被锁定的，Key Box 钥匙只由授权人员使用 1. Check the conformance between the access records with the access right list. 2. Check the control of the racks and key boxes to confirm if they are locked and used by authorized employees.					
防火墙电缆连接的正确性 Correctness of firewall cable connection	对防火墙各网络接口连接线状态与SA提供的备案图片进行比对，确保两者一致 Check that if all the connections of firewalls network port are conform to the reference picture.					
HSM电缆连接的正确性 Correctness of HSM cable connection	对HSM外观网络接口连接与SA提供的备案图片对比，确保两者一致 Check that if all the connections of HSMs network port are conform to the reference picture.					
HSM中的监控系统是否在正常时间内正式开启 Availability of monitoring systems for HSM protection	检查HSM室的CCTV及闯入警报系统是否在正常时间内工作 Check that if the CCTV and alarm systems are functioning appropriately in area where HSM stored.					
IT系统 IT System						
检查在生产是否有未授权添加、删除的客户端 Control of clients creation and deletion within production network domain	检查有无添加、删除的终端，申请单记录是否完整 特别是数据存储、处理终端的添加、删除 Check that if all the deletion and adding of terminal are with integrate application record, especially for the deletion and creation of data storage and processing.					

控制要求 Control	方法和要求 How and References	日期和时间 Date and Time	结果 Result	备注（抽样样品ID） Comments (IDs of Samples being Checked)
系统安全策略被实施包含所有系统的终端 Enforcement of system security policy on terminals within production network domain	检查GPO安全策略，包括账户锁定策略以及密码策略等。 检查屏幕保护策略，必须启用密码保护。 Check the GPO security policy: Enforced password history = 4 times · Max password age = 90 days · Min password age = 1 day · Min password length = 8 characters · Password must meet complexity requirements · Account lockout duration = 0 mins · Account lockout threshold = 6 invalid attempts · Reset account lockout after = 99999 mins			
检查备份 介质的保护情况 Protection for media with back-up data	包含敏感数据的存储介质需要双控访问 Check the dual control of the medias with sensitive data.			
IT系统/终端 IT System/ Terminal				
生产区域汇聚层网络端口 For port of convergence layer in production area	确保汇聚层接口的启用应得到记录，并将最新的记录提供给安全人员 Check that if the enabling of the port of convergence layer is documented and provided to security officers.			
网络接入端口、设备端口安全策略及其受控情况的检查 Security policy and control of network port and equipment port	检查网络设备上是否有未知网络连接 检查网络设备上的安全策略，包括访问策略、管理策略（例如可信、实名管理，默认管理的修改，管理方式等） 根据 Network Equipment Configuration 1. Check that if there is any unknown network connection on network equipment. 2. Check the security policy of network equipment, including access policy, mgt. policy (such as reliable and real name mgt., mgt. changes, mgt. methods etc.) According to Network Equipment Configuration			
关键PC Key PC	检查关键PC是否安装了不符合要求的软件，包含数据、接收处理PC; Check if the key PC is installed with unauthorized software, including data receiving and processing PC.			
IT系统/补丁 IT System/Patch				

控制要求 Control	方法和要求 How and References	日期和时间 Date and Time	结果 Result	备注（抽样样品ID） Comments (IDs of Samples being Checked)
系统、网管设备补丁的跟踪测试及安装 Patches testing and installation of system and network mgt. equipment	SA应该有补丁的跟踪测试、安装记录,并选取一台终端验证补丁是否正确安全 SA should maintain testing and installation records for patches. Choose one terminal to verify that if the patches are installed correctly and safely.			
《计算机档案记录表》是否与实际情况一致 Enforcement of Authorized Software List	SA应该有软件安装和配置的清单 检查终端，确保设备、软件、配置等与清单一致 配置的变更应有符合规定的申请、批准文件 SA should maintain software installation and configuration list. Check the terminal to confirm if the configuration is conducted according to the Authorized Software List. All the changes of configuration should be with application and authorization documentations as required.			
内部弱点扫描报告 Internal vulnerability scanning report	使用Nessus软件对生产网络内的IT设备（PC、服务器、防火墙）进行漏洞扫描，对严重和高危漏洞要在2天内进行补丁安装，授权情况下不超过一周；报告要经过逻辑安全员复核签名 Use Nessus to conduct vulnerability scanning for IT equipment within production network (PC, server, firewall). The serious and high risk vulnerability should be resolved within 2 days, any authorized extension should not exceed one week. Report should be signed by logical security officers to make confirmation.			
IT系统/存储 IT System/Storage				
授权笔记本使用 Use of authorized laptop	授权使用的笔记本必须设置Bios保护密码 可移动存储接口必须使用物理防护措施进行功能禁用 Check that if the authorized laptop has been set BIOS protection password. Check that if the removable storage port has been disabled by physical measures.			

控制要求 Control	方法和要求 How and References	日期和时间 Date and Time	结果 Result	备注（抽样样品ID） Comments (IDs of Samples being Checked)
硬盘的退役或维修 Decommissioning or repairing of hard disk	确保从高安全区域退出的硬盘是受控， 每个物理介质都须向安全部声明，敏感数据进行了安全处理 Check that if the decommissioned disk is under control and reported to security dept. Check that if the sensitive data contained is deleted securely.			
IT系统/系统账户控制与审计 IT System/System Account Control and Audit				
关键目录权限控制 Key Directory Right Control	关键目录是指存放生产数据的文件夹： 1、系统管理员账户不能读取关键目录内的文件，仅可进行目录权限的维护 2、检查确认没有离职人员账户拥有关键目录的访问权限 3、关键目录包括用于数据传输、处理的PC、服务器，例如：DatagetPC /PGP PC /数据员工作（入库）PC/数据备份PC等 Key directory is referring to the folders with production data: 1 Check that if the system administrator can read the documents within key directory? 2 Check that if the previous employee can access the key directory 3 Check that if the			
IT系统/FTP（SFTP）管理 IT System/FTP(SFTP) Management				
FTP账户维护 FTP Accounts Maintenance	FTP账户的建立应使用《IT账号开通及变更申请表》，设置应与申请单一致 Check that if the creation of FTP accounts are compliance to relevant applying records.			
FTP账户有效性审计 Audit the effectiveness of FTP accounts	SA人员应每月根据在线生成日志信息，清单不应包含不需要或未授权的账户存在；账户应是实名制持有使用 SA personnel should generate monthly log information based on online. Not-needed or unauthorized accounts should not exist. Account should be used by real-name registration.			
IT系统/监控 IT System/Monitor				
IDS/IPS设备的管理 IDS/IPS equipment MGT.	1、IDS/IPS授权的IT管理员进行管理 2、IT管理员应有自己的实名制账户 1 Authorized IT administrators manage the IDS/IPS. 2 IT manager should use his own account with is registered with his real-name.			

控制要求 Control	方法和要求 How and References	日期和时间 Date and Time	结果 Result	备注（抽样样品ID） Comments (IDs of Samples being Checked)
IDS/IPS系统完整性 IDS/IPS system integrity	IDS/IPS设备应被正确使用： 1、检查IDS/IPS设备的实时报警系统，确保系统运行正常，并且没有失败的告警 2、确保IDS/IPS设备的特征库得到了及时有效的更新 IDS/IPS should be used appropriately: 1 Check the real-time alarm system of IDS equipment, to confirm that the system is running well and there isn't any failing alarm. 2 Check that if the feature library is updated effectively and timely.			
IT系统/无线监控 IT System/Wireless Monitor				
对高安全区环境进行无线网络扫描监控 Wireless scanning for HSA	1、无线网络监控的区域应包括生产网络节点所在的全部区域，数据室、个人化车间、数据处理区 2、除生产机台的的无线组件外，不应有任何无线热点是用于生产的 3、生产网络工作站、PC、服务器上的无线网卡应是禁用的 1 Check that if the wireless scanning covers all the area with production network nodes, including server room, personalization workshop and data room. 2 Check that if there is any Wi-Fi using for production, excepting the wireless components of production equipment 3 Check that if the wireless card is disabled for work station, PC and server on production network.			
IT系统/防火墙 IT System/Firewall				
防火墙的管理设置 Firewall mgt. setting	现场检查防火墙设置： 1、防火墙上的管理账户密码应被设置为至少8位 2、检查防火墙的访问管理账户，确保没有离职、转岗员工的存在 3、检查防火墙的可信管理IP设置，应与《防火墙策略清单》一致 Check the firewall setting on-site: 1. The minimum length of firewall mgt. account must be set as 12 characters 2. Check the firewall mgt. accounts to confirm there is not any previous employees' accounts. 3. Check the reliable mgt. IP setting of firewall, to confirm that they are conformance to Firewall Configuration Checklist.			

控制要求 Control	方法和要求 How and References	日期和时间 Date and Time	结果 Result	备注（抽样样品ID） Comments (IDs of Samples being Checked)
防火墙访问控制设置 Access control for firewall	系统管理员应该定期对全部防火墙配置进行备份，配置修改前、后也要进行备份 System administrator should back-up the firewall configuration regularly, or after and before any changes.			
防火墙日志管理 Firewall log mgt.	防火墙应开启日志功能，并设置统一的日志服务器；日志应被备份保存，保存天数不少于12个月； The logging function of firewall must be enabled by using log server. Logs should be retained for at least 12 months.			
防火墙VPN访问管理 Firewall VPN access mgt.	定期对SA人员根据在线生成的日志进行检查，不应包含未授权或不需使用的账户存在 Check the log generated from system to confirm if there is any unauthorized or unnecessary accounts.			
IT系统/数据处理 IT System/Data Handling				
数据处理PC磁盘文件检查 Data processing PC	数据处理PC的本地磁盘中不应存储有敏感数据 Check the local disk of data processing PC to confirm that there isn't any sensitive data stored.			