安全领域	序号	控制项	基本准则	参照国际/内的标准	备注
账号	1.1	账号指定所有人	所有账号必须有指定的拥有人		
	1.2	标准账号	每一位人员会被分配唯一的标准账号，标准账号必须不能显示个人特性（如人员工作的部门），人员在所有系统建议使用标准账号。		
	1.3	账号使用追踪	所有账号必须能够确认其使用人员。		
	1.4	未被使用的账号	如果账号连续90天都没有被使用过，必须禁用该账号		开发
	1.5	账号的批核	所有账号的建立及权限增加必须通过账号申请程序，并获得部门领导或其委托者的批准，账号审批人必须审核申请人访问该信息系统在业务上的必要性及确认只授予申请人最小限度的系统权限		具体的账号申请流程待确定
	1.6	账号禁用	当人员离职、调岗、或被解除劳动合同时，账号必须在一个工作天内被禁用 特别说明：在特殊及不影响职责分离的情况下，调岗人员可在原来部门领导的审批下，继续使用原来账号权限，但审批期不应多于一个月。		
	1.7	账号解封	账号被禁用或被锁定，只能经账号管理员确认用户身份后或经信息安全部核准的自动解锁/密码重置设施，方能恢复账号和解除锁定。		
	1.8	人员休假	当人员进行长假期休假时，其生产系统的账号禁用。		
	1.9	特权账号管理	所有特权账号必须至少由两个或两组独立托管人监控，确保没有任何一个人知悉整个帐号密码。		
	1.10	账号管理账号的使用	账号管理账号只能用作账号管理（包括账号建立、更改、删除、密码重置、锁定及激活）的活动，除账号管理外，不能用作其他用途。		
	1.11	账号管理账号的日志	所有账号管理员的活动（包括账号的建立、更改、删除，账号的密码重置、锁定及激活）必须被完整记录。		
	1.12	系统服务账号	系统（包括操作系统、应用系统、数据库）底层的账号，只能用于系统与系统间的通讯或启停系统服务。 系统服务账号禁止被用作系统管理、维护等其他用途		
	1.13	系统默认账号	系统默认账号（如administrator等)必须被禁用、锁定、更改或作适当的配置，防止被使用。		
	1.14	应急账号	所有应急账号在紧急情况使用时，必须在两个获授权人员互相监控下使用，并确保没有一个人员知悉整个帐号密码。 应急账号在使用完后，必须尽快由托管人员更改其个别密码段。		
	2.1	强效密码使用	所有特权账号必须使用强效密码认证		
	2.2	强效密码	1)密码长度：至少为8为字符 2)密码字符：以系统可支持的字符组成，包括数字、字母和特殊字符。 3)密码必须至少有一个字母及一个数字组成。 4)强效密码标准： 密码由5个或以上不同的大写和小写字母、数字、特殊字符组成。 密码不能含有英文字典中的单词、汉字词的拼音或英文数字序列。 密码不能含有个人相关资料，如个人或家属人员的名字、出生日期等。 密码与帐号不能存在相同、相反、包含或者被包含关系。		
	2.3	密码有效期	密码有效期，必须至少每90天修改。		
	2.4	密码修改权限	除受最短有效期限制外，用户必须被允许随时修改密码		
	2.5	密码修改提示	密码在失效前至少7天内，建议系统在用户每次登陆时提示用户修改密码。		
	2.6	密码重用控制	用户禁止使用过去曾使用过的10个密码。		
	2.7	强制修改初始密码	用户首次登录系统或密码重置后第一次登录，密码必须被强制修改。		
	2.8	初始密码有效期	初始密码在发出后5天内仍未作出修改，账号建议被锁定。		

密码	2.9	旧密码重认证	密码在修改时，旧密码必须被重新认证。		
	2.10	密码存储	密码禁止以明文储存。 储存的密码必须使用杂乱编码或单向加密算法保护密码安全。 当不能以加密方式安全保存密码，密码必须使用物理及/或逻辑安全方式防止未获授权的读取。		
	2.11	密码保管	用户必须牢记密码。密码禁止被记录（如写在纸张上）保存。		
	2.12	密码使用	用户必须避免在不同环境使用同一密码 1)同一用户拥有多个账号的，必须避免不同账号间的密码相同或相近。 2)若测试环境和生产环境中存在同名账号，必须为其设置不同的密码，测试环境禁止使用生产环境密码。 3)用户禁止将公司以外的账号密码（如家庭上网密码、外部邮箱密码等）作为公司网路系统的账号密码。 4)用户禁止与家人、朋友共享公司系统的账号和密码。		
	2.13	密码转送/密码传送	密码必须被安全传送： 1）禁止通过传真等明文方式传送密码 2）通过邮件传送账号和密码时，必须将账号和密码分次传送，并在传送完毕后电话与接收人确认是否已经接收。 3）通过电话传送账号和密码前，必须先确认对方身份。 4）如果通过电话或邮件传送密码，接收密码的一方必须立即修改密码。		
	2.14	手工重置密码	1）电话支援人员不应单以声音来判别拥有人身份； 2）电话支援人员必须以多项信息识别重置要求者的身份 3）重置的密码必须复核密码要求，并且随意产生；		
	2.15	自动重置	1）密码 重置要求者必须在事前在密码重置系统中的不少于30条提问中注册不少于6条挑战性问题的答案； 2）挑战性问题答案可在密码初始时回应，否则重置要求者必须通过不低于登入该系统认证的方式，才可对挑战性问题进行注册或修改； 3）在密码重置时，要求者必须完全正确回答在注册挑战问题中随机抽取的3条问题； 4）要求者重置后的密码必须符合以上密码的要求； 5）挑战性问题的答案的存储必须符合“密码存储”的保存要求。		
	3.1	认证数据标准	认证数据是指用于确认用户身份的信息，包括但不限于密码、一次性密码、交易认证信息如PIN、CVV2等		暂空缺，如需要，可提供
	3.2	信息保护	所有保存秘密、机密、绝密信息的系统，用户必须以密码认证或强效认证来鉴别用户身份，保护信息的保密性、完整性和可用性。		

认证	3.3	认证数据保密	所有非一次性认证数据，包括但不限于密码、PIN、CVV2等，不论是在储存、传输中都必须妥善保护，以防泄露或被未获授权修改。		对于非一次性认证数据，需要在生成、传输、保管方面逐一实现： 1.认证数据生成，认证数据生成时，其必不能在任何地方进行展示或记录，具体要做到（1）在生成密码的页面屏蔽展示（2）不能在日志中记录密码的信息（银联要求不能记录密码明文以及密文）（3）生成后采用的保密方式 2.认证数据传输，认证数据生成后，必须以适当的方式传输，防止窃听者/攻击者能获取整个认证信息，采用的方式有： （1）加密传送，使用加密方式传输认证数据时，需要关注其采用的加密方式是否足够安全，若加密密措施失当，亦会造成认证数据泄露。 （2）人工分发，在某些情况下需要采用人工分发手段传输认证数据，需要了解认证数据是否能被轻易截取获得，可以采用Split Knowledge等方式传送密码，保证完整密码不为一个人知道，或通过多种途径分次发送密码。关键需要看业务方对密码分发的需求侧重点。 3.认证数据保存，主要涉及认证数据落地， （1）应首先了解该认证数据能否在该系统中落地，例如信用卡规定CVV2码是不能保存于系统；或根据银监规定除认证服务器，其他服务器均不能存放认证信息。 （2）了解认证数据落地的保护措施，例如A系统访问B系统时需要提供一个访问认证信息，而审查发现该认证信息直接以明文方式保存在A的访问配置文件中，若有第三方获得这份认证信息，则可以冒用A的身份登陆。
	3.4	认证数据传输	加密保护的认证信息必须实施端对端保护，认证数据从输入端直接加密及传输至认证端，如须在在非认证点解密必须有确实的业务操作需要，如必要的转加密发送至多余一个的认证点而各个点必要使用不同的加密密钥。		
	3.5	认证数据保存	认证数据禁止被保存于自动登录过程中，例如IE中的账号及密码保存。		
	3.6	认证数据记录	认证数据，包括明文及密文，禁止在任何认证处理过程中记录（包括但不限于日志）下来。		
	3.7	高风险系统访问	所有高风险系统（如资金管理系统、财务系统）的访问，必须使用强效认证，包括但不限于双因素认证。 双因素认证是指在下列三类认证方式中，选用两个不同类别的认证方式： *你所知道的（如密码）； *你所拥有的（电子证书、一次性密码令牌）； *你自己的（如虹膜、指纹）。		
	3.8	远程访问	所有对机密、绝密数据的远程访问，必须使用强效认证。		
	3.9	账号异常活动	用户一旦发现其账号有异常活动，必须立即修改密码，并通知信息安全部进行侦查。		
	3.10	显示登陆警告标语	在登陆前，建议展示关于进入系统所注意的事项及安全要求。		
	3.11	登陆展示	登陆成功后，系统必须显示上次成功登陆的时间以及自上次成功登陆以来失败登陆的次数。		
	3.12	禁止密码显示及记录	多次性密码必不能以明文显示、记录及存储		
	3.13	登陆日志记录	系统必须记录所有的系统登录信息，包括成功和失败的登录。		
	3.14	登录失败显示	登录失败时，系统必不能提示登录原始失败原因。如因为账号不存在或者密码错误的登录失败，皆只显示“登录认证错误”		
	3.15	登陆尝试控制	当连续5次登录系统失败后，账号必须锁定，如系统支持，当账号登录失败而被锁定时，建议用户与系统间的连线被自动断开		
	3.16	登录时效	如系统支持，必须开启空闲超时控制配置，空闲时间超过30分钟，连接必须注销用户登录及/或自动断开连接，用户必须重新登录系统再进行访问。 如系统没有空闲超时控制，必须有其他层面操作系统（如WINDOWS的屏幕保护程序)来辅助此系统功能		

授权	4.1	授权模型	所有的应用系统访问控制建议基于角色访问控制（Role-Based Access Control，RB	（RBAC标准和独立模型文档：http://csrc.nist.gov/groups/SNS/rbac/）	
	4.2	授权原则	1）权限应以角色的形式授予帐号，各角色的权限必须根据角色的职能授予。 2）系统的每个功能必须实现权限控制，每个行动可以分开个别授权，如信息资产的读、写、修改、删除、执行等行动可分别授予。 3）所有权限必须按照“知悉需要”的原则进行授权。 4）信息访问的授权必须遵循“权限最小化”原则，只开通必要的权限。 5）信息访问的授权必须遵循职责分离原则，必须不能存在不相容权限。 6）重要的信息系统的授权，必须设置复核功能。复核功能必须对所有复核的数据只能读取，不能更改。 7）为保证复核人员的独立性，系统复核功能必须确保输入、复核过程必须不能以同一帐号实施。	3）信息科技风险管理-风险防范措施-第17条 4）等保-主机安全-访问控制、信息科技风险管理-风险防范措施-第17条 5）信息科技风险管理-运行管理-第41条 6）证监会-信息技术基础设施-系统功能 7）证监会-信息技术人员-岗位设定	应建立角色权限控制功能，以实现职责分离规则的输入。
	4.3	访问策略	所有存有保密（内部、敏感、机密）信息的系统必须为信息资产设置访问控制策略。访问策略中应清晰定义每个或每组用户的访问控制规则和可以拥有的权限。	保监会-网络安全-访问控制 银监会-信息安全-认证安全	
	4.4	认证控制	所有存储保密信息的信息系统必须有认证控制，保护信息资产，使信息在未获得授权下，意外或刻意的被使用、发放、篡改或删除。	银监会-信息安全-认证安全	
	4.5	授权流程	1）授权请求必须基于合理的工作目的，并经过主管及信息拥有人的确认，所申请的权限必须与申请人的职权相对应。 2）帐号管理人必须核实帐号、权限申请，访客授予权限，核实信息包括但不限于申请人身份、批核人身份、申请人职责与权限申请相应性，申请权限与现有权限不能存在冲突。 3）当人员持有的帐号、权限不适用（如调岗、离司）时，其的直属主管或部门权限管理员必须立即通知帐号、权限管理部门，回收、取消相关帐号、权限。 4）当系统功能发生变更或下线，对应的授权必须进行变更或删除。		
	4.6	特权帐号	1）特权帐号是指在系统中拥有极大、访问资源广泛或有敏感控制性权限的强力帐号，这包括系统及帐号、权限管理员的帐号。 2）特权帐号权限必须限制于管理职权所需；特权帐号应评估双因素认证的可行性，在可能范围内必须实施。		
职责分离	5.1	职责分离基本原则	1）职责分离是不容许任何人员单独一个人进行整个业务的交易或操作程序，即由启动至完成的工序只由一个人控制。 2）职责分离是通过对公司内部进行合理的岗位划分和职责分配以防止对公司信息和信息系统进行恶意破坏、篡改，进行虚假交易的安全控制措施。 3）职责分离可以通过岗位分离、权限分离、操作分离等方式实现。		
	5.2	清晰的岗位职责	职责分离的前提是每个岗位都必须有明确的岗位职责说明。		要求系统能够提供帐号对应的部门岗位、角色、权限的定义描述。
	5.3	审批与执行的职责分离	审批及执行的职责及责任必须分由不同人员承担，审批及执行级别必须对应其人员职能。		
	5.4	双重控制	敏感及重要的工序、交易由一人执行时，必须由另一独立人员负责监控、核实，减少信息在未获授权下更改及被滥用的机会。 敏感及重要工序、交易亦可分拆并由两个或以上人员分别执行。		
	5.5	职责分离的权限	必须进行职责分离的权限包括但不限于： 录入与核实/申请与审批/申请与操作/操作与审计/账号、权限管理与其审批/账号、权限管理与系统应用/账号、权限管理与其审查		
	5.6	系统环境	开发、测试、及生产系统、设备及环境必须完全独立及分离。开发、测试人员禁止在生产环境拥有大于查询的权限。		
	5.7	网络、操作系统管理	网络配置、操作系统管理职责必须与生产运营职责分离。		
	5.8	操作系统管理	网络管理、操作系统管理及数据库管理必须实施职责分离。		

日志	6.1	监控范围	对系统行为的日志记录应考虑但不限于： 1）登入成功及失败 2）重要的业务及财务操作 3）系统报警和故障 4）信息系统配置信息变更和变更尝试 5）安全违规事件 6）特权操作 特权账号的使用，例如：超级账号、管理员账号、授权账号等 系统启动和终止 系统服务的启动和终止 系统时间的修改 账号的添加和删除 账号权限的修改 输入/输出设备加载和卸载		
	6.2	日志信息	日志类型包括但不限于： 应用系统日志 操作系统日志 数据库日志 服务器日志 网络日志 安全防护系统日志 日志必须记录以下信息; 用户ID 日期、时间（至少精确到秒） 终端身份和位置（IP或MAC） 主要标识（如客户号码、合同号码） 行动记录（事前及事后的数据转变）		
	6.3	日志防篡改	禁止非授权用户访问日志设备和日志信息 禁止编辑或删除日志文件 任何对日志文件的访问（如读、写、删除）尝试都必须被记录。		
	6.4	日志保存	日志的保存，必须按照法律、监管要求，如无特别声明，日志必须至少保存1年。		1.根据《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》规定，客户资料、客户交易记录，需至少保存5年。 2.根据《企业年金基金管理运作流程》要求，企业年金相关档案需保存至少15年。 3.其他资料的保存，如无规定，应保存至少1年。
	6.5	日志容量	系统上必须分配足够的空间保存日志，必须定期对日志进行备份和归档，防止因存储空间不足而导致的日志信息记录不完整。		
	6.6	日志启用	必须确保系统启用了日志功能； 必须确保日志记录功能在任何时候都能正常运行； 未经许可，严禁任何人停止或终端日志记录；		
	6.7	时钟同步	所有重要的信息处理设备的时钟必须使用公司标准的时钟源。对于不能进行时钟同步的信息处理设备，必须每月检查一次以保证时钟同步，此类系统时钟偏差禁止超过一分钟。		