ICS 03.060
A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0072—2012

金融行业信息系统信息安全等级保护测评指南

Testing and evaluation guide for classified protection of information system of financial industry

2012-07-06 发布　　2012-07-06 实施

中国人民银行 发布

目　　次

前　言

本标准是“金融行业信息系统等级保护”系列标准中的第二项标准。该系列标准的结构及名称如下：

金融行业信息系统信息安全等级保护实施指引

金融行业信息系统信息安全等级保护测评指南

金融行业信息安全等级保护测评服务安全指引

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会归口。

本标准负责起草单位：中国人民银行科技司。

本标准参加起草单位：中国金融电子化公司。

本标准主要起草人：王永红、王小青、张永福、王晓燕、王海涛、杨剑、白智勇、沈力克、徐明、许自强、仇宁宁、李凡、郑凯一、陈广辉、赵义斌、杨英、周庆斌。

本标准为首次发布。

引　言

金融行业重要的信息系统关系到国计民生，是国家信息安全重点保护对象，国家信息安全监管职能部门需要对其重要信息和信息系统的信息安全保护工作进行指导监督。

信息安全等级保护是国家在信息安全保障工作的一项基本制度，金融行业作为重要信息系统行业部门之一，应遵照实施该制度。围绕金融信息安全等级保护工作的开展，需要一系列适合金融行业的等级保护标准体系作为支撑，以规范和指导金融等级保护工作的实施。为此，人民银行科技司组织安全等级保护领域专家和相关技术人员，根据国家关于信息安全等级保护工作的相关制度和标准，制定符合金融行业特点的、切实可行的信息安全等级保护行业标准和实施指南。

在本标准文本中，标记为F类的黑体字是根据金融行业业务特点新增的安全要求，没有标记为F类的黑体字是对《信息系统安全等级保护基本要求》（GB/T 22239-2008）要求项进行增强的要求。

金融行业信息系统信息安全等级保护测评指南

1 范围

本标准规定了金融行业对信息系统安全等级保护测评评估的要求，包括对第二级信息系统、第三级信息系统和第四级信息系统进行安全测评评估的单元测评要求和信息系统整体测评要求等。根据金融行业信息系统的定级情况，不存在五级系统，而一级系统不需去公安机关备案，不作为测评重点。本标准略去对第一级信息系统和第五级信息系统进行单元测评的具体内容要求。

本标准适用于行业进行自测评（如第二级信息系统）、信息安全测评服务机构（如第三和第四级信息系统）对信息系统安全等级保护状况进行的安全测评评估。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 22239-2008　信息系统安全等级保护基本要求

JR/T 0003-2001　银行卡联网联合安全规范

JR/T 0013-2004　金融业星型网间互联安全规范

JR/T 0011-2004　银行集中式数据中心规范

JR/T 0023-2004　证券公司信息技术管理规范

JR/T 0026-2006　银行业计算机信息系统雷电防护技术规范

JR/T 0044-2008　银行业信息系统灾难恢复管理规范

JR/T 0055.4-2009　银行联网联合技术规范第4部分：数据安全传输控制

银发〔2002〕260号　中国人民银行关于加强银行数据集中安全工作的指导意见

银科技〔2006〕73号　中国人民银行信息系统安全配置指引

银办发〔2006〕154号　中国人民银行IT应急预案指引

银办发〔2006〕9号　中国人民银行计算机机房规范化工作指引

银发〔2010〕276号　中国人民银行计算机系统信息安全管理规定

银发〔2010〕276号　中国人民银行计算机系统信息安全管理规定

银监发〔2008〕50号　银行业金融机构重要信息系统投产及变更管理办法

银监会〔2009〕19号　商业银行信息科技风险管理指引

银监办发〔2009〕437号　银行、证券跨行业信息系统突发事件应急处置工作指引

银监办发〔2010〕112号　商业银行数据中心监管指引

中证协发〔2006〕　证券公司集中交易安全管理技术指引

中期协发〔2009〕　期货公司网上期货信息系统技术指引

中证协发〔2009〕154号　证券营业部信息技术指引

保监会令〔2003〕3号　保险业重大突发事件应急处理规定

3 概述

3.1 测评内容

信息系统安全等级保护状况测评评估，应包括两个方面的内容：一是安全控制测评，主要测评信息安全等级保护要求的基本安全控制在信息系统中的实施配置情况；二是系统整体测评，主要测评分析信息系统的整体安全性。其中，安全控制测评是信息系统整体安全测评的基础。

对安全控制测评的描述，使用工作单元方式组织。工作单元分为安全技术测评和安全管理测评两大类。安全技术测评包括：物理安全、网络安全、主机系统安全、应用安全和数据安全等五个层面上的安全控制测评；安全管理测评包括：安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理五个方面的安全控制测评。

系统整体测评涉及到信息系统的整体拓扑、局部结构，也关系到信息系统的具体安全功能实现和安全控制配置，与特定信息系统的实际情况紧密相关，内容复杂且充满系统个性。因此，全面地给出系统整体测评要求的完整内容、具体实施方法和明确的结果判定方法是很困难的。测评人员应根据特定信息系统的具体情况，结合本标准要求，确定系统整体测评的具体内容，在安全控制测评的基础上，重点考虑安全控制间、层面间以及区域间的相互关联关系，测评安全控制间、层面间和区域间是否存在安全功能上的增强、补充和削弱作用以及信息系统整体结构安全性、不同信息系统之间整体安全性等。

3.2 测评对象

测评对象是测评实施过程中涉及到的信息系统的构成成分，是客观存在的人员、文档、机制或者设备等。测评对象是根据该工作单元中的测评项要求提出的，与测评项的要求相适应。一般来说，实施测评时，面临的具体测评对象可以是单个人员、文档、机制或者设备等，也可能是由多个人员、文档、机制或者设备等构成的集合，它们分别需要使用到某个特定安全控制的功能。

3.3 测评指标

GB/T 22239-2008 中对不同等级信息系统的安全功能和措施提出了具体要求，等级测评应根据信息系统的定级情况选取相应的通用指标类（G），业务信息安全性指标类（S）、业务服务保证类（A）安全测评指标，并依据《信息安全技术 信息系统安全等级保护测评要求》和《信息安全技术 信息系统安全等级测评过程指南》对信息系统实施安全测评。

3.4 测评方法

3.4.1 现场测评方法

安全测评现场工作一般采用访谈、检查和测评等三类方法。

1) 访谈是测评人员通过与信息系统有关人员进行交流、讨论等活动以获取证据的一种方法；访谈使用到的工具主要是访谈列表。测评人员针对访谈列表上的问题，逐项与信息系统有关人员进行交流、讨论，根据被访谈人员的回答了解和确认信息系统的安全保护情况；
2) 检查是测评人员通过对测评对象进行观察、查验、分析等活动以获取证据的一种方法；检查使用到的工具主要是核查列表。测评人员针对核查列表上的问题，通过观察、查验、分析等活动，逐项核实。根据检查对象的不同，检查可以进一步分为文档审查、现场观测和配置核查等方式；
3) 测评是指测评人员对测评对象按照预定的方法/工具使其产生特定的响应等活动，然后通过查看、分析响应输出结果来获取证据的一种方法。

依据工具和实施过程的不同，测评可以进一步细分为信息获取、漏洞扫描、渗透测评、密码分析等方式。

1) 信息获取是指获取存活主机/设备的名称、IP 地址、操作系统、开放的服务端口以及特定的数据包等信息内容；
2) 漏洞扫描是指利用漏洞扫描设备对目标设备进行自动探测，发现这些主机/设备上各个对网络开放端口上存在的错误配置和已知安全漏洞；
3) 渗透测评是模拟黑客可能利用的攻击技术试图侵入信息系统获取信息资源的一种手段，通过渗透测试更加直观、有效地评估信息系统的安全状况。

从不同接入点对信息系统进行漏洞扫描和渗透测评，可以反映出信息系统在不同角度、不同视野下

的安全状况。

3.4.2 风险分析方法

风险分析过程包括：

1) 判断信息系统安全保护能力缺失（测评结果中的部分符合项和不符合项）被威胁利用导致安全事件发生的可能性，可能性的取值范围为高、中和低；
2) 判断安全事件对信息系统业务信息安全和系统服务安全造成的影响程度，影响程度取值范围为高、中和低；
3) 综合前两项的结果对信息系统面临的风险进行汇总和分等级，风险等级的取值范围为高、中和低；
4) 结合信息系统的安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的风险。

3.5 等级测评风险

在等级测评实施过程中，被测系统可能面临以下风险。

3.5.1 验证测评影响系统正常运行

在现场测评时，需要对设备和系统进行一定的验证测评工作，部分测评内容需要上机查看一些信息，这就可能对系统的运行造成一定的影响，甚至存在误操作的可能。

3.5.2 工具测评影响系统正常运行

在现场测评时，会使用一些技术测评工具进行漏洞扫描测评、性能测评甚至抗渗透能力测评。测评可能会对系统的负载造成一定的影响，漏洞扫描测评和渗透测评可能对服务器和网络通讯造成一定影响甚至可能出现服务器宕机、网络严重堵塞的情况。

3.5.3 敏感信息泄漏

泄漏被测系统状态信息，如网络拓扑、IP 地址、业务流程、安全机制、安全隐患和有关文档信息。

4 等级测评过程

4.1 测评准备活动

本活动是开展等级测评工作的前提和基础，是整个等级测评过程有效性的保证。测评准备工作是否充分直接关系到后续工作能否顺利开展。本活动的主要任务是掌握被测系统的详细情况，准备测评工具，为编制测评方案做好准备。

4.2 方案编制活动

本活动是开展等级测评工作的关键活动，为现场测评提供最基本的文档和指导方案。本活动的主要任务是确定与被测信息系统相适应的测评对象、测评指标及测评内容等，并根据需要重用或开发测评指导书测评指导书，形成测评方案。

4.3 现场测评活动

本活动是开展等级测评工作的核心活动。本活动的主要任务是按照测评方案的总体要求，严格执行测评指导书，分步实施所有测评项目，包括单元测评和整体测评两个方面，以了解系统的真实保护情况，获取足够证据，发现系统存在的安全问题。

4.4 分析与报告编制活动

本活动是给出等级测评工作结果的活动，是总结被测系统整体安全保护能力的综合评价活动。本活动的主要任务是根据现场测评结果等相关要求，通过单项测评结果判定、单元测评结果判定、整体测评和风险分析等方法，找出整个系统的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距导致被测系统面临的风险，从而给出等级测评结论，形成测评报告文本。

5 测评准备

5.1 项目启动

在项目启动任务中，应先组建等级测评项目组，从基本资料、人员、计划安排等方面为整个等级测评项目的实施作基本准备。

输入：委托测评协议书。

任务描述：

组建测评项目组，从人员方面做好准备，并编制项目计划书。项目计划书应包含项目概述、工作依据、技术思路、工作内容和项目组织等。

应交流项目相关主要资料，包括：被测系统总体描述文件，详细描述文件，安全保护等级定级报告，系统验收报告，安全总体方案，自查或上次等级测评报告（如果有），被测评单位的信息化建设状况与发展以及联络方式等。

输出/产品：项目计划书。

5.2 信息收集和分析

1) 收集等级测评需要的各种资料，包括测评委托单位的各种方针文件、规章制度及相关过程管理记录、被测系统总体描述文件、详细描述文件、安全保护等级定级报告、安全总体方案、安全现状评价报告、安全详细设计方案、用户指南、运行步骤、网络图表、配置管理文档等；
2) 将调查表格(具体可以参考公安部等级保护测评报告模板)提交给测评委托单位，督促被测系统相关人员准确填写调查表格；
3) 收回填写完成的调查表格，并分析调查结果，了解和熟悉被测系统的实际情况。分析的内容包括被测系统的基本信息、物理位置、行业特征、管理框架、管理策略、网络及设备部署、软硬件重要性及部署情况、范围及边界、业务种类及重要性、业务流程、业务数据及重要性、业务安全保护等级、用户范围、用户类型、被测系统所处的运行环境及面临的威胁等。这些信息可以重用自查或上次等级测评报告中的可信结果；
4) 如果调查表格填写不准确或不完善或存在相互矛盾的地方较多，测评机构应安排现场调查，与被测系统相关人员进行面对面的沟通和了解。

5.3 工具和表单准备

1) 测评人员调试本次测评过程中将用到的测评工具，包括漏洞扫描工具、渗透性测评工具、性能测评工具和协议分析工具等；
2) 测评人员模拟被测系统搭建测评环境(当要对一些重要的上线系统进行安全测试时，为了测试时不会影响系统的运行，可以搭建模拟环境进行测试)；
3) 准备和打印表单，主要包括：现场测评授权书、文档交接单、会议记录表单、会议签到表单等。

6 测评方案

6.1 测评对象确定

测评对象种类的选择需要在基本覆盖和数量上进行抽样，重点抽查主要的设备、设施、人员和文档等。可以抽查的测评对象种类主要考虑以下几个方面：

a) 主机房（包括其环境、设备和设施等）和部分辅机房，应将放置了服务于信息系统的局部（包括整体）或对信息系统的局部（包括整体）安全性起重要作用的设备、设施的辅机房选取作为测评对象；
b) 存储被测系统重要数据的介质的存放环境；
c) 办公场地；
d) 整个系统的网络拓扑结构；
e) 安全设备，包括防火墙、入侵检测设备和防病毒网关等；
f) 边界网络设备（可能会包含安全设备），包括路由器、防火墙、认证网关和边界接入设备（如楼层交换机）等；

g) 对整个信息系统或其局部的安全性起作用的网络互联设备，如核心交换机、汇聚层交换机、路由器等；
h) 承载被测系统主要业务或数据的服务器（包括其操作系统和数据库）；
i) 管理终端和主要业务应用系统终端；
j) 能够完成被测系统不同业务使命的业务应用系统；
k) 业务备份系统；
l) 信息安全主管人员、各方面的负责人员、具体负责安全管理的当事人、业务负责人；
m) 涉及到信息系统安全的所有管理制度和记录。

信息系统中配置相同的安全设备、边界网络设备、网络互联设备、服务器、终端以及备份设备，每类应至少抽查两台作为测评对象。

6.2 测评指标确定

主要是针对金融行业第二、第三、第四级系统的安全测评。其指标应包括《信息系统安全等级保护基本要求》中的通用指标类（G），业务信息安全性指标类（S）、业务服务保证类（A）和金融行业增强安全保护类（F）。F 类要求作为金融行业的增强性安全要求分布在 S、A、G 类的要求中。根据信息系统定级确定的业务服务保证类（A）、业务信息安全性指标类（S）和通用指标类（G）的级别确定测评指标。

第二、第三、第四级信息系统安全控制指标类型分别具体如表 1、表 2、表 3 所示：

6.2.1 第二级信息系统安全控制指标类型：

表 1 二级系统测评指标

测评指标					
技术/管理	安全分类	安全子类数量			
		S (2 级)	A (2 级)	G (2 级)	小计
安全技术	物理安全	1	1	8	10
	网络安全	1	—	5	6
	主机安全	2	1	3	6
	应用安全	4	2	1	7
	数据安全及备份恢复	2	1	—	3
安全管理	安全管理制度	—	—	5	5
	安全管理机构	—	—	3	3
	人员安全管理	—	—	5	5
	系统建设管理	—	—	9	9
	系统运维管理	—	—	12	12
合　　计					66

6.2.2 第三级信息系统安全控制指标类型：

表2 三级系统测评指标

测评指标					
技术/管理	安全分类	安全子类数量			
		S (3 级)	A (3 级)	G (3 级)	小计
安全技术	物理安全	1	1	8	10
	网络安全	1	—	6	7
	主机安全	3	1	3	7

	应用安全	5	2	2	9
	数据安全及备份恢复	2	1	—	3
安全管理	安全管理制度	—	—	5	5
	安全管理机构	—	—	3	3
	人员安全管理	—	—	5	5
	系统建设管理	—	—	11	11
	系统运维管理	—	—	13	13
合　　计					73

6.2.3 第四级信息系统安全控制指标类型：

表3 四级系统测评指标

测评指标					
技术/管理	安全分类	安全子类数量			
		S （4级）	A （4级）	G （4级）	小计
安全技术	物理安全	1	1	8	10
	网络安全	1	—	6	7
	主机安全	5	1	3	9
	应用安全	6	2	3	11
	数据安全及备份恢复	2	1	—	3
安全管理	安全管理制度	—	—	5	5
	安全管理机构	—	—	3	3
	人员安全管理	—	—	5	5
	系统建设管理	—	—	11	11
	系统运维管理	—	—	13	13
合　　计					77

6.3 测评工具接入点确认

信息系统应进行工具测评，工具测评可能用到漏洞扫描器、渗透测评工具集、协议分析仪等测评工具。

1) 确定需要进行工具测评的测评对象；
2) 选择测评路径。一般来说，测评工具的接入采取从外到内，从其他网络到本地网段的逐步逐点接入，即：测评工具从被测系统边界外接入、在被测系统内部与测评对象不同网段及同一网段内接入等几种方式；
3) 根据测评路径，确定测评工具的接入点；
4) 从被测系统边界外接入时，测评工具一般接在系统边界设备（通常为交换设备）上。在该点接入漏洞扫描器，扫描探测被测系统的主机、网络设备对外暴露的安全漏洞情况；
5) 从系统内部与测评对象不同网段接入时，测评工具一般接在与被测对象不在同一网段的内部核心交换设备上；
6) 在系统内部与测评对象同一网段内接入时，测评工具一般接在与被测对象在同一网段的交换设备上；
7) 结合网络拓扑图，采用图示的方式描述测评工具的接入点、测评目的、测评途径和测评对象等相关内容。

6.4 单元测评内容确定

把测评指标和测评方式结合到信息系统的具体测评对象上，就构成了可以具体测评的工作单元。具

体分为技术安全和管理安全，其中技术安全包括物理安全、网络安全、主机系统安全、应用安全、数据安全及备份恢复；安全管理包括安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理共 10 个方面。

6.5 测评方案编制

1) 根据委托测评协议书和填好的调研表格，提取项目来源、测评委托单位整体信息化建设情况及被测系统与单位其他系统之间的连接情况等；
2) 根据等级保护过程中的等级测评实施要求，将测评活动所依据的标准罗列出来；
3) 依据委托测评协议书和被测系统情况，估算现场测评工作量。工作量可以根据配置检查的节点数量和工具测评的接入点及测评内容等情况进行估算；
4) 根据测评项目组成员安排，编制工作安排情况；
5) 根据以往测评经验以及被测系统规模，编制具体测评计划，包括现场工作人员的分工和时间安排。在进行时间计划安排时，应尽量避开被测系统的业务高峰期，避免给被测系统带来影响。同时，在测评计划中应将具体测评所需条件以及测评需要的配合人员也一并给出，便于测评实施之前双方沟通协调、合理安排；
6) 汇总上述内容及方案编制活动的其他任务获取的内容形成测评方案文稿；
7) 评审和提交测评方案。测评方案初稿应通过测评项目组全体成员评审，修改完成后形成提交稿。然后，测评机构将测评方案提交给测评委托单位签字认可。

7 现场测评

7.1 单元测评

7.1.1 第二级信息系统单元测评

7.1.1.1 安全技术测评

7.1.1.1.1 物理安全

1) 物理位置的选择（G2）

测评项

a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内，**应选择交通、通信便捷地区**。

测评方式

访谈、检查。

测评对象

物理安全负责人，机房，办公场地，机房场地设计/验收文档。

测评实施

a) 应访谈物理安全负责人，询问现有机房和办公场地（放置终端计算机设备）的环境条件是否能够满足信息系统业务需求和安全管理需求，是否具有基本的防震、防风和防雨等能力；

b) 应检查机房和办公场地的设计/验收文档，是否有机房和办公场地所在建筑能够具有防震、防风和防雨等能力的说明；

c) 应检查机房和办公场地是否在具有防震、防风和防雨等能力的建筑内。

结果判定

a) 针对测评实施中的a）～c）均为肯定，则信息系统符合本单元测评项要求。

2) 物理访问控制（G2）

测评项

a) 机房出入口应能控制、鉴别和记录进入的人员；

b) 需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围；

c) **应对机房划分区域进行管理，如将机房划分为生产区、辅助区，其中生产区是指放置一般业务系统服务器、客户端（工作站）等设备的运行区域，辅助区是指放置供电、消防、空调等设备的区域。（F2）**

测评方式

访谈，检查。

测评对象

物理安全负责人，机房值守人员，机房，机房安全管理制度，值守记录，进入机房的登记记录，来访人员进入机房的审批记录。

测评实施

a) 应访谈物理安全负责人，了解具有哪些控制机房进出的能力；
b) 应访谈机房值守人员，询问是否认真执行有关机房出入的管理制度，是否对进入机房的人员记录在案；
c) 应检查机房安全管理制度，查看是否有关于机房出入方面的规定；
d) 应检查机房出入口是否有专人值守，是否有值守记录，以及进出机房的人员登记记录；检查机房是否不存在专人值守之外的出入口；
e) 应检查机房，是否有进入机房的人员身份鉴别措施，如戴有可见的身份辨识标识；
f) 应检查是否有来访人员进入机房的审批记录。

结果判定

a) 测评实施中 a）至少应包括制订了机房出入的管理制度，指定了专人在机房出入口值守，对进入的人员登记在案并进行身份鉴别，对来访人员须经批准、限制和监控其活动范围，则该项为肯定；
b) 测评实施中c）至少应包括制订了机房出入的管理制度，指定了专人在机房出入口值守，对进入的人员登记在案并进行身份鉴别，对来访人员须经批准、限制和监控其活动范围，则该项为肯定；
c) 测评实施中a）～f）均为肯定，则信息系统符合本单元测评项要求。

3) 防盗窃和防破坏（G2）

测评项

a) 应将主要设备放置在机房内；
b) 应将设备或主要部件进行固定，并设置明显的不易除去的标记；
c) 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；
d) 应对介质分类标识，存储在介质库或档案室中；
e) 主机房应安装必要的防盗报警设施；
f) **应建立机房设施与场地环境监控系统，对机房空调、消防、不间断电源（UPS）、供配电、门禁系统等重要设施实行全面监控。（F2）**

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，资产管理员，机房设施，设备管理制度文档，通信线路布线文档，报警设施的安装测评/验收报告。

测评实施

a) 应访谈物理安全负责人，采取了哪些防止设备、介质等丢失的保护措施；
b) 应访谈机房维护人员，询问主要设备放置位置是否做到安全可控,设备或主要部件是否进行了固定和标记,通信线缆是否铺设在隐蔽处;是否对机房安装的防盗报警设施进行定期维护检查；
c) 应访谈资产管理员，在介质管理中，是否进行了分类标识，是否存放在介质库或档案室中；

d) 应检查主要设备是否放置在机房内或其它不易被盗窃和破坏的可控范围内;检查主要设备或设备的主要部件的固定情况，是否不易被移动或被搬走，是否设置明显的无法除去的标记;
e) 应检查通信线缆铺设是否在隐蔽处（如铺设在地下或管道中等）;
f) 应检查机房防盗报警设施是否正常运行，并查看运行和报警记录;
g) 应检查介质的管理情况，查看介质是否有正确的分类标识，是否存放在介质库或档案室中;
h) 应检查是否有设备管理制度文档，通信线路布线文档，介质管理制度文档，介质清单和使用记录，机房防盗报警设施的安装测评/验收报告。

结果判定

a) 测评实施中a）至少应该包括制订了设备管理制度，主要设备放置位置做到安全可控,设备或主要部件进行了固定和标记，通信线缆铺设在隐蔽处，介质分类标识并存储在介质库或档案室，机房安装了防止进入盗窃和破坏的防盗报警设施，则该项为肯定;
b) 测评实施中a）～h）均为肯定，则信息系统符合本单元测评项要求。

4) 防雷击（G2）

测评项

a) 机房建筑应设置避雷装置;
b) 机房应设置交流电源地线。

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房设施（避雷装置，交流电源地线），建筑防雷设计/验收文档。

测评实施

a) 应访谈物理安全负责人，询问为防止雷击事件导致重要设备被破坏采取了哪些防护措施，机房建筑是否设置了避雷装置，是否通过验收或国家有关部门的技术检测;询问机房计算机供电系统是否有交流电源地线;
b) 应访谈机房维护人员，询问机房建筑避雷装置是否有人定期进行检查和维护;询问机房计算机系统接地（交流工作接地、安全保护接地、防雷接地）是否符合GB50174－2008《电子计算机机房设计规范》的要求;
c) 应检查机房是否有建筑防雷设计/验收文档，查看是否有地线连接要求的描述。

结果判定

a) 测评实施中a）至少应包括符合GB 50057－1994《建筑物防雷设计规范》（GB157《建筑防雷设计规范》）中的计算机机房防雷要求，如果在雷电频繁区域，装设浪涌电压吸收装置等，则该项为肯定;
b) 测评实施中b）要求地线的引线应和大楼的钢筋网及各种金属管道绝缘，交流工作接地的接地电阻不应大于4Ω，安全保护地的接地电阻不应大于4Ω;防雷保护地（处在有防雷设施的建筑群中可不设此地）的接地电阻不应大于10Ω的要求，则该项为肯定;
c) 测评实施中a）～c）均为肯定，则信息系统符合本单元测评项要求。

5) 防火（G2）

测评项

a) **机房应设置对计算机设备影响小的气体灭火设备和火灾自动报警系统;**
b) **机房内部通道设置、装饰材料、设备线缆等应满足消防要求，并通过消防验收。（F2）**

测评方式

访谈，检查。

测评对象

物理安全负责人，机房值守人员，机房设施，机房安全管理制度，机房防火设计/验收文档，火灾自动报警系统设计/验收文档。

测评实施

a) 应访谈物理安全负责人，询问机房是否设置了灭火设备，是否设置了火灾自动报警系统,是否有人负责维护该系统的运行，是否制订了有关机房消防的管理制度和消防预案，是否进行了消防培训；

b) 应访谈机房值守人员，询问对机房出现的消防安全隐患是否能够及时报告并得到排除；是否参加过机房灭火设备的使用培训，是否能够正确使用灭火设备和火灾自动报警系统；

c) 应检查机房是否设置了灭火设备，摆放位置是否合理，有效期是否合格；应检查机房火灾自动报警系统是否正常工作，查看是否有运行记录、报警记录、定期检查和维修记录；

d) 应检查是否有有关机房消防的管理制度文档，机房防火设计/验收文档，火灾自动报警系统的设计/验收文档。

结果判定：

a) 测评实施中a）～d）均为肯定，则信息系统符合本单元测评项要求。

6) 防水和防潮（G2）

测评项

a) **水管不宜穿过机房屋顶，但若有穿过地板应当采取保护防范措施；**

b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

c) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房设施（上下水装置，除湿装置），建筑防水和防潮设计/验收文档。

测评实施

a) 应访谈物理安全负责人，询问机房建设是否有防水防潮措施；如果机房内有上下水管安装，是否穿过屋顶和活动地板下，穿过墙壁和楼板的水管是否采取了可靠的保护措施；在湿度较高地区或季节是否有人负责机房防水防潮事宜，配备除湿装置；

b) 应访谈机房维护人员，询问机房是否出现过漏水和返潮事件；如果机房内有上下水管安装，是否经常检查是否有漏水情况；在湿度较高地区或季节是否有人负责机房防水防潮事宜，使用除湿装置除湿；如果出现机房水蒸气结露和地下积水的转移与渗透现象是否及时采取防范措施；

c) 应检查机房是否有建筑防水和防潮设计/验收文档，是否能够满足机房防水和防潮的需求；

d) 如果有管道穿过主机房墙壁和楼板处，应检查是否置套管，管道与套管之间是否采取可靠的密封措施；

e) 应检查机房是否不存在屋顶和墙壁等出现过漏水、渗透和返潮现象，机房及其环境是否不存在明显的漏水和返潮的威胁；如果出现漏水、渗透和返潮是否能够及时修复解决；

f) 如果在湿度较高地区或季节，应检查机房是否有湿度记录，是否有除湿装置并能够正常运行，是否有防止出现机房地下积水的转移与渗透的措施，是否有防水防潮处理记录。

结果判定

a) 如果测评实施中d）、f）中“如果”条件不成立，则该项为不适用；

b) 测评实施中a）～f）均为肯定，则信息系统符合本单元测评项要求。

7) 防静电（G2）

测评项

a) 关键设备应采用必要的接地防静电措施。

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房设施，防静电设计/验收文档。

测评实施

a) 应访谈物理安全负责人，询问机房是否采用必要的接地防静电措施，是否有控制机房湿度的措施；

b) 应访谈机房维护人员，询问是否经常检查机房湿度，并控制在GB2887中的规定的范围内；询问机房是否存在静电问题或因静电引起的故障事件；

c) 应检查机房是否有防静电设计/验收文档；

d) 应检查机房是否有安全接地，查看机房的相对湿度是否符合GB2887中的规定，查看机房是否明显存在静电现象。

结果判定

a) 测评实施中a）～d）均为肯定，则信息系统符合本单元测评项要求。

8) 温湿度控制（G2）

测评项

a) 应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房设施，温湿度控制设计/验收文档，温湿度记录、运行记录和维护记录。

测评实施

a) 应访谈物理安全负责人，询问机房是否配备了温湿度自动调节设施，保证温湿度能够满足计算机设备运行的要求，是否在机房管理制度中规定了温湿度控制的要求，是否有人负责此项工作；

b) 应访谈机房维护人员，询问是否定期检查和维护机房的温湿度自动调节设施，询问是否出现过温湿度影响系统运行的事件；

c) 应检查机房是否有温湿度控制设计/验收文档；

d) 应检查温湿度自动调节设施是否能够正常运行，查看温湿度记录、运行记录和维护记录；查看机房温湿度是否满足GB 2887-89《计算站场地技术条件》的要求。

结果判定

a) 测评实施中a）～d）均为肯定，则信息系统符合本单元测评项要求。

9) 电力供应（A2）

测评项

a) 应在机房供电线路上配置稳压器和过电压防护设备；

b) 应提供短期的备用电力供应，**备用供电措施(如蓄电池、发电机等)能提供超过1小时的供电时间；**

c) **机房重要区域、重要设备应提供UPS单独供电。（F2）**

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房设施（供电线路，稳压器，过电压防护设备，短期备用电源设备），电力供应安全设计/验收文档，检查和维护记录。

测评实施

a) 应访谈物理安全负责人，询问计算机系统供电线路是否与其他供电分开；询问计算机系统供电线路上是否设置了稳压器和过电压防护设备；是否设置了短期备用电源设备（如UPS），供电时间是否满足系统最低电力供应需求；
b) 应访谈机房维护人员，询问是否对在计算机系统供电线路上的稳压器、过电压防护设备、短期备用电源设备等进行定期检查和维护；是否能够控制电源稳压范围满足计算机系统运行正常；
c) 应检查机房是否有电力供应安全设计/验收文档，查看文档中是否标明单独为计算机系统供电，配备稳压器、过电压防护设备以及短期备用电源设备等要求；
d) 应检查计算机供电线路，查看计算机系统供电是否与其他供电分开；
e) 应检查机房，查看计算机系统供电线路上的稳压器、过电压防护设备和短期备用电源设备是否正常运行；
f) 应检查是否有稳压器、过电压防护设备以及短期备用电源设备等电源设备的检查和维护记录。

结果判定

a) 测评实施中a）~f）均为肯定，则信息系统符合本单元测评项要求。

10) 电磁防护（S2）

测评项

a) 电源线和通信线缆应隔离铺设，避免互相干扰。

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房设施，电磁防护设计/验收文档。

测评实施

a) 应访谈物理安全负责人，询问是否有防止外界电磁干扰和设备寄生耦合干扰的措施（包括设备外壳有良好的接地、电源线和通信线缆隔离等）；
b) 应访谈机房维护人员，询问是否对设备外壳做了良好的接地；是否做到电源线和通信线缆隔离；是否出现过因外界电磁干扰等问题引发的故障；
c) 应检查机房是否有电磁防护设计/验收文档；
d) 应检查机房设备外壳是否有安全接地；
e) 应检查机房布线，查看是否做到电源线和通信线缆隔离。

结果判定

a) 测评实施中a）～e）均为肯定，则信息系统符合本单元测评项要求。

在内容上，物理安全测评实施过程涉及 10 个工作单元，具体检查表请参见附录 A.1.1.1。

7.1.1.1.2 网络安全

1) 结构安全（G2）

测评项

a) 应保证关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；
b) 应保证接入网络和核心网络的带宽满足业务高峰期需要；
c) 应绘制与当前运行情况相符的网络拓扑结构图；
d) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；**生产网、互联网、办公网之间都应实现有效隔离。**

测评方式

访谈，检查，测评。

测评对象

网络管理员，边界和重要网络设备，网络拓扑图，网络设计/验收文档。

测评实施

a) 可访谈网络管理员，询问信息系统中的边界和关键网络设备的性能以及目前业务高峰流量情况；
b) 可访谈网络管理员，询问网段划分情况以及划分的原则；询问重要的网段有哪些，对重要网段的保护措施有哪些；
c) 可访谈网络管理员，询问网络的带宽情况；询问网络中带宽控制情况以及带宽分配的原则；
d) 可访谈网络管理员，询问网络设备上的路由控制策略措施有哪些，这些策略设计的目的是什么；
e) 应检查网络拓扑图，查看与当前运行情况是否一致；
f) 应检查网络设计/验收文档，查看边界和重要网络设备带宽占用报表是否有达到或超过处理能力记录；
g) 应检查网络设计/验收文档，查看是否有根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网和网段分配地址段的设计或描述；
h) 应检查边界和重要网络设备，查看是否配置路由控制策略（如使用静态路由等）建立安全的访问路径，在业务终端trace 业务服务器地址，查看访问路径所经节点是否符合路由控制策略；
i) 应检查边界和重要网络设备，检查是否将重要网段部署至网络边界与外部信息系统直连，重要网段与其他网段间是否使用防火墙、访问控制等手段隔离；应测评网络拓扑结构，可通过网络拓扑结构自动发现、绘制工具，验证实际的网络拓扑结构和网络拓扑结构图是否一致；
j) 应测评业务终端与业务服务器之间的访问路径，可通过使用路由跟踪工具，验证业务终端与业务服务器之间的访问路径的是否安全（如访问路径是否固定等）；
k) 应测评重要网段，验证其采取的网络地址与数据链路地址绑定措施或数据链路层地址与交换机端口绑定的措施是否有效（如试图使用非绑定地址，查看是否能正常访问等）。

结果判定

a) 如果测评实施中 f）～g）中缺少相应的文档，则该项为否定；
b) 如果测评实施中e）～k）均为肯定，则信息系统符合本单元测评项要求。

2) 访问控制（G2）

测评项

a) 应在网络边界部署访问控制设备，启用访问控制功能；
b) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为网段级；
c) 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户；
d) 应限制具有拨号访问权限的用户数量。

测评方式

访谈，检查，测评。

测评对象

网络管理员，边界网络设备（包括网络安全设备）。

测评实施

a) 可访谈安全员，询问采取的网络访问控制措施有哪些；询问访问控制策略的设计原则是什么；询问网络访问控制设备具备的访问控制功能（如是基于状态的，还是基于包过滤等）；
b) 应检查边界网络设备，查看其是否根据会话状态信息（如包括数据包的源地址、目的地址、源端口号、目的端口号、协议、出入的接口、会话序列号、发出信息的主机名等信息，并应支持地址通配符的使用）对数据流进行控制；
c) 应测评边界网络设备，可通过试图访问未授权的资源，验证访问控制措施是否能对未授权的访问行为的控制（如可以使用扫描工具探测等）。

结果判定

a) 测评实施中 b）~c）均为肯定，则信息系统符合本单元测评项要求。

3) 安全审计（G2）

测评项

a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息，**保存时间不少于一个月。**

测评方式

访谈，检查，测评。

测评对象

审计员，边界和重要网络设备（包括安全设备）审计记录，审计策略。

测评实施

a) 可访谈审计员，询问是否对网络系统中的边界和重要网络设备进行审计，审计包括哪些项；询问审计记录的主要内容有哪些；询问对审计记录的处理方式；

b) 应检查日志服务器或AAA服务器的审计记录，查看是否有网络系统中的网络设备运行状况、网络流量、用户行为等事件的记录；

c) 应检查日志服务器或AAA服务器的事件审计策略，查看是否包括：事件的日期和时间、用户、事件类型、事件成功情况，及其他与审计相关的信息。

d) 应检查日志服务器或AAA服务器的事件审计记录是否包括：事件的日期和时间、用户、事件类型、事件成功情况，及其他与审计相关的信息（如产生相应的事件，观察审计的记录看是否对这些事件的准确记录）。

结果判定

a) 测评实施中 b）~d）均为肯定，则信息系统符合本单元测评项要求。

4) 边界完整性检查（S2）

测评项

a) 应能够对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查。

测评方式

访谈，检查，测评。

测评对象

网络管理员，边界完整性检查设备/工具，边界完整性检查工具运行日志。

测评实施

a) 应检查边界完整性检查设备，查看是否有未安装非法外联客户端的计算机接入网络，若有是否采取进行定位、阻断；

b) 应检查边界完整性检查工具运行日志，查看运行是否正常（查看是否持续对网络全网段进行监控）；

c) 应检查边界完整性检查设备/工具的配置，查看是否正确配置对网络的内部用户未通过准许私自联到外部网络的行为进行有效监控；

d) 应测评边界完整性检查工具，是否能有效的发现“非法外联”的行为(如产生非法外联的动作，查看边界完整性检查工具是否能够及时发现该行为）。

结果判定

a) 测评实施中 b）~d）均为肯定，则信息系统符合本单元测评项要求。

5) 入侵防范（G2）

测评项

a) 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等。

测评方式

访谈，检查，测评。

测评对象

安全员，网络入侵防范设备。

测评实施

a) 可访谈安全员，询问网络入侵防范措施有哪些；询问是否有专门的设备对网络入侵进行防范；询问采取什么方式进行网络入侵防范规则库升级；
b) 应检查网络入侵防范设备，查看是否能检测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击、网络蠕虫攻击等；
c) 应检查网络入侵防范设备，查看其生产厂商是否为正规厂商，规则库是否为最新；
d) 应测评网络入侵防范设备，验证其监控策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备的反应）。

结果判定

a) 测评实施中b）～d）均为肯定，则信息系统符合本单元测评项要求。

6) 网络设备防护（G2）

测评项

a) 应对登录网络设备的用户进行身份鉴别；
b) 应对网络设备的管理员登录地址进行限制；
c) 网络设备用户的标识应唯一；
d) 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；
e) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
f) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
g) **应每月对网络设备的配置文件进行备份，发生变动时应及时备份；（F2）**
h) **应定期对网络设备运行状况进行检查；（F2）**
i) **对网络设备系统自带的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端口开放审批制度；（F2）**
j) **应定期检验网络设备软件版本信息；（F2）**
k) **应建立网络设备的时钟同步机制；（F2）**
l) **应定期检查并锁定或撤销网络设备中不必要的用户账号。（F2）**

测评方式

访谈，检查，测评。

测评对象

网络管理员，边界和重要网络设备（包括安全设备）。

测评实施

a) 可访谈网络管理员，是否对网络设备进行AAA认证或其他认证方式，若有登录AAA服务器，查看用户与管理员身份、权限是否匹配；
b) 应访谈网络管理员，询问网络设备的口令策略是什么；
c) 应检查边界和重要网络设备上的安全设置，查看其是否有对鉴别失败采取相应的措施的设置；查看其是否有限制非法登录次数的功能；

d) 应检查边界和重要网络设备上的安全设置，查看是否对主要网络设备的管理员登录地址进行限制；查看是否设置网络登录连接超时，并自动退出；查看是否实现设备特权用户的权限分离；查看是否对网络上的对等实体进行身份鉴别；
e) 应测评边界和重要网络设备的安全设置，验证鉴别失败处理措施采用错误密码登录网络设备数次，观察是否结束会话、限制非法登录次数），对网络设备的管理员登录地址进行限制（如使用任意地址登录，观察网络设备的动作等）等功能是否有效；
f) 应测评边界和重要网络设备的安全设置，验证其网络登录连接超自动退出的设置是否有效（如长时间连接无任何操作，观察观察网络设备的动作等）；
g) 应远程登录网络设备，看是否采用22端口SSH方式或其他加密方式；
h) 应对边界和重要网络设备进行渗透测评，通过使用各种渗透测评技术（如口令猜解等）对网络设备进行渗透测评，验证网络设备防护能力是否符合要求。
i) 应查看检查记录，是否定期对网络设备运行状况进行检查；
j) 应测评网络设备，是否关闭不必要的网络设备服务；
k) 应访谈网络设备管理员，是否定期检验网络设备软件版本信息并有书面记录；
l) 应访谈网络设备管理员，是否定期检查并锁定或撤销网络设备中多余的用户账号。

结果判定

a) 如网络设备的口令策略为口令长度6位以上，口令复杂（如规定字符应混有大、小写字母、数字和特殊字符），口令生命周期，新旧口令的替换要求（规定替换的字符数量）或为了便于记忆使用了令牌则b）满足测评要求；
b) 测评实施中b）~f）均为肯定，则信息系统符合本单元测评项要求。
网络安全测评主要涉及对象为网络互联设备、网络安全设备和网络拓扑结果等三大类对象，具体为：
1)核心交换机、接入交换机、接入路由器和拨号接入路由器等网络互联设备；
2)入侵检查系统、防火墙等网络安全设备；
3)信息系统的整体网络拓扑结果。

在内容上，网络安全层面测评实施过程涉及 6 个工作单元，具体内容请参见附录 A.1.1.2。

7.1.1.1.3 主机安全

1) 身份鉴别（S2）

测评项

a) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；
b) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，**关键系统的静态口令应在6位以上并由字母、数字、符号等混合组成并定期更换；**
c) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
d) 当**通过互联网**对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；
e) 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。

测评方式

访谈，检查，测评。

测评对象

系统管理员，数据库管理员，重要服务器操作系统，重要数据库管理系统，服务器操作系统文档，数据库管理系统文档。

测评实施

a) 应检查服务器操作系统和数据库管理系统身份鉴别功能是否具有《信息安全等级保护操作系统安全技术要求》和《信息安全等级保护数据库管理系统安全技术要求》第二级以上或TCSEC C2级以上的测评报告；
b) 可访谈系统管理员，询问操作系统的身份标识与鉴别机制采取何种措施实现；
c) 可访谈数据库管理员，询问数据库的身份标识与鉴别机制采取何种措施实现；
d) 应检查服务器操作系统文档和数据库管理系统文档,查看用户身份标识的唯一性是由什么属性来保证的（如用户名或者UID等）；
e) 检查服务器操作系统和数据库的用户，以及隶属的组，或UID是否唯一。
f) 应检查重要服务器操作系统和重要数据库管理系统，查看是否提供了身份鉴别措施（如用户名和口令等），其身份鉴别信息是否具有不易被冒用的特点，检查账户密码策略设置，例如，口令足够长，口令复杂（如规定字符应混有大、小写字母、数字和特殊字符），更新周期短,或为了便于记忆使用了令牌；
g) 应检查重要服务器操作系统和重要数据库管理系统，查看是否已配置了鉴别失败处理功能，设置了非法登录次数的限制值；查看是否设置登录连接超时处理功能，如自动退出；
h) 应测评重要服务器操作系统和重要数据库管理系统，可通过错误的用户名和口令试图登录系统，验证鉴别失败处理功能是否有效；
i) 应测评重要服务器操作系统和重要数据库管理系统，当进入系统时，是否先需要进行标识（如建立账号），而没有进行标识的用户不能进入系统；
j) 应测评重要服务器操作系统和重要数据库管理系统，添加一个新用户，其用户标识为系统原用户的标识（如用户名或UID），查看是否不会成功。

结果判定

a) 如果测评实施中 a）为肯定，则测评实施h）和i）为肯定；
b) 测评实施中e）～i）均为肯定，则信息系统符合本单元测评项要求。

2) 访问控制（S2）

测评项

a) 应启用访问控制功能，依据安全策略控制用户对资源的访问；
b) 应实现操作系统和数据库系统特权用户的权限分离；
c) 应限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；
d) 应及时删除多余的、过期的帐户，避免共享帐户的存在。

测评方式

检查，测评。

测评对象

重要服务器操作系统，重要数据库管理系统，安全策略。

测评实施

a) 应检查服务器操作系统和数据库管理系统的自主访问控制功能是否具有《信息安全等级保护操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第二级以上或TCSEC C2级以上的测评报告；
b) 应检查服务器操作系统和数据库管理系统的安全策略，查看是否明确主体（如用户）以用户和/或用户组的身份规定对客体（如文件或系统设备,目录表和存取控制表访问控制等）的访问控制，覆盖范围是否包括与信息安全直接相关的主体（如用户）和客体（如文件，数据库表等）及它们之间的操作（如读、写或执行）；
c) 应检查服务器操作系统和数据库管理系统的安全策略，查看是否明确主体（如用户）具有非敏感标记（如角色），并能依据非敏感标记规定对客体的访问；

d) 应检查重要服务器操作系统和重要数据库管理系统的访问控制列表，查看授权用户中是否不存在过期的帐号和无用的帐号等；访问控制列表中的用户和权限，是否与安全策略相一致；
e) 应检查重要服务器操作系统和重要数据库管理系统，查看客体（如文件，数据库表、视图、存储过程和触发器等）的所有者是否可以改变其相应访问控制列表的属性，得到授权的用户是否可以改变相应客体访问控制列表的属性；
f) 应查看重要服务器操作系统和重要数据库管理系统，查看匿名/默认用户的访问权限是否已被禁用或者严格限制（如限定在有限的范围内）；
g) 应测评重要服务器操作系统和重要数据库管理系统，依据系统访问控制的安全策略，试图以未授权用户身份/角色访问客体，验证是否不能进行访问。

结果判定

a) 如果测评实施中 a）为肯定，则测评实施e）和g）为肯定；
b) 测评实施中 b）～g）均为肯定，则信息系统符合本单元测评项要求。

3) 安全审计（G2）

测评项

a) 审计范围应覆盖到服务器上的每个操作系统用户和数据库用户；
b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；
c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；
d) 应保护审计记录，避免受到未预期的删除、修改或覆盖等，保存时间不少于一个月。

测评方式

访谈，检查，测评。

测评对象

安全审计员，重要服务器操作系统，重要数据库管理系统。

测评实施

a) 可访谈安全审计员，询问主机系统是否设置安全审计；询问主机系统对事件进行审计的选择要求和策略是什么；对审计日志的处理方式有哪些；
b) 应检查重要服务器操作系统和重要数据库管理系统，查看当前审计范围是否覆盖到每个用户；
c) 应检查重要服务器操作系统和重要数据库管理系统，查看审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、系统资源的异常使用、重要系统命令的使用（如删除客体）等；
d) 应检查重要服务器操作系统和重要数据库管理系统，查看审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容；
e) 应检查重要服务器操作系统和重要数据库管理系统，查看审计跟踪设置是否定义了审计跟踪极限的阈值，当存储空间被耗尽时，能否采取必要的保护措施，例如，报警并导出、丢弃未记录的审计信息、暂停审计或覆盖以前的审计记录等；
f) 应测评主要服务器操作系统和主要数据库管理系统，在系统上以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），测评安全审计的覆盖情况和记录情况与要求是否一致；
g) 应测评主要服务器操作系统和主要数据库管理系统，在系统上以某个系统用户试图删除、修改或覆盖审计记录，测评安全审计的保护情况与要求是否一致。

结果判定

a) 测评实施中 b）～g）均为肯定，则信息系统符合本单元测评项要求。

4) 入侵防范（G2）

测评项

a) 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器、系统软件预防性维护服务等方式保持系统补丁及时得到更新。

测评方式

访谈，检查，测评。

测评对象

系统管理员，主要服务器系统。

测评实施

b) 应与系统管理员访谈，询问主机系统是否采取入侵防范措施，入侵防范内容是否包括主机运行监视、资源使用超过值报警、特定进程监控、入侵行为检测、完整性检测等方面内容；

c) 应与系统管理员访谈，询问入侵防范产品的厂家、版本和在主机系统中的安装部署情况；询问是否进行过部署的改进或者更换过产品，是否按要求（如定期或实时）进行产品升级；

d) 应检查主要服务器系统，查看是否进行主机运行监视，监视的内容是否包括主机的CPU、硬盘、内存、网络等资源的使用情况，并给出资源使用历史记录；

e) 应检查主要服务器系统，查看是否设定资源报警阈值（如CPU、硬盘、内存、网络等资源的报警阈值）以便在资源使用超过规定数值时发出报警，并查看报警方式有哪些；

f) 应检查主要服务器系统，查看是否对特定进程（包括主要的系统进程，如WINDOWS 的Explorer进程）进行监控，是否可以设定非法进程列表；

g) 应检查主要服务器系统，查看是否对主机账户（如系统管理员）进行控制，以限制对重要账户的添加和更改等；

h) 应检查主要服务器系统，查看能否记录攻击者的源IP、攻击类型、攻击目标、攻击时间等，在发生严重入侵事件时是否提供报警（如声音、短信、EMAIL等）；

i) 应测评主要服务器系统，试图运行非法进程，验证其能否限制非法进程的运行；试图添加或更改重要账户，验证主机能否限制重要账户的添加和更改；

j) 应测评主要服务器系统，试图破坏重要程序（如执行系统任务的重要程序）的完整性，验证主机能否检测到重要程序的完整性受到破坏。

结果判定

a) 如果测评实施中b）中的厂家为正规厂家（如有销售许可），版本号较新，改进合理，定期升级，则该项为肯定；

b) 测评实施中 a）～f）均为肯定，则信息系统符合本单元测评项要求。

5) 恶意代码防范（G2）

测评项

a) 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；

b) 应支持防恶意代码软件的统一管理。

测评方式

访谈，检查。

测评对象

系统安全员，重要服务器系统，重要终端系统，网络防恶意代码产品，主机安全设计/验收文档。

测评实施

a) 应访谈系统安全员，询问主机系统是否采取恶意代码实时检测与查杀措施，恶意代码实时检测与查杀措施的部署情况如何；

b) 应检查主机恶意代码防范方面的设计/验收文档，查看描述的安装范围是否包括服务器和终端设备（包括移动设备）；

c) 应检查重要服务器系统和重要终端系统，查看是否安装实时检测与查杀恶意代码的软件产品；查看检测与查杀恶意代码软件产品的厂家、版本号和恶意代码库名称；

d) 应检查网络防恶意代码产品,查看厂家、版本号和恶意代码库名称。

结果判定

a) 如果测评实施中 a）中恶意代码实时检测与查杀措施的部署到服务器和重要终端，则该项为肯定；

b) 测评实施中 a）~ c）均为肯定，检查发现主机系统防恶意代码产品与网络防恶意代码产品使用不同的恶意代码库（如厂家、版本号和恶意代码库名称不相同等），则信息系统符合本单元测评项要求。

6) 资源控制（A2）

测评项

a) 应通过设定终端接入方式、网络地址范围等条件限制终端登录；

b) 应根据安全策略设置登录终端的操作超时锁定；

c) 应限制单个用户对系统资源的最大或最小使用限度。

测评方式

检查，测评。

测评对象

重要服务器操作系统。

测评实施

a) 应检查重要服务器操作系统，查看是否限制单个用户的多重并发会话数量；查看是否设定终端接入方式、网络地址范围等条件限制终端登录；

b) 应测评重要服务器操作系统，任选一个用户，登录服务器，试图发出多重并发会话，验证系统是否限制单个用户的会话数量；

c) 应测评重要服务器操作系统，任选一个用户帐户，登录服务器，用不同的终端接入方式、网络地址试图登录服务器，验证重要服务器操作系统是否通过终端接入方式、网络地址范围等条件限制终端登录；

d) 上机检查：主机操作系统、数据库、重要应用系统是否根据安全策略设置登录终端的操作超时锁定。

结果判定

a) 测评实施中 a）~d）均为肯定，则信息系统符合本单元测评项要求。

主机安全重点测评操作系统包括各网站服务器、应用服务器和数据库服务器等操作系统在内容上，系统安全层面实施过程涉及 6 个工作单元，具体内容请参见附录 A.1.1.3。

7.1.1.1.4 应用安全

1) 身份鉴别（S2）

测评项

a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；

b) 应提供用户身份标识唯一和鉴别信息复杂度检查功能,保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

c) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

d) 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

测评方式

访谈，检查，测评。

测评对象

系统管理员，重要应用系统，总体规划/设计文档。

测评实施

a) 可访谈系统管理员，询问应用系统是否采取身份标识和鉴别措施，具体措施有哪些；系统采取何种措施防止身份鉴别信息被冒用（如复杂性混有大、小写字母、数字和特殊字符，设定口令周期等）；
b) 检查应用系统是否有用户管理模块，是否对系统的用户账号和口令强度进行强制性要求；
c) 可访谈系统管理员，询问应用系统是否具有登录失败处理的功能，是如何进行处理的；
d) 可访谈系统管理员，询问应用系统对用户标识是否具有唯一性（如UID、用户名或其他信息在系统中是唯一的，用该标识能唯一识别该用户）；
e) 应检查总体规划/设计文档，查看其是否有系统采取了唯一标识（如用户名、UID或其他属性）的说明；
f) 应检查重要应用系统，查看其是否配备身份标识（如建立账号）和鉴别（如口令等）功能；查看其身份鉴别信息是否具有不易被冒用的特点，例如复杂性（如规定字符应混有大、小写字母、数字和特殊字符）或为了便于记忆使用了令牌；
g) 应检查重要应用系统，查看其是否配备并使用登录失败处理功能（如登录失败次数超过设定值，系统自动退出等）；
h) 应测评重要应用系统，验证其登录失败处理，非法登录次数限制，登录连接超时自动退出等功能是否有效；
i) 应测评应用系统，是否登录密码被设置为统一初始密码，是否有建议修改初始密码功能。

结果判定

a) 如果测评实施中 c）中相关文档中对用户进行唯一性标识的描述，则该项为肯定；
b) 测评实施中 d）～i）均为肯定，则信息系统符合本单元测评项要求。

2) 访问控制（S2）

测评项

a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；
b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；
c) 应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限；
d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
e) **生产系统应建立关键账户与权限的关系表。（F2）**

测评方式

访谈，检查，测评。

测评对象

系统管理员，重要应用系统。

测评实施

a) 应访谈系统管理员，询问业务系统是否提供访问控制措施，具体措施有哪些，自主访问控制的粒度如何；
b) 应检查重要应用系统，查看系统是否提供访问控制机制；是否依据安全策略控制用户对客体（如文件和数据库中的数据）的访问；
c) 应检查重要应用系统，查看其自主访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作；自主访问控制的粒度是否达到主体为用户级，客体为文件、数据库表级（如数据库表、视图、存储过程等）；
d) 应检查重要应用系统，查看应用系统是否有对授权主体进行系统功能操作和对数据访问权限进行设置的功能；

e) 应检查重要应用系统，查看其特权用户的权限是否分离（如将系统管理员、安全员和审计员的权限分离），权限之间是否相互制约；
f) 应检查重要应用系统，查看其是否有限制默认用户访问权限的功能，并已配置使用；
g) 应测评重要应用系统，可通过用不同权限的用户登录，查看其权限是否受到应用系统的限制，验证系统权限分离功能是否有效；
h) 应测评重要应用系统，可通过授权主体设置特定用户对系统功能进行操作和对数据进行访问的权限，然后以该用户登录，验证用户权限管理功能是否有效；
i) 应测评重要应用系统，可通过用默认用户（默认密码）登录，并用该用户进行操作（包括合法、非法操作），验证系统对默认用户访问权限的限制是否有效。

结果判定

a) 测评实施中 b）~ i）均为肯定，则信息系统符合本单元测评项要求。

3) 安全审计（G2）

测评项

a) 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；
b) 应保证**不提供**删除、修改或覆盖审计记录**的功能**；
c) 审计记录的内容至少应包括事件日期、时间、发起者信息、类型、描述和结果等，**保存时间不少于一个月。**

测评方式

访谈，检查，测评。

测评对象

审计员，重要应用系统。

测评实施

a) 可访谈安全审计员，询问应用系统是否设置安全审计；询问应用系统对事件进行审计的选择要求和策略是什么；对审计日志的处理方式有哪些；
b) 应检查重要应用系统，查看其当前审计范围是否覆盖到每个用户；
c) 应检查重要应用系统，查看其审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、重要系统命令的使用（如删除客体）等；
d) 应检查重要应用系统，查看其审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容；
e) 应检查重要应用系统，查看其审计跟踪设置是否定义了审计跟踪极限的阈值，当存储空间被耗尽时，能否采取必要的保护措施，例如，报警并导出、丢弃未记录的审计信息、暂停审计或覆盖以前的审计记录等；
f) 应测评重要应用系统，可通过非法终止审计功能或修改其配置，验证审计功能是否受到保护；
g) 应测评重要应用系统，在系统上以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），测评安全审计的覆盖情况和记录情况与要求是否一致；
h) 应测评重要应用系统，在系统上以某个系统用户试图删除、修改或覆盖审计记录，测评安全审计的保护情况与要求是否一致。

结果判定

a) 测评实施中 b）~ h）均为肯定，则信息系统符合本单元测评项要求。

4) 通信完整性（S2）

测评项

a) 应采用校验码技术保证通信过程中数据的完整性。

测评方式

访谈，检查，测评。

测评对象

安全员，设计/验收文档，重要应用系统。

测评实施

a) 可访谈安全员，询问业务系统是否有数据在传输过程中进行完整性保证的操作，具体措施是什么；

b) 应检查设计/验收文档，查看其是否有通信完整性的说明，如果有则查看其是否有系统是根据校验码判断对方数据包的有效性的描述；

c) 应测评重要应用系统，可通过获取通信双方的数据包，查看其是否有验证码。

结果判定

a) 测评实施中 b）～c）均为肯定，则信息系统符合本单元测评项要求。

5) 通信保密性（S2）

测评项

a) 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；

b) 应对通信过程中的敏感信息字段进行加密。

测评方式

访谈，测评。

测评对象

安全员，重要应用系统。

测评实施

a) 可访谈安全员，询问业务系统数据在存储和传输过程中是否采取保密措施（如在通信双方建立会话之前利用密码技术进行会话初始化验证，在通信过程中对敏感信息字段进行加密等），具体措施有哪些，是否所有应用系统的通信都采取了上述措施；

b) 应测评重要应用系统，查看当通信双方中的一方在一段时间内未作任何响应，另一方是否能自动结束会话；系统是否能在通信双方建立连接之前，利用密码技术进行会话初始化验证（如SSL建立加密通道前是否利用密码技术进行会话初始验证）；

c) 应测评重要应用系统，通过通信双方中的一方在一段时间内未作任何响应，查看另一方是否能自动结束会话，测评当通信双方中的一方在一段时间内未作任何响应，另一方是否能自动结束会话的功能是否有效；

d) 应测评重要应用系统，通过查看通信双方数据包的内容，查看系统在通信过程中，对敏感信息字段进行加密的功能是否有效。

结果判定

a) 测评实施中 b）～d）均为肯定，则信息系统符合本单元测评项要求。

6) 软件容错（A2）

测评项

a) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；

b) 在故障发生时，应用系统应能够继续提供一部分功能，确保能够实施必要的措施；

c) **应能够有效屏蔽系统技术错误信息，不将系统产生的错误信息直接反馈给客户。（F2）**

测评方式

访谈，检查，测评。

测评对象

安全员，重要应用系统。

测评实施

a) 可访谈系统管理员，询问业务系统是否有保证软件具有容错能力的措施（如对人机接口输入或通过通信接口输入的数据进行有效性检验等），具体措施有哪些；

b) 应检查重要应用系统，通过输入不同的数据格式或长度等进行验证，查看业务系统是否对人机接口输入（如用户界面的数据输入）或通信接口输入的数据进行有效性检验；是否允许按照操作的序列进行回退（如撤消操作）；是否在故障发生时继续提供一部分功能，确保能够实施必要的措施（如对重要数据的保存）；

c) 应测评重要应用系统，可通过输入的不同（如数据格式或长度等符合、不符合软件设定的要求），验证系统人机接口有效性检验功能是否正确；

d) 应测评重要应用系统，可通过多步操作，然后回退，验证系统能否按照操作的序列进行正确的回退；可通过给系统人为制造一些故障（如系统异常），验证系统能否在故障发生时继续提供一部分功能，并能实施必要的措施。

结果判定

a) 测评实施中 b）～d）均为肯定，则信息系统符合本单元测评项要求。

7) 资源控制（A2）

测评项

a) **对于有会话或短连接的应用系统**,当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

b) 应能够对应用系统的最大并发会话连接数进行限制；

c) **对于有会话的应用系统，**应能够对单个帐户的多重并发会话进行限制。

测评方式

访谈，检查，测评。

测评对象

系统管理员，重要应用系统。

测评实施

a) 可访谈系统管理员，询问业务系统是否有资源控制的措施（如对应用系统的最大并发会话连接数进行限制，是否禁止同一用户账号在同一时间内并发登录，是否对一个时间段内可能的并发会话连接数进行限制，对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额等），具体措施有哪些；

b) 应检查重要应用系统，查看系统是否有最大并发会话连接数的限制；

c) 应测评重要应用系统，可通过对系统进行进行超过最大并发会话连接数进行连接，验证系统能否正确地限制最大并发会话连接数；

d) 应测评重要应用系统，可通过在一个时间段内，用超过设定的并发连接数对系统进行连接，查看能否连接成功，验证系统对一个时间段内可能的并发会话连接数进行限制的功能是否正确。

结果判定

a) 测评实施中 b）～d）均为肯定，则信息系统符合本单元测评项要求。

在内容上，应用安全层面实施过程涉及 7 个工作单元，具体内容请参见附录 A.1.1.4。

7.1.1.1.5 数据安全及备份恢复

1) 数据完整性（S2）

测评项

a) 应能够检测到鉴别信息和重要业务数据在传输过程中完整性受到破坏。

测评方式

访谈，检查。

测评对象

安全员，系统管理员，重要应用系统，设计/验收文档，相关证明性材料（如证书、检验报告等）。

测评实施

a) 可访谈安全员，询问业务系统数据在传输过程中是否有完整性保证措施，具体措施有哪些；

b) 应检查操作系统、网络设备、数据库管理系统的设计/验收文档或相关证明性材料（如证书、检验报告等）等，查看其是否有能检测/验证到系统管理数据（如WINDOWS域管理、目录管理数据）、鉴别信息（如用户名和口令）和用户数据（如用户数据文件）在传输过程中完整性受到破坏；能否检测/验证到系统管理数据（如WINDOWS注册表、系统文件）、身份鉴别信息（如用户名和口令存储文件）和用户数据（如用户数据文件）在存储过程中未授权的修改与破坏；能否检测到系统管理数据、鉴别信息和用户数据在操作过程中完整性受到破坏；如果有相关信息，查看其配置如何；

c) 应检查重要应用系统，查看其是否配备检测/验证系统管理数据、鉴别信息和用户数据在传输过程中完整性受到破坏的功能；是否配备检测/验证系统管理数据、身份鉴别信息和用户数据在存储过程中未授权修改与破坏的功能；是否具备检测/验证系统管理数据、鉴别信息和用户数据在操作过程中完整性受到破坏的功能。

结果判定

a) 如果测评实施中 b）缺少相关材料，则该项为否定；

b) 测评实施中 b）～c）均为肯定，则信息系统符合本单元测评项要求。

2) 数据保密性（S2）

测评项

a) 应采用加密或其他保护措施实现鉴别信息的存储保密性。

测评方式

访谈，检查，测评。

测评对象

系统管理员、网络管理员、安全员、数据库管理员，操作系统，网络设备，数据库管理系统，重要应用系统，设计/验收文档。

测评实施

a) 可访谈网络管理员，询问信息系统中的网络设备的鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性；是否采用加密或其他保护措施实现存储保密性；

b) 可访谈系统管理员，询问信息系统中的操作系统的鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性；是否采用加密或其他保护措施实现存储保密性；

c) 可访谈数据库管理员，询问信息系统中的数据库管理系统的鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性；是否采用加密或其他保护措施实现存储保密性；

d) 可访谈安全员，询问信息系统中的应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性；是否采用加密或其他保护措施实现存储保密性；

e) 可访谈安全员，询问当使用便携式和移动式设备时，是否加密或者采用可移动磁盘存储敏感信息；

f) 可访谈安全员，询问系统采用的密码算法和密钥是否符合国家密码管理规定；

g) 应检查操作系统、网络设备、数据库管理系统、重要应用系统设计/验收文档，查看其是否有关于其鉴别信息、敏感的系统管理数据和敏感的用户数据采用加密或其他有效措施实现传输保密性描述，是否有采用加密或其他保护措施实现存储保密性的描述；

h) 应检查重要应用系统，查看其鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性描述，是否采用加密或其他保护措施实现存储保密性；

i) 应测评重要应用系统，通过用嗅探工具获取系统传输数据报，查看其是否采用加密或其他有效措施实现传输保密性。

结果判定

a) 如果缺少设计/验收文档，测评实施中g）为否定；

b) 测评实施中g）～i）均为肯定，则信息系统符合本单元测评项要求。

3) 数据备份和恢复（A2）

测评项

a) 应能够对重要信息进行备份和恢复；

b) 应提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性。

测评方式

访谈，检查。

测评对象

系统管理员、网络管理员、安全员、数据库管理员，重要应用系统，重要应用系统设计/验收文档。

测评实施

a) 可访谈网络管理员，询问信息系统中的网络设备是否提供用户有选择的备份重要信息的功能；是否提供重要网络设备、通信线路和服务器的硬件冗余；

b) 可访谈系统管理员，询问信息系统中的操作系统是否提供用户有选择的备份重要信息的功能；

c) 可访谈数据库管理员，询问信息系统中的数据库管理系统是否提供用户有选择的备份重要信息的功能；

d) 应检查重要应用系统设计/验收文档，查看其是否有描述应用系统提供用户有选择的备份重要信息的功能的描述；

e) 应检查操作系统、网络设备、数据库管理系统、关键应用系统，查看其是否配置有选择的备份和恢复重要信息恢复的功能，其配置是否正确；

f) 应检查重要网络设备、通信线路和服务器是否提供硬件冗余。

结果判定

a) 如果缺少设计/验收文档，测评实施中d）为否定；

b) 测评实施中d）～f）均为肯定，则信息系统符合本单元测评项要求。

数据安全层面分布在网络安全、主机安全和应用安全等层面进行测评，在内容上，数据安全层面实施过程涉及 3 个工作单元，具体内容请参见附录 A.1.1.5。

7.1.1.2 安全管理测评

7.1.1.2.1 安全管理制度

1) 管理制度(G2)

测评项

a) 应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；

b) 应对安全管理活动中重要的管理内容建立安全管理制度；

c) 应对安全管理人员或操作人员执行的重要管理操作建立操作规程。

测评方式

访谈，检查。

测评对象

安全主管，总体方针、政策性文件和安全策略文件，安全管理制度清单，操作规程。

测评实施

a) 应检查文档规范中是否制定信息安全工作的总体方针、政策性文件和安全策略等，是否对重要管理内容建立安全管理制度，是否对重要管理操作制定操作规程；
b) 应检查信息安全工作的总体方针、政策性文件和安全策略文件，查看文件是否明确机构安全工作的总体目标、范围、方针、原则、责任等；
c) 应检查安全管理制度清单，查看是否覆盖物理、网络、主机系统、数据、应用和管理等层面；
d) 应检查是否具有重要管理操作的操作规程，如系统维护手册和用户操作规程等。

结果判定

a) 测评实施中 a）～d）均为肯定，则信息系统符合本单元测评项要求。

2) 制定和发布(G2)

测评项

a) 由**金融机构总部科技部门**负责负责制定适用全机构范围安全管理制度，各分支机构的科技部门负责制定适用辖内安全管理制度；
b) 应组织相关人员对制定的安全管理制度进行论证和审定；
c) 应将安全管理制度以某种方式发布到相关人员手中。

测评方式

访谈，检查。

测评对象

安全主管，制度制定和发布要求管理文档，评审记录，安全管理制度。

测评实施

a) 应检查安全管理制度是否在信息安全职能部门的总体负责下统一制定，参与制定人员有哪些；
b) 应访谈安全主管，询问安全管理制度的制定程序，是否对制定的安全管理制度进行论证和审定，论证和评审方式如何（如召开评审会、函审、内部审核等），是否按照统一的格式标准或要求制定；
c) 应检查制度制定和发布要求管理文档，查看文档是否说明安全管理制度的制定和发布程序、格式要求及版本编号等相关内容；
d) 应检查管理制度评审记录，查看是否有相关人员的评审意见；
e) 应检查安全管理制度的发布过程是否正式有效，并以某种方式发布到相关人员手中。

结果判定

a) 测评实施中 a）～e）均为肯定，则信息系统符合本单元测评项要求。

3) 评审和修订(G2)

测评项

a) 应定期对安全管理制度进行评审，对存在不足或需要改进的安全管理制度进行修订。

测评方式

访谈，检查。

测评对象

安全主管，安全管理制度列表，评审记录。

测评实施

a) 应检查制度修订评审记录和需要定期评审的安全管理制度列表，查看列表是否注明评审周期；
b) 是否定期对安全管理制度进行评审，发现存在不足或需要改进的是否进行修订，评审周期多长，评审、修订程序如何，维护措施如何；

c) 应检查是否具有需要定期评审的安全管理制度列表；

d) 应检查安全管理制度评审记录，查看记录日期与评审周期是否一致；如果对制度做过修订，检查是否有修订版本的安全管理制度。

结果判定

a) 测评实施中 a）～i）均为肯定，则信息系统符合本单元测评项要求。

安全管理制度测评对象主要为管理制度、制定和发布、评审和修订 3 个控制点相关的文件资料和工作记录，具体内容请参见附录 A.1.2.1。

7.1.1.2.2 安全管理机构

1) 岗位设置(G2)

测评项

a) **信息安全管理工作应实行统一领导、分级管理，总部统一领导分支机构的信息安全管理，各机构负责本单位和辖内的信息安全管理；(F2)**

b) **除科技部门外，其他部门均应指定至少一名部门计算机安全员，具体负责本部门的信息安全管理工作，协同科技部门开展信息安全管理工作；（F2）**

c) 应设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；

d) 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责。

测评方式

访谈，检查。

测评对象

安全主管，安全管理某方面的负责人，部门、岗位职责文件。

测评实施

a) 应访谈安全主管，询问是否设立安全管理机构（即信息安全管理工作的职能部门，可以由其它部门兼职）；机构内部设置情况如何，是否明确机构内各部门的职责分工；

b) 应访谈安全主管，询问是否设立安全管理各个方面的负责人，设置了哪些工作岗位（如安全主管、安全管理各个方面的负责人、机房管理员、系统管理员、网络管理员和安全员等重要岗位），是否明确各个岗位的职责分工；

c) 应访谈安全主管、安全管理某方面的负责人，询问其岗位职责包括哪些内容；检查科技部门内部岗位职责；

d) 应检查部门、岗位职责文件，查看文件是否明确安全管理机构的职责，是否明确机构内各部门的职责和分工，部门职责是否涵盖物理、网络和系统等各个方面；查看文件是否明确设置安全主管、安全管理各个方面的负责人、机房管理员、系统管理员、网络管理员和安全员等各个岗位，各个岗位的职责范围是否清晰，是否明确岗位人员应具有的技能要求，人员是否备案。

结果判定

a) 如果测评实施中 c）被访谈人员表述与文件描述一致，则该项为肯定；

b) 测评实施中 a）～d）均为肯定，则信息系统符合本单元测评项要求。

2) 人员配备(G2)

测评项

a) 应配备一定数量的系统管理员、网络管理员、安全管理员等；

b) 安全管理员不能兼任网络管理员、系统管理员、数据库管理员等。

测评方式

访谈，检查。

测评对象

安全主管，人员配备要求的相关文档，管理人员名单。

测评实施

a) 应访谈安全主管，询问各个安全管理岗位人员（按照岗位职责文件询问，包括机房管理员、系统管理员、数据库管理员、网络管理员、安全员等重要岗位人员）配备情况，包括数量、专职还是兼职等；
b) 应检查人员配备相关文档，查看岗位分工列表和定期轮岗情况（含轮岗周期、轮岗手续等）查看是否明确应配备哪些安全管理人员，是否包括机房管理员、系统管理员、数据库管理员、网络管理员、安全员等重要岗位人员；
c) 应检查岗位分工名单，查看其是否明确机房管理员、系统管理员、数据库管理员、网络管理员、安全管理员等重要岗位人员的信息，确认安全管理员没有兼任网络管理员、系统管理员、数据库管理员等。

结果判定

a) 如果测评实施中 a）设置的安全员没有兼任网络管理员、系统管理员、数据库管理员等，则该项为肯定；
b) 测评实施中 a）～c）均为肯定，则信息系统符合本单元测评项要求。

3) 授权和审批(G2)

测评项

a) 应根据各个部门和岗位的职责明确授权审批部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批；
b) 应针对关键活动建立审批流程，并由批准人签字确认。

测评方式

访谈，检查。

测评对象

安全主管，关键活动的批准人，审批事项列表，审批文档。

测评实施

a) 应检查是否对信息系统中的关键活动进行审批；
b) 应检查关键活动的审批（如网络系统、应用系统、数据库管理系统、重要服务器和设备等重要资源的访问，重要管理制度的制定和发布，人员的配备、培训和产品的采购等），
c) 应检查审批事项列表，查看列表是否明确须审批事项、审批部门、批准人及审批程序等；
d) 应检查经审批的文档，查看是否具有批准人和审批部门的核准。

结果判定

a) 测评实施中 a）～d）均为肯定，则信息系统符合本单元测评项要求。

4) 沟通和合作(G2)

测评项

a) 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通；
b) 应加强与兄弟单位、公安机关、电信公司的合作与沟通。

测评方式

访谈，检查。

测评对象

安全主管，安全管理人员，会议文件，会议记录，外联单位说明文档。

测评实施

a) 应访谈安全主管，询问是否经常与公安机关、电信公司和兄弟单位联系，联系方式有哪些，与组织机构内其他部门之间有哪些合作内容，沟通、合作方式有哪些；
b) 应访谈安全主管，询问是否召开过部门间协调会议，组织其它部门人员共同协助处理信息系统安全有关问题，安全管理机构内部是否召开过安全工作会议部署安全工作的实施，参加会议的部门和人员有哪些，会议结果如何；

c) 应访谈安全管理人员（从系统管理员和安全员等人员中抽查），询问其与外单位人员，与组织机构内其他部门人员，与内部各部门管理人员之间的沟通方式和主要沟通内容有哪些；
d) 应检查部门间协调会议文件或会议记录，查看是否有会议内容、会议时间、参加人员、会议结果等的描述；
e) 应检查安全工作会议文件或会议记录，查看是否有会议内容、会议时间、参加人员、会议结果等的描述；
f) 应检查外联单位说明文档，查看外联单位是否包含公安机关、电信公司及兄弟公司，是否说明外联单位的联系人和联系方式等内容。

结果判定

a) 测评实施中 a）～f）均为肯定，则信息系统符合本单元测评项要求。

5) 审核和检查(G2)

测评项

a) 安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

测评方式

访谈，检查。

测评对象

安全主管，安全员，安全检查记录。

测评实施

a) 应检查是否组织人员定期对信息系统进行安全检查，检查周期多长，是否明确检查内容；
b) 检查人员有哪些，检查程序是否按照系统相关策略和要求进行，检查结果如何；
c) 应检查安全检查记录，查看记录时间与检查周期是否一致，文档中是否有检查内容、检查人员、检查结果等的描述。

结果判定

a) 测评实施中a）～c）均为肯定，则信息系统符合本单元测评项要求。

安全管理机构测评对象主要为岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查 5 个控制点相关的文件资料和工作记录。具体内容请参见附录 A.1.2.2。

7.1.1.2.3 人员安全管理

1) 人员录用(G2)

测评项

a) 应指定或授权专门的部门或人员负责人员录用；
b) 应规范人员录用过程，对被录用人员的身份、背景和专业资格等进行审查，对其所具有的技术技能进行考核；
c) 应与从事关键岗位的人员签署保密协议；
d) **对信息安全管理人员应实行备案管理。信息安全管理人员的配备和变更情况，应及时报上一级科技部门备案，金融机构总部信息管理人员在总部科技部门备案；（F2）**
e) **凡是因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员，不得从事信息安全管理工作。（F2）**

测评方式

访谈，检查。

测评对象

人事负责人，人事工作人员，人员录用要求管理文档，人员审查文档或记录，考核文档或记录，保密协议。

测评实施

a) 应访谈人事负责人，询问在人员录用时对人员条件有哪些要求，目前录用的安全管理和技术人员是否有能力完成与其职责相对应的工作；
b) 应访谈人事工作人员，询问在人员录用时是否对被录用人的身份、背景、专业资格和资质进行审查，录用后是否与其签署保密协议，是否对其说明工作职责；
c) 应检查人员录用要求管理文档，查看是否说明录用人员应具备的条件，如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等；
d) 应检查是否具有人员录用时对录用人身份、背景、专业资格或资质等进行审查的相关文档或记录，查看是否记录审查内容和审查结果等；
e) 应检查技能考核文档或记录，查看是否记录考核内容和考核结果等；
f) 应检查保密协议，查看是否有保密范围、保密责任、违约责任、协议的有效期限和责任人签字等。

结果判定

a) 测评实施中a）～f）均为肯定，则信息系统符合本单元测评项要求。

2) 人员离岗（G2）

测评项

a) 应规范人员离岗过程，及时终止离岗员工的所有访问权限；
b) 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
c) **应办理严格的调离手续，并保证离岗人员负责的信息技术系统的口令必须立即更换。**

测评方式

访谈，检查。

测评对象

安全主管，人事工作人员，安全处理记录，保密承诺文档。

测评实施

a) 应访谈安全主管，询问是否及时终止离岗人员所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备等；
b) 应访谈人事工作人员，询问调离手续包括哪些，是否要求调离人员承诺相关保密义务后方可离开；
c) 应检查是否具有对离岗人员的安全处理记录，如交还身份证件、设备等的登记记录；
d) 应检查保密承诺文档，查看是否有调离人员的签字。

结果判定

a) 测评实施中 a）～d）均为肯定，则信息系统符合本单元测评项要求。

3) 人员考核（G2）

测评项

a) 应定期对各个岗位的人员进行安全技能及安全认知的考核。

测评方式

访谈。

测评对象

安全主管，人事工作人员。

测评实施

a) 应访谈安全主管，询问是否有人负责定期对各个岗位人员进行安全技能及安全知识的考核；
b) 应访谈人事工作人员，询问对各个岗位人员的考核情况，考核周期多长，考核内容有哪些；询问对人员的安全审查情况，审查内容有哪些（如操作行为、社会关系、社交活动等），是否全面；
c) 应访谈人事工作人员，询问对违背安全策略和规定的人员有哪些惩戒措施。

结果判定

a) 如果测评实施中b）被访谈人员表述审查内容包含社会关系、社交活动、操作行为等各个方面，则该项为肯定；

b) 如果测评实施中c）被访谈人员表述与文件描述一致，则该项为肯定；

c) 测评实施中a）～c）均为肯定，则信息系统符合本单元测评项要求。

4) 安全意识教育和培训(G2)

测评项

a) 应制定安全教育和培训计划；

b) 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；

c) **每年至少对信息安全管理人员进行一次信息安全培训；（F2）**

d) 应告知人员相关的安全责任和惩戒措施，并对违反违背安全策略和规定的人员进行惩戒。

测评方式

访谈，检查。

测评对象

安全主管，安全员，系统管理员，网络管理员，培训计划，培训记录。

测评实施

a) 应访谈安全主管，询问是否制定安全教育和培训计划并按计划对各个岗位人员进行安全教育和培训，以什么形式进行，效果如何；

b) 应检查安全责任和惩戒措施相关制度和惩戒记录；

c) 应检查安全教育和培训计划文档，查看计划是否明确了培训目的、培训方式、培训对象、培训内容、培训时间和地点等，培训内容是否包含信息安全基础知识、岗位操作规程等；

d) 应检查是否具有安全教育和培训记录，查看记录是否有培训人员、培训内容、培训结果等的描述；查看记录与培训计划是否一致。

结果判定

a) 如果测评实施中b）访谈人员能够表述清楚询问内容，且安全职责、惩戒措施和岗位操作规程表述与文件描述一致，则该项为肯定；

b) 测评实施中a）～d）均为肯定，则信息系统符合本单元测评项要求。

5) 外部人员访问管理(G2)

测评项

a) **各机构指定责任部门负责非涉密计算机系统和网络相关的外部人员访问授权审批，批准后由专人全程陪同或监督，并登记备案；**

b) **获得外部人员访问授权的所有机构和个人应与金融机构签订安全保密协议，不得进行未授权的增加、删除、修改、查询数据操作，不得复制和泄漏金融机构的任何信息；（F2）**

c) **外部人员进入金融机构进行现场实施时，应事先提交计划操作内容，金融机构人员应在现场陪同外部人员，核对操作内容并记录。（F2）**

测评方式

访谈，检查。

测评对象

安全主管，安全管理人员，安全责任合同书或保密协议，第三方人员访问管理文档，登记记录。

测评实施

a) 应检查对第三方人员（如向系统提供服务的系统软、硬件维护人员，业务合作伙伴、评估人员等）的访问采取哪些管理措施，是否要求第三方人员访问前与机构签署安全责任合同书或保密协议；

b) 应访谈安全管理人员，询问对第三方人员访问重要区域（如访问主机房等）采取哪些措施，是否经有关负责人批准才能访问，是否由专人陪同或监督，是否进行记录并备案管理；
c) 应检查安全责任合同书或保密协议，查看是否有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等；
d) 应检查第三方人员访问管理文档，查看是否规定对第三方人员访问哪些重要区域应经过负责人批准；
e) 应检查第三方人员访问重要区域的登记记录，查看记录是否描述了第三方人员访问重要区域的进入时间、离开时间、访问区域及陪同人等信息；
f) 检查获得外部人员访问授权的所有单位和个人是否与金融机构签订安全保密协议，是否进行未授权的增加、删除、修改、查询数据操作，是否发生过复制和泄金融机构的任何信息的事件。

结果判定

a) 测评实施中a）～f）均为肯定，则信息系统符合本单元测评项要求。

人员安全管理测评对象主要为人员录用、人员离岗、人员考核、安全意识教育培训和外部人员访问管理 5 个控制点相关的文件资料和工作记录，具体内容请参见附录 A.1.2.3。

7.1.1.2.4 系统建设管理

1) 系统定级（G2）

测评项

a) 应明确信息系统的边界和安全保护等级；
b) 应以书面的形式说明信息系统确定为某个安全保护等级的方法和理由；
c) 应确保信息系统的定级结果经过相关部门的批准。

测评方式

访谈，检查。

测评对象

安全主管，系统划分文档，系统定级文档，系统属性说明文档。

测评实施

a) 应访谈安全主管，询问划分信息系统的方法和确定信息系统安全保护等级的方法是否参照定级指南的指导，是否对其进行明确描述；定级结果是否获得了相关部门（如上级主管部门）的批准；
b) 应检查系统划分相关文档，查看文档是否明确描述信息系统划分的方法和理由；
c) 应检查系统定级文档，查看文档是否给出信息系统的安全保护等级，是否给出安全等级保护措施组成SxAyGz值；查看定级结果是否有相关部门的批准盖章；
d) 应检查系统属性说明文档，查看文档是否明确了系统使命、业务、网络、硬件、软件、数据、边界、人员等。

结果判定

a) 测评实施中a）没有上级主管部门的，如果有安全主管的批准，则该项为肯定；
b) 测评实施中a）～e）均为肯定，则信息系统符合本单元测评项要求。

2) 安全方案设计（G2）

测评项

a) 应根据系统的安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
b) 应以书面形式描述对系统的安全保护要求、策略和措施等内容，形成系统的安全方案；
c) 应对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案；
d) 应组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。

测评方式

访谈，检查。

测评对象

系统建设负责人，安全方案，详细设计方案，专家论证文档。

测评实施

a) 应访谈系统建设负责人，询问是否根据系统的安全级别选择基本安全措施，是否依据风险分析的结果补充和调整安全措施，做过哪些调整；

b) 应访谈系统建设负责人，询问是否制定系统的安全方案并根据安全方案制定出系统详细设计方案指导安全系统建设和安全产品采购，是否组织相关部门和有关安全技术专家对安全设计方案进行论证和审定，安全设计方案是否经过安全主管领导或管理层的批准；

c) 应检查系统的安全方案，查看方案是否描述系统的安全保护要求，是否详细描述了系统的安全策略，是否详细描述了系统对应的安全措施等内容；

d) 应检查系统的详细设计方案，查看详细设计方案是否对应安全方案进行细化，是否有安全建设方案和安全产品采购方案；查看方案是否有经过安全主管领导或管理部门的批准盖章；

e) 应检查专家论证文档，查看是否有相关部门和有关安全技术专家对安全设计方案的评审意见。

结果判定

a) 测评实施中a）～e）均为肯定，则信息系统符合本单元测评项要求。

3) 产品采购和使用（G2）

测评项

a) 应确保安全产品采购和使用符合国家的有关规定；

b) 应确保密码产品采购和使用符合国家密码主管部门的要求；

c) 应指定或授权专门的部门负责产品的采购；

d) **购置扫描、检测类信息安全产品应报本机构科技主管部门批准、备案；（F2）**

e) **扫描、检测类信息安全产品仅限于本机构信息安全管理人员或经主管领导授权的网络管理员使用；（F2）**

f) **应定期查看各类信息安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取应急措施并按规定程序报告；（F2）**

g) **应定期对各类信息安全产品产生的日志和报表进行备份存档；（F2）**

h) **应及时升级维护信息安全产品，凡超过使用期限的或不能继续使用的信息安全产品，要按照固定资产报废审批程序处理。（F2）**

测评方式

访谈，检查。

测评对象

安全主管，系统建设负责人，信息安全产品。

测评实施

a) 应访谈安全主管，询问是否有专门的部门负责产品的采购，由何部门负责；

b) 应访谈系统建设负责人，询问系统信息安全产品的采购情况，是否有产品采购清单指导产品采购，采购过程如何控制；

c) 应访谈系统建设负责人，询问系统是否采用了密码产品，密码产品的使用是否符合国家密码主管部门的要求；

d) 应检查系统使用的有关信息安全产品（边界安全设备、重要服务器操作系统、数据库等）是否符合国家的有关规定；

e) 应检查密码产品的使用情况是否符合密码产品使用、管理的相关规定，如《商用密码管理条例》规定任何单位只能使用经过国家密码管理机构认可的商用密码产品，商用密码产品发生故障，必须有国家密码管理机构指定的单位维修，报废商用密码产品应向国家密码管理机构备案等。

结果判定

a) 如果测评实施中c）访谈说明没有采用密码产品，则测评实施c）、e）为不适用；

b) 测评实施中a）～e）均为肯定，则信息系统符合本单元测评项要求。

4) 自行软件开发(G2)

测评项

a) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；

b) 应确保开发环境与实际运行环境物理分开；

c) **应确保开发人员和测试人员分离，开发人员不能兼任系统管理员或业务操作人员，确保测试数据和测试结果受到控制；（F2）**

d) 应确保提供软件设计的相关文档和使用指南，并由专人负责保管。

测评方式

访谈，检查。

测评对象

系统建设负责人，软件设计的相关文档和使用指南，文档使用控制记录。

测评实施

a) 应访谈系统建设负责人，询问系统是否自主开发软件，自主开发是否有相应的控制措施，是否在独立的模拟环境中编写、调试和完成；

b) 应访谈系统建设负责人，询问系统开发文档是否由专人负责保管，负责人是何人，如何控制使用（如限制使用人员范围并做使用登记等）；

c) 应检查是否具有软件设计的相关文档（应用软件设计程序文件、源代码文档等）和软件使用指南或操作手册和维护手册等；

d) 应检查软件开发环境与系统运行环境在物理上是否是分开的；

e) 应检查是否具有系统开发文档的使用控制记录。

结果判定

a) 测评实施中a）～e）均为肯定，则信息系统符合本单元测评项要求。

5) 外包软件开发(G2)

测评项

a) 应根据开发要求检测软件质量；

b) 应在软件安装之前检测软件包中可能存在的恶意代码；

c) 应确保提供软件设计的相关文档和使用指南；

d) **应定期对外包服务活动和外包服务商的服务能力进行审核和评估；(F2)**

e) 应要求开发单位提供软件源代码，并审查软件中可能存在的后门；

f) **应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要；（F2）**

g) **应禁止外包服务商转包并严格控制分包，保证外包服务水平；（F2）**

h) **应制定数据中心外包服务应急计划，制订供应商替换方案，以应对外包服务商破产、不可抗力或其它潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。（F2）**

测评方法

访谈，检查。

测评对象

系统建设负责人，软件开发安全协议，软件开发文档。

测评实施

a) 应访谈系统建设负责人，询问在外包软件前是否对软件开发单位以书面文档形式（如软件开发安全协议）规范软件开发单位的责任、开发过程中的安全行为、开发环境要求和软件质量等相关内容，是否具有能够独立的对软件进行日常维护和使用所需的文档；
b) 应访谈系统建设负责人，询问软件交付前是否依据开发协议的技术指标对软件功能和性能等进行验收检测，验收检测是否是由开发商和委托方共同参与，软件安装之前是否检测软件中的恶意代码，检测工具是否是第三方的商业产品；
c) 应检查软件开发协议是否规定知识产权归属、安全行为等内容；
d) 应检查是否具有需求分析说明书、软件设计说明书和软件操作手册等开发文档。

结果判定

a) 测评实施中 a）~ d）均为肯定，则信息系统符合本单元测评项要求。

6) 工程实施(G2)

测评项

a) 应指定或授权专门的部门或人员负责工程实施过程的管理；
b) 应制定详细的工程实施方案，**并制定相关过程控制文档**，控制工程实施过程。

测评方法

访谈，检查。

测评对象

系统建设负责人，工程安全建设协议，工程实施方案。

测评实施

a) 应访谈系统建设负责人，询问是否以书面形式（如工程安全建设协议）约束工程实施方的工程实施行为；
b) 应访谈系统建设负责人，询问是否指定专门人员或部门按照工程实施方案的要求对工程实施过程进行进度和质量控制；
c) 应检查工程安全建设协议，查看其内容是否覆盖工程实施方的责任、任务要求和质量要求等方面内容，约束工程实施行为；
d) 应检查工程实施方案，查看其内容是否覆盖工程时间限制、进度控制和质量控制等方面内容。

结果判定

a) 测评实施中 a）~ d）均为肯定，则信息系统符合本单元测评项要求。

7) 测评验收(G2)

测评项

a) 应对系统进行安全性测试验收；
b) 在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；
c) 应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认；
d) **对于在生产系统上进行的测试工作，必须制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划，确保生产系统的安全。（F2）**

测评方法

访谈，检查。

测评对象

系统建设负责人，系统测评方案，系统测评记录，系统测评报告，系统验收报告。

测评实施

a) 应访谈系统建设负责人，询问在信息系统正式运行前，是否根据设计方案或合同要求对信息系统进行独立的安全性测评；

b) 应访谈系统建设负责人，询问是否对测评过程（包括测评前、测评中和测评后）进行文档化要求，是否根据设计方案或合同要求组织相关部门和人员对测评报告进行符合性审定；

c) 应检查工程测评方案，查看其是否对参与测评部门、人员和现场操作过程等进行要求；查看测评记录是否详细记录了测评时间、人员、现场操作过程和测评结果等方面内容；查看测评报告是否提出存在问题及改进意见等；

d) 应检查是否具有系统验收报告。

结果判定

a) 测评实施中 a）～d）均为肯定，则信息系统符合本单元测评项要求。

8) 系统交付 (G2)

测评项

a) 应制定系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

b) **系统建设单位应在完成建设任务后将系统建设过程文档和系统运维文档全部移交科技部门；**

c) **外部建设单位应与金融机构签署相关知识产权保护协议和保密协议，不得将系统采用的关键安全技术措施和核心安全功能设计对外公开；（F2）**

d) 应对负责系统运行维护的技术人员进行相应的技能培训。

测评方法

访谈，检查。

测评对象

系统建设负责人，系统交付清单，服务承诺书，培训记录。

测评实施

a) 应访谈系统建设负责人，询问交接手续是什么，系统交接工作是否按照该手续办理，是否根据交接清单对所交接的设备、文档、软件等进行清点，交接清单是否满足合同的有关要求；

b) 应访谈系统建设负责人，询问目前的信息系统是否由内部人员独立进行运行维护，如果是，系统建设实施方是否对运维技术人员进行过培训，针对哪些方面进行过培训，是否以书面形式承诺对系统运行维护提供一定的技术支持服务，系统是否具有支持其独立运行维护的文档；

c) 应检查系统交付清单，查看其是否具有系统建设文档（如系统建设方案）、指导用户进行系统运维的文档（如服务器操作规程书）以及系统培训手册等文档名称；

d) 应检查是否具有系统建设方的服务承诺书和对系统进行的培训记录。

结果判定

a) 测评实施中 a）～d）均为肯定，则信息系统符合本单元测评项要求。

9) 安全服务商选择(G2)

测评项

a) **选择信息安全服务提供商时应评估其资质、经营行为、业绩、服务体系和服务品质等要素；（F2）**

b) 应确保安全服务商的选择符合国家的有关规定；

c) 应与选定的安全服务商签订与安全相关的协议，明确约定相关责任；

d) 应确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同。

测评方法

访谈。

测评对象

系统建设负责人。

测评实施

a) 应访谈系统建设负责人，询问对信息系统进行安全规划、设计、实施、维护、测评等服务的安全服务单位是否符合国家有关规定。

结果判定

a) 测评实施中 a）为肯定，则信息系统符合本单元测评项要求。

系统建设管理测评对象主要为系统定级、安全方案设计、产品采购、自行软件开发、外包软件开发、工程实施、测评验收、系统交付和安全服务商选择 9 个控制点相关的文件资料和工作记录，具体内容请参见附录 A.1.2.4。

7.1.1.2.5 系统运维管理

1) 环境管理(G2)

测评项

a) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；

b) **机房应采用结构化布线系统，配线机柜内如果配备理线架，应做到跳线整齐，跳线与配线架统一编号，标记清晰；（F2）**

c) **应指定部门负责机房安全，**指派专人担任机房管理员，对机房的出入进行管理，定期巡查机房运行状况，对机房供配电、空调、温湿度控制等设施进行维护管理；**填写机房值班记录、巡视记录；**

d) **机房人员进出机房必须使用主管部门制发的证件；（F2）**

e) **机房管理员应经过相关培训，掌握机房各类设备的操作要领；（F2）**

f) **应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养；（F2）**

g) **机房出入口和内部应安装7*24小时录像监控设施，录像至少保存一周；（F2）**

h) **机房应设置弱电井，并留有可扩展空间；（F2）**

i) 应加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等。

测评方式

访谈，检查。

测评对象

物理安全负责人，机房安全管理制度，机房进出登记表。

测评实施

a) 应访谈物理安全负责人，询问是否对机房基本设施（如空调、供配电设备等）进行定期维护，由何部门/何人负责，维护周期多长；

b) 应访谈物理安全负责人，询问是否指定人员负责机房安全管理工作，对机房的出入管理是否要求进行制度化和文档化；

c) 应访谈物理安全负责人，询问是否对保证办公环境的保密性采取相应措施，如人员调离后权力收回等；

d) 应检查机房安全管理制度，查看其内容是否覆盖机房物理访问、物品带进、带出机房和机房环境安全等方面；

e) 应检查机房进出登记表，查看其是否记录外来人员进出时间、人员姓名和访问原因等方面内容。

结果判定

a) 测评实施中 a）～e）均为肯定，则信息系统符合本单元测评项要求。

2) 资产管理(G2)

测评项

a) 应编制与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；

b) 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为。

测评方式

访谈，检查。

测评对象

安全主管，资产管理员，资产清单，资产安全管理制度，设备。

测评实施

a) 应访谈安全主管，询问是否指定资产管理的责任人员或部门，由何部门/何人负责；
b) 应访谈物理安全负责人，询问是否对资产管理要求文档化；
c) 应访谈资产管理员，询问是否依据资产的重要程度对资产进行赋值和标识管理，不同类别的资产是否采取不同的管理措施；
d) 应检查资产清单，查看其内容是否覆盖资产责任人、所属级别、所处位置和所属部门等方面；
e) 应检查资产安全管理制度，询问是否明确资产管理的责任部门、责任人等方面要求；
f) 应检查资产清单中的设备，查看其是否具有相应标识。

结果判定

a) 测评实施中 a）～f）均为肯定，则信息系统符合本单元测评项要求。

3) 介质管理(G2)

测评项

a) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理；
b) **所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放；（F2）**
c) 应对介质归档和查询等进行登记记录，管理员应根据存档介质的目录清单定期盘点；
d) **对于重要文档，如是纸质文档则应实行借阅登记制度，未经相关部门领导批准，任何人不得将文档转借、复制或对外公开，如是电子文档则应采用 OA 等电子化办公审批平台进行管理；（F2）**
e) 应对需要送出维修的介质，首先清除其中的敏感数据，防止信息的非法泄漏；
f) **对载有敏感信息存储介质的销毁，应报有关部门备案，由科技部门进行信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录。信息消除处理仅限于存储介质仍将在金融机构内部使用的情况，否则应进行信息的不可恢复性销毁；（F2）**
g) **应按照统一格式对技术文档进行编写并及时更新，达到能够依靠技术文档恢复系统正常运行的要求；（F2）**
h) **应制定移动存储介质使用规范，并定期核查移动存储介质的使用情况；（F2）**
i) 应根据所承载数据和软件的重要程度对介质进行分类和标识管理；
j) 应定期**对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。（F2）**

测评方式

访谈，检查。

测评对象

资产管理员，介质管理记录，各类介质。

测评实施

a) 应访谈资产管理员，询问介质的存放环境是否有保护措施，防止其被盗、被毁、被未授权修改以及信息的非法泄漏，是否有专人管理；
b) 应访谈资产管理员，询问是否对介质的使用管理要求文档化，是否根据介质的目录清单对介质的使用现状进行定期检查，是否对介质进行分类和标识管理；
c) 应访谈资产管理员，询问对送出维修或销毁介质之前是否做过安全处理（如清除其中的敏感数据）；
d) 应检查介质管理记录，查看其是否记录介质的存储、归档和借用等情况；
e) 应检查介质，查看是否对其进行了分类，并具有不同标识。

结果判定

a) 如果测评实施中 a）中在防火、防水、防盗等方面均有措施，则该项为肯定；
b) 测评实施中 a）～e）均为肯定，则信息系统符合本单元测评项要求。

4) 设备管理(G2)

测评项

a) 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；
b) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；
c) **新购置的设备应经过测试，测试合格后方能投入使用；（F2）**
d) **各机构科技部门负责对信息系统相关的各种设备（包括备份和冗余设备）、线路等进行维护管理；（F2）**
e) **应做好设备登记工作，制定设备管理规范，落实设备使用者的安全保护责任；（F2）**
f) **需要废止的设备，应由科技部门使用专用工具进行数据信息消除处理，如废止设备不再使用或调配到金融机构以外的单位，应由科技部门对其数据信息存储设备进行消磁或物理粉碎等不可恢复性销毁处理；（F2）**
g) **设备确需送外单位维修时，应彻底清除所存的工作相关信息，并与设备维修厂商签订保密协议，与密码设备配套使用的设备送修前必须请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息；（F2）**
h) **应制定规范化的故障处理流程，建立详细的故障日志(包括故障发生的时间、范围、现象、处理结果和处理人员等内容)；（F2）**
i) 应确保信息处理设备必须经过审批才能带离机房或办公地点。

测评方式

访谈，检查。

测评对象

资产管理员，系统管理员，审计员，服务器操作规程，设备审批、发放管理文档，设备使用管理文档，服务器操作日志。

测评实施

a) 应访谈资产管理员，询问是否对各类设施、设备指定专人或专门部门进行定期维护，由何部门/何人维护，维护周期多长；
b) 应访谈资产管理员，询问是否对设备选用的各个环节（选型、采购、发放等）进行审批控制，是否对设备带离机构进行审批控制，设备的操作和使用是否要求规范化管理；
c) 应访谈系统管理员，询问其对服务器是否进行正确配置，对服务器的操作是否按操作规程进行；
d) 应访谈审计员，询问对服务器的操作是否建立日志，日志文件如何管理，是否定期检查管理情况；
e) 应检查设备使用管理文档，查看其内容是否覆盖终端计算机、便携机和网络设备等使用、操作原则、注意事项等方面；
f) 应检查设备审批、发放管理文档，查看其内容是否对设备选型、采购和发放等环节的申报和审批作出规定；
g) 应检查服务器操作规程，查看其内容是否覆盖服务器如何启动、停止、加电、断电等操作。

结果判定

a) 测评实施中 a）～g）均为肯定，则信息系统符合本单元测评项要求。

5) 网络安全管理(G2)

测评项

a) 应建立网络安全运行管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期、**重要文件备份**等方面作出规定；
b) **应对网络环境运行状态进行巡检，巡检应保留记录，并有操作和复核人员的签名；（F2）**
c) **金融业网间互联安全实行统一规范、分级管理、各负其责的安全管理模式，未经金融机构科技主管部门核准，任何机构不得自行与外部机构实施网间互联；（F2）**
d) **应制定远程访问控制规范，确因工作需要进行远程访问的，应由访问发起机构科技部门核准，提请被访问机构科技部门（岗）开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施；（F2）**
e) **各机构以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经金融机构科技主管部门批准，不得在金融机构内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用；（F2）**
f) **信息安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不得对外公开，未经金融机构科技主管部门授权，任何外部机构与人员不得检测或扫描金融机构内部网络；**
g) **应制定网络接入管理规范，任何设备接入网络前，接入方案应经过科技部门的审核，审核批准后方可接入网络并分配相应的网络资源。**

测评方法

访谈，检查。

测评对象

安全主管，安全员，网络管理员，审计员，网络漏洞扫描报告，网络安全管理制度，系统外联授权书，网络审计日志。

测评实施

a) 查阅网络安全管理制度，查看其内容是否覆盖网络安全配置（包括网络设备的安全策略、授权访问、最小服务、升级与打补丁）、审计日志保存时间、升级与打补丁等方面应访谈安全主管，询问是否指定专人负责维护网络运行日志、监控记录和分析处理报警信息等网络安全管理工作；
b) 查阅网络管理员分工，并调阅网络安全运行维护档案；
c) 调阅网络管理员参加网络安全技术培训的文档，检查网间互联设备上配置，并与审批记录进行比对；
d) 在相关网络设备上检查远程访问控制设置，并调阅远程访问审核记录；
e) 调阅非法外联监控系统的记录，并在国际互联网用机上检查是否存储有敏感工作信息；
f) 检查网络视频服务是否作了跨区域限制，如可以跨区域点播是否经科技部门批准；
g) 应访谈网络管理员，询问是否根据厂家提供的软件升级版本对网络设备进行过升级，目前的版本号为多少，升级前是否对重要文件（帐户数据、配置数据等）进行备份，采取什么方式进行备份；是否对网络设备进行过漏洞扫描，对扫描出的漏洞是否及时修补；
h) 检查网络设备的配置文件备份；
i) 调阅网络变更记录中的审批、变更时间、配置参数备份；
j) 检查计算机接入国际互联网的申请记录上保密部门的授权；
k) 应访谈安全员，询问系统网络的外联种类有哪些（互联网、合作伙伴企业网、上级部门网络等），是否都得到授权与批准，由何部门/何人批准；
l) 应访谈审计员，询问是否规定网络审计日志的保存时间，多长时间；
m) 应检查网络漏洞扫描报告，查看其内容是否覆盖网络存在的漏洞、严重级别、原因分析和改进意见等方面；

n) 应检查网络安全管理制度，查看其是否覆盖网络设备的安全策略、授权访问、最小服务、升级与打补丁、维护记录、日志内容、日志保存时间等方面内容；
o) 应检查是否具有内部网络外联的授权批准书；应检查是否具有内部网络所有外联的授权批准书，调阅计算机变更用途记录；
p) 对互联网上下载的信息进行病毒检测；
q) 应检查在规定的保存时间范围内是否存在网络审计日志。

结果判定

a) 测评实施中 a）~q）均为肯定，则信息系统符合本单元测评项要求。

6) 系统安全管理(G2)

测评项

a) 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定；
b) 应根据业务需求和系统安全分析确定系统的访问控制策略；
c) **系统管理员不得对业务数据进行任何增加、删除、修改等操作，系统管理员确需对计算机系统数据库进行技术维护性操作的，应征得业务部门同意，并详细记录维护信息过程；（F2）**
d) **每年应至少进行一次漏洞扫描，对发现的系统安全漏洞及时进行修补；（F2）**
e) 应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；
f) 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作；
g) 应定期对运行日志和审计数据进行分析，以便及时发现异常行为。

测评方法

访谈，检查。

测评对象

安全主管，安全员，系统管理员，系统审计员，系统安全管理制度，系统审计日志，系统漏洞扫描报告。

测评实施

a) 应访谈安全主管，询问是否指定专人负责系统安全管理；
b) 应访谈系统管理员，询问是否对系统安全进行制度化管理；
c) 应访谈系统管理员，询问是否定期对系统安装安全补丁程序，在安装系统补丁前是否对重要文件（系统配置、系统用户数据等）进行备份，采取什么方式进行；是否对系统进行过漏洞扫描，发现漏洞是否及时修补；
d) 应访谈安全员，询问是否根据业务需求和系统安全分析确定系统访问控制策略；
e) 应访谈系统管理员，询问对系统用户是否进行分类，不同类别的用户是否只具有完成其工作的最低权限；对不常用的系统缺省用户是否采取了一定的处理手段阻止其继续使用（如删除或禁用）；
f) 应访谈审计员，询问是否规定系统审计日志的保存时间，多长时间；
g) 应检查在规定的保存时间范围内是否存在系统审计日志；
h) 应检查系统漏洞扫描报告，查看其内容是否覆盖系统存在的漏洞、严重级别、原因分析和改进意见等方面；
i) 应检查系统安全管理制度，查看其内容是否覆盖系统安全策略、授权访问、最小服务、升级与打补丁、维护记录、日志、系统帐户等方面做出具体要求。

结果判定

a) 测评实施中 a）~i）均为肯定，则信息系统符合本单元测评项要求。

7) 恶意代码防范管理(G2)

测评项

a) 应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；

b) 金融机构客户端应统一安装病毒防治软件，设置用户密码和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序；（F2）

c) 应指定专人对网络和主机进行恶意代码检测并保存检测记录；

d) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。

测评方法

访谈，检查。

测评对象

系统运维负责人，恶意代码防范管理文档，恶意代码检测记录。

测评实施

a) 应访谈系统运维负责人，询问是否对员工进行基本恶意代码防范意识的教育，如告知应及时升级软件版本，使用外来设备、网络上接收文件和外来计算机或存储设备接入网络系统之前进行病毒检查；

b) 应访谈系统运维负责人，询问是否指定专人对恶意代码进行检测，并保存记录；

c) 应检查恶意代码防范管理文档，查看其内容是否对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面做出规定；

d) 应检查是否具有恶意代码检测记录。

结果判定

a) 测评实施中 a）~ d）均为肯定，则信息系统符合本单元测评项要求。

8) 密码管理(G2)

测评项

a) 选用的密码产品和加密算法应符合国家相关密码管理政策规定；

b) **应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员必须是本机构在编的正式员工；（F2）**

c) **系统管理员、数据库管理员、网络管理员、业务操作人员均须设置口令密码，并定期更换，口令密码的强度应满足不同安全性要求。（F2）**

测评方法

访谈。

测评对象

安全员。

测评实施

a) 应访谈安全员，询问密码算法和密钥的使用是否遵照国家密码管理规定。

结果判定

a) 测评实施中 a）为肯定，则信息系统符合本单元测评项要求。

9) 变更管理(G2)

测评项

a) 应确认系统中要发生的重要变更，并制定相应的变更方案，**包括变更的组织结构与实施计划、操作步骤、影响分析等，以便于评估变更带来的风险**；系统发生重要变更前，应向主管领导申请，审批后方可实施变更，并在实施后向相关人员通告；

b) **变更前应做好系统和数据的备份。风险较大的变更，应在变更后对系统的运行情况进行跟踪。（F2）**

测评方法

访谈，检查。

测评对象

系统运维负责人，变更方案，变更管理制度，系统变更申请书。

测评实施

a) 应访谈系统运维负责人，询问是否制定变更方案指导系统执行变更，变更是否要求制度化管理；
b) 应访谈系统运维负责人，询问重要系统变更前是否得到有关领导的批准，由何人批准，对发生的变更情况是否通知了所有相关人员，以何种方式通知；
c) 应检查系统变更方案，查看其是否对变更类型、变更原因、变更过程、变更前评估等方面进行说明；
d) 应检查变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容；
e) 应检查重要系统的变更申请书，查看其是否有主管领导的批准。

结果判定

a) 测评实施中 a）～e）均为肯定，则信息系统符合本单元测评项要求。

10) 备份与恢复管理(G2)

测评项

a) 应对备份信息的备份方式、备份频度、存储介质和保存期等进行规范；
b) 根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；
c) **灾难备份中心的选址应综合考虑生产中心与灾难备份中心交通和电讯的便利性与多样性，以及灾难备份中心当地的业务与技术支持能力、电讯资源、地理地质环境、公共资源与服务配套能力等外部支持条件；（F2）**
d) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；
e) **恢复及使用备份数据时需要提供相关口令密码的，应妥善保管口令密码密封与数据备份介质；（F2）**
f) **应建立灾难恢复计划，定期开展灾难恢复培训，并根据实际情况进行灾难恢复演练。（F2）**

测评方法

访谈，检查。

测评对象

系统管理员，数据库管理员，网络管理员，备份管理文档，备份和恢复策略文档，备份设备操作流程文档。

测评实施

a) 应访谈系统管理员、数据库管理员和网络管理员，询问是否识别出需要定期备份的业务信息、系统数据及软件系统，主要有哪些；对其的备份工作是否以文档形式规范了备份方式、频度、介质、保存期等内容，数据备份和恢复策略是否文档化；
b) 应访谈系统管理员、数据库管理员和网络管理员，询问其对备份和冗余设备的安装、配置和启动工作是否根据一定的流程进行，是否指定专人对备份和冗余设备的有效性定期维护和检查，多长时间检查一次；
c) 应检查是否具有规定备份方式、频度、介质、保存期的文档；
d) 应检查数据备份和恢复策略文档，查看其内容是否覆盖数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面；

e) 应检查备份设备操作流程文档，查看其是否规定备份和冗余设备的安装、配置、启动、关闭等操作流程。

结果判定

a) 测评实施中 a）～e）均为肯定，则信息系统符合本单元测评项要求。

11) 安全事件处置(G2)

测评项

a) 应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

b) 应制定安全事件报告和处置管理制度，明确安全事件类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；

c) 应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分；

d) 应记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生；

e) **应建立有效的技术保障机制，确保在安全事件处置过程中不会因技术能力缺乏而导致处置中断或延长应急处置时间。（F2）**

测评方法

访谈，检查。

测评对象

系统运维负责人，安全事件报告和处置管理制度，安全事件定级文档，安全事件记录分析文档。

测评实施

a) 应访谈系统运维负责人，询问是否告知用户在发现安全弱点和可疑事件时应及时报告，是否对所报告的安全事件进行记录并保存；

b) 应访谈系统运维负责人，询问是否对安全事件处置进行制度化管理；

c) 应访谈系统运维负责人，询问本系统已发生的和需要防止发生的安全事件主要有哪几类，对识别出的安全事件是否根据其对系统的影响程度划分不同等级，划分为几级；

d) 应检查安全事件报告和处置管理制度，查看其内容是否明确与安全事件有关的工作职责，包括报告单位（人）、接报单位（人）和处置单位等职责；

e) 应检查安全事件定级文档，查看其内容是否明确安全事件的定义、安全事件等级划分的原则、等级描述等方面内容；

f) 应检查安全事件记录分析文档，查看其是否记录引发安全事件的原因，是否记录事件处理过程，**是否采取措施避免其再次发生。**

结果判定

a) 测评实施中 a）～f）为肯定，则信息系统符合本单元测评项要求。

12) 应急预案管理(G2)

测评项

a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括应急组织机构、启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容，**并由应急预案涉及的相关机构签字盖章**；

b) 应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次；

c) **金融机构应急领导小组应严格按照行业、机构的相关规定和要求对外发布信息，机构内其它部门或者个人不得随意接受新闻媒体采访或对外发表个人看法；（F2）**

d) **突发事件应急处置领导小组统一领导计算机系统的应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业信息安全监管部门；（F2）**

e) **应定期对原有的应急预案重新评估，并根据安全评估结果，定期修订、演练，并进行专项内部审计。（F2）**

测评方法

访谈，检查。

测评对象

系统运维负责人，应急响应预案文档。

测评实施

a) 应访谈系统运维负责人，询问是否制定不同事件的应急预案，是否对系统相关人员进行应急预案培训，培训内容是什么，多长时间举办一次；

b) 应检查应急响预案文档，查看其内容是否覆盖启动预案的条件、应急处理流程、系统恢复流程和事后教育等内容；

c) 调阅突发事件应急处置领导小组组织文件及职责。

结果判定

a) 测评实施中 a）～c）均为肯定，则信息系统符合本单元测评项要求。

系统运维管理测评对象主要为环境管理、资产管理、介质管理、设备管理、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置以及应急预案管理 12 个控制点相关的文件资料和工作记录，具体内容请参见附录 A.1.2.5。

7.1.2 第三级信息系统单元测评

7.1.2.1 安全技术测评

7.1.2.1.1 物理安全

1) 物理位置的选择(G3)

测评项

a) 机房和办公场地应选择在具有防震、**承重**、防风和防雨等能力的建筑内，**应选择交通、通信便捷地区**；

b) 机房场地应避免设在建筑物的顶层或地下室，以及用水设备的下层或隔壁；

c) **机房应避开火灾危险程度高的区域，周围100米内不得有加油站、煤气站等危险建筑和重要军事目标。（F3）**

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房，办公场地，机房场地设计/验收文档。

测评实施

a) 应访谈物理安全负责人，询问现有机房和办公场地（放置终端计算机设备）的环境条件是否能够满足信息系统业务需求和安全管理需求，是否具有基本的防震、防风和防雨等能力；询问机房场地是否符合选址要求；

b) 应访谈机房维护人员，询问是否存在因机房和办公场地环境条件引发的安全事件或安全隐患；如果某些环境条件不能满足，是否及时采取了补救措施；

c) 应检查机房和办公场地的设计/验收文档，查看是否有机房和办公场地所在建筑能够具有防震、防风和防雨等能力的说明；查看是否有机房场地的选址说明；查看是否与机房和办公场地实际情况相符合；

d) 应检查机房和办公场地是否在具有防震、防风和防雨等能力的建筑内；

e) 应检查机房场地是否避免在建筑物的高层或地下室，以及用水设备的下层或隔壁；

f) 应检查机房场地是否避免设在强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区；

g) 如果机房和办公场地的显示器、打印机等设备有敏感或密级信息输出，应检查设备摆放位置是否为不易被无关人员看到的隐蔽位置。

结果判定

a) 如果测评实施中a）中机房场地的选址符合不在建筑物的高层或地下室，以及用水设备的下层或隔壁；不在强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区等要求，则该项为肯定；

b) 如果测评实施中g）中“如果”条件不成立，则该项为不适用；

c) 测评实施中a）～g）均为肯定，则信息系统符合本单元测评项要求。

2) 物理访问控制(G3)

测评项

a) 机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员；

b) 需进入机房的来访人员应经过申请和审批流程，**由金融机构专人陪同**，并限制和监控其活动范围，**对于重要区域还应限制来访人员携带的随身物品；**

c) 应对机房划分区域进行管理，如将机房划分为核心区、生产区、辅助区，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域，**其中核心区是指装有关键业务系统服务器、主要通信设备、网络控制器、通讯保密设备和（或）系统打印设备的要害区域，生产区是指放置一般业务系统服务器、客户端（工作站）等设备的运行区域，辅助区是指放置供电、消防、空调等设备的区域；**

d) 重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

测评方式

访谈，检查。

测评对象

物理安全负责人，机房值守人员，机房设施（电子门禁系统），机房安全管理制度，值守记录，进入机房的登记记录，来访人员进入机房的审批记录，电子门禁系统记录。

测评实施

a) 应访谈物理安全负责人，了解具有哪些控制机房进出的能力；

b) 应访谈物理安全负责人，如果业务或安全管理需要，是否对机房进行了划分区域管理，是否对各个区域都有专门的管理要求；

c) 应访谈机房值守人员，询问是否认真执行有关机房出入的管理制度，是否对进入机房的人员记录在案；

d) 应检查机房安全管理制度，查看是否有关于机房出入方面的规定；

e) 应检查机房出入口是否有专人值守，是否有值守记录，以及进出机房的人员登记记录；检查机房是否存在电子门禁系统控制之外的出入口；

f) 应检查机房是否有进入机房的人员身份鉴别措施，如戴有可见的身份辨识标识；

g) 应检查是否有来访人员进入机房的审批记录；

h) 应检查机房区域划分是否合理，是否在机房重要区域前设置交付或安装等过渡区域；是否对不同区域设置不同机房或者同一机房的不同区域之间设置有效的物理隔离装置（如隔墙等）；

i) 应检查机房或重要区域配置的电子门禁系统是否有验收文档或产品安全资质；

j) 应检查电子门禁系统是否正常工作（不考虑断电后的工作情况）；查看电子门禁系统运行、维护记录；查看监控进入机房的电子门禁系统记录，是否能够鉴别和记录进入的人员身份。

结果判定

a) 如果有机房出入的管理制度，指定了专人在机房出入口值守，对进入的人员登记在案并进行身份鉴别，对来访人员须经批准、限制和监控其活动范围，机房或重要区域配置了电子门禁系统，则测评实施中a）为肯定；

b) 如果测评实施中b）认为没有必要对机房进行划分区域管理（如果安全管理需要，计算机设备宜采用分区布置，如可分为主机区、存贮器区、数据输入区、数据输出区、通信区和监控调度区等），则测评实施h）不适用；

c) 如果有机房出入的管理制度，指定了专人在机房出入口值守，对进入的人员登记在案并进行身份鉴别，对来访人员须经批准、限制和监控其活动范围，电子门禁系统管理，则测评实施中d）为肯定；

d) 测评实施中a）～ j）均为肯定，则信息系统符合本单元测评项要求。

3) 防盗窃和防破坏(G3)

测评项

a) 应将主要设备放置在机房内；

b) 应将设备或主要部件放入机柜中进行固定放置，并设置明显的标签，标注不易除去的标记；

c) 应将通信线缆铺设在隐蔽处，可架空铺设在地板下或置于管道中，**强弱电需隔离铺设并进行统一标识；**

d) 应对磁带、光盘等介质分类标识，存储在介质库或档案室的金属防火柜中；

e) **应建立机房设施与场地环境监控系统，进行24小时连续监视，并对监视录像进行记录，监控对象包括机房空调、消防、不间断电源（UPS）、门禁系统等重要设施，监控记录至少保存3个月；（F3）**

f) **机房主要设备工作间安装红外线探测设备等光电防盗设备，一旦发现有破坏性入侵即时显示入侵部位，并驱动声光报警装置。（F3）**

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，资产管理员，机房设施，设备管理制度文档，通信线路布线文档，防盗报警系统和监控报警系统的安装测评/验收报告。

测评实施

a) 应访谈物理安全负责人，采取了哪些防止设备、介质等丢失的保护措施；

b) 应访谈机房维护人员，询问主要设备放置位置是否做到安全可控,设备或主要部件是否进行了固定和标记，通信线缆是否铺设在隐蔽处；是否设置了冗余或并行的通信线路；是否对机房安装的防盗报警系统和监控报警系统进行定期维护检查；

c) 应访谈资产管理员，在介质管理中，是否进行了分类标识，是否存放在介质库或档案室中；询问对设备或存储介质携带出工作环境是否规定了审批程序、内容加密、专人检查等安全保护的措施；

d) 应检查主要设备是否放置在机房内或其它不易被盗窃和破坏的可控范围内；检查主要设备或设备的主要部件的固定情况，是否不易被移动或被搬走，是否设置明显的无法除去的标记；

e) 应检查通信线缆铺设是否在隐蔽处（如铺设在地下或管道中等）；

f) 应检查介质的管理情况，查看介质是否有正确的分类标识，是否存放在介质库或档案室中，并且进行分类存放（满足磁介质、纸介质等的存放要求），红外报警等措施；

g) **应检查机房防盗报警设施是否正常运行，并查看运行和报警记录；应检查机房的摄像、传感等监控报警系统是否正常运行，并查看运行记录、监控记录和报警记录。验证是否有相应的保存一段时间的记录**；

h) 应检查有关设备或存储介质携带出工作环境的审批记录，以及专人对内容加密进行检查的记录；

i) 应检查是否有设备管理制度文档，通信线路布线文档，介质管理制度文档，介质清单和使用记录，机房防盗报警设施的安全资质材料、安装测评/验收报告；查看文档中的条文是否与设备放置位置、设备或主要部件保护、通信线缆铺设等实际情况一致。

结果判定

a) 如果有设备管理制度，主要设备放置位置做到安全可控,设备或主要部件进行了固定和标记，通信线缆铺设在隐蔽处，介质分类标识并存储在介质库或档案室，机房安装了防止进入盗窃和破坏的利用光、电等技术设置的机房防盗报警系统；设备或存储介质携带出工作环境的审批程序、内容加密、专人检查等措施；机房设置了摄像、传感等监控报警系统，则测评实施中a）为肯定；

b) 测评实施中a）～i）均为肯定，则信息系统符合本单元测评项要求。

4) 防雷击(G3)

测评项

a) 机房建筑应设置避雷针等避雷装置；

b) 应设置**通过国家认证的**防雷保安器，防止感应雷；

c) 机房应设置交流电源地线。

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房设施，建筑防雷设计/验收文档。

测评实施

a) 应访谈物理安全负责人，询问为防止雷击事件导致重要设备被破坏采取了哪些防护措施，机房建筑是否设置了避雷装置，是否通过验收或国家有关部门的技术检测；询问机房计算机系统接地是否设置了专用地线；是否在电源和信号线增加有资质的避雷装置，以避免感应雷击；

b) 应访谈机房维护人员，询问机房建筑避雷装置是否有人定期进行检查和维护；询问机房计算机系统接地（交流工作接地、安全保护接地）是否符合**GB50174－2008**《电子计算机机房设计规范》的要求；

c) 应检查机房是否有建筑防雷设计/验收文档，机房接地设计/验收文档，查看是否有地线连接要求的描述，与实际情况是否一致；

d) 应检查机房是否在电源和信号线增加有资质的避雷装置,以避免感应雷击。

结果判定

a) 如果计算机机房防雷符合GB 50057－1994《建筑物防雷设计规范》（GB157《建筑防雷设计规范》）要求，而且如果是在雷电频繁区域，装设浪涌电压吸收装置等，则测评实施中a）为肯定；

b) 如果地线的引线和大楼的钢筋网及各种金属管道绝缘，交流工作接地的接地电阻不大于4Ω，安全保护地的接地电阻不大于4Ω；防雷保护地（处在有防雷设施的建筑群中可不设此地）的接地电阻不大于10Ω的要求，则测评实施中b）为肯定；

c) 测评实施中a）～d）均为肯定，则信息系统符合本单元测评项要求。

5) 防火(G3)

测评项

a) 机房应设置有效的自动灭火系统，**能够通过在机房内、基本工作房间内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位应设置烟感、温感等多种方式自动检测火情、自动报警；**

b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；

c) 机房应采取区域隔离防火措施，将重要设备与其他设备隔离开；

d) **机房应设置自动消防报警系统，并备有一定数量的对计算机设备影响小的气体灭火器。消防报警系统应具有与空调系统、新风系统、门禁系统联动的功能，一般工作状态为手动触发；（F3）**

e) **机房内所使用的设备线缆应符合消防要求，纸张，磁带和胶卷等易燃物品，要放置于金属制的防火柜内；（F3）**

f) **采用管网式洁净气体灭火系统或高压细水雾灭火系统的主机房，应同时设置两种火灾探测器，且火灾报警系统应与灭火系统联动；凡设置洁净气体灭火系统的主机房，应配置专用空气呼吸器或氧气呼吸器；（F3）**

g) **应定期检查消防设施，每半年至少组织一次消防演练；（F3）**

h) **机房应设置二个以上消防逃生通道，同时应保证机房内各分区到各消防通道的道路通畅，方便人员逃生时使用。在机房通道上应设置显著的消防标志。（F3）**

测评方式

访谈，检查

测评对象

物理安全负责人，机房值守人员，机房设施，机房安全管理制度，机房防火设计/验收文档，自动消防系统设计/验收文档。

测评实施

a) 应访谈物理安全负责人，询问机房是否设置了灭火设备，是否设置了自动检测火情、自动报警、自动灭火的自动消防系统，是否有专人负责维护该系统的运行，是否制订了有关机房消防的管理制度和消防预案，是否进行了消防培训；

b) 应访谈机房值守人员，询问对机房出现的消防安全隐患是否能够及时报告并得到排除；是否参加过机房灭火设备的使用培训，是否能够正确使用灭火设备和自动消防系统（喷水不适用于机房）；

c) 应检查机房是否设置了自动检测火情（如使用温感、烟感探测器）、自动报警、自动灭火的自动消防系统，摆放位置是否合理，有效期是否合格；应检查自动消防系统是否正常工作，查看运行记录、报警记录、定期检查和维修记录；

d) 应检查是否有机房消防方面的管理制度文档；检查是否有机房防火设计/验收文档；检查是否有机房自动消防系统的设计/验收文档，文档是否与现有消防配置状况一致；检查是否有机房及相关房间的建筑材料、区域隔离防火措施的验收文档或消防检查验收文档；

e) 应检查机房是否采取区域隔离防火措施，将重要设备与其他设备隔离开；

f) **应检查机房消防报警系统是否可与空调系统、新风系统、门禁系统、UPS等进行联动。**

结果判定

a) 测评实施中a）～e）均为肯定，则信息系统符合本单元测评项要求。

6) 防水和防潮(G3)

测评项

a) **水管不宜穿过机房屋顶，但若有穿过地板应当采取保护防范措施；**

b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

c) **为便于地下积水的转移，漏水隐患区域地面周围应设排水沟和地漏，当采用吊顶上布置空调风口时，风口位置不宜设置在设备正上方以避免水蒸气结露和渗透；**

d) 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房设施，建筑防水和防潮设计/验收文档，机房湿度记录，

除湿装置运行记录。

测评实施

a) 应访谈物理安全负责人，询问机房建设是否有防水防潮措施；如果机房内有上下水管安装，是否避免穿过屋顶和活动地板下，穿过墙壁和楼板的水管是否采取了的保护措施，如设置套管；在湿度较高地区或季节是否有人负责机房防水防潮事宜，配备除湿装置；

b) 应访谈机房维护人员，询问机房是否出现过漏水和返潮事件；如果机房内有上下水管安装，是否经常检查是否有漏水情况；如果出现机房水蒸气结露和地下积水的转移与渗透现象是否采取防范措施；

c) 应检查机房是否有建筑防水和防潮设计/验收文档，是否与机房防水防潮的实际情况一致；

d) 如果有管道穿过主机房墙壁和楼板处，应检查是否有必要的保护措施，如设置套管等；

e) 应检查机房是否不存在屋顶和墙壁等出现过漏水、渗透和返潮现象，机房及其环境是否不存在明显的漏水和返潮的威胁；如果出现漏水、渗透和返潮现象是否能够及时修复解决；

f) 如果在湿度较高地区或季节，应检查机房是否有湿度记录，是否有除湿装置并能够正常运行，是否有防止出现机房地下积水的转移与渗透的措施，是否有防水防潮处理记录和除湿装置运行记录，与机房湿度记录情况是否一致。

结果判定

a) 如果测评实施中d）、f）中“如果”条件不成立，则该项为不适用；

b) 测评实施中a）～f）均为肯定，则信息系统符合本单元测评项要求。

7) 防静电(G3)

测评项

a) 主要设备应采用必要的接地防静电措施；

b) 机房应采用防静电地板；

c) **主机房和辅助区内的工作台面宜采用导静电或静电耗散材料。（F3）**

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房设施，防静电设计/验收文档，湿度记录。

测评实施

a) 应访谈物理安全负责人，询问机房是否采用必要的接地等防静电措施，是否有控制机房湿度的措施；在静电较强地区的机房是否采取了有效的防静电措施；

b) 应访谈机房维护人员，询问是否经常检查机房湿度，并控制在GB2887中的规定的范围内；询问机房是否存在静电问题或因静电引起的故障事件；如果存在静电时是否及时采取消除静电的措施；

c) 应检查机房是否有防静电设计/验收文档，查看其描述内容与实际情况是否一致；

d) 应检查机房是否有安全接地，查看机房的相对湿度的记录是否符合GB2887中的规定，查看机房是否不存在明显的静电现象；

e) 如果在静电较强的地区，应检查机房是否了采用了如防静电地板、防静电工作台、以及静电消除剂和静电消除器等措施。

结果判定

a) 测评实施中e）中有效的防静电措施，可以包括如防静电地板、防静电工作台，或静电消除剂和静电消除器等措施的部分或全部，则该项为肯定；

b) 如果测评实施中e）中“如果”条件不成立，则该项为不适用；

c) 测评实施中a）～e）均为肯定，则信息系统符合本单元测评项要求。

8) 温湿度控制(G3)

测评项

a) **设备开机时主机房的温、湿度应执行A级，基本工作间可根据设备要求按A，B两级执行，其他辅助房间应按设备要求确定；**

开机时计算机机房内的温、湿度，应符合下表4的规定：

表4 机房温湿度三级要求

级别 / 项目	A 级		B 级
	夏天	冬天	全年
温度	23±1℃	20±2℃	18~28℃
相对湿度(开机时)	40%~55%		35%~75%
相对湿度(停机时)	40%~70%		20%~80%
温度变化率	< 5℃/h 并不得结露		< 10℃/h 并不得结露

b) **机房应采用专用空调设备，空调机应带有通信接口，通信协议应满足机房监控系统的要求；（F3）**

c) **空调系统的主要设备应有备份，空调设备在容量上应有一定的余量；（F3）**

d) **安装在活动地板上及吊顶上的送风口、回风口应采用难燃材料或非燃材料；（F3）**

e) **采用空调设备时，应设置漏水报警装置，并设置防水小堤，还应注意冷却塔、泵、水箱等供水设备的防冻、防火措施。（F3）**

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房设施，温湿度控制设计/验收文档，温湿度记录、运行记录和维护记录。

测评实施

a) 应访谈物理安全负责人，询问机房是否配备了恒温恒湿系统，保证温湿度能够满足计算机设备运行的要求，是否在机房管理制度中规定了温湿度控制的要求，是否有人负责此项工作；

b) 应访谈机房维护人员，询问是否定期检查和维护机房的温湿度自动调节设施，询问是否出现过温湿度影响系统运行的事件；

c) 应检查机房是否有温湿度控制设计/验收文档，是否能够满足系统运行需要，是否与当前实际情况相符合；

d) 应检查恒温恒湿系统是否能够正常运行，查看是否有温湿度记录、运行记录和维护记录；查看机房温、湿度是否满足GB 2887-89《计算站场地技术条件》的要求。

结果判定

a) 测评实施中a）～d）均为肯定，则信息系统符合本单元测评项要求。

9) 电力供应(A3)

测评项

a) 应在机房供电线路上配置稳压器和过电压防护设备；

b) **应按照双路供电的原则**设置冗余或并行的电力电缆线路为计算机系统供电；

c) **应建立发电机等备用供电系统（如备用发电机），以备供电系统临时停电时启用，并确保备用供电系统能在UPS供电时间内到位，每年需进行备用供电系统的模拟演练，并定期对备用电力供应设备进行检修和维护，确保其能正常使用；**

d) **UPS供电系统的冗余方式应采用N+1、N+2、2N、2(N+1) 等方式。没有建立柴油发电机应急供电系统的单位，UPS后备时间至少2小时；（F3）**

e) **机房内要求采用机房专用插座，机房内分别设置维修和测试用电源插座，两者应有明显区别标志。市电、UPS电源插座分开，满足负荷使用要求；（F3）**

f) **计算机系统应选用铜芯电缆，避免铜、铝混用。若不能避免时，应采用铜铝过渡头连接；（F3）**

g) **机房应设置应急照明和安全出口指示灯，供配电柜（箱）和分电盘内各种开关、手柄、按钮应标志清晰，防止误操作。（F3）**

测评方式

访谈，检查，测评。

测评对象

物理安全负责人，机房维护人员，机房设施，电力供应安全设计/验收文档，检查和维护记录。

测评实施

a) 应访谈物理安全负责人，询问计算机系统供电线路是否与其他供电分开；询问计算机系统供电线路上是否设置了稳压器和过电压防护设备；是否设置了短期备用电源设备（如UPS），供电时间是否满足系统最低电力供应需求；是否安装了冗余或并行的电力电缆线路（如双路供电方式）；是否建立备用供电系统（如备用发电机）；如无发电机应急供电系统UPS后备时间是否至少2小时；

b) 应访谈机房维护人员，询问是对在计算机系统供电线路上的稳压器、过电压防护设备、短期备用电源设备等进行定期检查和维护；是否能够控制电源稳压范围满足计算机系统运行正常；

c) 应访谈机房维护人员，询问冗余或并行的电力电缆线路（如双路供电方式）在双路供电切换时是否能够对计算机系统正常供电；是否定期检查备用供电系统（如备用发电机），是否能够在规定时间内正常启动和正常供电；

d) 应检查机房是否有电力供应安全设计/验收文档，查看文档中是否标明单独为计算机系统供电，配备稳压器、过电压防护设备、备用电源设备以及冗余或并行的电力电缆线路等要求；查看与机房电力供应实际情况是否一致；

e) 应检查计算机供电线路，查看计算机系统供电是否与其他供电分开；

f) 应检查机房，查看计算机系统供电线路上的稳压器、过电压防护设备和短期备用电源设备是否正常运行，查看供电电压是否正常；

g) 应检查是否有稳压器、过电压防护设备以及短期备用电源设备等电源设备的检查和维护记录，以及冗余或并行的电力电缆线路切换记录，备用供电系统运行记录；以及上述计算机系统供电的运行记录，是否能够符合系统正常运行的要求；

h) 应测评安装的冗余或并行的电力电缆线路（如双路供电方式），是否能够进行双路供电切换；

i) 应测评备用供电系统（如备用发电机）是否能够在规定时间内正常启动和正常供电；

结果判定

a) 测评实施中a）～i）均为肯定，则信息系统符合本单元测评项要求。

10) 电磁防护(S3)

测评项

a) 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；

b) 电源线和通信线缆应隔离铺设，避免互相干扰；

c) 应对关键设备和磁介质实施电磁屏蔽；

d) **计算机系统设备网络布线不得与空调设备、电源设备的无电磁屏蔽的布线平行；交叉时，应尽量以接近于垂直的角度交叉，并采取防延燃措施。(F3)**

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房设施，电磁防护设计/验收文档。

测评实施

a) 应访谈物理安全负责人，询问是否有防止外界电磁干扰和设备寄生耦合干扰的措施（包括设备外壳有良好的接地；电源线和通信线缆隔离等）；是否对处理秘密级信息的设备采取了防止电磁泄露的措施；
b) 应访谈机房维护人员，询问是否对设备外壳做了良好的接地；是否做到电源线和通信线缆隔离；是否出现过因电磁防护问题引发的故障；处理秘密级信息的设备是否为低辐射设备，是否安装了满足BMB4-2000《电磁干扰器技术要求和测评方法》要求的二级电磁干扰器；
c) 应检查机房是否有电磁防护设计/验收文档，查看其描述内容与实际情况是否一致；
d) 应检查机房设备外壳是否有安全接地；
e) 应检查机房布线，查看是否做到电源线和通信线缆隔离；
f) 应检查使用电磁干扰器的涉密设备开机，是否同时开启电磁干扰器。

结果判定

a) 测评实施中a）～f）均为肯定，则信息系统符合本单元测评项要求。

在内容上，物理安全测评实施过程涉及10个工作单元，具体检查表请参见附录A.2.1.1。

7. 1. 2. 1. 2 网络安全

1) 结构安全 (G3)

测评项

a) 应保证主要网络设备和通信线路冗余，主要网络设备业务处理能力能满足业务高峰期**需要的1倍以上，双线路设计时，宜由不同的服务商提供；**
b) 应保证网络各个部分的带宽满足业务高峰期需要；
c) 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；
d) 应绘制与当前运行情况相符的网络拓扑结构图；
e) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段，**生产网、互联网、办公网之间都应实现有效隔离；**
f) 应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；
g) 应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。

测评方式

访谈，检查，测评。

测评对象

网络管理员，边界和主要网络设备，网络拓扑图，网络设计/验收文档。

测评实施

a) 可访谈网络管理员，询问信息系统中的边界和主要网络设备的性能以及目前业务高峰流量情况；
b) 可访谈网络管理员，询问网段划分情况以及划分的原则；询问重要的网段有哪些，对重要网段的保护措施有哪些；
c) 可访谈网络管理员，询问网络的带宽情况；询问网络中带宽控制情况以及带宽分配的原则；
d) 可访谈网络管理员，询问网络设备上的路由控制策略措施有哪些，这些策略设计的目的是什么；
e) 应检查网络拓扑图，查看其与当前运行情况是否一致；
f) 应检查网络设计/验收文档，查看边界和主要网络设备的带宽占用报表是否有达到或超过处理能力记录；

g) 应检查网络设计/验收文档，查看是否有根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网和网段分配地址段的设计或描述；

h) 应检查边界和主要网络设备，查看是否配置路由控制策略（如使用静态路由等）建立安全的访问路径，在业务终端trace 业务服务器地址，查看访问路径所经节点是否符合路由控制策略；

i) 应检查边界和主要网络设备，检查是否将重要网段部署至网络边界与外部信息系统直连，重要网段与其他网段间是否使用防火墙、访问控制等手段隔离；

j) 应检查边界和主要网络设备，查看是否有对带宽进行控制的策略（如路由、交换设备上的QOS策略配置情况，专用的带宽管理设备的配置策略等），这些策略能否保证在网络发生拥堵的时候优先保护重要业务（如重要业务的主机的优先级要高于非重要业务的主机）；

k) 应测评网络拓扑结构，可通过网络拓扑结构自动发现、绘制工具，验证实际的网络拓扑结构和网络拓扑结构图是否一致；

l) 应测评业务终端与业务服务器之间的访问路径，可通过使用路由跟踪工具，验证业务终端与业务服务器之间的访问路径是否安全（如访问路径是否固定等）；

m) 应测评重要网段，验证其采取的网络地址与数据链路地址绑定措施**或数据链路层地址与交换机端口绑定的措施**是否有效（如试图使用非绑定地址，查看是否能正常访问等）；

n) 应测评网络带宽分配策略，可通过使用带宽测评工具，测评网络带宽分配是否有效。

结果判定

a) 如果测评实施中 f）～g）中缺少相应的文档，则该项为否定；

b) 测评实施中 e）～n）均为肯定，则信息系统符合本单元测评项要求。

2) 访问控制(G3)

测评项

a) 应在网络边界部署访问控制设备，启用访问控制功能；

b) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；

c) 应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制；

d) 应在会话处于非活跃一定时间或会话结束后终止网络连接；

e) 应在网络区域边界(互联网区域边界、外部区域边界和内部区域边界)对网络最大流量数及**网络并发连接数进行监控**；

f) 重要网段应采取技术手段防止地址欺骗；

g) 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户；

h) **应对拨号接入用户采用数字证书认证机制，**并限制具有拨号访问权限的用户数量；

i) **网络设备应按最小安全访问原则设置访问控制权限。（F3）**

测评方式

访谈，检查，测评。

测评对象

安全员，**网络管理员，**边界网络设备（包括网络安全设备）。

测评实施

a) 可访谈安全员，询问采取的网络访问控制措施有哪些；询问访问控制策略的设计原则是什么；询问访问控制策略是否做过调整，以及调整后和调整前的情况如何；

b) 应检查边界网络设备，查看其是否根据会话状态信息（如包括数据包的源地址、目的地址、源端口号、目的端口号、协议、出入的接口、会话序列号、发出信息的主机名等信息，并应支持地址通配符的使用）对数据流进行控制；

c) 应检查边界网络设备(业务网纵向防火墙和金融城市网防火墙)，查看其是否对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；
d) 应检查边界网络设备，查看是否能设置会话处于非活跃的时间或会话结束后自动终止网络连接；查看是否能设置网络最大流量数及网络并发连接数；
e) 应检查主要网络设备，查看是否有访问控制措施（如 VLAN，访问控制列表，MAC 地址绑定）控制便携式和移动式设备接入网络；
f) 应测评边界网络设备，可通过试图访问未授权的资源，验证访问控制措施对未授权的访问行为的控制是否有效（如可以使用扫描工具来探测等）；
g) 应测评主要网络设备，可通过试图用移动设备接入网络，验证网络设备的访问控制策略是否有效；
h) 应对网络访问控制措施进行渗透测评，可通过采用多种渗透测评技术（如 http 隧道等），验证网络访问控制措施是否不存在明显的弱点。

结果判定

a) 测评实施中 b）~ g）均为肯定，则信息系统符合本单元测评项要求。

3) 安全审计(G3)

测评项

a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；
b) 审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c) 应能够根据记录数据进行分析，并生成审计报表；
d) 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等，**保存时间不少于半年。**

测评方式

访谈，检查，测评。

测评对象

审计员，边界和主要网络设备。

测评实施

a) 可访谈审计员，询问网络系统中的边界和关键网络设备是否设置安全审计，包括哪些项；询问审计记录的主要内容有哪些；对审计记录的处理方式有哪些；
b) 应检查日志服务器或AAA服务器，查看审计记录是否包含网络系统中的网络设备运行状况、网络流量、用户行为等；
c) 应检查日志服务器或AAA服务器，查看事件审计记录是否包括：事件的日期和时间、用户、事件类型、事件成功情况，及其他与审计相关的信息；
d) 应检查日志服务器或AAA服务器，查看是否可以对特定事件，按照指定方式进行实时报警（如声音、EMAIL、短信等）；
e) 应检查日志服务器或AAA服务器，查看是否为授权用户浏览和分析审计数据具备生成报表的功能（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表；
f) 应测评日志服务器或 AAA 服务器，可通过以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），验证安全审计的覆盖情况和记录情况与要求是否一致；
g) 应测评日志服务器或 AAA 服务器，可通过以某个系统用户试图删除、修改或覆盖审计记录，验证安全审计的保护情况与要求是否一致。

结果判定

a) 测评实施中 b）~ g）均为肯定，则信息系统符合本单元测评项要求。

4) 边界完整性检查(S3)

测评项

a) 应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；
b) 应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

测评方式

访谈，检查，测评。

测评对象

安全员，**网络管理员**，边界完整性检查设备，边界完整性检查设备运行日志。

测评实施

a) 应检查边界完整性检查设备，查看是否有未安装非法外联客户端的计算机接入网络，若有是否采取进行定位、阻断；
b) 应检查边界完整性检查设备运行日志，**查看运行是否正常（查看是否持续对网络全网段进行监控）；**
c) 应检查边界完整性检查设备，查看是否设置了同时对非法联接到内网和非法联接到外网的行为进行监控；查看是否对发现的非法联接行为进行有效的阻断；
d) 应测评边界完整性检查设备，测评是否能有效的发现“非法外联”的行为（如产生非法外联的动作，查看边界完整性检查设备是否能够发现该行为）；
e) 应测评边界完整性检查设备，测评是否确定出“非法外联”设备的位置，并对其进行有效阻断（如产生非法外联的动作，查看边界完整性检查设备是否能够准确定位并阻断）；
f) 应测评边界完整性检查设备，测评是否能够对非授权设备私自联到网络的行为进行检查，并准确定出位置，对其进行有效阻断（如产生非法接入的动作，查看测评边界完整性检查设备是否能准确的发现，准确的定位并产生阻断）。

结果判定

a) 测评实施中 b）~ f）均为肯定，则信息系统符合本单元测评项要求。

5) 入侵防范(G3)

测评项

a) 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、注入式攻击、IP碎片攻击和网络蠕虫攻击等；
b) 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

测评方式

访谈，检查，测评。

测评对象

安全员，网络入侵防范设备。

测评实施

a) 可访谈安全员，询问网络入侵防范措施有哪些；是否有专门的设备对网络入侵进行防范；询问网络入侵防范规则库的升级方式；
b) 应检查网络入侵防范设备，查看是否能检测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击、网络蠕虫攻击等；
c) 应检查网络入侵防范设备，查看入侵事件记录中是否包括入侵的源IP、攻击的类型、攻击的目的、攻击的时间等；
d) 应检查网络入侵防范设备，查看其生产厂商是否为正规厂商，规则库是否为最新；
e) 应测评网络入侵防范设备，验证其监控策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备的反应）；

f) 应测评网络入侵防范设备，验证其报警策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备是否能实时报警）。

结果判定

a) 测评实施中b）~ f）均为肯定，则信息系统符合本单元测评项要求。

6) 恶意代码防范(G3)

测评项

a) 应在**与外单位和互联网连接的**网络边界处对恶意代码进行检测和清除；

b) 应定期对恶意代码防护设备进行代码库升级和系统更新。

测评方式

访谈，检查。

测评对象

安全员，防恶意代码产品，设计/验收文档，恶意代码产品运行日志。

测评实施

a) 可访谈安全员，询问系统中的网络防恶意代码防范措施是什么；询问恶意代码库的更新策略；询问防恶意代码产品的有哪些主要功能；询问系统是否发生过针对恶意代码入侵的安全事件；

b) 应检查设计/验收文档，查看其是否有在网络边界及核心业务网段处有对恶意代码采取相关措施（如是否有防病毒网关），防恶意代码产品是否有实时更新的功能的描述；

c) 应检查恶意代码产品运行日志，查看是否持续运行；

d) 应检查在网络边界及核心业务网段处是否根据恶意代码特征采取措施从网络层进行检测和清除；

e) 应检查防恶意代码产品，查看是否为正规厂商生产，运行是否正常，恶意代码库是否为最新版本；

f) 应检查防恶意代码产品的配置策略，查看是否支持恶意代码防范的统一管理（如查看是否为分布式部署，集中管理等）。

结果判定

a) 如果测评实施中b）中缺少相应的文档，则该项为否定；

b) 测评实施中b）~ f）均为肯定，则信息系统符合本单元测评项要求。

7) 网络设备防护(G3)

测评项

a) 应对登录网络设备的用户进行身份鉴别；

b) 应对网络设备的管理员登录地址进行限制；

c) 网络设备用户的标识应唯一；

d) 主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；

e) 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

f) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；

g) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；

h) 应实现设备特权用户的权限分离；

i) **应定期对网络设备的配置文件进行备份，发生变动时应及时备份；（F3）**

j) **应定期对网络设备运行状况进行检查；（F3）**

k) **对网络设备系统自带的的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端口开放审批制度；（F3）**

l) **应定期检验网络设备软件版本信息，避免使用软件版本中出现安全隐患；（F3）**

m) **应建立网络设备的时钟同步机制；（F3）**

n) **应定期检查并锁定或撤销网络设备中不必要的用户账号。（F3）**

测评方式

访谈，检查，测评。

测评对象

网络管理员，边界和主要网络设备。

测评实施

a) 可访谈网络管理员，是否对网络设备进行AAA认证或其他认证方式，若有登录AAA服务器，查看用户与管理员身份、权限是否匹配；
b) 应访谈网络管理员，询问网络设备的口令策略是什么；
c) 应检查边界和主要网络设备上的安全设置，查看其是否有对鉴别失败采取相应的措施的设置；查看是否有限制非法登录次数的功能；
d) 应检查边界和主要网络设备上的安全设置，查看是否对边界和主要网络设备的管理员登录地址进行限制；查看是否设置网络登录连接超时，并自动退出；查看是否实现设备特权用户的权限分离；查看是否对网络上的对等实体进行身份鉴别；应测评边界和主要网络设备的安全设置，验证鉴别失败处理措施（采用错误密码登录网络设备数次，观察是否结束会话、限制非法登录次数），对网络设备的管理员登录地址进行限制（如使用任意地址登录，观察网络设备的动作等）等功能是否有效；
e) 应测评边界和主要网络设备的安全设置，验证其网络登录连接超时自动退出的设置是否有效（如长时间连接无任何操作，观察观察网络设备的动作等）；
f) 应对边界和主要网络设备进行渗透测评，通过使用各种渗透测评技术（如口令猜解等）对网络设备进行渗透测评，验证网络设备防护能力是否符合要求；
g) 应登录远程登录网络设备，看是否采用22端口SSH方式或其他加密方式；
h) 应实现设备特权用户的权限分离；
i) 应上机查阅备份文件；
j) **应访谈网络管理员，并检查是否定期对网络设备运行状况进行检查；**
k) **应访谈网络管理员是否关闭不必要的网络设备服务；**
l) **应现场访谈网络管理员是否定期检验网络设备软件版本信息并有书面记录；**
m) **应访谈网络管理员是否定期检查并锁定或撤销网络设备中多余的用户账号。**

结果判定

a) 如网络设备的口令策略为口令长度8位以上，口令复杂（如规定字符应混有大、小写字母、数字和特殊字符），口令生命周期，新旧口令的替换要求（规定替换的字符数量）或为了便于记忆使用了令牌；则测评实施中b）满足测评要求；
b) 测评实施中b）~ m）均为肯定，则信息系统符合本单元测评项要求。

在内容上，网络安全层面测评实施过程涉及 7 个工作单元，具体内容请参见附录 A.2.1.2。

7. 1. 2. 1. 3 主机安全

1) 身份鉴别(S3)

测评项

a) 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性；
b) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；
c) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，**系统的静态口令应在7位以上并由字母、数字、符号等混合组成并每三个月更换口令；**
d) 应启用登录失败处理功能，可采取结束会话、限制登录间隔、限制非法登录次数和自动退出等措施；

e) **主机系统应对与之相连的服务器或终端设备进行身份标识和鉴别，当对服务器进行远程管理时，应采取加密措施，防止鉴别信息在网络传输过程中被窃听；（F3）**

f) 宜采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别，**例如以密钥证书、动态口令卡、生物特征等作为身份鉴别信息。**

测评方式

访谈，检查，测评。

测评对象

系统管理员，数据库管理员，主要服务器操作系统，主要数据库管理系统，服务器操作系统文档，数据库管理系统文档。

测评实施

a) 应检查服务器操作系统和数据库管理系统身份鉴别功能是否具有《信息安全等级保护操作系统安全技术要求》和《信息安全等级保护数据库管理系统安全技术要求》第二级以上或TCSEC C2级以上的测评报告；

b) 可访谈系统管理员，询问操作系统的身份标识与鉴别机制采取何种措施实现，目前系统提供了哪些身份鉴别措施和鉴别失败处理措施；

c) 可访谈数据库管理员，询问数据库的身份标识与鉴别机制采取何种措施实现，目前系统提供了哪些身份鉴别措施和鉴别失败处理措施；

d) 应检查服务器操作系统文档和数据库管理系统文档，查看用户身份标识的唯一性是由什么属性来保证的（如用户名或者 UID 等）；

e) 检查服务器操作系统和数据库的用户，以及隶属的组，或 UID 是否唯一。

f) 应检查主要服务器操作系统和主要数据库管理系统，查看是否提供了身份鉴别措施（如用户名和口令等），其身份鉴别信息是否具有不易被冒用的特点，检查账户密码策略设置，例如，口令足够长，口令复杂（如规定字符应混有大、小写字母、数字和特殊字符），口令生命周期，新旧口令的替换要求（如规定替换的字符数量）或为了便于记忆使用了令牌；

g) 应检查主要服务器操作系统和主要数据库管理系统，查看身份鉴别是否采用两个及两个以上身份鉴别技术的组合来进行身份鉴别（如采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技术和数字证书方式的身份鉴别技术中的任意两个组合）；

h) 应检查主要服务器操作系统和主要数据库管理系统，查看是否已配置了鉴别失败处理功能，并设置了非法登录次数的限制值，对超过限制值的登录终止其鉴别会话或临时封闭帐号；查看是否设置网络登录连接超时，并自动退出；查看是否设置鉴别警示信息；

i) 应检查主要服务器操作系统，查看服务器操作系统是否对与之相连的服务器或终端设备进行身份标识和鉴别；

j) 应测评主要服务器操作系统和主要数据库管理系统，可通过错误的用户名和口令试图登录系统，验证鉴别失败处理功能是否有效；

k) 应测评主要服务器操作系统和主要数据库管理系统，当进入系统时，是否先需要进行标识（如建立账号），而没有进行标识的用户不能进入系统；

l) 应测评主要服务器操作系统和主要数据库管理系统，添加一个新用户，其用户标识为系统原用户的标识（如用户名或 UID），查看是否不会成功；

m) 应测评主要服务器操作系统和主要数据库管理系统，删除一个用户标识，然后再添加一个新用户，其用户标识和所删除的用户标识一样（如用户名/UID），查看是否不能成功；

n) 应测评主要服务器操作系统，可通过使用未进行身份标识和鉴别的主机连接该服务器，验证主机系统能否正确地对与之相连的服务器或终端设备进行身份标识和鉴别；

o) 应渗透测评主要服务器操作系统，可通过使用口令破解工具等，对服务器操作系统进行用户口令强度检测，查看能否破解用户口令，破解口令后能否登录进入系统；

p) 应渗透测评主要服务器操作系统，验证已存在的非授权账号（如安装一些服务后会系统会增加的新账号）是否不能与系统进行交互式登录管理；

q) 应渗透测评主要服务器操作系统，测评是否存在绕过认证方式进行系统登录的方法，例如，认证程序存在的 BUG，社会工程或其他手段等。

结果判定

a) 如果测评实施中a）为肯定，则测评实施j）、k）和l）为肯定；

b) 如果不采用用户名/口令方式的进行身份鉴别，则测评实施中n）不适用；

c) 如果测评实施中o）中能破解口令，则该项为否定；

d) 如果测评实施中p）中没有常见的绕过认证方式进行系统登录的方法，则该项为肯定；

e) 测评实施中e）～m）均为肯定，则信息系统符合本单元测评项要求。

2) 访问控制(S3)

测评项

a) 应启用访问控制功能，依据安全策略控制用户对资源的访问；

b) 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；

c) 应实现操作系统和数据库系统特权用户的权限分离；

d) 应禁用或严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；

e) 应及时删除多余的、过期的帐户，避免共享帐户的存在；

f) 应对重要信息资源设置敏感标记；

g) 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

测评方式

检查，测评。

测评对象

主要服务器操作系统，主要数据库管理系统，安全策略。

测评实施

a) 应检查服务器操作系统和数据库管理系统的自主访问控制功能是否具有《信息安全等级保护操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第二级以上或TCSEC C2级以上的测评报告；

b) 应检查服务器操作系统和数据库管理系统的安全策略，查看是否明确主体（如用户）以用户和/或用户组的身份规定对客体（如文件或系统设备,目录表和存取控制表访问控制等）的访问控制，覆盖范围是否包括与信息安全直接相关的主体（如用户）和客体（如文件，数据库表等）及它们之间的操作（如读、写或执行）；

c) 应检查服务器操作系统和数据库管理系统的安全策略，查看是否明确主体（如用户）具有非敏感标记（如角色），并能依据非敏感标记规定对客体的访问；

d) 应检查主要服务器操作系统和主要数据库管理系统的访问控制列表，查看授权用户中是否不存在过期的帐号和无用的帐号等；访问控制列表中的用户和权限，是否与安全策略相一致；

e) 应检查主要服务器操作系统和主要数据库管理系统，查看客体（如文件,数据库表、视图、存储过程和触发器等）的所有者是否可以改变其相应访问控制列表的属性，得到授权的用户是否可以改变相应客体访问控制列表的属性；

f) 应检查主要服务器操作系统和主要数据库管理系统，查看特权用户的权限是否进行分离，如可分为系统管理员、安全管理员、安全审计员等；查看是否采用最小授权原则（如系统管理员只能对系统进行维护，安全管理员只能进行策略配置和安全设置，安全审计员只能维护审计信息等）；

g) 应检查主要服务器操作系统和主要数据库管理系统，查看在系统管理员、安全管理员、安全审计员之间是否设置了相互制约关系（如系统管理员、安全管理员等不能对审计日志，安全审计员管理不了审计数据的开启、关闭、删除等重要事件的审计日志等）；

h) 应查看主要服务器操作系统和主要数据库管理系统，查看匿名/默认用户的访问权限是否已被禁用或者严格限制（如限定在有限的范围内）；

i) 应测评主要服务器操作系统和主要数据库管理系统，依据系统访问控制的安全策略，试图以未授权用户身份/角色访问客体，验证是否不能进行访问。

结果判定

a) 如果测评实施中a）为肯定，则测评实施e）和i）为肯定；

b) 测评实施中b）～i）均为肯定，则信息系统符合本单元测评项要求。

3) 安全审计(G3)

测评项

a) 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；

b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用、**账号的分配、创建与变更、审计策略的调整、审计系统功能的关闭与启动**等系统内重要的安全相关事件；

c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等，**并定期备份审计记录，涉及敏感数据的记录保存时间不少于半年**；

d) 应能够根据记录数据进行分析，并生成审计报表；

e) 应保护审计进程，避免受到未预期的中断；

f) 应保护审计记录，避免受到未预期的删除、修改或覆盖等。

测评方式

访谈，检查，测评。

测评对象

安全审计员，主要服务器操作系统，重要终端操作系统，主要数据库管理系统。

测评实施

a) 可访谈安全审计员，询问主机系统是否设置安全审计；询问主机系统对事件进行审计的选择要求和策略是什么；对审计日志的处理方式有哪些；

b) 应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看当前审计范围是否覆盖到每个用户；

c) 应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、系统资源的异常使用、重要系统命令的使用（如删除客体）等；

d) 应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容；

e) 应检查主要服务器和重要终端操作系统，查看是否为授权用户浏览和分析审计数据提供专门的审计工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表；

f) 应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看能否对特定事件指定实时报警方式（如声音、EMAIL、短信等）；

g) 应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计跟踪设置是否定义了审计跟踪极限的阈值，当存储空间被耗尽时，能否采取必要的保护措施，例如，报警并导出、丢弃未记录的审计信息、暂停审计或覆盖以前的审计记录等；

h) 应测评主要服务器操作系统、重要终端操作系统和主要数据库管理系统，可通过非法终止审计功能或修改其配置，验证审计功能是否受到保护；

i) 应测评主要服务器操作系统、重要终端操作系统和主要数据库管理系统，在系统上以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），测评安全审计的覆盖情况和记录情况与要求是否一致；

j) 应测评主要服务器操作系统、重要终端操作系统和主要数据库管理系统，在系统上以某个系统用户试图删除、修改或覆盖审计记录，测评安全审计的保护情况与要求是否一致。

结果判定

a) 测评实施中b）～j）均为肯定，则信息系统符合本单元测评项要求。

4) 剩余信息保护(S3)

测评项

a) 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他**使用人员**前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他**使用人员**前得到完全清除。

测评方式

访谈，检查。

测评对象

系统管理员，数据库管理员，主要服务器操作系统维护/操作手册，主要数据库管理系统维护/操作手册。

测评实施

a) 应检查服务器操作系统和数据库管理系统的剩余信息保护（用户数据保密性保护/客体重用）功能是否具有《信息安全等级保护 操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第二级以上的测评报告；

b) 应与系统管理员访谈，询问操作系统用户的鉴别信息存储空间，被释放或再分配给其他用户前是否得到完全清除；系统内的文件、目录等资源所在的存储空间，被释放或重新分配给其他用户前是否得到完全清除；

c) 应与数据库管理员访谈，询问数据库管理员用户的鉴别信息存储空间，被释放或再分配给其他用户前是否得到完全清除；数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前是否得到完全清除；

d) 应检查主要操作系统和主要数据库管理系统维护操作手册，查看是否明确用户的鉴别信息存储空间，被释放或再分配给其他用户前的处理方法和过程；文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前的处理方法和过程。

结果判定

a) 如果测评实施中 a）为肯定，则测评实施 b）～d）为肯定；

b) 测评实施中 b）～d）均为肯定，则信息系统符合本单元测评项要求。

5) 入侵防范(G3)

测评项

a) 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

b) 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施**或在检测到完整性即将受到破坏时进行事前阻断；**

c) 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器、系统软件预防性维护服务等方式保持系统补丁及时得到更新。

测评方式

访谈，检查，测评。

测评对象

系统管理员，主要服务器系统。

测评实施

a) 应与系统管理员访谈，询问主机系统是否采取入侵防范措施，入侵防范内容是否包括主机运行监视、资源使用超过值报警、特定进程监控、入侵行为检测、完整性检测等方面内容；
b) 应与系统管理员访谈，询问入侵防范产品的厂家、版本和在主机系统中的安装部署情况；询问是否进行过部署的改进或者更换过产品，是否按要求（如定期或实时）进行产品升级；
c) 应检查主要服务器系统，查看是否进行主机运行监视，监视的内容是否包括主机的 CPU、硬盘、内存、网络等资源的使用情况，并给出资源使用历史记录；
d) 应检查主要服务器系统，查看是否设定资源报警阈值（如 CPU、硬盘、内存、网络等资源的报警阈值）以便在资源使用超过规定数值时发出报警，并查看报警方式有哪些；
e) 应检查主要服务器系统，查看是否对特定进程（包括主要的系统进程，如 WINDOWS 的 Explorer 进程）进行监控，是否可以设定非法进程列表；
f) 应检查主要服务器系统，查看是否对主机账户（如系统管理员）进行控制，以限制对重要账户的添加和更改等；
g) 应检查主要服务器系统，查看能否记录攻击者的源 IP、攻击类型、攻击目标、攻击时间等，在发生严重入侵事件时是否提供报警（如声音、短信、EMAIL 等）；
h) 应测评主要服务器系统，试图运行非法进程，验证其能否限制非法进程的运行；试图添加或更改重要账户，验证主机能否限制重要账户的添加和更改；
i) 应测评主要服务器系统，试图破坏重要程序（如执行系统任务的重要程序）的完整性，验证主机能否检测到重要程序的完整性受到破坏。

结果判定

a) 如果测评实施中 b）中的厂家为正规厂家（如有销售许可），版本号较新，改进合理，定期升级，则该项为肯定；
b) 测评实施中 a）~ f）均为肯定，则信息系统符合本单元测评项要求。

6) 恶意代码防范(G3)

测评项

a) **应安装国家安全部门认证的正版防恶意代码软件，对于依附于病毒库进行恶意代码查杀的软件应及时更新防恶意代码软件版本和恶意代码库，对于非依赖于病毒库进行恶意代码防御的软件，如主动防御类软件，应保证软件所采用的特征库有效性与实时性，对于某些不能安装相应软件的系统可以采取其他安全防护措施来保证系统不被恶意代码攻击；**
b) 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；
c) 应支持防恶意代码的统一管理；
d) **应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。（F3）**

测评方式

访谈，检查，测评。

测评对象

系统安全员，主要服务器系统，主要终端系统，网络防恶意代码产品，主机安全设计/验收文档。

测评实施

a) 应访谈系统安全员，询问主机系统是否采取恶意代码实时检测与查杀措施，恶意代码实时检测与查杀措施的部署情况如何，因何改进过部署或者更换过产品，是否按要求（如定期或实时）进行产品升级；
b) 应检查主机恶意代码防范方面的设计/验收文档，查看描述的安装范围是否包括服务器和终端设备（包括移动设备）；
c) 应检查主要服务器系统和主要终端系统，查看是否安装实时检测与查杀恶意代码的软件产品，查看实时检测与查杀恶意代码的软件产品是否支持恶意代码防范的统一管理功能，查看检测与查杀恶意代码软件产品的厂家、版本号和恶意代码库名称；
d) 应检查网络防恶意代码产品，查看厂家、版本号和恶意代码库名称。

结果判定

a) 如果测评实施中a）中恶意代码实时检测与查杀措施的部署到所有服务器和重要终端，则该项为肯定；
b) 测评实施中a）~c）均为肯定，检查发现主机系统防恶意代码产品与网络防恶意代码产品使用不同的恶意代码库（如厂家、版本号和恶意代码库名称不相同等），则信息系统符合本单元测评项要求。

7) 资源控制(A3)

测评项

a) 应通过设定终端接入方式、网络地址范围等条件限制终端登录；
b) 应根据安全策略设置登录终端的操作超时锁定；
c) 应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况；
d) 应限制单个用户对系统资源的最大或最小使用限度；
e) 应能够对系统的服务水平降低到预先规定的最小值进行检测和报警；
f) 所有的服务器应全部专用化，不使用服务器进行收取邮件、浏览互联网操作。（F3）

测评方式

检查，测评。

测评对象

主要服务器操作系统。

测评实施

a) 应检查主要服务器操作系统，查看是否限制单个用户的多重并发会话数量；查看是否设置登录终端的操作超时锁定和鉴别失败锁定，以及是否规定解锁或终止方式；查看是否配置了终端接入方式、网络地址范围等条件限制终端登录；
b) 上机检查：主机操作系统、数据库、重要应用系统是否根据安全策略设置登录终端的操作超时锁定；
c) 应检查主要服务器操作系统，查看是否对一个时间段内可能的并发会话连接数进行限制，是否禁止同一用户账号在同一时间内并发登录，是否限制单个用户对系统资源（如 CPU、内存和硬盘等）的最大或最小使用限度；
d) 在上机检查或在运维监控系统中查看是否对重要服务器的相关资源进行监测。
e) 应检查主要服务器操作系统，查看是否在服务水平降低到预先规定的最小值时，能检测和报警，报警的方式有哪些，能否已根据安全策略设定主体（如进程）的服务优先级，并根据优先级分配系统资源，保证优先级低的主体处理能力不会影响到优先级高的主体的处理能力；
f) 应测评主要服务器操作系统，任选一个用户，登录服务器，试图发出多重并发会话，验证系统是否限制单个用户的多重并发会话；试图在一段时间内建立一些并发会话连接，验证系统是否对一定时间段内的并发会话连接数进行限制；

g) 应测评重要服务器操作系统，任选一个用户帐户，登录服务器，用不同的终端接入方式、网络地址试图登录服务器，验证重要服务器操作系统是否通过终端接入方式、网络地址范围等条件限制终端登录；

h) 应测评主要服务器操作系统，试图使服务水平降低到预先规定的最小值，验证系统能否正确检测和报警；

i) 应测评主要服务器操作系统，任选一个用户，登录服务器，在一定时间内不进行任何动作，验证主要服务器操作系统能否对操作超时的终端进行锁定；任选一个用户，可通过多次失败登录服务器，验证服务器能否对鉴别失败的终端进行锁定，锁定后能否按照规定的解锁或终止方式进行解锁或终止。

结果判定

a) 测评实施中 a）~ i）均为肯定，则信息系统符合本单元测评项要求。

主机安全重点测评操作系统包括各网站服务器、应用服务器和数据库服务器等操作系统在内容上，系统安全层面实施过程涉及 7 个工作单元，具体内容请参见附录 A.2.1.3。

7. 1. 2. 1. 4 应用安全

1) 身份鉴别(S3)

测评项

a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；

b) **应对同一用户的关键操作采用两种或两种以上组合的鉴别技术实现用户身份鉴别；如使用磁卡、IC卡、动态密码卡、动态口令设备、手机短信动态密码、指纹识别等方式加强鉴别；**

c) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

d) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

e) 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数；

f) **应用软件应能在指定的闲置时间间隔到期后，自动锁定客户端的使用；（F3）**

g) **对于系统自动分配或者预设的强度较弱的初始密码，系统应强制用户首次登录时修改初始密码；（F3）**

h) **修改密码时，不允许新设定的密码与旧密码相同。（F3）**

测评方式

访谈，检查，测评。

测评对象

系统管理员，主要应用系统，设计/验收文档，操作规程和操作记录。

测评实施

a) 可访谈系统管理员，询问应用系统是否采取身份标识和鉴别措施，具体措施有哪些；系统采取何种措施防止身份鉴别信息被冒用（如复杂性混有大、小写字母、数字和特殊字符，口令周期等）；

b) 检查应用系统是否有用户管理模块，是否对系统的用户账号和口令强度进行强制性要求；

c) 可访谈系统管理员，询问应用系统是否具有登录失败处理的功能，是如何进行处理的；询问应用系统对用户标识在整个生命周期内是否具有唯一性（如UID、用户名或其他信息在系统中是唯一的，用该标识在整个生命周期内能唯一识别该用户）；

d) 应检查设计/验收文档，查看文档中是否有系统采取了唯一标识（如用户名、UID或其他属性）的描述；

e) 应检查操作规程和操作记录，查看其是否有身份标识和鉴别的操作规程、审批记录和操作记录；

f) 应检查主要应用系统，查看其是否采用了两个及两个以上身份鉴别技术的组合来进行身份鉴别（如采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技术中的任意两个组合）；对有抗抵赖要求的系统，查看其是否采用数字证书方式的身份鉴别技术；

g) 应检查主要应用系统，查看其是否配备身份标识（如建立账号）和鉴别（如口令等）功能；查看其其身份鉴别信息是否具有不易被冒用的特点，例如复杂性（如规定字符应混有大、小写字母、数字和特殊字符）或为了便于记忆使用了令牌；

h) 应检查主要应用系统，查看其是否配备并使用登录失败处理功能（如登录失败次数超过设定值，系统自动退出等）；

i) 应测评主要应用系统，验证其登录失败处理，非法登录次数限制，登录连接超时自动退出等功能是否有效；

j) 应测评主要应用系统，验证其是否及时清除存储空间中动态使用的鉴别信息（如登录系统，退出系统后重新登录系统，查看上次登录的鉴别信息是否存在）；

k) 应测评主要应用系统，验证其是否有鉴别警示功能（如系统有三次登录失败则锁定该用户的限制，则应给用户必要的提示）；

l) 应渗透测评主要应用系统，测评身份鉴别信息是否不易被冒用（如通过暴力破解或其他手段进入系统，对WEB系统可采用SQL注入等绕过身份鉴别的方法）；

m) **应测评系统初始密码是否在首次登录时被要求强制修改；**

n) **应测评修改密码是否与旧密码相同。**

结果判定

a) 如果测评实施中c）中相关文档有用户唯一性标识的描述，则该项为肯定；

b) 如果测评实施中d）中缺少相应的文档，则该项为否定；

c) 测评实施中c）~n）均为肯定，则信息系统符合本单元测评项要求。

2) 访问控制(S3)

测评项

a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；

b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；

c) 应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限；

d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；

e) **应有生产系统关键账户与权限的关系表；（F3）**

f) **宜**具有对重要信息资源设置敏感标记的功能；

g) **宜**依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

测评方式

访谈，检查，测评。

测评对象

系统管理员，主要应用系统。

测评实施

a) 可访谈系统管理员，询问业务系统是否提供访问控制措施，具体措施有哪些，自主访问控制的粒度如何；

b) 应检查主要应用系统，查看系统是否提供访问控制机制；是否依据安全策略控制用户对客体（如文件和数据库中的数据）的访问；

c) 应检查主要应用系统，查看其自主访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作；自主访问控制的粒度是否达到主体为用户级，客体为文件、数据库表级（如数据库表、视图、存储过程等）；

d) 应检查主要应用系统，查看应用系统是否有对授权主体进行系统功能操作和对数据访问权限进行设置的功能；
e) 应检查主要应用系统，查看其特权用户的权限是否分离（如将系统管理员、安全员和审计员的权限分离），权限之间是否相互制约（如系统管理员、安全管理员等不能对审计日志进行管理，安全审计员不能管理审计功能的开启、关闭、删除等重要事件的审计日志等）；
f) 应检查主要应用系统，查看其是否有限制默认用户访问权限的功能，并已配置使用；
g) 应测评主要应用系统，可通过用不同权限的用户登录，查看其权限是否受到应用系统的限制，验证系统权限分离功能是否有效；
h) 应测评主要应用系统，可通过授权主体设置特定用户对系统功能进行操作和对数据进行访问的权限，然后以该用户登录，验证用户权限管理功能是否有效；
i) 应测评主要应用系统，可通过用默认用户（默认密码）登录，并用该用户进行操作（包括合法、非法操作），验证系统对默认用户访问权限的限制是否有效；
j) 应渗透测评主要应用系统，测评自主访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作（如试图绕过系统访问控制机制等操作）。

结果判定

a) 测评实施中b）~j）均为肯定，则信息系统符合本单元测评项要求。

3) 安全审计(G3)

测评项

a) 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；
b) 应保证无法单独中断审计进程，**不提供**删除、修改或覆盖审计记录**的功能**；
c) 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等，**并定期备份审计记录，保存时间不少于半年**；
d) 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能；
e) 对于从互联网客户端登陆的应用系统，应在每次用户登录时提供用户上一次成功登录的日期、时间、方法、位置等信息，以便用户及时发现可能的问题。（F3）

测评方式

访谈，检查，测评。

测评对象

安全审计员，主要应用系统。

测评实施

a) 可访谈安全审计员，询问应用系统是否有安全审计功能，对事件进行审计的选择要求和策略是什么，对审计日志的保护措施有哪些；
b) 应检查主要应用系统，查看其当前审计范围是否覆盖到每个用户；
c) 应检查主要应用系统，查看其审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、系统资源的异常使用、重要系统命令的使用（如删除客体）等；
d) 应检查主要应用系统，查看其审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容；
e) 应检查主要应用系统，查看其是否为授权用户浏览和分析审计数据提供专门的审计工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表；
f) 应检查主要应用系统，查看其能否对特定事件指定实时报警方式（如声音、EMAIL、短信等）；
g) 应测评主要应用系统，可通过非法终止审计功能或修改其配置，验证审计功能是否受到保护；

h) 应测评主要应用系统，在系统上以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），测评安全审计的覆盖情况和记录情况与要求是否一致；

i) 应测评主要应用系统，在系统上以某个系统用户试图删除、修改或覆盖审计记录，验证安全审计的保护情况与要求是否一致。

结果判定

a) 测评实施中b）～i）均为肯定，则信息系统符合本单元测评项要求。

4) 剩余信息保护(S3)

测评项

a) 应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

测评方式

访谈，检查，测评。

测评对象

系统管理员，设计/验收文档。

测评实施

a) 可访谈系统管理员，询问系统是否采取措施保证对存储介质中的残余信息进行删除（无论这些信息是存放在硬盘上还是在内存中），具体措施有哪些；

b) 应检查设计/验收文档，查看其是否有关于系统在释放或再分配鉴别信息所在存储空间给其他用户前如何将其进行完全清除（无论这些信息是存放在硬盘上还是在内存中）的描述；

c) 应检查设计/验收文档，查看其是否有关于释放或重新分配系统内文件、目录和数据库记录等资源所在存储空间给其他用户前如何进行完全清除的描述；

d) 应测评主要应用系统，用某用户登录系统并进行操作后，在该用户退出后用另一用户登录，试图操作（读取、修改或删除等）其他用户产生的文件、目录和数据库记录等资源，查看是否成功，验证系统提供的剩余信息保护功能是否正确（确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除）。

结果判定

a) 如果测评实施中b）～c）缺少相关材料，则该项为否定；

b) 测评实施中b）～d）均为肯定，则信息系统符合本单元测评项要求。

5) 通信完整性(S3)

测评项

a) 应采用密码技术保证通信过程中**关键**数据的完整性。

测评方式

访谈，检查，测评。

测评对象

安全员，主要应用系统，设计/验收文档。

测评实施

a) 可访谈安全员，询问业务系统是否有数据在传输过程中进行完整性保证的操作，具体措施是什么；

b) 应检查设计/验收文档，查看其是否有通信完整性的说明，如果有则查看其是否有系统是根据校验码判断对方数据包的有效性的，用密码计算通信数据报文的报文验证码的描述；

c) 应测评主要应用系统，可通过获取通信双方的数据包，查看通信报文是否含有验证码。

结果判定

a) 测评实施中b）~c）均为肯定，则信息系统符合本单元测评项要求。

6) 通信保密性(S3)

测评项

a) 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；

b) **对于通过互联网对外提供服务的系统，在**通信过程中的整个报文或会话过程，**应通过专用的通信协议或加密的方式保证通信过程的机密性**进行加密。

测评方式

访谈，检查，测评。

测评对象

安全员，主要应用系统，相关证明材料（证书）。

测评实施

a) 可访谈安全员，询问业务系统数据在存储和传输过程中是否采取保密措施（如在通信双方建立连接之前利用密码技术进行会话初始化验证，在通信过程中对敏感信息字段进行加密等），具体措施有哪些；

b) 应检查相关证明材料（证书），查看应用系统采用的密码算法是否符合国家有关部门要求；

c) 应测评主要应用系统，查看当通信双方中的一方在一段时间内未作任何响应，另一方是否能自动结束会话；系统是否能在通信双方建立会话之前，利用密码技术进行会话初始化验证（如SSL建立加密通道前是否利用密码技术进行会话初始验证）；在通信过程中，是否对整个报文或会话过程进行加密；

d) 应测评主要应用系统，通过通信双方中的一方在一段时间内未作任何响应，查看另一方是否能自动结束会话，测评当通信双方中的一方在一段时间内未作任何响应，另一方是否能自动结束会话的功能是否有效；

e) 应测评主要应用系统，通过查看通信双方数据包的内容，查看系统在通信过程中，对整个报文或会话过程进行加密的功能是否有效。

结果判定

a) 如果测评实施中b）缺少相关材料，则该项为否定；

b) 测评实施中b）~e）均为肯定，则信息系统符合本单元测评项要求。

7) 抗抵赖(G3)

测评项

a) 应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能，**原发证据包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录，交易系统还应能够详细记录用户合规交易数据，如业务流水号、账户名、IP地址、交易指令等信息以供审计，并能够追溯到用户**；

b) 应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能，**接受证据应用系统操作与管理记录至少应包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录，交易系统还应能够详细记录用户合规交易数据，如业务流水号、账户名、IP地址、交易指令等信息以供审计，并能够追溯到用户。**

测评方式

访谈，测评。

测评对象

安全员，主要应用系统。

测评实施

a) 检查系统在传送数据时是否采用数字签名、是否产生有效的认证码等抗抵赖的措施；

b) 应测评主要应用系统，通过双方进行通信，查看系统是否提供在请求的情况下为数据原发者或接收者提供数据原发证据的功能；是否提供在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

结果判定

a) 测评实施中b）为肯定，则信息系统符合本单元测评项要求。

8) 软件容错(A3)

测评项

a) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；

b) 应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复；

c) 应能够有效屏蔽系统技术错误信息，不将系统产生的错误信息直接反馈给客户。（F3）

测评方式

访谈，检查，测评。

测评对象

系统管理员，主要应用系统。

测评实施

a) 可访谈系统管理员，询问业务系统是否有保证软件具有容错能力的措施（如对人机接口输入或通过通信接口输入的数据进行有效性检验等），具体措施有哪些；

b) 应检查主要应用系统，通过输入不同的数据格式或长度等进行验证，查看业务系统是否对人机接口输入（如用户界面的数据输入）或通信接口输入的数据进行有效性检验；是否允许按照操作的序列进行回退（如撤消操作）；是否在故障发生时继续提供一部分功能，确保能够实施必要的措施（如对重要数据的保存）；

c) 应测评主要应用系统，可通过输入的不同（如数据格式或长度等符合、不符合软件设定的要求），验证系统人机接口有效性检验功能是否正确；

d) 应测评主要应用系统，可通过多步操作，然后回退，验证系统能否按照操作的序列进行正确的回退；

e) 应测评主要应用系统，可通过给系统人为制造一些故障（如系统异常），验证系统能否在故障发生时实时检测到故障状态并报警，能否自动保护当前所有状态。

结果判定

a) 测评实施中b）～e）均为肯定，则信息系统符合本单元测评项要求。

9) 资源控制(A3)

测评项

a) **对于有会话或短连接的应用系统**，当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

b) 应能够对系统的最大并发会话连接数进行限制；

c) **对于有会话的应用系统，**应能够对单个帐户的多重并发会话进行限制；

d) 应能够对一个时间段内可能的并发会话连接数进行限制；

e) **宜**能够对**系统占用的资源设定限额，超出限额时给出提示信息**；

f) 应能够对系统服务水平降低到预先规定的最小值进行检测和报警；

g) 应提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。

测评方式

访谈，检查，测评。

测评对象

系统管理员，主要应用系统。

测评实施

a) 可访谈系统管理员，询问业务系统是否有资源控制的措施（如对应用系统的最大并发会话连接数进行限制，是否禁止同一用户账号在同一时间内并发登录，是否对一个时间段内可能的并发会话连接数进行限制，对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额等），具体措施有哪些；

b) 应检查主要应用系统，查看是否有限制单个用户的多重并发会话；系统是否有最大并发会话连接数的限制，是否有对一个时间段内可能的并发会话连接数进行限制；是否能根据安全策略设定主体的服务优先级，根据优先级分配系统资源，保证优先级低的主体处理能力不会影响到优先级高的主体的处理能力；

c) 应检查主要应用系统，查看是否根据安全策略设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式；是否禁止同一用户账号在同一时间内并发登录；是否对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额；

d) 应检查主要应用系统，查看是否根据安全属性（用户身份、访问地址、时间范围等）允许或拒绝用户建立会话连接；查看是否有服务水平最小值的设定，当系统的服务水平降低到预先设定的最小值时，系统报警；

e) 应测评主要应用系统，可通过对系统进行超过单个用户的多重并发会话连接，验证系统能否正确地限制单个用户的多重并发会话数；可通过对系统进行超过最大并发会话连接数进行连接，验证系统能否正确地限制最大并发会话连接数；

f) 应测评主要应用系统，可通过在一个时间段内，用超过设定的并发连接数对系统进行连接，查看能否连接成功，验证系统对一个时间段内可能的并发会话连接数进行限制的功能是否正确；

g) 应测评主要应用系统，可通过设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式，制造操作超时和鉴别失败，验证系统能否锁定，解锁或终止方式是否和设定的方式相同；

h) 应测评主要应用系统，可通过按照安全属性（用户身份、访问地址、时间范围等）设定允许或拒绝某个用户建立会话连接，然后用该用户进行对应的操作，验证查看系统能否正确地根据安全属性允许或拒绝用户建立会话连接；试图使服务水平降低到预先规定的最小值，验证系统能否正确检测并报警。

结果判定

a) 测评实施中b）～h）均为肯定，则信息系统符合本单元测评项要求。

在内容上，应用安全层面实施过程涉及 9 个工作单元，具体内容请参见附录 A.2.1.4。

7.1.2.1.5 数据安全及备份恢复

1) 数据完整性(S3)

测评项

a) 应能够检测到系统管理数据、鉴别信息和重要业务数据在**采集、传输、使用和存储过程**中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

测评方式

访谈，检查。

测评对象

安全员，**系统管理员**，主要应用系统，设计/验收文档，相关证明性材料（如证书、检验报告等）。

测评实施

a) 可访谈安全员，询问业务系统数据在存储、传输过程中是否有完整性保证措施，具体措施有哪些；在检测到完整性错误时是否能恢复，恢复措施有哪些；

b) 应检查操作系统、网络设备、数据库管理系统的设计/验收文档或相关证明性材料（如证书、检验报告等）等，查看其是否有能检测/验证到系统管理数据（如 WINDOWS 域管理、目录管理数据）、鉴别信息（如用户名和口令）和用户数据（如用户数据文件）在传输过程中完整性受到破坏，能检测到系统管理数据、身份鉴别信息和用户数据（如防火墙的访问控制规则）在存储过程中完整性受到破坏，能检测到重要系统完整性受到破坏，在检测到完整性错误时采取必要的恢复措施的描述；如果有相关信息，查看其配置是否正确；

c) 应检查主要应用系统，查看其是否配备检测/验证系统管理数据、鉴别信息和用户数据在传输过程中完整性受到破坏的功能；是否配备检测/验证系统管理数据、身份鉴别信息和用户数据在存储过程中完整性受到破坏的功能；是否配备检测/验证重要系统/模块完整性受到破坏的功能；在检测/验证到完整性错误时能采取必要的恢复措施；

d) 应检查主要应用系统，查看其是否配备检测系统完整性受到破坏的功能；并在检测到完整性错误时采取必要的恢复措施。

结果判定

a) 如果测评实施中 b）缺少相关材料，则该项为否定；

b) 测评实施中 b）~ d）均为肯定，则信息系统符合本单元测评项要求。

2) 数据保密性(S3)

测评项

a) 应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据**采集、传输、使用和存储过程**的保密性。

测评方式

访谈，检查，测评。

测评对象

系统管理员、网络管理员、安全员、数据库管理员，主要应用系统，设计/验收文档，相关证明性材料（如证书等）。

测评实施

a) 可访谈网络管理员，询问信息系统中的网络设备的鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性；是否采用加密或其他保护措施实现存储保密性；

b) 可访谈系统管理员，询问信息系统中的操作系统的鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性；是否采用加密或其他保护措施实现存储保密性；

c) 可访谈数据库管理员，询问信息系统中的数据库管理系统的鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性；是否采用加密或其他保护措施实现存储保密性；

d) 可访谈安全员，询问信息系统中的应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性；是否采用加密或其他保护措施实现存储保密性；

e) 可访谈安全员，询问当使用便携式和移动式设备时，是否加密或者采用可移动磁盘存储敏感信息；

f) 应检查操作系统、网络设备、数据库管理系统、关键应用系统的设计/验收文档，查看其是否有关于鉴别信息、敏感的系统管理数据和敏感的用户数据采用加密或其他有效措施实现传输保密性描述，是否有采用加密或其他保护措施实现存储保密性的描述；

g) 应检查相关证明性材料（如证书或其他相关材料等），查看其是否有特定业务通信的通信信道符合相关的国家规定的说明；

h) 应检查主要应用系统，查看其鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性描述，是否采用加密或其他保护措施实现存储保密性；

i) 应测评主要应用系统，通过用嗅探工具获取系统传输数据包，查看其是否采用了加密或其他有效措施实现传输保密性。

结果判定

a) 如果测评实施中 f）缺少相关材料，则该项为否定；

b) 如果没有相关证明性材料（如证书、检验报告等），则 g）为否定；

c) 测评实施中 f）～i）均为肯定，则信息系统符合本单元测评项要求。

3) 数据备份和恢复(A3)

测评项

a) 应提供本地数据备份与恢复功能，采取实时备份与异步备份或增量备份与完全备份的方式，增量数据备份每天一次，**完全数据备份每周一次**，备份介质场外存放，**数据保存期限依照国家相关规定**；

b) 应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地；

c) **对于同城数据备份中心，应与生产中心直线距离至少达到30公里，可以接管所有核心业务的运行；对于异地数据备份中心，应与生产中心直线距离至少达到100公里；（F3）**

d) **为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果；（F3）**

e) **数据备份存放方式应以多冗余方式，完全数据备份至少保证以一个星期为周期的数据冗余；**

f) **异地备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，"就绪状态"指备份中心的所需资源(相关软硬件以及数据等资源)已完全满足但设备cpu还没有运行；"运行状态"指备份中心除所需资源完全满足要求外，cpu也在运行状态。（F3）**

测评方式

访谈，检查。

测评对象

系统管理员，网络管理员，数据库管理员，操作系统，网络设备，数据库管理系统，主要应用系统，设计/验收文档。

测评实施

a) 可访谈网络管理员，询问信息系统中的网络设备是否提供自动备份机制对重要信息进行本地和异地备份功能；是否提供对重要信息进行恢复的功能；是否提供重要网络设备、通信线路和服务器的硬件冗余；

b) 可访谈系统管理员，询问信息系统中的操作系统是否提供自动备份机制对重要信息进行本地和异地备份功能；是否提供对重要信息进行恢复的功能；

c) 可访谈数据库管理员，询问信息系统中的数据库管理系统是否提供自动备份机制对重要信息进行本地和异地备份功能；是否提供重要业务系统的本地系统级热备份；是否提供对重要信息进行恢复的功能；

d) 应检查设计/验收文档，查看其是否有关于操作系统、网络设备、数据库管理系统、应用系统配置有本地系统级热备份和重要信息恢复功能的描述；

e) 应检查操作系统、网络设备、数据库管理系统、主要应用系统，查看其是否配置有本地/异地备份和重要信息恢复的功能，其配置是否正确；

f) 应检查重要网络设备、通信线路和服务器是否提供硬件冗余；

g) 应检查重要业务系统是否配备本地系统级热备份的功能。

结果判定

a) 如果没有设计/验收文档，测评实施中 d） 则该项为否定；

b) 测评实施中 d）～e）均为肯定，则信息系统符合本单元测评项要求。

数据安全层面分布在网络安全、主机安全和应用安全等层面进行测评，在内容上，数据安全层面实施过程涉及 3 个工作单元，具体内容请参见附录 A.2.1.5。

7.1.2.2 安全管理测评

7.1.2.2.1 安全管理制度

1) 管理制度(G3)

测评项

a) 应制定信息安全工作的总体方针和安全策略，说明安全工作的总体目标、范围、原则和安全框架等，**并编制形成信息安全方针制度文件**；

b) 应对安全管理活动中各类管理内容建立安全管理制度；

c) 应对科技管理人员或操作人员执行的日常管理操作建立操作规程；

d) 应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。

测评方式

访谈，检查。

测评对象

安全主管，总体方针、政策性文件和安全策略文件，安全管理制度清单，操作规程，评审记录。

测评实施

a) 应检查的制度体系是否由安全政策、安全策略、管理制度、操作规程等构成，是否定期对安全管理制度体系进行评审，评审周期多长；

b) 应检查信息安全工作的总体方针、政策性文件和安全策略文件，查看文件是否明确机构安全工作的总体目标、范围、方针、原则、责任等，是否明确信息系统的安全策略；

c) 应检查安全管理制度清单，查看是否覆盖物理、网络、主机系统、数据、应用、管理等层面；

d) 应检查是否具有重要管理操作的操作规程；

e) 应检查是否具有安全管理制度体系的评审记录，查看记录日期与评审周期是否一致，是否记录了相关人员的评审意见。

结果判定

a) 测评实施中 a）～e）均为肯定，则信息系统符合本单元测评项要求。

2) 制定和发布(G3)

测评项

a) **由金融机构总部科技部门负责制定适用全机构范围的安全管理制度，各分支机构的科技部门负责制定适用辖内的安全管理制度；（F3）**

b) 安全管理制度应具有统一的格式，并进行版本控制；

c) 应组织相关人员对制定的安全管理制度进行论证和审定；

d) 安全管理制度应通过正式、有效的方式发布；

e) 安全管理制度应注明发布范围，并对收发文进行登记。

测评方式

访谈，检查。

测评对象

安全主管，制度制定和发布要求管理文档，评审记录，安全管理制度，收发登记记录。

测评实施

a) 应检查安全管理制度是否在信息安全领导小组或委员会的总体负责下统一制定，参与制定人员有哪些；

b) 应访谈安全主管，询问安全管理制度的制定程序，是否对制定的安全管理制度进行论证和审定，论证和评审方式如何（如召开评审会、函审、内部审核等），是否按照统一的格式标准或要求制定；
c) 应检查制度制定和发布要求管理文档，查看文档是否说明安全管理制度的制定和发布程序、格式要求及版本编号等相关内容；
d) 应检查管理制度评审记录，查看是否有相关人员的评审意见；
e) 应检查安全管理制度的发布过程是否正式有效，并以某种方式发布到相关；
f) 应检查安全管理制度的收发登记记录，查看收发是否符合规定程序和发布范围要求。

结果判定

a) 测评实施中 a）~ f）均为肯定，则信息系统符合本单元测评项要求。

3) 评审和修订(G3)

测评项

a) 信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；
b) **应该建立对门户网站内容发布的审核、管理和监控机制；（F3）**
c) 应定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。

测评方式

访谈，检查。

测评对象

安全主管，管理人员，安全管理制度列表，评审记录，安全管理制度对应负责人或负责部门的清单。

测评实施

a) 应访谈安全主管，询问是否定期对安全管理制度进行评审，由何部门/何人负责；
b) 应访谈管理人员（负责定期评审、修订和日常维护的人员），询问定期对安全管理制度的评审、修订情况和日常维护情况，评审周期多长，评审、修订程序如何，维护措施如何；
c) 应访谈管理人员（负责人员），询问系统发生重大安全事故、出现新的安全漏洞以及技术基础结构和组织结构等发生变更时是否对安全管理制度进行审定，对需要改进的制度是否进行修订；
d) 应检查制度修订评审记录和需要定期评审的安全管理制度列表，查看列表是否注明评审周期；
e) 是否定期对安全管理制度进行评审，发现存在不足或需要改进的是否进行修订，评审周期多长，评审、修订程序如何，维护措施如何；
f) 应检查安全管理制度评审记录，查看记录日期与评审周期是否一致；如果对制度做过修订，检查是否有修订版本的安全管理制度；
g) 应检查是否具有系统发生重大安全事故、出现新的安全漏洞以及技术基础结构和组织结构等发生变更时对安全管理制度进行审定的记录；
h) 应检查是否具有需要定期修订的安全管理制度列表，查看列表是否注明评审周期；
i) 应检查是否具有所有安全管理制度对应相应负责人或者负责部门的清单。

结果判定

a) 测评实施中 a）~ i）均为肯定，则信息系统符合本单元测评项要求。

安全管理制度测评对象主要为管理制度、制定和发布、评审和修订 3 个控制点相关的文件资料和工作记录。具体内容请参见附录 A.2.2.1。

7. 1. 2. 2. 2 安全管理机构

1) 岗位设置(G3)

测评项

a) **金融机构信息安全管理工作实行统一领导、分级管理，总部统一领导分支机构的信息安全管理，各机构负责本单位和辖内的信息安全管理；(F3)**

b) **应设立由本机构领导、业务与技术相关部门主要负责人组成的信息安全领导小组，负责协调本机构及辖内信息安全管理工作，决策本机构及辖内信息安全重大事宜；**

c) **应设立专门的信息科技风险审计岗位，负责信息科技审计制度和流程的实施，制订和执行信息科技审计计划，对信息科技整个生命周期和重大事件等进行审计；（F3）**

d) 应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；

e) 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责；

f) **金融机构的主要负责人为本单位计算机信息系统安全保护工作的第一责任人。金融机构的计算机信息系统安全保护领导小组、专职部门和专(兼)职安全管理人员以及其他有关人员应当协助第一责任人组织落实有关规定；（F3）**

g) **应坚持三分离原则，实现前后台分离、开发与操作分离、技术与业务分离，信息技术人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务；（F3）**

h) **除科技部门外，其他部门均应指定至少一名部门计算机安全员，具体负责本部门的信息安全管理工作，协同科技部门开展信息安全管理工作。（F3）**

测评方式

访谈，检查。

测评对象

安全主管，安全管理某方面的负责人，领导小组日常管理工作的负责人，系统管理员，网络管理员，安全员，部门、岗位职责文件，委任授权书，工作记录。

测评实施

a) 应访谈安全主管，询问是否设立指导和管理信息安全工作的委员会或领导小组，其最高领导是否由单位主管领导委任或授权的人员担任；

b) 应访谈安全主管，询问是否设立专职的安全管理机构（即信息安全管理工作的职能部门）；机构内部门设置情况如何，是否明确各部门职责分工；

c) 应访谈安全主管，询问是否设立安全管理各个方面的负责人，设置了哪些工作检查是否明确各个岗位（如安全主管、安全管理各个方面的负责人、机房管理员、系统管理员、网络管理员、安全员等重要岗位）的职责分工；

d) 应访谈安全主管、安全管理某方面的负责人、信息安全管理委员会或领导小组日常管理工作的负责人、系统管理员、网络管理员和安全员，询问其岗位职责包括哪些内容；

e) 应检查部门、岗位职责文件，查看文件是否明确安全管理机构的职责，是否明确机构内各部门的职责和分工，部门职责是否涵盖物理、网络和系统等各个方面；查看文件是否明确设置安全主管、安全管理各个方面的负责人、机房管理员、系统管理员、网络管理员、安全员等各个岗位，各个岗位的职责范围是否清晰，否明确岗位人员应具有的技能要求，人员是否备案；

f) 应检查信息安全管理委员会或领导小组是否具有单位主管领导对其最高领导的委任授权书；

g) 应检查信息安全管理委员会职责文件，查看是否明确描述委员会的职责和其最高领导岗位的职责；

h) 应检查安全管理各部门和信息安全管理委员会或领导小组是否具有日常管理工作执行情况的文件或工作记录（如会议记录/纪要和信息安全工作决策文档等）。

结果判定

a) 如果测评实施中 d）被访谈人员表述与文件描述一致，则该项为肯定；

b) 测评实施中 a）~ h）均为肯定，则信息系统符合本单元测评项要求。

2) 人员配备(G3)

测评项

a) 应配备一定数量的系统管理员、网络管理员、安全管理员等；

b) 应配备专职信息安全管理人员，**实行A、B 岗制度**，不可兼任；

c) 关键事务岗位应配备多人共同管理。

测评方式

访谈，检查。

测评对象

安全主管，人员配备要求管理文档，管理人员名单。

测评实施

a) 应检查人员配备相关文档，查看岗位分工列表和定期轮岗情况（含轮岗周期、轮岗手续等）应访谈安全主管，询问各个安全管理岗位人员（按照岗位职责文件询问，包括机房管理员、系统管理员、数据库管理员、网络管理员、安全员等重要岗位人员）配备情况，包括数量、专职还是兼职等；

b) 应访谈安全主管，询问对哪些关键岗位实行定期轮岗，定期轮岗情况如何，轮岗周期多长，轮岗手续如何；

c) 应检查人员配备要求管理文档，查看是否明确应配备哪些安全管理人员，是否包括机房管理员、系统管理员、数据库管理员、网络管理员、安全员等重要岗位人员并明确应配备专职的安全员；查看是否明确对哪些关键岗位（应有列表）实行定期轮岗并明确轮岗周期、轮岗手续等相关内容；

d) 应检查岗位分工名单，确认其是否明确机房管理员、系统管理员、数据库管理员、网络管理员、安全员等重要岗位人员的信息，确认安全管理员是否是专职人员；

e) 应检查关键事务岗位多人管理情况（含定期轮岗情况、轮岗周期和轮岗手续等）。

结果判定

a) 如果测评实施中 a）设置的安全员是专职的，则该项为肯定；

b) 测评实施中 a）~e）均为肯定，则信息系统符合本单元测评项要求。

3) 授权和审批(G3)

测评项

a) 应根据各部门和岗位的的职责明确授权审批事项、审批部门和批准人等；

b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；

c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；

d) 应记录审批过程并保存审批文档；

e) **用户应被授予完成所承担任务所需的最小权限，重要岗位的员工之间应形成相互制约的关系。权限变更应执行相关审批流程，并有完整的变更记录；（F3）**

f) **应建立系统用户及权限清单，定期对员工权限进行检查核对，发现越权用户要查明原因并及时调整，同时清理过期用户权限，做好记录归档。（F3）**

测评方式

访谈，检查。

测评对象

安全主管，关键活动的批准人，授权管理文件，审批文档，审批记录，审查记录，消除授权记录。

测评实施

a) 应检查是否规定对信息系统中的关键活动进行审批，审批部门是何部门，批准人是何人，他们的审批活动是否得到授权；询问是否定期审查、更新审批项目，审查周期多长；
b) 应检查是否建立针对系统变更、重要操作、物理访问和系统接入等事项的审批程序，按照审批程序执行审批过程应访谈关键活动的批准人，询问其对关键活动的审批范围包括哪些（如网络系统、应用系统、数据库管理系统、重要服务器和设备等重要资源的访问，重要管理制度的制定和发布，人员的配备、培训，产品的采购，第三方人员的访问、管理，与合作单位的合作项目等），审批程序如何；
c) 应检查关键活动的审批过程记录，查看记录的审批程序与文件要求是否一致；
d) 应检查审查记录，查看记录日期是否与审查周期一致；
e) 应检查是否具有对不再适用的权限及时取消授权的记录。

结果判定

a) 测评实施中 a）～e）均为肯定，则该测评项符合要求。

4) 沟通和合作(G3)

测评项

a) 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题，**并形成会议纪要**；
b) 应加强与兄弟单位、公安机关、电信公司的合作与沟通；
c) 应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通；
d) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；
e) 应聘请信息安全专家作为安全顾问，指导信息安全建设，参与安全规划和安全评审等。

测评方式

访谈，检查。

测评对象

安全主管，安全管理人员，会议文件，会议记录，外联单位说明文档，安全顾问名单。

测评实施

a) 应访谈安全主管，询问是否建立与外单位（公安机关、电信公司、兄弟单位、供应商、业界专家、专业的安全公司、安全组织等），与组织机构内其它部门之间及内部各部门管理人员之间的沟通、合作机制，与外单位和其他部门有哪些合作内容，沟通、合作方式有哪些；
b) 应检查信息安全领导小组、部门间协调、安全检查等会议文件或会议记录，查看是否有会议内容、会议时间、参加人员、会议结果等的描述应访谈安全主管，询问是否召开过部门间协调会议，组织其它部门人员共同协助处理信息系统安全有关问题，安全管理机构内部是否召开过安全工作会议部署安全工作的实施，参加会议的部门和人员有哪些，会议结果如何；信息安全领导小组或者安全管理委员会是否定期召开例会；
c) 应访谈安全主管，询问是否聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等；
d) 应访谈安全管理人员（从系统管理员和安全员等人员中抽查），询问其与外单位人员，与组织机构内其他部门人员，与内部各部门管理人员之间的沟通方式和主要沟通内容有哪些；
e) 应检查部门间协调会议文件或会议记录，查看是否有会议内容、会议时间、参加人员和结果等的描述；
f) 应检查安全工作会议文件或会议记录，查看是否有会议内容、会议时间、参加人员和会议结果等的描述；
g) 应检查信息安全领导小组或者安全管理委员会定期例会会议文件或会议记录，查看是否有会议内容、会议时间、参加人员、会议结果等的描述；

h) 应检查检查外联单位列表，是否建立与外联单位（公安机关、电信公司、兄弟单位、供应商、业界专家、专业的安全公司、安全组织等）之间的沟通、合作机制，是否说明外联单位的联系人和联系方式等内容；

i) 应检查是否具有安全顾问名单或者聘请安全顾问的证明文件，查看由安全顾问指导信息安全建设、参与安全规划和安全评审的相关文档或记录，是否具有由安全顾问签字的相关建议信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等相关记录文档。

结果判定

a) 测评实施中 a）～i）均为肯定，则信息系统符合本单元测评项要求。

5) 审核和检查(G3)

测评项

a) 应制定安全审核和安全检查制度规范安全审核和安全检查工作，按要求定期开展安全审核和安全检查活动；

b) 安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；

c) 应由内部人员或上级机构定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

d) 应制定安全检查表格，实施安全检查，汇总安全检查数据，形成安全检查报告，**要求限期整改的需要对相关整改情况进行后续跟踪，并将每次安全检查报告和整改落实情况整理汇总后，报上一级机构科技部门备案；**

e) **应制定违反和拒不执行安全管理措施规定的处罚细则。（F3）**

测评方式

访谈，检查。

测评对象

安全主管，安全员，安全检查制度，安全检查报告，审计分析报告，安全检查过程记录，安全检查表格。

测评实施

a) 应检查是否组织人员定期对信息系统进行安全检查，检查周期多长，是否定期分析、评审异常行为的审计记录；

b) 应检查安全检查包含哪些内容，检查人员有哪些，检查程序是否按照系统相关策略和要求进行，是否制定安全检查表格实施安全检查，检查结果如何，是否对检查结果进行通报，通报形式、范围如何；

c) 应检查安全检查制度文档，查看文档是否规定检查内容、检查程序和检查周期等，检查内容是否包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等，是否包括用户账号情况、系统漏洞情况、系统审计情况等；

d) 应检查安全检查报告，查看报告日期与检查周期是否一致，报告中是否有检查内容、检查人员、检查数据汇总表、检查结果等的描述；

e) 应检查安全检查过程记录，查看记录的检查程序与文件要求是否一致；

f) 应查看报告日期与检查周期是否一致，报告中是否有分析人员、异常问题和分析结果等的描述，是否对发现的问题提出相应的措施；

g) 应检查是否具有安全检查表格。

结果判定

a) 测评实施中 a）～g）均为肯定，则信息系统符合本单元测评项要求。

安全管理机构测评对象主要为岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查 5 个控制点相关的文件资料和工作记录。具体内容请参见附录 A.2.2.2

7.1.2.2.3 人员安全管理

1) 人员录用(G3)

测评项

a) 应指定或授权专门的部门或人员负责人员录用；

b) 应严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；

c) 应与员工签署保密协议；

d) 应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议；

e) **对信息安全管理人员应实行备案管理，信息安全管理人员的配备和变更情况，应及时报上一级科技部门备案，金融机构总部信息管理人员在总部科技部门备案；（F3）**

f) **凡是因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员，不得从事信息安全管理工作。（F3）**

测评方式

访谈，检查。

测评对象

人事负责人，人事工作人员，人员录用要求管理文档，人员审查文档或记录，考核文档或记录，保密协议，岗位安全协议，审查记录。

测评实施

a) 应访谈人事负责人，询问在人员录用时对人员条件有哪些要求，目前录用的安全管理和技术人员是否有能力完成与其职责相对应的工作；

b) 应访谈人事工作人员，询问在人员录用时是否对被录用人的身份、背景、专业资格和资质进行审查，对技术人员的技术技能进行考核，录用后是否与其签署保密协议，是否对其说明工作职责；

c) 应访谈人事负责人，询问对从事关键岗位的人员是否从内部人员中选拔，是否要求其签署岗位安全安全协议，是否定期对关键岗位人员进行信用审查，审查周期多长；

d) 应检查人员录用要求管理文档，查看是否说明录用人员应具备的条件，如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等；

e) 应检查是否具有人员录用时对录用人身份、背景、专业资格和资质等进行审查的相关文档或记录，查看是否记录审查内容和审查结果等；

f) 应检查技能考核文档或记录，查看是否记录考核内容和考核结果等；

g) 应检查保密协议，查看是否有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容；

h) 应检查岗位安全协议，查看是否有岗位安全责任、违约责任、协议的有效期限和责任人签字等内容；

i) 应检查信用审查记录，查看是否记录了审查内容和审查结果等，查看审查时间与审查周期是否一致。

结果判定

a) 测评实施中 a）～i）均为肯定，则信息系统符合本单元测评项要求。

2) 人员离岗(G3)

测评项

a) 应严格规范人员离岗过程，及时终止离岗员工的所有访问权限；

b) 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；

c) 应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开，**并保证离岗人员负责的信息技术系统的口令必须立即更换**。

测评方式

访谈，检查。

测评对象

安全主管，人事工作人员，人员离岗管理文档，保密承诺文档。

测评实施

a) 应访谈安全主管，询问是否及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备等；

b) 应访谈人事工作人员，询问调离手续包括哪些，是否要求调离人员承诺相关保密义务后方可离开；

c) 应检查人员离岗的管理文档，查看是否规定了调离手续和离岗要求等；

d) 应检查是否具有交还身份证件和设备等的记录；

e) 应检查保密承诺文档，查看是否有调离人员的签字。

结果判定

a) 测评实施中 a）～e）均为肯定，则信息系统符合本单元测评项要求。

3) 人员考核(G3)

测评项

a) 应定期对各个岗位的人员进行安全技能及安全认知的考核；

b) 应对关键岗位的人员进行全面、严格的安全审查和技能考核；

c) 应对考核结果进行记录并保存。

测评方式

访谈，检查。

测评对象

安全主管，人事工作人员，人员考核记录。

测评实施

a) 应访谈安全主管，询问是否有人负责定期对各个岗位人员进行安全技能及安全知识的考核；

b) 应访谈人事工作人员，询问对各个岗位人员的考核情况，考核周期多长，考核内容有哪些；询问对人员的安全审查情况，审查人员是否包含所有岗位人员，审查内容有哪些（如操作行为、社会关系、社交活动等），是否全面；

c) 应访谈人事工作人员，询问对违背安全策略和规定的人员有哪些惩戒措施；

d) 应检查考核记录，查看记录的考核人员是否包括各个岗位的人员，考核内容是否包含安全知识、安全技能等；查看记录日期与考核周期是否一致。

结果判定

a) 如果测评实施中 b）被访谈人员表述审查内容包含社会关系、社交活动、操作行为等各个方面，则该项为肯定；

b) 如果测评实施中 c）被访谈人员表述与文件描述一致，则该项为肯定；

c) 测评实施中 a）～d）均为肯定，则信息系统符合本单元测评项要求。

4) 安全意识教育和培训(G3)

测评项

a) 应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划；

b) 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，**普及信息安全基础知识、规范岗位操作、提高安全技能；**

c) **每年至少对信息安全管理人员进行一次信息安全培训；（F3）**

d) 应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒；

e) 应对安全教育和培训的情况和结果进行记录并归档保存。

测评方式

访谈，检查。

测评对象

安全主管，安全员，系统管理员，网络管理员，数据库管理员，培训计划，培训记录。

测评实施

a) 应检查是否制定安全教育和培训计划并按计划对各个岗位人员进行安全教育和培训；

b) 应检查安全责任和惩戒措施相关制度和惩戒记录；

c) 应检查安全教育和培训计划文档，查看是否具有不同岗位的培训计划；查看计划是否明确了培训目的、培训方式、培训对象、培训内容、培训时间和地点等，培训内容是否包含信息安全基础知识、岗位操作规程等；

d) 应检查是否具有安全教育和培训记录，查看记录是否有培训人员、培训内容、培训结果等的描述；查看记录与培训计划是否一致。

结果判定

a) 如果测评实施中b）访谈人员能够表述清楚询问内容，且安全职责、惩戒措施和岗位操作规程表述与文件描述一致，则该项为肯定；

b) 测评实施中a）～d）均为肯定，则信息系统符合本单元测评项要求。

5) 外部人员访问管理(G3)

测评项

a) **各机构指定责任部门负责非涉密计算机系统和网络相关的外部人员访问授权审批，批准后由专人全程陪同或监督，并登记备案；**

b) **应对允许被外部人员访问的金融机构计算机系统和网络资源建立存取控制机制、认证机制，列明所有用户名单及其权限，其活动应受到监控；**

c) **获得外部人员访问授权的所有单位和个人应与金融机构签订安全保密协议，不得进行未授权的增加、删除、修改、查询数据操作，不得复制和泄漏金融机构的任何信息。（F3）**

测评方式

访谈，检查。

测评对象

安全主管，安全管理人员，安全责任合同书或保密协议，第三方人员访问管理文档，访问批准文档，登记记录。

测评实施

a) 应访谈安全主管，询问对第三方人员（如向系统提供服务的系统软、硬件维护人员，业务合作伙伴、评估人员等）的访问采取哪些管理措施，是否要求第三方人员访问前与机构签署安全责任合同书或保密协议；

b) 应访谈安全管理人员，询问对第三方人员访问重要区域（如访问主机房、重要服务器或设备、保密文档等）采取哪些措施，是否经有关负责人书面批准，是否由专人全程陪同或监督，是否进行记录并备案管理；

c) 应检查安全责任合同书或保密协议，查看是否有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等；

d) 应检查第三方人员访问管理文档，查看是否明确第三方人员包括哪些人员，允许第三方人员访问的范围（区域、系统、设备、信息等内容），第三方人员进入条件（对哪些重要区域的访问须提出书面申请批准后方可进入），第三方人员进入的访问控制（由专人全程陪同或监督等）和第三方人员的离开条件等；

e) 应检查第三方人员访问重要区域批准文档，查看是否有第三方人员访问重要区域的书面申请，是否有批准人允许访问的批准签字等；

f) 应检查第三方人员访问重要区域的登记记录，查看记录是否描述了第三方人员访问重要区域的进入时间、离开时间、访问区域、访问设备或信息及陪同人等信息。

结果判定

a) 测评实施中 a）~ f）均为肯定，则该测评项符合要求。

人员安全管理测评对象主要为人员录用、人员离岗、人员考核、安全意识教育培训和外部人员访问管理 5 个控制点相关的文件资料和工作记录。具体内容请参见附录 A.2.2.3。

7.1.2.2.4 系统建设管理

1) 系统定级(G3)

测评项

a) 应明确信息系统的边界和安全保护等级；

b) 应以书面的形式说明确定信息系统为某个安全保护等级的方法和理由；

c) 应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定；

d) 应确保信息系统的定级结果经过相关部门的批准。

测评方式

访谈，检查。

测评对象

安全主管，系统划分文档，系统定级文档，专家论证文档，系统属性说明文档。

测评实施

a) 应访谈安全主管，询问划分信息系统的方法和确定信息系统安全保护等级的方法是否参照定级指南的指导，是否对其进行明确描述；是否组织相关部门和有关安全技术专家对定级结果进行论证和审定，定级结果是否获得了相关部门（如上级主管部门）的批准；

b) 应检查系统划分文档，查看文档是否明确描述信息系统划分的方法和理由；

c) 应检查系统定级文档，查看文档是否给出信息系统的安全保护等级，是否明确描述确定信息系统为某个安全保护等级的方法和理由，是否给出安全等级保护措施组成SxAyGz值；查看定级结果是否有相关部门的批准盖章；

d) 应检查专家论证文档，查看是否有专家对定级结果的论证意见；

e) 应检查系统属性说明文档，查看文档是否明确了系统使命、业务、网络、硬件、软件、数据、边界、人员等。

结果判定

a) 测评实施中a）没有上级主管部门的，如果有安全主管的批准，则该项为肯定；

b) 测评实施中b）~ e）均为肯定，则信息系统符合本单元测评项要求。

2) 安全方案设计(G3)

测评项

a) 应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；

b) 应根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施；

c) 应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划、安全性需求分析、和详细设计方案，并形成配套文件；

d) 应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、安全性需求分析、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施；

e) 应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、安全性需求分析、详细设计方案等相关配套文件。

测评方式

访谈，检查。

测评对象

安全主管，系统建设负责人，总体安全策略文档，安全技术框架，安全管理策略文档，总体建设规划书，详细设计方案，专家论证文档，维护记录。

测评实施

a) 应访谈安全主管，询问是否授权专门的部门对信息系统的安全建设进行总体规划，由何部门/何人负责；

b) 应访谈系统建设负责人，询问是否制定近期和远期的安全建设工作计划，是否根据系统的安全级别选择基本安全措施，是否依据风险分析的结果补充和调整安全措施，做过哪些调整；

c) 应访谈系统建设负责人，询问是否根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案等；

d) 应访谈系统建设负责人，询问是否组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略等相关配套文件进行论证和审定，并经过管理部门的批准；

e) 应访谈系统建设负责人，询问是否根据安全测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件，维护周期多长；

f) 应检查系统的安全建设工作计划，查看文件是否明确了系统的近期安全建设计划和远期安全建设计划；

g) 应检查系统总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等配套文件，查看各个文件是否有机构管理层的批准；

h) 应检查专家论证文档，查看是否有相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的论证意见；

i) 应检查是否具有总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的维护记录或修订版本，查看记录日期与维护周期是否一致。

结果判定

a) 测评实施中a）～i）均为肯定，则信息系统符合本单元测评项要求。

3) 产品采购和使用(G3)

测评项

a) 应确保安全产品采购和使用符合国家的有关规定；

b) 应确保密码产品采购和使用符合国家密码主管部门的要求；

c) 应指定或授权专门的部门负责产品的采购，**设备采购应坚持公开、公平、公正的原则，宜采用招标、邀标等形式完成；**

d) **各机构购置扫描、检测类信息安全产品应报本机构科技主管部门批准、备案；（F3）**

e) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单；

f) **扫描、检测类信息安全产品仅限于本机构信息安全管理人员或经主管领导授权的网络管理员使用；（F3）**

g) **应定期查看各类信息安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取控制措施并按规定程序报告；（F3）**

h) **应定期对各类信息安全产品产生的日志和报表进行备份存档，至少保存3个月；（F3）**

i) **应及时升级维护信息安全产品，凡超过使用期限的或不能继续使用的信息安全产品，要按照固定资产报废审批程序处理。（F3）**

测评方式

访谈，检查。

测评对象

安全主管，系统建设负责人，产品采购管理制度，产品选型测评结果记录，候选产品名单审定记录。

测评实施

a) 应访谈安全主管，询问是否有专门的部门负责产品的采购，由何部门负责；

b) 应访谈系统建设负责人，询问系统信息安全产品的采购情况，采购产品前是否预先对产品进行选型测评确定产品的候选范围，是否有产品采购清单指导产品采购，采购过程如何控制，是否定期审定和更新候选产品名单，审定周期多长；

c) 应访谈系统建设负责人，询问系统是否采用了密码产品，密码产品的使用是否符合国家密码主管部门的要求；

d) 应检查产品采购管理制度，查看内容是否明确采购过程的控制方法（如采购前对产品做选型测评，明确需要的产品性能指标，确定产品的候选范围，通过招投标方式确定采购产品等）和人员行为准则等方面；

e) 应检查系统使用的有关信息安全产品（边界安全设备、重要服务器操作系统、数据库等）是否符合国家的有关规定；

f) 应检查密码产品的使用情况是否符合密码产品使用、管理的相关规定，例如《商用密码管理条例》规定任何单位只能使用经过国家密码管理机构认可的商用密码产品，商用密码产品发生故障，必须有国家密码管理机构指定的单位维修，报废商用密码产品应向国家密码管理机构备案，《计算机信息系统保密工作暂行规定》规定涉密系统配置合格的保密专用设备，所采取的保密措施应与所处理信息的密级要求相一致等；

g) 应检查是否具有产品选型测评结果记录、候选产品名单审定记录或更新的候选产品名单。

结果判定

a) 如果测评实施中c）访谈说明没有采用密码产品，则测评实施c）、f）为不适用；

b) 测评实施中a）～g）均为肯定，则信息系统符合本单元测评项要求。

4) 自行软件开发(G3)

测评项

a) **应制定软件开发管理制度和代码编写安全规范，明确说明开发过程的控制方法和人员行为准则，要求开发人员参照规范编写代码，不得在程序中设置后门或恶意代码程序；（F3）**

b) 应确保开发环境与实际运行环境物理分开，**应确保开发人员和测试人员分离，开发人员不能兼任系统管理员或业务操作人员，**确保测试数据和测试结果受到控制；

c) 应确保提供软件设计的相关文档和使用指南，并由专人负责保管；

d) 应确保对程序资源库的修改、更新、发布进行授权和批准；

e) **在软件开发过程中，应同步完成相关文档手册的编写工作，保证相关资料的完整性和准确性。（F3）**

测评方式

访谈，检查。

测评对象

系统建设负责人，软件设计相关文档和使用指南，审批文档或记录，文档使用控制记录。

测评实施

a) 应访谈系统建设负责人，询问系统是否自主开发软件，是否对程序资源库的修改、更新、发布进行授权和批准，授权部门是何部门，批准人是何人，软件开发是否有相应的控制措施，是否要求开发人员不能做测评人员（即二者分离），是否在独立的模拟环境中编写、调试和完成；

b) 应访谈系统建设负责人，询问系统开发文档是否由专人负责保管，负责人是何人，如何控制使用（如限制使用人员范围并做使用登记等），测评数据和测评结果是否受到控制；
c) 应检查是否具有软件设计的相关文档（应用软件设计程序文件、源代码说明文档等）和软件使用指南或操作手册和维护手册等；
d) 应检查软件开发环境与系统运行环境在物理上是否是分开的；
e) 应检查对程序资源库的修改、更新、发布进行授权和审批的文档或记录，查看是否有批准人的签字；
f) 应检查是否具有系统软件开发相关文档（软件设计和开发程序文件、测评数据、测评结果、维护手册等）的使用控制记录。

结果判定

a) 测评实施中a）～f）均为肯定，则信息系统符合本单元测评项要求。

5) 外包软件开发(G3)

测评项

a) 应根据开发需求检测软件质量；
b) 应在软件安装之前检测软件包中可能存在的恶意代码；
c) 应要求开发单位提供软件设计的相关文档和使用指南；
d) 应要求开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道；
e) **应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要；（F3）**
f) **应要求外包服务商每年至少开展一次信息安全风险评估并提交评估报告，应要求外包服务商聘请外部机构定期对其进行安全审计并提交审计报告，督促其及时整改发现的问题；（F3）**
g) **应禁止外包服务商转包并严格控制分包，保证外包服务水平；（F3）**
h) **应制定数据中心外包服务应急计划，制订供应商替换方案，以应对外包服务商破产、不可抗力或其它潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。（F3）**

测评方法

访谈，检查。

测评对象

系统建设负责人，软件开发安全协议，软件开发文档，软件培训文档。

测评实施

a) 应访谈系统建设负责人，询问在外包软件前是否对软件开发单位以书面文档形式（如软件开发安全协议）规范软件开发单位的责任、开发过程中的安全行为、开发环境要求、软件质量、开发后的服务承诺等内容；
b) 应访谈系统建设负责人，询问是否具有独立对软件进行日常维护和使用所需的文档，开发单位是否为软件的正常运行和维护提供过技术支持，以何种方式进行；
c) 应访谈系统建设负责人，询问软件交付前是否依据开发协议的技术指标对软件功能和性能等进行验收检测，验收检测是否是由开发商和委托方共同参与；软件安装之前是否检测软件中的恶意代码，检测工具是否是第三方的商业产品；
d) 应检查软件开发协议，查看其是否规定知识产权归属、安全行为等内容；
e) 应检查是否具有需求分析说明书、软件设计说明书、软件操作手册等开发文档以及用户培训计划、程序员培训手册等后期技术支持文档。

结果判定

a) 测评实施中 a）～e）均为肯定，则信息系统符合本单元测评项要求。

6) 工程实施(G3)

测评项

a) 应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则；
b) 应指定或授权专门的部门或人员负责工程实施过程的管理；
c) 应制定详细的工程实施方案控制实施过程，并制定相关过程控制文档，并要求工程实施单位能正式地执行安全工程过程；
d) **应制定灾难备份系统集成与测试计划并组织实施。通过技术和业务测试，确认灾难备份系统的功能与性能达到设计指标要求；（F3）**
e) **网络系统的建设、升级、扩充等工程应经过科学的规划、充分的论证和严格的技术审查，有关材料应妥善保存并接受主管部门的检查。（F3）**

测评方法

访谈，检查。

测评对象

系统建设负责人，工程安全建设协议，工程实施方案，工程实施管理制度。

测评实施

a) 应访谈系统建设负责人，询问是否以书面形式（如工程安全建设协议）约束工程实施方的工程实施行为；
b) 应访谈系统建设负责人，询问是否指定专门人员或部门按照工程实施方案的要求对工程实施过程进行进度和质量控制，是否将控制方法和工程人员行为规范制度化，是否要求工程实施单位提供其能够安全实施系统建设的资质证明和能力保证；
c) 应检查工程安全建设协议，查看其是否规定工程实施方的责任、任务要求、质量要求等方面内容，约束工程实施行为；
d) 应检查工程实施方案，查看其是否规定工程时间限制、进度控制、质量控制等方面内容，工程实施过程是否按照实施方案形成各种文档，如阶段性工程报告；
e) 应检查工程实施管理制度，查看其是否规定工程实施过程的控制方法（如内部阶段性控制或外部监理单位控制）、实施参与人员的各种行为等方面内容。

结果判定

a) 测评实施中 a）～e）均为肯定，则信息系统符合本单元测评项要求。

7) 测评验收(G3)

测评项

a) 应对系统测试验收的控制方法和人员行为准则进行书面规定；
b) **应由项目承担单位（部门）或公正的第三方制定安全测试方案，对系统进行安全性测试，出具安全性测试报告，测试报告报科技部门审查；(F3)**
c) 在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；
d) 应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作；
e) 应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认；
f) **新建应用系统投入生产运行前应进行不少于1个月的模拟运行和不少于3个月的试运行。（F3）**

测评方法

访谈，检查。

测评对象

系统建设负责人，测评方案，测评记录，测评报告，验收报告，验收测评管理制度。

测评实施

a) 应访谈系统建设负责人，询问在信息系统正式运行前，是否委托第三方测评机构根据设计方案或合同要求对信息系统进行独立的安全性测评；

b) 应访谈系统建设负责人，询问是否指定专门部门负责测评验收工作，由何部门负责，是否对测评过程（包括测评前、测评中和测评后）进行文档化要求和制度化要求；
c) 应访谈系统建设负责人，询问是否根据设计方案或合同要求组织相关部门和人员对测评报告进行符合性审定；
d) 应检查工程测评方案，查看其是否对参与测评部门、人员、现场操作过程等进行要求；查看测评记录是否详细记录了测评时间、人员、操作过程、测评结果等方面内容；查看测评报告是否提出存在问题及改进意见等；
e) 应检查是否具有系统验收报告；
f) 应检查验收测评管理制度是否对系统验收测评的过程控制、参与人员的行为等进行规定。

结果判定

a) 测评实施中 a）~ f）均为肯定，则信息系统符合本单元测评项要求。

8) 系统交付(G3)

测评项

a) 应对系统交付的控制方法和人员行为准则进行书面规定；
b) 应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
c) **系统建设单位应在完成建设任务后将系统建设过程文档和系统运维文档全部移交科技部门；（F3）**
d) 系统建设单位应对负责系统运行维护的技术人员进行相应的技能培训；
e) 应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作；
f) **外部建设单位应与金融机构签署相关知识产权保护协议和保密协议，不得将系统采用的关键安全技术措施和核心安全功能设计对外公开。（F3）**

测评方法

访谈，检查。

测评对象

系统建设负责人，系统交付清单，服务承诺书，系统培训记录，系统交付管理制度。

测评实施

a) 应访谈系统建设负责人，询问交接手续是什么，系统交接工作是否由专门部门按照该手续办理，是否根据交付清单对所交接的设备、文档、软件等进行清点，交付清单是否满足合同的有关要求；是否对交付工作进行制度化要求；
b) 应访谈系统建设负责人，询问目前的信息系统是否由内部人员独立运行维护，如果是，系统建设实施方是否对运维技术人员进行过培训，针对哪些方面进行过培训，是否以书面形式承诺对系统运行维护提供一定的技术支持服务，是否按照服务承诺书的要求进行过技术支持，以何形式进行，系统是否具有支持其独立运行维护所需的文档；
c) 应检查系统交付清单，查看其是否具有系统建设文档（如系统建设方案）、指导用户进行系统运维的文档（如服务器操作规程书）以及系统培训手册等文档名称；
d) 应检查是否具有系统建设方的服务承诺书和对系统进行的培训记录；
e) 应检查系统交付管理制度，查看其是否规定了交付过程的控制方法和对交付参与人员的行为限制等方面内容；
f) 检查金融机构与外部建设单位签订的合同或协议，是否有相关约束条款来保证。系统采用的关键安全技术措施和核心安全功能设计不对外公开。

结果判定

a) 如果测评实施中 a）、d）中因没有出现交接工作中的问题而没有对相关文档做过改进，则以上两项不适用；

b) 测评实施中 a）~ f）均为肯定，则信息系统符合本单元测评项要求。

9) 系统备案(G3)

测评项

a) 应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用；

b) 应将系统等级及相关材料报系统主管部门备案；

c) 应将系统等级及其他要求的备案材料报相应公安机关备案。

测评方式

访谈，检查。

测评对象

安全主管，文档管理员，备案记录。

测评实施

a) 应访谈安全主管，询问是否有专门的人员或部门负责管理系统定级、系统属性等文档，由何部门/何人负责；

b) 应访谈文档管理员，询问对系统定级、系统属性等文档采取哪些控制措施（如限制使用范围、使用登记记录等）；

c) 应检查是否具有将系统定级文档和系统属性说明文件等材料报主管部门备案的记录或备案文档；

d) 应检查是否具有将系统等级、系统属性和等级划分理由等备案材料报相应公安机关备案的记录或证明；

e) 应检查是否具有系统定级文档和系统属性说明文件等相关材料的使用控制记录。

结果判定

测评实施中 c）~ e）为肯定，则信息系统符合本单元测评项要求。

10) 等级测评(G3)

测评项

a) 在系统运行过程中，应至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改；

b) 应在系统发生变更时及时对系统进行等级测评。发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改；

c) 应选择具有**公安部认可的《全国等级保护测评机构推荐目录》中**的测评单位进行等级测评，并与测评单位签订安全保密协议；

d) 应指定或授权专门的部门或人员负责等级测评的管理。

测评方法

访谈、检查。

测评对象

系统建设负责人。

测评实施

a) 应访谈系统建设负责人，询问是否有等级测评相关的规范要求等文档。是否可按公安部对三级系统的要求进行每年的等级测评并整改；

b) 应访谈系统建设负责人，询问当系统级别发生变化时，是否能及时调整相应的等级保护要求；

c) 应访谈系统建设负责人，询问是否有等级测评机构选择的相关规定，是否有相关留痕文档；

d) 应访谈系统建设负责人，询问是否有专门的部门或人员负责等级测评管理的工作。

结果判定

a) 测评实施中 a）~d）为肯定，则信息系统符合本单元测评项要求。

11) 安全服务商选择(G3)

测评项

a) **选择信息安全服务提供商时应评估其资质、经营行为、业绩、服务体系和服务品质等要素；（F3）**

b) 应确保安全服务商的选择符合国家的有关规定；

c) 应与选定的安全服务商签订与安全相关的协议，明确约定相关责任；

d) 应确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同。

测评方法

访谈。

测评对象

系统建设负责人。

测评实施

a) 应访谈系统建设负责人，询问对信息系统进行安全规划、设计、实施、维护、测评等服务的安全服务单位是否符合国家有关规定。

结果判定

a) 测评实施中 a）为肯定，则信息系统符合本单元测评项要求。

系统建设管理测评对象主要为系统定级、安全方案设计、产品采购、自行软件开发、外包软件开发、工程实施、测评验收、系统交付、系统备案、等级测评和安全服务商选择 11 个控制点相关的文件资料和工作记录。具体内容请参见附录 A.2.2.4。

7.1.2.2.5 系统运维管理

1) 环境管理(G3)

测评项

a) 应建立集中的机房，统一为各信息系统提供运行环境。机房设施配备应符合国家计算机机房有关标准要求；

b) **机房应采用结构化布线系统，配线机柜内如果配备理线架，应做到跳线整齐，跳线与配线架统一编号，标记清晰；（F3）**

c) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；

d) **应指定部门负责机房安全，**指派专人担任机房管理员，对机房的出入进行管理，定期巡查机房运行状况，对机房供配电、空调、温湿度控制等设施进行维护管理，**填写机房值班记录、巡视记录；**

e) **机房管理员应经过相关培训，掌握机房各类设备的操作要领；（F3）**

f) **应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养；（F3）**

g) **机房人员进出机房必须使用主管部门制发的证件；（F3）**

h) **应单独设置弱电井，并留有足够的可扩展空间；（F3）**

i) **机房所在区域应安装24小时视频监控录像装置，重要机房区域实行24小时警卫值班，机房实行封闭式管理，设置一个主出入口和一个或多个备用出入口，出入口控制、入侵报警和电视监控设备运行资料应妥善保管，保存期限不少于3个月，销毁录像等资料应经机构主管领导批准后实施；（F3）**

j) 应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。

测评方式

访谈，检查。

测评对象

物理安全负责人，机房值守人员，机房工作人员，机房安全管理制度，办公环境管理文档，设备维护记录，机房进出登记表，机房电子门禁系统及其电子记录。

测评实施

a) 应访谈物理安全负责人，询问是否指定专人或部门对机房基本设施（如空调、供配电设备等）进行定期维护，由何部门/何人负责，维护周期多长；
b) 应访谈物理安全负责人，询问是否指定人员负责机房安全管理工作，对机房进出管理是否要求制度化和文档化；
c) 应访谈机房值守人员，询问对外来人员进出机房是否采用人工记录和电子记录双重控制；
d) 应访谈工作人员，询问对办公环境的保密性要求事项；
e) 应检查机房安全管理制度，查看其内容是否覆盖机房物理访问、物品带进、带出机房、机房环境安全等方面；
f) 应检查办公环境管理文档，查看其内容是否对工作人员离开座位后的保密行为（如清理桌面文件和屏幕锁定等）、人员调离办公室后的行为等方面进行规定；
g) 应检查机房进出登记表，查看是否记录外来人员进出时间、人员姓名、访问原因等内容；查看是否具有电子门禁系统，电子记录文档是否有时间、人员等信息；
h) 应检查机房基础设施维护记录，查看是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。

结果判定

a) 如果测评实施中c）中访谈人员能够表述出针对办公环境保密性注意事项（如离开座位后应退出登录，并收好敏感性文件等），则该项为肯定；
b) 测评实施中a）~h）均为肯定，则信息系统符合本单元测评项要求。

2) 资产管理(G3)

测评项

a) 应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
b) 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为；
c) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
d) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

测评方式

访谈，检查。

测评对象

安全主管，物理安全负责人，资产管理员，资产清单，资产安全管理制度，信息分类标识文档，设备。

测评实施

a) 应访谈安全主管，询问是否指定资产管理的责任人员或部门,由何部门/何人负责；
b) 应访谈物理安全负责人，询问是否对资产管理要求文档化和制度化；
c) 应访谈资产管理员，询问是否依据资产的重要程度对资产进行赋值和标识管理，不同类别的资产是否采取不同的管理措施；
d) 应检查资产清单，查看其内容是否覆盖资产责任人、所属级别、所处位置、所属部门等方面；
e) 应检查资产安全管理制度，查看其内容是否覆盖资产使用、借用、维护等方面；
f) 应检查信息分类文档，查看其内容是否规定了分类标识的原则和方法（如根据信息的重要程度、敏感程度或用途不同进行分类）；
g) 应检查资产清单中的设备，查看其是否具有相应标识。

结果判定

a) 如果测评实施中c）中访谈人员能够描述出不同的资产管理措施，则该项为肯定；
b) 如果测评实施中g）中设备标识与信息分类标识文档中所要求的一致，则该项为肯定；
c) 测评实施中a）-g）均为肯定，则信息系统符合本单元测评项要求。

3) 介质管理(G3)

测评项

a) 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；
b) 应确保介质存放在安全的环境中，并有明确标识，对各类介质进行控制和保护，并实行存储环境专人管理；
c) **所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放；（F3）**
d) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行安全控制，**应选择安全可靠的传递、交接方式，做好防信息泄露控制措施；**
e) 应对介质归档和查询等进行登记记录，管理员应根据存档介质的目录清单定期盘点；
f) **对于重要文档，如是纸质文档则应实行借阅登记制度，未经相关部门领导批准，任何人不得将文档转借、复制或对外公开，如是电子文档则应采用OA等电子化办公审批平台进行管理；（F3）**
g) **应按照统一格式对技术文档进行编写并及时更新，达到能够依靠技术文档恢复系统正常运行的要求；（F3）**
h) 应对带出工作环境的存储介质进行内容加密和监控管理；
i) 应对送出维修的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁；
j) **对载有敏感信息存储介质的销毁，应报有关部门备案，由科技部门进行信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录，信息消除处理仅限于存储介质仍将在金融机构内部使用的情况，否则应进行信息的不可恢复性销毁；（F3）**
k) **应制定移动存储介质使用规范，并定期核查移动存储介质的使用情况；（F3）**
l) **应建立重要数据多重备份机制，其中至少1份备份介质应存放于科技部门指定的同城或异地安全区域；（F3）**
m) 应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理；
n) **应对技术文档实行有效期管理，对于超过有效期的技术文档降低保密级别，对已经失效的技术文档定期清理，并严格执行技术文档管理制度中的销毁和监销规定；（F3）**
o) **应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。（F3）**

测评方式

访谈，检查。

测评对象

资产管理员，介质管理记录，介质安全管理制度，各类介质，介质存放地，异地存放地。

测评实施

a) 应访谈资产管理员，询问介质的存放环境是否有保护措施，防止其被盗、被毁、被未授权修改以及信息的非法泄漏，是否有专人管理；
b) 应访谈资产管理员，询问是否对介质的使用管理要求制度化和文档化，是否根据介质的目录清单对介质的使用现状进行定期检查，是否定期对其完整性（数据是否损坏或丢失）和可用性（介质是否受到物理破坏）进行检查，是否根据所承载数据和软件的重要性对介质进行分类和标识管理；
c) 应访谈资产管理员，询问对介质带出工作环境（如送出维修或销毁）和重要介质中的数据和软件是否进行保密性处理；对保密性较高的介质销毁前是否有领导批准，对送出维修或销毁的介

质是否对数据进行净化处理；询问对介质的物理传输过程是否要求选择可靠传输人员、严格介质的打包（如采用防拆包装置）、选择安全的物理传输途径、双方在场交付等环节的控制；

d) 应访谈资产管理员，询问是否对某些重要介质实行异地存储，异地存储环境是否与本地环境相同；

e) 应检查介质管理记录，查看其是否记录介质的存储、归档、借用等情况；

f) 应检查介质管理制度，查看其内容是否覆盖介质的存放环境、使用、维护和销毁等方面；

g) 应检查介质，查看是否对其进行了分类，并具有不同标识；

h) 应检查介质本地存放地的实际环境条件是否安全，异地存放地的环境要求和管理要求是否与本地相同，是否有专人对存放地进行管理。

结果判定

a) 测评实施中a）～h）均为肯定，则信息系统符合本单元测评项要求。

4) 设备管理(G3)

测评项

a) 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；

b) 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等；

c) **设备确需送外单位维修时，应彻底清除所存的工作相关信息，并与设备维修厂商签订保密协议，与密码设备配套使用的设备送修前必须请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息，并派专人在场监督；（F3）**

d) **制定规范化的故障处理流程，建立详细的故障日志(包括故障发生的时间、范围、现象、处理结果和处理人员等内容)；（F3）**

e) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；

f) **各机构科技部门负责对信息系统相关的各种设备（包括备份和冗余设备）、线路等进行维护管理；（F3）**

g) **新购置的设备应经过测试，测试合格后方能投入使用；（F3）**

h) **应做好设备登记工作，制定设备管理规范，落实设备使用者的安全保护责任；（F3）**

i) **需要废止的设备，应由科技部门使用专用工具进行数据信息消除处理，如废止设备不再使用或调配到金融机构以外的单位，应由科技部门对其数据信息存储设备进行消磁或物理粉碎等不可恢复性销毁处理，同时备案；（F3）**

j) 应确保信息处理设备必须经过审批才能带离机房或办公地点。

测评方式

访谈，检查。

测评对象

资产管理员，系统管理员，审计员，设备审批管理文档，设备操作规程，设备使用管理文档，设施、软硬件维护管理制度，设备维护记录，服务器操作日志，配置文档。

测评实施

a) 应访谈资产管理员，询问是否对各类设施、设备指定专人或专门部门进行定期维护，由何部门/何人维护，维护周期多长；

b) 应访谈资产管理员，询问是否对设备选用的各个环节（如选型、采购、发放等）进行审批控制，是否对设备带离机构进行审批控制，设备的操作和使用是否要求规范化管理；

c) 应访谈系统管理员，询问其是否在统一安全策略下，对服务器进行正确配置，对服务器的操作是否按操作规程进行；

d) 应访谈系统管理员，询问其是否对软硬件维护进行制度化管理；
e) 应访谈审计员，询问对服务器的操作是否建立日志，日志文件如何管理，是否定期检查管理情况；
f) 应检查设备审批、发放管理文档，查看其是否对设备选型、采购、发放以及带离机构等环节的申报和审批作出规定；查看是否具有设备的选型、采购、发放等过程的申报材料和审批报告；
g) 应检查设备使用管理文档，查看其内容是否覆盖终端计算机、便携机和网络设备等使用、操作原则、注意事项等方面；
h) 应检查服务器操作规程，查看其内容是否覆盖服务器如何启动、停止、加电、断电等操作；
i) 应检查软硬件维护制度，查看其是否覆盖维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等方面。

结果判定

a) 测评实施中 a）-i）均为肯定，则信息系统符合本单元测评项要求。

5) 监控管理和安全管理中心(G3)

测评项

a) 应对通信线路、网络设备、主机和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存；
b) **应建立计算机系统运行监测周报、月报或季报制度，统计分析运行状况；（F3）**
c) 应定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，**发现重大隐患和运行事故应及时协调解决，并报上一级单位相关部门；**
d) 应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。

测评方式

访谈，检查。

测评对象

系统运维负责人，监控记录文档。

测评实施

a) 应访谈系统运维负责人，询问其是否监控主要服务器的各项资源指标，如CPU、内存、进程和磁盘等使用情况；
b) 应访谈系统运维负责人，询问目前信息系统是否由机构自身负责运行维护，如果是，系统运行所产生的文档如何进行管理（如责任书、授权书、许可证、各类策略文档、事故报告处理文档、安全配置文档、系统各类日志等）；
c) 应检查监控记录，查看是否记录监控对象、监控内容、监控的异常现象处理等方面。

结果判定

a) 测评实施中 a）～c）均为肯定，则信息系统符合本单元测评项要求。

6) 网络安全管理(G3)

测评项

a) 应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作，**并有操作和复核人员的签名，维护记录应至少妥善保存3 个月**；
b) 应建立网络安全运行管理制度，对网络安全配置(**最小服务配置**)、日志保存时间、安全策略、升级与打补丁、口令更新周期、**重要文件备份**等方面作出规定；
c) **应制定网络接入管理规范，任何设备接入网络前，接入方案应经过科技部门的审核，审核批准后方可接入网络并分配相应的网络资源；**

d) **应制定远程访问控制规范，确因工作需要进行远程访问的，应由访问发起机构科技部门核准，提请被访问机构科技部门（岗）开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施；（F3）**

e) **各机构以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经科技主管部门批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用；（F3）**

f) **信息安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不得对外公开，未经科技主管部门授权，任何外部机构与人员不得检测或扫描机构内部网络；（F3）**

g) **金融业网间互联安全实行统一规范、分级管理、各负其责的安全管理模式，未经金融机构科技主管部门核准，任何机构不得自行与外部机构实施网间互联；（F3）**

h) **所有网间互联应用系统和外联网络区应定期进行威胁评估和脆弱性评估并提供威胁和脆弱性评估报告。（F3）**

测评方法

访谈，检查。

测评对象

安全主管，安全员，网络管理员，审计员，网络漏洞扫描报告，网络安全管理制度，系统外联授权书，网络审计日志。

测评实施

a) 查阅网络安全管理制度，查看其内容是否覆盖网络安全配置（包括网络设备的安全策略、授权访问、最小服务、升级与打补丁）、审计日志保存时间、升级与打补丁等方面应访谈安全主管，询问是否指定专人负责维护网络运行日志、监控记录和分析处理报警信息等网络安全管理工作；

b) 应访谈安全员，询问是否对网络安全的管理工作（包括网络安全配置、网络用户、日志等方面）制度化，；查阅网络管理员分工，并调阅网络安全运行维护档案；

c) 调阅网络管理员参加网络安全技术培训的文档，检查网间互联设备上配置，并与审批记录进行比对；

d) 调阅非法外联监控系统的记录，并在国际互联网用机上检查是否存储有敏感工作信息；

e) 应访谈安全员，询问网络的外联种类有哪些（互联网、合作伙伴企业网、上级部门网络等），是否都得到授权与批准，由何部门/何人批准；是否定期检查违规联网的行为；

f) 在相关网络设备上检查远程访问控制设置，并调阅远程访问审核记录；

g) 检查网络视频服务是否作了跨区域限制，如可以跨区域点播是否经科技部批准；

h) 应访谈网络管理员，询问是否根据厂家提供的软件升级版本对网络设备进行过升级，目前的版本号为多少，升级前是否对重要文件（帐户数据和配置数据等）进行备份，采取什么方式进行；是否对网络设备进行过漏洞扫描，对扫描出的漏洞是否及时修补；

i) 检查网络设备的配置文件备份，检查网络设备的最小服务配置是如何实现的，调阅配置文件的离线备份；

j) 调阅网络变更记录中的审批、变更时间、配置参数备份；

k) 检查计算机接入国际互联网的申请记录上保密部门的授权；

l) 应检查网络漏洞扫描报告，查看其内容是否覆盖网络存在的漏洞、严重级别、原因分析、改进意见等方面；

m) 应检查网络安全管理制度，查看其内容是否覆盖网络安全配置（包括网络设备的安全策略、授权访问、最小服务、升级与打补丁）、网络帐户（用户责任、义务、风险、权限审批、权限分配、帐户注销等）、审计日志以及配置文件的生成、备份、变更审批、符合性检查等方面；

n) 应检查是否具有内部网络所有外联的授权批准书;应检查是否具有内部网络所有外联的授权批准书，调阅计算机变更用途记录；
o) 对互联网上下载的信息进行病毒检；
p) 应检查在规定的保存时间范围内是否存在网络审计日志。

结果判定

a) 测评实施中 a）~ p）均为肯定，则信息系统符合本单元测评项要求。

7) 系统安全管理(G3)

测评项

a) 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定；
b) 应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则；
c) **系统管理员不得兼任业务操作人员，系统管理员不得对业务数据进行任何增加、删除、修改等操作，系统管理员确需对数据库系统进行业务数据维护操作的，应征得业务部门书面同意，并详细记录维护内容、人员、时间等信息；（F3）**
d) **应每半年至少进行一次漏洞扫描，对发现的系统安全漏洞及时进行修补，扫描结果应及时上报；（F3）**
e) 应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装，并对系统变更进行记录；
f) 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，**重要计算机系统的系统设置要求至少两人在场；**
g) 应定期对运行日志和审计数据进行分析，以便及时发现异常行为；
h) **系统用户权限变更应以书面记录，并经相关管理层批准。（F3）**

测评方法

访谈，检查。

测评对象

安全主管，安全员，系统管理员，审计员，系统安全管理制度，系统审计日志，系统漏洞扫描报告。

测评实施

a) 应访谈安全主管，询问是否指定专人负责系统安全管理；检查本单位的安全管理制度中队系统安全策略、安全配置、日志管理和日常操作流程等方面的规定；
b) 应访谈系统管理员，询问对系统工具的使用（如脆弱性扫描工具）是否采取措施控制不同使用人员及数量；
c) 应访谈系统管理员，询问是否定期对系统安装安全补丁程序，是否在测评环境中测评其对应用系统的影响；在安装系统补丁前是否对重要文件（系统配置、系统用户数据等）进行备份，采取什么方式进行；是否对系统进行过漏洞扫描，发现漏洞是否进行及时修补；
d) 应访谈安全员，询问是否将系统安全管理工作（包括系统安全配置、系统帐户、审计日志等）制度化；
e) 应访谈系统管理员，询问对不常用的系统缺省用户是否采取了一定的处理手段阻止其继续使用（如删除或禁用）；是否对系统帐户安全管理情况是否定期进行检查和分析，发现问题如何处理；
f) 应访谈审计员，询问是否规定系统审计日志保存时间，多长时间；
g) 应检查在规定的保存时间范围内是否存在系统审计日志；

h) 应检查系统漏洞扫描报告，查看其内容是否覆盖系统存在的漏洞、严重级别、原因分析、改进意见等方面；

i) 应检查系统安全管理制度，查看其内容是否覆盖系统安全配置（包括系统的安全策略、授权访问、最小服务、升级与打补丁）、系统帐户（用户责任、义务、风险、权限审批、权限分配、帐户注销等）、审计日志以及配置文件的生成、备份、变更审批、符合性检查等方面。

结果判定

a) 测评实施中a）～i）均为肯定，则信息系统符合本单元测评项要求。

8) 恶意代码防范管理(G3)

测评项

a) 应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取网络上接收文件或邮件之前，先进行病毒检查，对存储设备接入网络系统之前也应进行病毒检查；

b) **金融机构客户端应统一安装病毒防治软件，设置用户密码和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序；（F3）**

c) 应指定专人对网络和主机进行恶意代码检测并保存检测记录；

d) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定；

e) 应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，对防病毒系统不能自动清除的计算机病毒，提出解决办法，并形成书面的报表和总结汇报。

测评方法

访谈，检查。

测评对象

系统运维负责人，安全员，恶意代码防范管理制度，恶意代码检测记录，恶意代码升级记录，恶意代码分析报告，恶意代码集中防范管理中心。

测评实施

a) 应访谈系统运维负责人，询问是否对员工进行基本恶意代码防范意识教育，如告知应及时升级软件版本，使用外来设备、网络上接收文件和外来计算机或存储设备接入网络系统之前应进行病毒检查；

b) 应访谈系统运维负责人，询问是否指定专人对恶意代码进行检测，并保存记录；

c) 应访谈安全员，询问是否将恶意代码防范管理工作（包括防恶意代码软件的授权使用、代码库升级和防范工作情况汇报等）制度化，对其执行情况是否进行检查，检查周期多长；

d) 应访谈安全员，询问是否建立恶意代码防护管理中心，对整个系统的恶意代码管理工作是否实行统一集中管理（统一升级、检测、分析等），是否对恶意代码库的升级情况进行记录，对截获的危险病毒或恶意代码是否进行及时分析处理，并形成书面的报表和总结汇报；

e) 应访谈工作人员，询问其是否熟知恶意代码基本的防范手段，主要包括哪些；

f) 应检查恶意代码防范管理制度，查看其内容是否覆盖防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面；

g) 应检查是否具有恶意代码检测记录、恶意代码库升级记录和分析报告，查看升级记录是否记录升级时间、升级版本等内容；查看分析报告是否描述恶意代码的特征、修补措施等内容；

h) 应检查是否具有恶意代码集中防范管理中心。

结果判定

a) 如果测评实施中 e）中访谈人员回答内容与测评实施 a）回答内容基本一致，则该项为肯定；

b) 测评实施中 a）～h）均为肯定，则信息系统符合本单元测评项要求。

9) 密码管理(G3)

测评项

a) 选用的密码产品和加密算法应符合国家相关密码管理政策规定；

b) **应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员必须是本机构在编的正式员工，并逐级进行备案，规范密钥管理；（F3）**

c) **主机管理员、数据库管理员、网络管理员、业务操作人员均须设置口令密码，至少每3 个月更换一次，口令密码的强度应满足不同安全性要求；（F3）**

d) **敏感计算机系统和设备的口令密码设置应在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经科技部门主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码使用后应立即更改并再次密封存放；（F3）**

e) **密钥注入、密钥管理功能调试和密钥档案的保管应由专人负责。密钥资料须保存在保险柜内。保险柜钥匙由专人负责。使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录；（F3）**

f) **确因工作需要经授权可远程接入内部网络的用户，应妥善保管其身份认证介质及口令密码，不得转借他人使用。（F3）**

测评方法

访谈，检查。

测评对象

安全员，密码管理制度。

测评实施

a) 应访谈安全员，询问密码算法和密钥的使用是否遵照国家密码管理规定；

b) 应检查是否具有密码使用管理制度。

结果判定

a) 测评实施中 a）～b）均为肯定，则信息系统符合本单元测评项要求。

10) 变更管理(G3)

测评项

a) **变更管理应流程化、文档化和制度化，变更流程中应明确变更发起方、实施方的职责，应明确变更方案的测试、审批流程及实施策略，对有可能影响客户利益的变更应事先通知客户并得到客户的确认；（F3）**

b) 应确认系统中要发生的变更，并制定变更方案，**包括变更的组织结构与实施计划、操作步骤、应急及回退方案等，变更方案应经过测试，对于无法测试或不具备测试条件的变更，应得到充分论证和审批**；

c) 应建立变更管理制度，系统发生变更前，向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告；

d) 应建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录；

e) 应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练；

f) **变更前做好系统和数据的备份。风险较大的变更，应在变更后对系统的运行情况进行跟踪；（F3）**

g) **如果需要使用生产环境进行测试，应纳入变更管理，并制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划，确保生产系统的安；（F3）**

h) **当生产中心发生变更时，应同步分析灾备系统变更需求并进行相应的变更，评估灾备恢复的有效性；应尽量减少紧急变更。（F3）**

测评方法

访谈，检查。

测评对象

系统运维负责人，变更方案，系统变更申请书，变更管理制度，变更申报和审批程序文档，变更失败恢复程序文档，变更方案评审记录，变更过程记录文档。

测评实施

a) 应访谈系统运维负责人，询问是否制定变更方案指导系统执行变更；目前系统发生过哪些变更，变更过程是否文档化并保存，是否修改相关的操作流程（如系统配置发生变更后，相应的操作流程是否修改）；

b) 应访谈系统运维负责人，询问重要系统变更前是否根据申报和审批程序得到有关领导的批准，由何人批准，对发生的变更情况是否通知了所有相关人员，以何种方式通知；变更方案是否经过评审；

c) 应访谈系统运维负责人，询问变更失败后的恢复程序、工作方法和人员职责是否文档化，恢复过程是否经过演练；

d) 应检查重要系统的变更申请书，查看其是否有主管领导的批准；

e) 应检查系统变更方案，查看其是否对变更类型、变更原因、变更过程、变更前评估等方面进行规定；

f) 应检查变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容；

g) 应检查变更控制的申报、审批程序，查看其是否规定需要申报的变更类型、申报流程、审批部门、批准人等方面内容；

h) 应检查变更失败恢复程序，查看其是否规定变更失败后的恢复流程；

i) 应检查是否具有变更方案评审记录和变更过程记录文档。

结果判定

a) 如果系统没有发生过变更，则测评实施中 i）不适用；

b) 测评实施中 a）~ i）均为肯定，则信息系统符合本单元测评项要求。

11) 备份与恢复管理(G3)

测评项

a) 应制定数据备份与恢复相关安全管理制度，对备份信息的备份方式、备份频度、存储介质、保存期等进行规范；

b) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；

c) 应建立控制数据备份和恢复过程的程序，记录备份过程，对需要采取加密或数据隐藏处理的备份数据，进行备份和加密操作时要求两名工作人员在场，所有文件和记录应妥善保存；

d) **应每年至少进行一次重要信息系统专项灾备切换演练，每三年至少进行一次重要信息系统全面灾备切换演练，根据不同的应急恢复内容，确定演练的周期，并指定专人管理和维护应急预案，根据人员、信息资源等变动情况以及演练情况适时予以更新和完善，确保应急预案的有效性和灾难发生时的可获取性；（F3）**

e) **应定期对备份数据的有效性进行检查，每次抽检数据量不低于5%。备份数据要实行异地保存；（F3）**

f) **恢复及使用备份数据时需要提供相关口令密码的，应把口令密码密封后与数据备份介质一并妥善保管；（F3）**

g) **灾难恢复的需求应定期进行再分析，再分析周期最长为三年，当生产中心环境、生产系统或业务流程发生重大变更时，单位应立即启动灾难恢复需求再分析工作，依据需求分析制定灾难恢复策略；（F3）**

h) **应建立健全灾难恢复计划，恢复计划至少要包括灾难恢复范围和目标、灾难切换规程、灾后重续运行操作指引、各系统灾难切换操作手册；（F3）**

i) **金融机构应根据信息系统的灾难恢复工作情况，确定审计频率。单位应每年至少组织一次内部灾难恢复工作审计；（F3）**

j) **应定期开展灾难恢复培训，并根据实际情况进行灾难恢复演练；（F3）**

k) **应建立灾难备份系统，主备系统实际切换时间应少于60分钟，灾备系统处理能力应不低于主用系统处理能力的50%，通信线路应分别接入主备系统，有条件时可采用主、备系统处理能力相同、轮换交替使用的双系统模式。（F3）**

测评方法

访谈，检查。

测评对象

系统管理员，数据库管理员，网络管理员，备份管理文档，备份和恢复策略文档，备份设备操作流程文档，备份和恢复程序文档，备份过程记录文档。

测评实施

a) 应访谈系统管理员、数据库管理员和网络管理员，询问是否识别出需要定期备份的业务信息、系统数据及软件系统，主要有哪些；对其备份工作是否以文档形式规范了备份方式、频度、介质、保存期等内容，数据备份和恢复策略是否文档化，备份和恢复过程是否文档化；

b) 应访谈系统管理员、数据库管理员和网络管理员，询问其对备份及冗余设备的安装、配置和启动工作是否根据一定的流程进行，是否记录操作过程，是否保存记录文档，是否指定专人对备份设备的有效性定期维护和检查，多长时间检查一次；

c) 应访谈系统管理员、数据库管理员和网络管理员，询问是否定期执行恢复程序，周期多长，系统是否按照恢复程序完成恢复，如有问题，是否针对问题改进恢复程序或调整其他因素；

d) 应检查是否具有规定备份方式、频度、介质、保存期的文档；

e) 应检查数据备份和恢复策略文档，查看其内容是否覆盖数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面；

f) 应检查备份设备操作流程文档，查看其是否备份及冗余设备的安装、配置、启动、关闭等操作流程；

g) 应检查备份过程记录文档，查看其内容是否覆盖备份时间、备份内容、备份操作、备份介质存放等内容。

结果判定

a) 测评实施中 a）～g）均为肯定，则信息系统符合本单元测评项要求。

12) 安全事件处置(G3)

测评项

a) 应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

b) 应制定安全事件报告和处置管理制度，明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；

c) 应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分；

d) 应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；

e) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；

f) 对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序；

g) **应建立有效的技术保障机制，确保在安全事件处置过程中不会因技术能力缺乏而导致处置中断或延长应急处置时间。（F3）**

测评方法

访谈，检查。

测评对象

系统运维负责人，工作人员，安全事件记录分析文档，安全事件报告和处置管理制度，安全事件报告和处理程序文档。

测评实施

a) 应访谈系统运维负责人，询问是否告知用户在发现安全弱点和可疑事件时应及时报告，安全事件的报告和响应处理过程是否制度化和文档化，不同安全事件是否采取不同的处理和报告程序；
b) 应访谈系统运维负责人，询问本系统已发生的和需要防止发生的安全事件主要有哪几类，对识别出的安全事件是否根据其对系统的影响程度划分不同等级，划分为几级，划分方法是否参照了国家相关管理部门的技术资料，主要参照哪些；
c) 应访谈工作人员，询问其不同安全事件的报告流程；
d) 应检查安全事件报告和处置管理制度，查看其是否明确与安全事件有关的工作职责，包括报告单位（人）、接报单位（人）和处置单位等职责；
e) 应检查安全事件定级文档，查看其内容是否明确安全事件的定义、安全事件等级划分原则、等级描述等方面内容；
f) 应检查安全事件记录分析文档，查看其是否记录引发安全事件的原因，是否记录事件处理过程，不同安全事件是否采取不同措施避免其再次发生；
g) 应检查安全事件报告和处理程序文档，查看其是否根据不同安全事件制定不同的处理和报告程序，是否明确具体报告方式、报告内容、报告人等方面内容。

结果判定

a) 如果测评实施中c）中访谈回答与g）中描述一致，则该项为肯定；
b) 测评实施中a）～g）为肯定，则信息系统符合本单元测评项要求。

13) 应急预案管理(G3)

测评项

a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括应急组织机构、启动应急预案的条件、应急处理流程、系统恢复流程、**事件信息收集、分析、报告制度、**事后教育和培训等内容**，业务处理系统应急预案的编制工作应由相关业务部门和科技部门共同完成，并由预案涉及的相关机构签字盖章；**
b) 应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；
c) 应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次；
d) **在与第三方合作的业务中，应建立并完善内部责任机制和与相关机构之间的协调机制，制定完整的应急预案及应急协调预案，并定期参加联合演练；（F3）**
e) **突发事件应急处置领导小组应统一领导计算机系统的应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业信息安全监管部门；（F3）**
f) **金融机构应急领导小组应及时向新闻媒体发布相关信息，严格按照行业、机构的相关规定和要求对外发布信息，机构内其它部门或者个人不得随意接受新闻媒体采访或对外发表个人看法；（F3）**
g) **实施报告制度和启动应急预案的单位应当实行重大突发事件24小时值班制度；（F3）**
h) **应定期对原有的应急预案重新评估，并根据安全评估结果，定期修订、演练，并进行专项内部审计；（F3）**

i) **应急演练结束后，金融机构应撰写应急演练情况总结报告，总结报告包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练结论。（F3）**

测评方法

访谈，检查。

测评对象

系统运维负责人，应急响应预案文档，应急预案培训记录，应急预案演练记录，应急预案审查记录。

测评实施

a) 应访谈系统运维负责人，询问是否制定不同事件的应急预案，是否对系统相关人员进行应急预案培训，培训内容是什么，多长时间举办一次，是否定期对应急预案进行演练，演练周期多长，是否对应急预案定期进行审查并更新；

b) 应访谈系统运维负责人，询问是否具有应急预案小组，是否具备应急设备并能正常工作，应急预案执行所需资金是否做过预算并能够落实；

c) 应检查应急响应预案文档，查看其内容是否覆盖启动预案的条件、应急处理流程、系统恢复流程、事后教育等内容；

d) 应检查是否具有应急预案培训记录、演练记录和审查记录；

e) 调阅突发事件应急处置领导小组组织文件及职责；

f) 了解应急事件公告发布情况；

g) 调阅应急预案评估材料。

结果判定

a) 测评实施中 a）～g）均为肯定，则信息系统符合本单元测评项要求

系统运维管理测评对象主要为环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置以及应急预案管理 13 个控制点相关的文件资料和工作记录。具体内容请参见附录 A.2.2.5。

7.1.3 第四级信息系统单元测评

7.1.3.1 安全技术测评

7.1.3.1.1 物理安全

1) 物理位置的选择(G4)

测评项

a) 机房应选择在具有防震、**承重**、防风和防雨等能力的建筑内，**应选择交通、通信便捷地区**；

b) **机房应避开火灾危险程度高的区域，周围100米内不得有加油站、煤气站等危险建筑和重要军事目标；（F4）**

c) 机房场地应避免设在建筑物的顶层或地下室，以及用水设备的下层或隔壁。

测评方法

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房，办公场地，机房场地设计/验收文档。

测评实施

a) 应访谈物理安全负责人，询问现有机房和办公场地（放置终端计算机设备）的环境条件是否能够满足信息系统业务需求和安全管理需求，是否具有基本的防震、防风和防雨等能力；询问机房场地是否符合选址要求；机房与办公场地是否尽量安排在一起或物理位置较近；

b) 应访谈机房维护人员，询问是否存在因机房和办公场地环境条件引发的安全事件或安全隐患；如果某些环境条件不能满足，是否及时采取了补救措施；

c) 应检查机房和办公场地的设计/验收文档，是否有机房和办公场地所在建筑能够具有防震、防风和防雨等能力的说明；是否有机房场地的选址说明；是否与机房和办公场地实际情况相符合；
d) 应检查机房和办公场地是否在具有防震、防风和防雨等能力的建筑内；
e) 应检查机房场地是否避免在建筑物的高层或地下室，以及用水设备的下层或隔壁；
f) 应检查机房场地是否避免设在强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区；
g) 如果机房和办公场地的终端显示器、打印机等设备有敏感或密级信息输出，应检查设备摆放位置是否为不易被无关人员看到的隐蔽位置；
h) **应检查机房是否避开火灾危险程度高的区域，周围 100 米内是否没有加油站、煤气站等危险建筑。**

结果判定

a) 测评实施中c）机房场地的选址符合不在建筑物的高层或地下室，以及用水设备的下层或隔壁；不在强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区等要求，则该项为肯定；
b) 如果测评实施中g）中“如果”条件不成立，则该项为不适用；
c) 测评实施中a）～h）均为肯定，则信息系统符合本单元测评项要求。

2) 物理访问控制(G4)

测评项

a) 机房出入口应安排专人值守并配置电子门禁系统，控制、鉴别和记录进入的人员；
b) 需进入机房的来访人员应经过申请和审批流程，由金融机构专人陪同，并限制和监控其活动范围，**对于重要区域还应限制来访人员携带的随身物品；**
c) 应对机房划分区域进行管理，如将机房划分为核心区、生产区、辅助区，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域，**其中核心区是指装有关键业务系统服务器、主要通信设备、网络控制器、通讯保密设备和（或）系统打印设备的要害区域，生产区是指放置一般业务系统服务器、客户端（工作站）等设备的运行区域，辅助区是指放置供电、消防、空调等设备的区域；**
d) 重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员。

测评方式

访谈，检查。

测评对象

物理安全负责人，机房值守人员，机房，机房设施（电子门禁系统），机房安全管理制度，进入机房的登记记录，来访人员进入机房的审批记录，电子门禁系统记录。

测评实施

a) 应访谈物理安全负责人，了解具有哪些控制机房进出的能力；
b) 应访谈物理安全负责人，如果业务或安全管理需要，是否对机房进行了划分区域管理，是否对各个区域都有专门的管理要求；是否严格控制来访人员进入或一般不允许来访人员进入；
c) 应访谈机房值守人员，询问是否认真执行有关机房出入的管理制度，是否对进入机房的人员记录在案；
d) 应检查机房安全管理制度，查看是否有关于机房出入方面的规定；
e) 应检查机房出入口是否有专人值守，是否有值守记录，以及进出机房的人员登记记录；检查机房是否存在电子门禁系统控制之外的出入口；
f) 应检查机房，是否有进入机房的人员身份鉴别措施，如戴有可见的身份辨识标识；
g) 应检查是否有来访人员进入机房的审批记录，进出机房的有关记录是否保存足够的时间；

h) 应检查机房区域划分是否合理，是否在机房重要区域前设置交付或安装等过度区域；是否对不同区域设置不同机房或者同一机房的不同区域之间设置有效的物理隔离装置（如隔墙等）；
i) 应检查机房或重要区域配置的电子门禁系统是否有验收文档或产品安全认证资质；
j) 应检查每道电子门禁系统是否都能正常工作；查看每道电子门禁系统运行、维护记录；查看监控进入机房的电子门禁系统记录，是否能够鉴别和记录进入的人员身份；
k) 应检查视频监控设备是否正常工作，是否能够监视和记录进入的人员活动情况，查看运行和维护记录，监视记录是否保存足够的时间。

结果判定

a) 测评实施中a）至少应包括制订了机房出入的管理制度，指定了专人在机房出入口值守，对进入的人员登记在案并进行身份鉴别，对来访人员须经批准、限制和监控其活动范围，机房配置了电子门禁系统，重要区域配置了第二道电子门禁系统，视频监控设备，该测评实施才为肯定；
b) 如果测评实施中b）认为没有必要对机房进行划分区域管理（如果安全管理需要，计算机设备宜采用分区布置，如可分为主机区、存贮器区、数据输入区、数据输出区、通信区和监控调度区等），则测评实施h）不适用；
c) 测评实施中d）至少应包括制订了机房出入的管理制度，指定了专人在机房出入口值守，对进入的人员登记在案并进行身份鉴别，对来访人员须经批准、限制和监控其活动范围，两道电子门禁系统的管理，该测评实施才为肯定；
d) 测评实施中a）~k）均为肯定，则信息系统符合本单元测评项要求。

3) 防盗窃和防破坏(G4)

测评项

a) 应将主要设备放置在机房内；
b) 应将设备或主要部件放入机柜中进行固定放置并配备安全锁，并设置明显的标签，标注不易除去的标记；
c) 应将通信线缆铺设在隐蔽处，可架空铺设在地板下或置于管道中，**强弱电需隔离铺设并进行统一标识；**
d) 应对磁带、光盘等介质分类标识，存储在介质库或档案室的金属防火柜中；
e) 应利用光、电等技术设置机房防盗报警系统，如**安装红外线探测设备等光电防盗设备，一旦发现有破坏性入侵即时显示入侵部位，并驱动声光报警装置；**
f) **应建立机房设施与场地环境监控系统，进行24小时连续监视，并对监视录像进行记录，监控对象包括机房空调、消防、不间断电源（UPS）、门禁系统等重要设备、设施及其所在区域，监控记录至少保存3个月。（F4）**

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，资产管理员，机房设施，设备管理制度文档，通信线路布线文档，防盗报警系统和监控报警系统的安装测评/验收报告。

测评实施

a) 应访谈物理安全负责人，采取了哪些防止设备、介质等丢失的保护措施；
b) 应访谈机房维护人员，询问主要设备放置位置是否做到安全可控,设备或主要部件是否进行了固定和标记，通信线缆是否铺设在隐蔽处；是否对机房安装的防盗报警系统和监控报警系统进行定期维护检查；
c) 应访谈资产管理员，在介质管理中，是否进行了分类标识，是否存放在介质库或档案室中；询问对设备或存储介质携带出工作环境是否规定了审批程序、内容加密、专人检查等安全保护的措施；

d) 应检查主要设备是否放置在机房内或其它不易被盗窃和破坏的可控范围内；检查主要设备或设备的主要部件的固定情况，是否不易被移动或被搬走，是否设置明显的无法除去的标记；是否有设备物理位置图，是否经常检查设备物理位置的变化；
e) 应检查通信线缆铺设是否在隐蔽处（如铺设在地下或管道中等）；
f) 应检查介质的管理情况，查看介质是否有正确的分类标识，是否存放在介质库或档案室中；是否有异地保存的措施；
g) 应检查机房防盗报警设施是否正常运行，并查看运行和报警记录；应检查机房的摄像、传感等监控报警系统是否正常运行，并查看运行记录、监控记录和报警记录；
h) 应检查有关设备或存储介质携带出工作环境的审批记录，以及专人对内容加密进行检查的记录；各种有关的记录是否保存足够的时间；
i) 应检查是否有设备管理制度文档，通信线路布线文档，介质管理制度文档，介质清单和使用记录，机房防盗报警设施的安全资质材料、安装测评/验收报告；查看文档中的条文是否与设备放置位置、设备或主要部件保护、通信线缆铺设等实际情况一致；
j) **应访谈物理安全负责人，并查看是否使用摄像头或其他访问控制机制，以监控个人对敏感区域的物理访问。检查收集的数据并与其他入口相关联，是否至少保存三个月，法律另有规定的除外。**

结果判定

a) 测评实施中a）中至少应该包括制订了设备管理制度，主要设备放置位置做到安全可控,设备或主要部件进行了固定和标记,通信线缆铺设在隐蔽处,介质分类标识并存储在介质库或档案室，机房安装了防止进入盗窃和破坏的利用光、电等技术设置的机房防盗报警系统；设备或存储介质携带出工作环境的审批程序、内容加密、专人检查等措施；机房设置了摄像、传感等监控报警系统，该测评实施才为肯定；
b) 测评实施中a）~j）均为肯定，则信息系统符合本单元测评项要求。

4) 防雷击(G4)

测评项

a) 机房建筑应设置避雷针等避雷装置；
b) 应设置**通过国家认证的**防雷保安器，防止感应雷；
c) 机房应设置交流电源地线。

测评方式

访谈，检查，测评。

测评对象

物理安全负责人，机房维护人员，机房设施，建筑防雷设计/验收文档。

测评实施

a) 应访谈物理安全负责人，询问为防止雷击事件导致重要设备被破坏采取了哪些防护措施，机房建筑是否设置了避雷装置，是否通过验收或国家有关部门的技术检测；询问机房计算机系统接地是否设置了专用地线；是否在电源和信号线增加有资质的避雷装置，以避免感应雷击；
b) 应访谈机房维护人员，询问机房建筑避雷装置是否有人定期进行检查和维护；询问机房计算机系统接地（交流工作接地、安全保护接地、防雷接地）是否符合**GB50174－2008**《电子计算机机房设计规范》的要求；
c) 应检查机房是否有建筑防雷设计/验收文档，机房接地设计/验收文档，查看是否有地线连接要求的描述，与实际情况是否一致；
d) 应检查机房是否在电源和信号线增加有资质的避雷装置,以避免感应雷击；
e) 应测评机房安全保护地、防雷保护地、交流工作地的接地电阻，是否达到了**GB50174－2008**《电子计算机机房设计规范》的接地电阻要求。

结果判定

a) 测评实施中a）至少还应包括符合GB 50057－1994《建筑物防雷设计规范》（GB157《建筑防雷设计规范》）中的计算机机房防雷要求，如果在雷电频繁区域，是否装设浪涌电压吸收装置等，则该项为肯定；
b) 测评实施中b）要求地线的引线应和大楼的钢筋网及各种金属管道绝缘，交流工作接地的接地电阻不应大于4Ω，安全保护地的接地电阻不应大于4Ω；防雷保护地（处在有防雷设施的建筑群中可不设此地）的接地电阻不应大于10Ω的要求，则该项为肯定；
c) 测评实施中a）～e）均为肯定，则信息系统符合本单元测评项要求。

5) 防火(G4)

测评项

a) 机房应设置有效的自动灭火系统，**能够通过在机房内、基本工作房间内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位应设置烟感、温感等多种方式**自动检测火情、自动报警；
b) **机房应备有对计算机设备影响小的气体灭火器；（F4）**
c) **机房及相关的工作房间和辅助房应采用至少2级耐火等级的建筑材料；（F4）**
d) 机房应采取区域隔离防火措施，将重要设备与其他设备隔离开；
e) **机房应设置自动消防报警系统（自动和手动两种触发装置齐全），并备有灭火器。消防报警系统应具有与空调系统、新风系统、门禁系统联动的功能，一般工作状态为手动触发；（F4）**
f) **机房内所使用的设备线缆应符合消防要求，纸张，磁带和胶卷等易燃物品，要放置于金属制的防火柜内；（F4）**
g) **采用管网式洁净气体灭火系统或高压细水雾灭火系统的主机房，应同时设置两种火灾探测器，且火灾报警系统应与灭火系统联动；凡设置洁净气体灭火系统的主机房，应配置专用空气呼吸器或氧气呼吸器；（F4）**
h) **应定期检查消防设施，每半年至少组织一次消防演练；（F4）**
i) **机房应设置二个以上消防逃生通道，同时应保证机房内各分区到各消防通道的道路通畅，方便人员逃生时使用。在机房通道上应设置显著的消防标志。（F4）**

测评方式

访谈，检查。

测评对象

物理安全负责人，机房值守人员，机房设施，机房安全管理制度，机房防火设计/验收文档，自动消防系统设计/验收文档。

测评实施

a) 应访谈物理安全负责人，询问机房是否设置了灭火设备，是否设置了自动检测火情、自动报警、自动灭火的自动消防系统，是否有专人负责维护该系统的运行，是否制订了有关机房消防的管理制度和消防预案，是否进行了消防培训；
b) 应访谈机房值守人员，询问对机房出现的消防安全隐患是否能够及时报告并得到排除；是否参加过机房灭火设备的使用培训，是否能够正确使用灭火设备和自动消防系统（喷水不适用于机房）；是否能够做到随时注意防止和消灭火灾隐患；
c) 应检查机房是否设置了自动检测火情（如使用温感、烟感探测器）、自动报警、自动灭火的自动消防系统，摆放位置是否合理，有效期是否合格；应检查自动消防系统是否正常工作，查看运行记录、报警记录、定期检查和维修记录；
d) 应检查是否有机房消防方面的管理制度文档； 检查是否有机房防火设计/验收文档；检查是否有机房自动消防系统的设计/验收文档，文档是否与现有消防配置状况一致；检查是否有机房及相关房间的建筑材料、区域隔离防火措施的验收文档或消防检查验收文档；

e) 应检查机房是否采取区域隔离防火措施，将重要设备与其他设备隔离开；
f) 应检查机房是否设置防火救生门以及应急照明设备；
g) **应检查机房是否设置自动消防报警系统（自动和手动两种触发装置齐全），并备有灭火器。消防报警系统应具有与空调系统、新风系统、门禁系统、UPS联动的功能，一般工作状态为手动触发。**

结果判定

a) 测评实施中a）～g）均为肯定，则信息系统符合本单元测评项要求。

6) 防水和防潮(G4)

测评项

a) **水管不宜穿过机房屋顶，但若有穿过地板应当采取保护防范措施；**
b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
c) **为便于地下积水的转移，漏水隐患区域地面周围应设排水沟和地漏，当采用吊顶上布置空调风口时，风口位置不宜设置在设备正上方以避免水蒸气结露和渗透；**
d) 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房设施，建筑防水和防潮设计/验收文档，防水检测报警系统设计/验收文档，机房湿度记录，除湿装置运行记录。

测评实施

a) 应访谈物理安全负责人，询问机房建设是否有防水防潮措施；如果机房内有上下水管安装，是否穿过屋顶和活动地板下，穿过墙壁和楼板的水管是否采取必要的保护措施，如设置套管；在湿度较高地区或季节是否有人负责机房防水防潮事宜，配备除湿装置；
b) 应访谈机房维护人员，询问机房是否出现过漏水和返潮事件；如果机房内有上下水管安装，是否经常检查是否有漏水情况；在湿度较高地区或季节是否有人负责机房防水防潮事宜，使用除湿装置除湿；如果出现机房水蒸气结露和地下积水的转移与渗透现象是否采取防范措施；
c) 应检查机房是否有建筑防水和防潮设计/验收文档，是否能够满足机房防水和防潮的需求，是否机房防水防潮的实际情况一致；
d) 如果有管道穿过主机房墙壁和楼板处，应检查是否有必要的保护措施，如设置套管等；
e) 应检查机房是否不存在屋顶和墙壁等出现过漏水、渗透和返潮现象，机房及其环境是否不存在明显的漏水和返潮的威胁；如果出现漏水、渗透和返潮现是否能够及时修复解决；
f) 如果在湿度较高地区或季节，应检查机房是否有湿度记录，是否有除湿装置并能够正常运行，是否有防止出现机房地下积水的转移与渗透的措施，是否有防水防潮处理记录和除湿装置运行记录，与机房湿度记录情况是否一致；
g) 如果机房受到漏水威胁很高，应检查是否设置水敏感的检测仪表或元件，对机房进行防水检测和报警，查看该仪表或元件是否正常运行以及运行记录，是否有人负责此项工作。

结果判定

a) 如果测评实施中d）、f）、g）中“如果”条件不成立，则该项为不适用；
b) 测评实施中a）～g）均为肯定，则信息系统符合本单元测评项要求。

7) 防静电(G4)

测评项

a) 设备应采用必要的接地防静电措施；
b) 机房应采用防静电地板；
c) **进入机房应准备鞋套，减少带入机房的灰尘；（F4）**

d) 应采用静电消除器等装置，减少静电的产生；

e) **主机房和辅助区内的工作台面宜采用导静电或静电耗散材料。（F4）**

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房设施，防静电设计/验收文档，湿度记录，除湿操作记录。

测评实施

a) 应访谈物理安全负责人，询问机房是否采用必要的接地等防静电措施，是否有控制机房湿度的措施；在静电较强地区的机房是否采取了有效的防静电措施；

b) 应访谈机房维护人员，询问是否经常检查机房湿度，并控制在GB2887中的规定的范围内；询问机房是否存在静电问题或因静电引起的故障事件；如果存在静电时是否及时采取消除静电的措施；

c) 应检查机房是否有防静电设计/验收文档，与实际情况是否一致；

d) 应检查机房是否有安全接地，查看机房的相对湿度的记录是否符合GB2887中的规定，查看机房是否不存在明显的静电现象；

e) 如果在静电较强的地区，应检查机房是否了采用了如防静电地板、防静电工作台、以及静电消除剂和静电消除器等措施；应查看使用静电消除剂或静电消除器等的除湿操作记录；

f) 在静电较强的地区，应测评机房的相对湿度是否符合GB2887中的规定。

结果判定

a) 测评实施中e）中有效的防静电措施，可以包括如防静电地板、防静电工作台，或静电消除剂和静电消除器等措施的部分或全部，则该项为肯定；

b) 如果测评实施中e）中“如果”条件不成立，则该项为不适用；

c) 测评实施中a）～f）均为肯定，则信息系统符合本单元测评项要求。

8) 温湿度控制(G4)

测评项

a) **设备开机时主机房的温、湿度应执行A级，基本工作间可根据设备要求按A，B两级执行，其他辅助房间应按设备要求确定；**

开机时计算机机房内的温、湿度，应符合表5的规定：

表5 机房温湿度四级要求

级别 / 项目	A 级		B 级
	夏天	冬天	全年
温度	23±1℃	20±2℃	18~28℃
相对湿度(开机时)	40%~55%		35%~75%
相对湿度(停机时)	40%~70%		20%~80%
温度变化率	< 5℃/h 并不得结露		< 10℃/h 并不得结露

b) **机房应采用专用空调设备，空调机应带有通信接口，通信协议应满足机房监控系统的要求；（F4）**

c) **空调系统的主要设备应有备份，空调设备在容量上应有一定的余量；（F4）**

d) **安装在活动地板上及吊顶上的送风口、回风口应采用难燃材料或非燃材料；（F4）**

e) **采用空调设备时，应设置漏水报警装置，并设置防水小堤，还应注意冷却塔、泵、水箱等供水设备的防冻、防火措施。（F4）**

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房设施，温湿度控制设计/验收文档，温湿度记录、运行记录和维护记录。

测评实施

a) 应访谈物理安全负责人，询问机房是否配备了恒温恒湿系统，保证温湿度能够满足计算机设备运行的要求，是否在机房管理制度中规定了温湿度控制的要求，是否有人负责此项工作；
b) 应访谈机房维护人员，询问是否定期检查和维护机房的温湿度自动调节设施，询问是否出现过温湿度影响系统运行的事件；
c) 应检查机房是否有温湿度控制设计/验收文档，是否能够满足系统运行需要，是否与当前实际情况相符合；
d) 应检查恒温恒湿系统是否能够正常运行，查看温湿度记录、运行记录和维护记录；查看机房温、湿度是否满足GB 2887-89《计算站场地技术条件》的要求。

结果判定

a) 测评实施中a）～d）均为肯定，则信息系统符合本单元测评项要求。

9) 电力供应(A4)

测评项

a) **计算机系统供电应与其他供电分开；（F4）**
b) 应在机房供电线路上配置稳压器和过电压防护设备；
c) **应按照双路供电的原则设置**冗余或并行的电力电缆线路为计算机系统供电；
d) **应建立发电机等备用供电系统（如备用发电机），以备临时供电系统停电时启用，并确保备用供电系统能在UPS供电时间内到位，每年需进行备用供电系统的模拟演练，并定期对备用电力供应设备进行检修和维护，确保其能正常使用；**
e) **UPS供电系统的冗余方式应采用N+1、N+2、2N、2(N+1) 等方式，负载功率小于单机UPS额定功率的80%，并通过两路独立市电提供UPS输入，,UPS后备时间至少4小时。核心区域、重要设备应由不同的UPS提供双回路供电；（F4）**
f) **机房内要求采用机房专用插座，机房内分别设置维修和测试用电源插座，两者应有明显区别标志。市电、UPS电源插座分开，满足负荷使用要求；（F4）**
g) **计算机系统应选用铜芯电缆，避免铜、铝混用。若不能避免时，应采用铜铝过渡头连接；（F4）**
h) **机房应设置应急照明和安全出口指示灯，供配电柜（箱）和分电盘内各种开关、手柄、按钮应标志清晰，防止误操作。（F4）**

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房设施，电力供应安全设计/验收文档，检查和维护记录。

测评实施

a) 应访谈物理安全负责人，询问计算机系统供电线路是否与其他供电分开；询问计算机系统供电线路上是否设置了稳压器和过电压防护设备；是否设置了短期备用电源设备（如UPS），供电时间是否满足系统最低电力供应需求；是否安装了冗余或并行的电力电缆线路（如双路供电方式）；是否建立备用供电系统（如备用发电机）；
b) 应访谈机房维护人员，询问是对在计算机系统供电线路上的稳压器、过电压防护设备、短期备用电源设备等进行定期检查和维护；是否能够控制电源稳压范围满足计算机系统运行正常；

c) 应访谈机房维护人员，询问冗余或并行的电力电缆线路（如双路供电方式）在双路供电切换时是否能够对计算机系统正常供电；是否定期检查备用供电系统（如备用发电机），是否能够在规定时间内正常启动和正常供电；

d) 应检查机房是否有电力供应安全设计/验收文档，查看文档中是否标明单独为计算机系统供电，配备稳压器、过电压防护设备、备用电源设备以及冗余或并行的电力电缆线路等要求；查看与机房电力供应实际情况是否一致；

e) 应检查计算机供电线路，查看计算机系统供电是否与其他供电分开；

f) 应检查机房，查看计算机系统供电线路上的稳压器、过电压防护设备和短期备用电源设备是否正常运行，查看供电电压是否正常；

g) 应检查是否有稳压器、过电压防护设备以及短期备用电源设备等电源设备的检查和维护记录，以及冗余或并行的电力电缆线路切换记录，备用供电系统运行记录；以及上述计算机系统供电的运行记录，是否能够符合系统正常运行的要求；

h) 应测评安装的冗余或并行的电力电缆线路（如双路供电方式），是否能够进行双路供电切换；

i) 应测评备用供电系统（如备用发电机）是否能够在规定时间内正常启动和正常供电；

j) **应检查UPS供电系统的冗余方式应采用N+1、N+2、2N、2(N+1) 等方式，负载功率小于单机UPS额定功率的65%，并通过两路独立市电提供UPS输入。如没有建立柴油发电机应急供电系统的单位，UPS后备时间是否至少2小时。核心区域、重要设备是否由不同的UPS提供双回路供电；**

结果判定

a) 测评实施中a）~j）均为肯定，则信息系统符合本单元测评项要求。

10) 电磁防护(S4)

测评项

a) 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；

b) 电源线和通信线缆应隔离铺设，避免互相干扰；

c) 应对关键区域和**重要设备**以及磁介质实施电磁屏蔽；

d) **计算机系统设备网络布线不得与空调设备、电源设备的无电磁屏蔽的布线平行；交叉时，应尽量以接近于垂直的角度交叉，并采取防延燃措施。(F4)**

测评方式

访谈，检查。

测评对象

物理安全负责人，机房维护人员，机房设施，电磁防护设计/验收文档，电子屏蔽装置或屏蔽机房设计/验收文档，电磁泄露测评报告。

测评实施

a) 应访谈物理安全负责人，询问是否有防止外界电磁干扰和设备寄生耦合干扰的措施（包括设备外壳有良好的接地；电源线和通信线缆隔离等）；是否对处理秘密级信息的设备采取了防止电磁泄露的措施；是否在必要时对机房采用了电子屏蔽或安装屏蔽机房；

b) 应访谈机房维护人员，询问是否对设备外壳做了良好的接地；是否做到电源线和通信线缆隔离；是否出现过因电磁防护问题引发的故障；处理秘密级信息的设备是否为低辐射设备，是否安装了满足BMB4-2000《电磁干扰器技术要求和测评方法》要求的二级电磁干扰器；

c) 应检查机房是否有电磁防护设计/验收文档，与实际情况是否一致；是否有电子屏蔽或屏蔽机房设计/验收文档；是否有电子屏蔽或屏蔽机房的管理制度文档；

d) 应检查机房是设备外壳是否有安全接地；

e) 应检查机房布线，查看是否做到电源线和通信线缆隔离；

f) 应检查使用电磁干扰器的涉密设备开机，是否同时开启电磁干扰器；

g) 如果对机房采用了电子屏蔽，应检查在机房有设备运行时是否开启了电子屏蔽装置；如果安装了屏蔽机房，应检查进入机房的电源线和非光纤通信线是否经过滤波器，光纤通信线是否经过波导管，机房门是否及时关闭，屏蔽机房是否定期测评电磁泄露，应查看电磁泄露测评报告；

h) 如果对机房采用了电子屏蔽或安装了屏蔽机房，应测评屏蔽机房的电磁泄露状况（参考标准GB12190-90 高性能屏蔽效能的测量方法）。

结果判定

a) 测评实施中g）、h）中“如果”条件不成立，则该项为不适用；

b) 测评实施中a）～h）均为肯定，则信息系统符合本单元测评项要求。

在内容上，物理安全测评实施过程涉及 10 个工作单元，具体检查表请参见附录 A.3.1.1。

7. 1. 3. 1. 2 网络安全

1) 结构安全 (G4)

测评项

a) 应保证**主要网络设备和通信线路**冗余，**主要网络设备业务处理能力能**满足业务高峰期**需要的2倍以上，双线路设计时，宜由不同的服务商提供；**

b) 应保证网络各个部分的带宽满足业务高峰期需要；

c) 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；

d) 应绘制与当前运行情况相符的网络拓扑结构图；

e) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段，**生产网、互联网、办公网之间都应实现有效隔离；**

f) 应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；

g) 应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机；

h) **应使用前置设备实现跨机构联网系统与入网金融机构业务主机系统的隔离，防止外部系统直接对入网金融机构业务主机的访问和操作；（F4）**

i) **应使用专用网络用于金融机构间的重要信息交换，与公用数据网络隔离；（F4）**

j) **机构应至少通过两条主干链路接入跨机构交易交换网络，并可根据实际情况选择使用专用的通信链路。两条主干链路应具有不同的路由，当一条链路发生异常时，另一条链路应能承载全部的交易数据。（F4）**

测评方式

访谈，检查，测评。

测评对象

网络管理员，边界和主要网络设备，网络拓扑图，网络设计/验收文档。

测评实施

a) 可访谈网络管理员，询问信息系统中的边界和主要网络设备的性能以及目前业务高峰流量情况；

b) 可访谈网络管理员，询问网段划分情况以及划分的原则；询问重要的网段有哪些，对重要网段的保护措施有哪些；

c) 可访谈网络管理员，询问网络的带宽情况；询问网络中带宽控制情况以及带宽分配的原则；

d) 可访谈网络管理员，询问网络设备上的路由控制策略措施有哪些，这些策略设计的目的是什么；

e) 应检查网络拓扑图，查看与当前运行情况是否一致；

f) 应检查网络设计/验收文档，查看边界和主要网络设备的带宽占用报表是否有达到或超过处理能力记录；

g) 应检查设计/验收文档，查看是否有是否根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网和网段分配地址段的设计或描述；

h) 应检查边界和主要网络设备，查看是否配置路由控制策略（如使用静态路由等）建立安全的访问路径，在业务终端trace 业务服务器地址，查看访问路径所经节点是否符合路由控制策略；

i) 应检查边界和主要网络设备，检查是否将重要网段部署至网络边界与外部信息系统直连，重要网段与其他网段间是否使用防火墙、访问控制等手段隔离；

j) 应检查边界和主要网络设备，查看是否有对带宽进行控制的策略（如路由、交换设备上的QOS策略配置情况，专用的带宽管理设备的配置策略等），并且这些策略能否保证在网络发生拥堵的时候优先保护重要业务（如重要业务的主机的优先级要高于非重要业务的主机）；

k) 应测评网络拓扑结构，可通过网络拓扑结构自动发现、绘制工具，验证实际的网络拓扑结构和网络拓扑结构图是否一致；

l) 应测评业务终端与业务服务器之间的访问路径，可通过使用路由跟踪工具，验证业务终端与业务服务器之间的访问路径的是否安全（如访问路径是否固定等）；

m) **应测评重要网段，验证其采取的网络地址与数据链路地址绑定措施或数据链路层地址与交换机端口绑定的措施是否有效（如试图使用非绑定地址，查看是否能正常访问等）；**

n) 应测评网络带宽分配策略，可通过使用带宽测评工具，验证网络带宽分配是否有效；

o) **应访谈网络管理员，是否使用专用网络用于入网银行与信息交换中心的联网，与公用数据网络隔离；**

p) **应访谈网络管理员，是否使用前置设备实现跨行联网系统与入网银行业务主机系统的隔离，防止外部系统直接对入网银行业务主机的访问和操作；**

q) **应访谈网络管理员，机构是否至少通过两条主干链路接入跨行交易交换网络，并可根据实际情况选择使用DDN、FR或其它方式的通信链路。两条主干链路应具有不同的路由，当一条链路发生异常时，另一条链路应能承载全部的交易数据；**

r) **应访谈网络管理员，机构是否保证拥有至少一条备份线路（如拨号线路）与跨行交易交换网络相连，当两条主干链路都发生异常时，备份链路应能承担所有的交易数据；**

s) **应访谈网络管理员并检查，机构与交换中心之间的连接是否由本地 IP 地址、端口号和远程 IP 地址、端口号唯一确定。**

结果判定

a) 如果测评实施中 f）～g）中缺少相应的文档，则该项为否定；

b) 测评实施中 e）～s）均为肯定，则信息系统符合本单元测评项要求。

2) 访问控制(G4)

测评项

a) 应在网络边界部署访问控制设备，启用访问控制功能；

b) 应不允许数据带通用协议通过；

c) 应根据数据的敏感标记允许或拒绝数据通过；

d) 应不开放远程拨号访问功能；

e) 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户；

f) 应在网络区域边界(互联网区域边界、外部区域边界和内部区域边界)**对**网络最大流量数**及网络并发连接数进行监控；**

g) **网络设备应按最小安全访问原则设置访问控制权限。（F4）**

测评方式

访谈，检查，测评。

测评对象

安全员，**网络管理员**，边界和主要网络设备。

测评实施

a) 可访谈安全员，询问采取网络访问控制的措施有哪些；询问访问控制策略的设计原则；询问访问控制策略是否做过调整，以及调整后和调整前的情况如何；

b) 应检查主要网络设备，查看是否有相应的访问控制措施（如 VLAN，访问控制列表，MAC 地址绑定）禁止便携式和移动式设备接入网络；

c) 应检查边界网络设备，查看是否有相应的访问控制措施来实现禁止数据带通用协议通过；

d) 应测评边界和主要网络设备，可通过试图用移动设备接入网络，测评网络设备的访问控制措施是否有效；

e) 应测评边界和主要网络设备，可通过发送带通用协议的数据（如使用 http 隧道工具），测评访问控制措施是否有效阻断这种连接；

f) 限制对无线访问点、网关和手持式设备的物理访问；

g) 应关闭不使用的网络通讯端口。

结果判定

a) 测评实施中 b）~ f）均为肯定，则信息系统符合本单元测评项要求。

3) 安全审计(G4)

测评项

a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；

b) 审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c) 应能够根据记录数据进行分析，并生成审计报表；

d) 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等，**保存时间不少于一年；**

e) 应定义审计跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施，防止审计数据丢失；

f) 应根据信息系统的统一安全策略，实现集中审计，时钟保持与时钟服务器同步。

测评方式

访谈，检查，测评。

测评对象

审计员，边界和主要网络设备（包括安全设备）。

测评实施

a) 可访谈审计员，询问是否对网络系统中的边界和关键网络设备的审计包括哪些项；询问审计记录的主要内容有哪些；对审计记录的处理方式有哪些；

b) 应检查日志服务器或AAA服务器，查看审计策略是否对网络系统中的网络设备运行状况、网络流量、用户行为等进行全面的监测、记录；

c) 应检查日志服务器或AAA服务器，查看事件审计策略是否包括：事件的日期和时间、用户、事件类型、事件成功情况，及其他与审计相关的信息；

d) 应检查日志服务器或AAA服务器，查看是否可以对特定事件，是否提供指定方式的实时报警（如声音、EMAIL、短信等）；

e) 应检查日志服务器或AAA服务器，查看其是否为授权用户浏览和分析审计数据具备生成报表的功能（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表；

f) 应检查日志服务器或 AAA 服务器，查看其审计跟踪设置是否定义了审计跟踪极限的阈值，当存储空间被耗尽时，能否采取必要的保护措施，例如，报警并导出、丢弃未记录的审计信息、暂停审计或覆盖以前的审计记录等；

g) 应测评日志服务器或 AAA 服务器，可通过以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），验证安全审计的覆盖情况和记录情况与要求是否一致；
h) 应测评日志服务器或 AAA 服务器，可通过以某个系统用户试图删除、修改或覆盖审计记录，验证安全审计的保护情况与要求是否一致；
i) 应测评日志服务器或 AAA 服务器，验证其能否跟踪监测到可能的安全侵害事件，并终止违规进程的功能是否正确（如产生一定的安全侵害事件，查看安全审计能否检测到该事件，并终止其进程）。

结果判定

a) 测评实施中 b）~ i）均为肯定，则信息系统符合本单元测评项要求。

4) 边界完整性检查(S4)

测评项

a) 应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；
b) 应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

测评方式

访谈，检查，测评。

测评对象

安全员，**网络管理员**，边界完整性检查设备，边界完整性检查设备运行日志。

测评实施

a) 应检查边界完整性检查设备，查看是否有未安装非法外联客户端的计算机接入网络，若有是否采取进行定位、阻断；
b) 应检查边界完整性检查工具运行日志，**查看运行是否正常（查看是否持续对网络全网段进行监控）；**
c) 应检查边界完整性检查设备/工具，查看是否设置了同时对非法联接到内网和非法联接到外网的行为进行监控；查看是否对发现的非法联接行为进行有效的阻断；
d) 应该检查边界网络设备，查看是否设置相关措施能够根据信息流控制策略和信息流的敏感标记，阻止重要信息的流出（网络设备标记，指定路由信息标记）；
e) 应测评边界完整性检查设备，测评是否能有效的发现“非法外联”的行为（如产生非法外联的动作，查看边界完整性检查设备是否能够发现该行为）；
f) 应测评边界完整性检查设备，测评是否确定出“非法外联”设备的位置，并对其进行有效阻断（如产生非法外联的动作，查看边界完整性检查设备是否能够准确定位并阻断）；
g) 应测评边界完整性检查设备，测评是否能够对非授权设备私自联到网络的行为进行检查，并准确定出位置，对其进行有效阻断（如产生非法接入的动作，查看测评边界完整性检查设备是否能准确的发现，准确的定位并产生阻断）。

结果判定

a) 测评实施中 b）~ g）均为肯定，则信息系统符合本单元测评项要求。

5) 入侵防范(G4)

测评项

a) 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、注入式攻击、IP碎片攻击和网络蠕虫攻击等；
b) 当检测到攻击行为时，应记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警及自动采取相应动作；
c) **入侵检测的管理系统应做到分级管理，对系统的部署做到逐级分布。（F4）**

测评方式

访谈，检查，测评。

测评对象

安全员，网络入侵防范设备。

测评实施

a) 可访谈安全员，询问网络入侵防范措施有哪些；是否有专门的设备对网络入侵进行防范；询问网络入侵防范规则库的升级方式；
b) 应检查网络入侵防范设备，查看是否能检测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击、网络蠕虫攻击等入侵事件；
c) 应检查网络入侵防范设备，查看入侵事件记录中是否包括入侵的源IP、攻击的类型、攻击的目的、攻击的时间等；查看是否设置了安全警告方式（如采取屏幕实时提示、E-mail告警、声音告警等）；
d) 应检查网络入侵防范设备，查看其生产厂商是否为正规厂商，规则库是否为最新；
e) 应测评网络入侵防范设备，验证其监控策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备的反应）；
f) 应测评网络入侵防范设备，验证其报警策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备是否能实时报警）。

结果判定

a) 测评实施中b）~ f）均为肯定，则信息系统符合本单元测评项要求。

6) 恶意代码防范(G4)

测评项

a) 应在**与外单位与互联网连接的**网络边界处对恶意代码进行检测和清除；
b) 应定期对恶意代码防护设备进行代码库升级和系统更新。

测评方式

访谈，检查。

测评对象

安全员，防恶意代码产品，设计/验收文档， 恶意代码产品运行日志。

测评实施

a) 可访谈安全员，询问系统中的网络防恶意代码防范措施是什么；询问恶意代码库的更新策略；询问防恶意代码产品的有哪些主要功能；询问系统是否发生过针对恶意代码入侵的安全事件；
b) 应检查设计/验收文档，查看其是否有在网络边界及核心业务网段处是否有对恶意代码的采取相关措施（如是否有防病毒网关），防恶意代码产品是否有实时更新的功能的描述；
c) 应检查恶意代码产品运行日志，查看是否持续运行；
d) 应检查在网络边界及核心业务网段处是否根据恶意代码特征采取措施从网络层进行检测和清除；
e) 应检查防恶意代码产品，查看是否为正规厂商生产，运行是否正常，恶意代码库是否为最新版本；
f) 应检查防恶意代码产品的配置策略，查看是否支持恶意代码防范的统一管理（如查看是否为分布式部署，集中管理等）。

结果判定

a) 如果测评实施中b）中缺少相应的文档，则该项为否定；
b) 测评实施中b）~ f）均为肯定，则信息系统符合本单元测评项要求。

7) 网络设备防护(G4)

测评项

a) 应对登录网络设备的用户进行身份鉴别；

b) 应对网络设备的管理员登录地址进行限制；
c) 网络设备用户的标识应唯一；
d) 主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；
e) 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；
f) 网络设备用户的身份鉴别信息至少应有一种是不可伪造的；
g) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
h) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
i) 应实现设备特权用户的权限分离；
j) **对网络设备系统自带的的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端口开放审批制度；（F4）**
k) **应每季度检验网络设备软件版本信息，并通过有效测试验证进行相应的升级；（F4）**
l) **应建立网络设备的时钟同步机制；（F4）**
m) **应每月对网络设备的配置文件进行备份，发生变动时应及时备份；（F4）**
n) **应每季度检查并锁定或撤销网络设备中不必要的用户账号。（F4）**

测评方式

访谈，检查，测评。

测评对象

网络管理员，边界和主要网络设备（包括安全设备）。

测评实施

a) 可访谈网络管理员，是否对网络设备进行AAA认证或其他认证方式，若有登录AAA服务器，查看用户与管理员身份、权限是否匹配；
b) 应访谈网络管理员，询问采取的网络设备的口令策略是什么；
c) 应检查边界和主要网络设备的安全设置，查看其是否有对鉴别失败采取相应的措施的设置；查看是否有限制非法登录次数的功能；
d) 应检查边界和主要网络设备的安全设置，查看是否对主要网络设备的管理员登录地址进行限制；查看是否设置网络登录连接超时，并自动退出；查看是否实现设备特权用户的权限分离；查看是否对网络上的对等实体进行身份鉴别；应测评边界和主要网络设备的安全设置，验证鉴别失败处理措施是否有效（采用错误密码登录网络设备数次，观察是否结束会话、限制非法登录次数，对网络设备的管理员登录地址进行限制（如使用任意地址登录，观察网络设备的动作等）等功能是否有效；
e) 应测评边界和主要网络设备的安全设置，验证其网络登录连接超自动退出的设置是否有效（如长时间连接无任何操作，观察观察网络设备的动作等）；
f) 应对边界和主要网络设备进行渗透测评，通过使用各种渗透测评技术（如口令猜解等）对网络设备进行渗透测评，验证网络设备防护能力是否符合要求；
g) 应登录远程登录网络设备，看是否采用22端口SSH方式或其他加密方式；
h) 应上机查阅备份文件；
i) **应查看检查表，是否每周对网络设备运行状况进行检查；**
j) **应检查是否关闭不必要的网络设备服务；**
k) **应现场访谈网络设备管理员是否每周检验网络设备软件版本信息并书面记录，并通过有效测试验证进行相应的升级；**
l) **应访谈网络设备管理员，是否每周检查并锁定或撤销网络设备中多余的用户账号。**

结果判定

a) 如果网络设备的口令策略为口令长度8位以上，口令复杂（如规定字符应混有大、小写字母、数字和特殊字符），口令生命周期，新旧口令的替换要求（规定替换的字符数量）或为了便于记忆使用了令牌；则测评实施中b）满足测评要求；

b) 测评实施中b）～h）均为肯定，则信息系统符合本单元测评项要求。

在内容上，网络安全层面测评实施过程涉及7个工作单元，具体内容请参见附录A.3.1.2。

7.1.3.1.3 主机安全

1) 身份鉴别（S4）

测评项

a) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；

b) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，**系统的静态口令应在8位以上并由字母、数字、符号等混合组成，至少每月更换口令一次；**

c) 应启用登录失败处理功能，可采取结束会话、限制登录间隔、限制非法登录次数和自动退出等措施；

d) **应设置鉴别警示信息，当出现越权访问或尝试非法访问时，系统会自动提示未授权访问；**

e) **主机系统应对与之相连的服务器或终端设备进行身份标识和鉴别，当通过互联网对服务器进行远程管理时，应采取加密措施，防止鉴别信息在网络传输过程中被窃听；（F4）**

f) 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性；

g) 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别，并且身份鉴别信息至少有一种是不可伪造的，**例如以密钥证书、动态口令卡、生物特征等作为身份鉴别信息。（F4）**

测评方式

访谈，检查，测评。

测评对象

系统管理员，数据库管理员，主要服务器操作系统，主要数据库管理系统，服务器操作系统文档，数据库管理系统文档。

测评实施

a) 应检查服务器操作系统和数据库管理系统身份鉴别功能是否具有《信息安全等级保护操作系统安全技术要求》和《信息安全等级保护数据库管理系统安全技术要求》第二级以上或TCSEC C2级以上的测评报告；

b) 可访谈系统管理员，询问操作系统的身份标识与鉴别机制采取何种措施实现，目前系统提供了哪些身份鉴别措施和鉴别失败处理措施；

c) 可访谈数据库管理员，询问数据库的身份标识与鉴别机制采取何种措施实现，目前系统提供了哪些身份鉴别措施和鉴别失败处理措施；

d) 应检查服务器操作系统文档和数据库管理系统文档，查看用户身份标识的唯一性是由什么属性来保证的（如用户名或者 UID 等）；

e) 应检查主要服务器操作系统和主要数据库管理系统，查看是否提供了身份鉴别措施（如用户名和口令等），身份鉴别信息是否具有不易被冒用的特点，检查账户密码策略设置，例如，口令足够长，口令复杂（如规定字符应混有大、小写字母、数字和特殊字符），口令生命周期，新旧口令的替换要求（如规定替换的字符数量）或为了便于记忆使用了令牌；

f) 应检查主要服务器操作系统和主要数据库管理系统，查看身份鉴别是否采用两个以上身份鉴别技术的组合来进行身份鉴别（如采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技术和数字证书方式的身份鉴别技术中的任意两个组合），并且有一种是不易伪造的（如数字证书或生物识别技术）；

g) 应检查主要服务器操作系统和主要数据库管理系统，查看是否已配置了鉴别失败处理功能，并设置了非法登录次数的限制值，对超过限制值的登录终止其鉴别会话，并封闭帐号；查看是否设置网络登录连接超时，并自动退出；

h) 应检查重要服务器操作系统，查看服务器操作系统是否对与之相连的服务器或终端设备进行身份标识和鉴别；

i) 应测评主要服务器操作系统和主要数据库管理系统，可通过错误的用户名和口令试图登录系统，验证鉴别失败处理功能是否有效；

j) 应测评主要服务器操作系统和主要数据库管理系统，当进入系统时，是否先需要进行标识（如建立账号），而没有进行标识的用户不能进入系统；

k) 应测评主要服务器操作系统和主要数据库管理系统，添加一个新用户，其用户标识为系统原用户的标识（如用户名或 UID），查看是否不会成功；

l) 应测评主要服务器操作系统和主要数据库管理系统，删除一个用户标识，然后再添加一个新用户，其用户标识和所删除的用户标识一样（如用户名/UID），查看是否不能成功；

m) 应测评主要服务器操作系统，可通过使用未进行身份标识和鉴别的主机连接该服务器，验证主机系统能否正确地对与之相连的服务器或终端设备进行身份标识和鉴别；

n) 应渗透测评主要服务器操作系统，可通过使用口令破解工具等，对服务器操作系统进行用户口令强度检测，查看能否破解用户口令，破解口令后能否登录进入系统；

o) 应渗透测评主要服务器操作系统，验证已存在的非授权账号（如安装一些服务后会系统会增加的新账号）是否不能与系统进行交互式登录管理；

p) 应渗透测评主要服务器操作系统，测评是否存在绕过认证方式进行系统登录的方法，例如，认证程序存在的安全漏洞，社会工程或其他手段等；

q) 检查服务器操作系统和数据库的用户，以及隶属的组，或 UID 是否唯一。

结果判定

a) 如果测评实施中a）为肯定，则测评实施j）、k）和l）为肯定；

b) 如果不采用用户名/口令方式的进行身份鉴别，则测评实施中n）不适用；

c) 如果测评实施中o）中能破解口令，则该项为否定；

d) 如果测评实施中p）中没有常见的绕过认证方式进行系统登录的方法，则该项为肯定；

e) 测评实施中e）~ m）均为肯定，则信息系统符合本单元测评项要求。

2) 安全标记（S4）

测评项

a) 应对所有主体和客体设置敏感标记。

测评方式

检查，测评

测评对象

主要服务器操作系统，主要数据库管理系统，安全策略。

测评实施

a) 应检查服务器操作系统和数据库管理系统的安全标记功能是否具有《信息安全等级保护 操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第二级以上或TCSEC C2级以上的测评报告；

b) 应检查服务器操作系统和数据库管理系统的安全标记，查看是否明确主体和客体敏感标记。

3) 访问控制(S4)

测评项

a) 应依据安全策略和所有主体和客体设置的敏感标记控制主体对客体的访问；

b) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表、记录和字段级；

c) 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；

d) 应实现操作系统和数据库系统特权用户的权限分离，**系统管理员只具备操作系统的运维管理权限，数据库管理员只具备数据库的运维管理权限；**

e) 应禁用或严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；

f) 应及时删除多余的、过期的帐户，避免共享帐户的存在。

测评方式

检查，测评。

测评对象

主要服务器操作系统，主要数据库管理系统，安全策略。

测评实施

a) 应检查服务器操作系统和数据库管理系统的自主访问控制功能是否具有《信息安全等级保护操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第二级以上或TCSEC C2级以上的测评报告；

b) 应检查服务器操作系统和数据库管理系统的安全策略，查看是否明确主体（如用户）以用户和/或用户组的身份规定对客体（如文件或系统设备,目录表和存取控制表访问控制等）的访问控制，覆盖范围是否包括与信息安全直接相关的主体（如用户）和客体（如文件，数据库表等）及它们之间的操作（如读、写或执行）；

c) 应检查服务器操作系统和数据库管理系统的安全策略，查看是否明确主体（如用户）具有非敏感标记（如角色），并能依据非敏感标记规定对客体的访问；

d) 应检查主要服务器操作系统和主要数据库管理系统的访问控制列表，查看授权用户中是否不存在过期的帐号和无用的帐号等；访问控制列表中的用户和权限，是否与安全策略相一致；

e) 应检查主要服务器操作系统和主要数据库管理系统，查看客体（如文件,数据库表、记录、字段等）的所有者是否可以改变其相应访问控制列表的属性，得到授权的用户是否可以改变相应客体访问控制列表的属性；

f) 应检查主要服务器操作系统和主要数据库管理系统，查看特权用户的权限是否进行分离，如可分为系统管理员、安全管理员、安全审计员等；查看是否采用最小授权原则（如系统管理员只能对系统进行维护，安全管理员只能进行策略配置和安全设置，安全审计员只能维护审计信息等）；

g) 应检查主要服务器操作系统和主要数据库管理系统，查看在系统管理员、安全管理员、安全审计员之间是否设置了相互制约关系（如系统管理员、安全管理员等不能对审计日志，安全审计员管理不了审计数据的开启、关闭、删除等重要事件的审计日志等）；

h) 应查看主要服务器操作系统和主要数据库管理系统，查看匿名/默认用户的访问权限是否已被禁用或者严格限制（如限定在有限的范围内）；

i) 应查看主要服务器操作系统，查看匿名/默认用户是否已被禁用；

j) 应测评主要服务器操作系统和主要数据库管理系统，依据系统访问控制的安全策略，试图以未授权用户身份/角色访问客体，验证是否不能进行访问。

结果判定

a) 如果测评实施中a）为肯定，则测评实施e）和j）为肯定；

b) 测评实施中b）~j）均为肯定，则信息系统符合本单元测评项要求。

4) 可信路径(S4)

测评项

a) **对通过互联网远程访问操作系统、数据库系统的用户进行身份鉴别时，**系统与用户之间应能够建立一条安全的信息传输路径；

b) 在用户**通过互联网远程访问操作系统、数据库系统时**，系统与用户之间应能够建立一条安全的信息传输路径。

测评方式

访谈，检查。

测评对象

安全管理员，主要服务器操作系统，主要数据库管理系统，服务器操作系统文档，数据库管理系统文档。

测评实施

a) 应检查服务器操作系统和数据库管理系统的可信路径功能是否具有《信息安全等级保护 操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第四级以上的测评报告；
b) 可访谈安全管理员，询问在什么情况下起用可信路径进行初始登录和/或鉴别；目前系统提供了哪些可信路径；
c) 应检查服务器操作系统文档，查看系统提供了哪些可信路径功能；
d) 应检查主要服务器操作系统，查看文档声称的可信路径功能是否有效；
e) 应访谈安全管理员，询问在什么情况下起用可信路径进行初始登录和/或鉴别；目前系统提供了哪些可信路径；
f) 应检查数据库管理系统文档，查看系统提供了哪些可信路径功能；
g) 应检查主要数据库管理系统，查看文档声称的可信路径功能是否有效。

结果判定

a) 如果测评实施中a）为肯定，则测评实施d）和g）为肯定；
b) 测评实施中d）和g）为肯定，则信息系统符合本单元测评项要求。

5) 安全审计(G4)

测评项

a) 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；
b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用、**账号的分配、创建与变更、审计策略的调整、审计系统功能的关闭与启动**等系统内重要的安全相关事件；
c) 审计记录应包括日期和时间、类型、主体标识、客体标识、事件的结果等，**并定期备份审计记录，保存时间不少于一年**；
d) 应能够根据记录数据进行分析，并生成审计报表；
e) 应保护审计进程，避免受到未预期的中断；
f) 应保护审计记录，避免受到未预期的删除、修改或覆盖等；
g) 应能够根据信息系统的统一安全策略，实现集中审计。

测评方式

访谈，检查，测评。

测评对象

安全审计员，主要服务器和重要终端操作系统，主要数据库管理系统。

测评实施

a) 可访谈安全审计员，询问主机系统是否设置安全审计；询问主机系统对事件进行审计的选择要求和策略是什么；对审计日志的处理方式有哪些；
b) 应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看当前审计范围是否覆盖到每个用户；
c) 应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、自主访问控制的所有操作记录、重要

用户行为（如用超级用户命令改变用户身份，删除系统表）、系统资源的异常使用、重要系统命令的使用（如删除客体）等；

d) 应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容；

e) 应检查主要服务器和重要终端操作系统，查看是否为授权用户浏览和分析审计数据提供专门的审计工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表；

f) 应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看能否对特定事件指定实时报警方式（如声音、EMAIL、短信等）；

g) 应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计跟踪设置是否定义了审计跟踪极限的阈值，当存储空间接近极限时，能指定采取必要的措施（如报警并导出）；当存储空间被耗尽时，终止可审计事件的发生；

h) 应检查主要服务器、重要终端操作系统和主要数据库管理系统，查看是否提供集中审计系统连接的接口，并能根据集中审计系统的要求发送审计数据；

i) 应检查主要服务器和重要终端操作系统的时钟，查看是否与时钟服务器的时间保持同步；

j) 应测评主要服务器操作系统、重要终端操作系统和主要数据库管理系统，可通过非法终止审计功能或修改其配置，验证审计功能是否受到保护；

k) 应测评主要服务器操作系统、重要终端操作系统和主要数据库管理系统，在系统上以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），测评安全审计的覆盖情况和记录情况与要求是否一致；

l) 应测评主要服务器操作系统、重要终端操作系统和主要数据库管理系统，在系统上以某个系统用户试图删除、修改或覆盖审计记录，测评安全审计的保护情况与要求是否一致；

m) 应测评主要服务器操作系统、重要终端操作系统和主要数据库管理系统，产生一些安全侵害事件，查看安全审计能否跟踪监测到这些安全侵害事件，并终止违规进程。

结果判定

a) 测评实施中b）-m）均为肯定，则信息系统符合本单元测评项要求。

6) 剩余信息保护(S4)

测评项

a) 应保证操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他**使用人员**前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他**使用人员**前得到完全清除。

测评方式

访谈，检查。

测评对象

系统管理员，数据库管理员，主要服务器操作系统维护/操作手册，主要数据库管理系统维护/操作手册。

测评实施

a) 应检查服务器操作系统和数据库管理系统的剩余信息保护（用户数据保密性保护/客体重用）功能是否具有《信息安全等级保护 操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第二级以上的测评报告；

b) 应与系统管理员访谈，询问操作系统用户的鉴别信息存储空间，被释放或再分配给其他用户前是否得到完全清除；系统内的文件、目录等资源所在的存储空间，被释放或重新分配给其他用户前是否得到完全清除；

c) 应与数据库管理员访谈，询问数据库管理员用户的鉴别信息存储空间，被释放或再分配给其他用户前是否得到完全清除；数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前是否得到完全清除；

d) 应检查主要操作系统和主要数据库管理系统维护操作手册，查看是否明确用户的鉴别信息存储空间，被释放或再分配给其他用户前的处理方法和过程；文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前的处理方法和过程。

结果判定

a) 如果测评实施中 a）为肯定，则测评实施 b）-d）为肯定；

b) 测评实施中 b）~ d）均为肯定，则信息系统符合本单元测评项要求。

7) 入侵防范(G4)

测评项

a) 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

b) 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施**或在检测到完整性即将受到破坏时进行事前阻断；**

c) 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器、系统软件预防性维护服务等方式保持系统补丁及时得到更新。

测评方式

访谈，检查，测评。

测评对象

系统管理员，主要服务器系统。

测评实施

a) 应访谈系统管理员，询问主机系统是否采取入侵防范措施，入侵防范内容是否包括主机运行监视、资源使用超过值报警、特定进程监控、入侵行为检测、完整性检测等方面内容；

b) 应访谈系统管理员，询问入侵防范产品的厂家、版本和在主机系统中的安装部署情况；询问是否进行过部署的改进或者更换过产品，是否按要求（如定期或实时）进行产品升级；

c) 应检查主要服务器系统，查看是否进行主机运行监视，监视的内容是否包括主机的 CPU、硬盘、内存、网络等资源的使用情况，并给出资源使用历史记录；

d) 应检查主要服务器系统，查看是否设定资源报警阈值（如 CPU、硬盘、内存、网络等资源的报警阈值）以便在资源使用超过规定数值时发出报警，并查看报警方式有哪些；

e) 应检查主要服务器系统，查看是否对特定进程（包括主要的系统进程，如 WINDOWS 的 Explorer 进程）进行监控，是否可以设定非法进程列表；

f) 应检查主要服务器系统，查看是否对主机账户（如系统管理员）进行控制，以限制对重要账户的添加和更改等；

g) 应检查主要服务器系统，查看能否记录攻击者的源 IP、攻击类型、攻击目标、攻击时间等，在发生严重入侵事件时是否提供报警（如声音、短信、EMAIL 等），在其响应处置方式中是否包含有对某些入侵事件的阻断，并已配置使用；

h) 应测评主要服务器系统，试图运行非法进程，验证其能否限制非法进程的运行；试图添加或更改重要账户，验证主机能否限制重要账户的添加和更改；

i) 应测评主要服务器系统，试图破坏重要程序（如执行系统任务的重要程序）的完整性，验证主机能否检测到重要程序的完整性受到破坏。

结果判定

a) 如果测评实施中 b）中的厂家为正规厂家（如有销售许可），版本号较新，改进合理，定期升级，则该项为肯定；

b) 测评实施中 a）~ i）均为肯定，则信息系统符合本单元测评项要求。

8) 恶意代码防范(G4)

测评项

a) 应安装**国家安全部门认证的正版**防恶意代码软件，**对于依附于病毒库进行恶意代码查杀的软件**应及时更新防恶意代码软件版本和恶意代码库，**对于非依赖于病毒库进行恶意代码防御的软件，如主动防御类软件，应保证软件所采用的特征库有效性与实时性，对于某些不能安装相应软件的系统可以采取其他安全防护措施来保证系统不被恶意代码攻击；**

b) 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；

c) 应支持防恶意代码的统一管理；

d) **应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。（F4）**

测评方式

访谈，检查，测评。

测评对象

安全员，主要服务器，主要终端，网络防恶意代码产品，主机安全设计/验收文档。

测评实施

a) 应访谈安全员，询问主机系统是否采取恶意代码实时检测与查杀措施，恶意代码实时检测与查杀措施的部署情况如何，因何改进过部署或者更换过产品，是否按要求（如定期或实时）进行产品升级；

b) 应检查主机恶意代码防范方面的设计/验收文档，查看描述的安装范围是否包括服务器和终端设备（包括移动设备）；

c) 应检查主要服务器系统和主要终端系统，查看是否安装实时检测与查杀恶意代码的软件产品，查看实时检测与查杀恶意代码的软件产品是否支持恶意代码防范的统一管理功能，查看检测与查杀恶意代码软件产品的厂家、版本号和恶意代码库名称；

d) 应检查网络防恶意代码产品，查看其厂家、版本号和恶意代码库名称。

结果判定

a) 如果测评实施中a）中恶意代码实时检测与查杀措施的部署到所有服务器和重要终端，则该项为肯定；

b) 测评实施中a）~ d）均为肯定，检查发现主机系统防恶意代码产品与网络防恶意代码产品使用不同的恶意代码库（如厂家、版本号和恶意代码库名称不相同等），则信息系统符合本单元测评项要求。

9) 资源控制(A4)

测评项

a) 应通过设定终端接入方式、网络地址范围等条件限制终端登录；

b) 应根据安全策略设置登录终端的操作超时锁定；

c) 应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况；

d) 应限制单个用户对系统资源的最大或最小使用限度；

e) **应定期对系统的性能和容量进行规划，**能够对系统的服务水平降低到预先规定的最小值进行检测和报警；

f) **所有的服务器应全部专用化，不使用服务器进行收取邮件、浏览互联网操作。（F4）**

测评方式

检查，测评。

测评对象

主要服务器操作系统。

测评实施

a) 应检查主要服务器操作系统，查看是否限制单个用户的多重并发会话数量；查看是否设置登录终端的操作超时锁定和鉴别失败锁定，以及是否规定解锁或终止方式；查看是否配置了终端接入方式、网络地址范围等条件限制终端登录；

b) 上机检查：主机操作系统、数据库、重要应用系统是否根据安全策略设置登录终端的操作超时锁定；

c) 应检查重要服务器操作系统，查看是否对一个时间段内可能的并发会话连接数进行限制，是否禁止同一用户账号在同一时间内并发登录，是否限制单个用户对系统资源（如 CPU、内存和硬盘等）的最大或最小使用限度；

d) 在上机检查或在运维监控系统中查看是否对重要服务器的相关资源进行监测。

e) 应检查重要服务器操作系统，查看是否在服务水平降低到预先规定的最小值时，能检测和报警，报警的方式有哪些，能否已根据安全策略设定主体（如进程）的服务优先级，并根据优先级分配系统资源，保证优先级低的主体处理能力不会影响到优先级高的主体的处理能力；

f) 应测评主要服务器操作系统，任选一个用户，登录服务器，试图发出多重并发会话，验证系统是否限制单个用户的多重并发会话；试图在一段时间内建立一些并发会话连接，验证系统是否对一定时间段内的并发会话连接数进行限制；

g) 应测评重要服务器操作系统，任选一个用户帐户，登录服务器，用不同的终端接入方式、网络地址试图登录服务器，验证重要服务器操作系统是否通过终端接入方式、网络地址范围等条件限制终端登录；

h) 应测评主要服务器操作系统，试图使服务水平降低到预先规定的最小值，验证系统能否正确检测和报警；

i) 应测评主要服务器操作系统，任选一个用户，登录服务器，在一定时间内不进行任何动作，验证主要服务器操作系统能否对操作超时的终端进行锁定；任选一个用户，可通过多次失败登录服务器，验证服务器能否对鉴别失败的终端进行锁定，锁定后能否按照规定的解锁或终止方式进行解锁或终止。

结果判定

a) 测评实施中 a）～i）均为肯定，则信息系统符合本单元测评项要求。

主机安全重点测评操作系统包括各网站服务器、应用服务器和数据库服务器等操作系统在内容上，系统安全层面实施过程涉及 9 个工作单元，具体内容请参见附录 A.3.1.3。

7.1.3.1.4 应用安全

1) 身份鉴别(S4)

测评项

a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；

b) 应对同一用户**的关键操作**采用两种或两种以上组合的鉴别技术实现用户身份鉴别，其中一种是不可伪造的；**如使用磁卡、IC卡、动态密码卡、动态口令设备、手机短信动态密码、指纹识别等方式加强鉴别；**

c) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

d) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

e) 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数；

f) **应用软件应能在指定的闲置时间间隔到期后，自动锁定客户端的使用；（F4）**

g) **系统应强制客户首次登录时修改初始密码；（F4）**

h) **修改密码时，不允许新设定的密码与旧密码相同。（F4）**

测评方式

访谈，检查，测评。

测评对象

系统管理员，应用系统，设计/验收文档，操作规程。

测评实施

a) 可访谈系统管理员，询问应用系统是否采取身份标识和鉴别措施，具体措施有哪些；系统采取何种措施防止身份鉴别信息被冒用（如复杂性混有大、小写字母、数字和特殊字符，口令周期等）；

b) 检查应用系统是否有用户管理模块，是否对系统的用户账号和口令强度进行强制性要求。

c) 可访谈系统管理员，询问应用系统是否具有登录失败处理的功能，是如何进行处理的；询问应用系统对用户标识在整个生命周期内是否具有唯一性（如UID、用户名或其他信息在系统中是唯一的，用该标识在整个生命周期内能唯一识别该用户）；

d) 应检查设计/验收文档，查看系统是否有系统采取了唯一标识（如用户名、UID或其他属性）的说明；

e) 应检查操作规程和操作记录，查看其是否有管理身份标识和鉴别的操作规程、审批记录和操作记录；

f) 应检查应用系统，查看其是否采用了两个及两个以上身份鉴别技术的组合来进行身份鉴别（如采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技术中的任意两个组合），其中应有一种应是不可伪造的（如数字证书或生物识别技术）；对有抗抵赖要求的系统，查看其是否采用数字证书方式的身份鉴别技术；

g) 应检查应用系统，查看其是否配备身份标识（如建立账号）和鉴别（如口令等）功能；查看其其身份鉴别信息是否具有不易被冒用的特点，例如复杂性（如规定字符应混有大、小写字母、数字和特殊字符）或为了便于记忆使用了令牌；

h) 应检查应用系统，查看其是否配备并使用登录失败处理功能（如登录失败次数超过设定值，系统自动退出等）；

i) 应测评应用系统，验证其登录失败处理，非法登录次数限制，登录连接超时自动退出等功能是否有效；

j) 应测评应用系统，验证其是否及时清除存储空间中动态使用的鉴别信息（如登录系统，退出系统后重新登录系统，查看上次登录的鉴别信息是否存在）；

k) 应测评应用系统，验证其是否有鉴别警示功能（如系统有三次登录失败则锁定该用户的限制，则应给用户必要的提示）；

l) 应渗透测评应用系统，测评身份鉴别信息是否不易被冒用（如通过暴力破解或其他手段进入系统，对WEB系统可采用SQL注入等绕过身份鉴别的方法）；

m) **应测评系统，是否登录密码以密码信封方式发送给客户或者登录密码被设置为统一初始密码，系统是否强制客户首次登录时修改初始密码；**

n) **应测评修改密码是否与旧密码相同。**

结果判定

a) 如果测评实施中d）中相关文档有用户唯一性标识的描述，则该项为肯定；

b) 如果测评实施中d）中缺少相应的文档，则该项为否定；

c) 测评实施中c）～m）均为肯定，则信息系统符合本单元测评项要求。

2) 安全标记(S4)

测评项

a) **应**提供为主体和客体设置安全标记的功能并在安装后启用。

测评方式

访谈，检查，测评。

测评对象

系统管理员，应用系统。

测评实施

a) 可访谈系统管理员，询问业务系统是否提供主体和客体设置安全标记的功能；

b) 应检查应用系统，查看系统是否提供安全标记功能；是否依据安全标记的功能进行相应的应用。

结果判定

a) 测评实施中a）～b）均为肯定，则信息系统符合本单元测评项要求。

3) 访问控制(S4)

测评项

a) 应提供自主访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；

b) 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；

c) 应由授权主体配置访问控制策略，并禁止默认帐户的访问；

d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；

e) **应有生产系统内关键账户与权限的关系表；（F4）**

f) **宜**应具有对重要信息资源设置敏感标记的功能；

g) **宜**通过比较安全标记来确定是授予还是拒绝主体对客体的访问。

测评方式

访谈，检查，测评。

测评对象

系统管理员，应用系统。

测评实施

a) 可访谈系统管理员，询问业务系统是否提供访问控制措施，具体措施有哪些，自主访问控制的粒度如何；

b) 应检查应用系统，查看系统是否提供访问控制机制；是否依据安全策略控制用户对客体（如文件和数据库中的数据）的访问；

c) 应检查应用系统，查看其自主访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作；自主访问控制的粒度是否达到主体为用户级，客体为文件、数据库表级（如数据库表、视图、存储过程等）；

d) 应检查应用系统，查看应用系统是否有对授权主体进行系统功能操作和对数据访问权限进行设置的功能；

e) 应检查应用系统，查看其特权用户的权限是否分离（如将系统管理员、安全员和审计员的权限分离），权限之间是否相互制约（如系统管理员、安全管理员等不能对审计日志进行管理，安全审计员不能管理审计功能的开启、关闭、删除等重要事件的审计日志等）；

f) 应检查应用系统，查看其是否有限制默认用户访问权限的功能，并已配置使用；

g) 应检查应用系统，查看其是否通过比较安全标签来确定是授予还是拒绝主体对客体的访问的功能是否有效；

h) 应测评应用系统，可通过用不同权限的用户登录，查看其权限是否受到应用系统的限制，验证系统权限分离功能是否有效；

i) 应测评应用系统，可通过授权主体设置特定用户对系统功能进行操作和对数据进行访问的权限，然后以该用户登录，验证用户权限管理功能是否有效；

j) 应测评应用系统，可通过用默认用户登录（默认密码），并用该用户进行操作（包括合法、非法操作），验证系统对默认用户访问权限的限制是否有效；

k) 应渗透测评应用系统，测评自主访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作（如试图绕过系统访问控制机制等操作）；

l) 应渗透测评应用系统，通过试图对系统进行绕过访问控制的操作，查看系统自主访问控制是否存在缺陷。

结果判定

a) 测评实施中b）～k）均为肯定，则信息系统符合本单元测评项要求。

4) 可信路径(S4)

测评项

a) 在应用系统对用户进行身份鉴别时，应能够建立一条安全的信息传输路径；

b) 在用户通过应用系统对资源进行访问时，应用系统应保证在被访问的资源与用户之间应能够建立一条安全的信息传输路径。

测评方式

访谈，检查。

测评对象

安全管理员，主要应用系统，应用系统文档，数据库管理系统文档等。

测评实施

a) 应检查应用系统的可信路径功能是否具有《信息安全等级保护 操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第四级以上的测评报告；

b) 可访谈安全管理员，询问在什么情况下起用可信路径进行初始登录和/或鉴别；目前系统提供了哪些可信路径；

c) 应检查应用系统文档，查看系统提供了哪些可信路径功能；

d) 应检查应用系统，查看文档声称的可信路径功能是否有效；

e) 应访谈安全管理员，询问在什么情况下起用可信路径进行初始登录和/或鉴别；目前系统提供了哪些可信路径；

f) 应检查数据库管理系统文档，查看系统提供了哪些可信路径功能；

g) 应检查主要数据库管理系统，查看文档声称的可信路径功能是否有效。

结果判定

a) 如果测评实施中a）为肯定，则测评实施d）和g）为肯定；

b) 测评实施中d）和g）为肯定，则信息系统符合本单元测评项要求。

5) 安全审计(G4)

测评项

a) 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；

b) 应保证无法单独中断审计进程，**不提供**删除、修改或覆盖审计记录**的功能**；

c) 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等，**并定期备份审计记录，保存时间不少于一年**；

d) 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能；

e) 应根据系统统一安全策略，提供集中审计接口；

f) **对于从互联网客户端登陆的应用系统，应在每次用户登录时提供用户上一次成功登录的日期、时间、方法、位置等信息，以便用户及时发现可能的问题。（F4）**

测评方式

访谈，检查，测评。

测评对象

审计员，应用系统。

测评实施

a) 可访谈安全审计员，询问应用系统是否设置安全审计功能，对事件进行审计的选择要求和策略是什么，对审计日志的保护措施有哪些；
b) 应检查应用系统，查看其当前审计范围是否覆盖到每个用户；
c) 应检查应用系统，查看其审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、系统资源的异常使用、重要系统命令的使用（如删除客体）等；
d) 应检查应用系统，查看安全相关事件的记录是否包括了日期和时间、类型、主体标识、客体标识、客体敏感标记、事件的结果等信息；
e) 应检查应用系统，查看其审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容；
f) 应检查应用系统，查看其是否为授权用户浏览和分析审计数据提供专门的审计工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表；
g) 应检查应用系统，查看其能否对特定事件指定实时报警方式（如声音、EMAIL、短信等）；
h) 应检查应用系统，查看其审计跟踪设置是否定义了审计跟踪极限的阈值，当存储空间被耗尽时，能否采取必要的保护措施，例如，报警并导出、丢弃未记录的审计信息、暂停审计或覆盖以前的审计记录等；
i) 应检查应用系统，查看其安全审计是否是根据信息系统的统一安全策略，实现集中审计的；
j) 应测评应用系统，可通过非法终止审计功能或修改其配置，验证审计功能是否受到保护；
k) 应测评应用系统，在系统上以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），测评安全审计的覆盖情况和记录情况与要求是否一致；
l) 应测评应用系统，在系统上以某个系统用户试图删除、修改或覆盖审计记录，验证安全审计的保护情况与要求是否一致；
m) 应测评应用系统，制造一些安全事件，查看安全审计是否能跟踪监测到可能的安全侵害事件，并终止违规进程，验证其功能是否正确。

结果判定

a) 测评实施中b）~ m）均为肯定，则信息系统符合本单元测评项要求。

6) 剩余信息保护(G4)

测评项

a) 应保证用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

测评方式

访谈，检查，测评。

测评对象

系统管理员，设计/验收文档。

测评实施

a) 可访谈管理员，询问系统是否采取措施保证对存储介质中的残余信息进行删除（无论这些信息是存放在硬盘上还是在内存中），具体措施有哪些；
b) 应检查设计/验收文档，查看其是否有关于系统在释放或再分配鉴别信息所在存储空间给其他用户前如何将其进行完全清除（无论这些信息是存放在硬盘上还是在内存中）的描述；

c) 应检查设计/验收文档，查看其是否有关于释放或重新分配系统内文件、目录和数据库记录等资源所在存储空间给其他用户前如何进行完全清除的描述；

d) 应测评主要应用系统，用某用户登录系统并进行操作后，在该用户退出后用另一用户登录，试图操作（读取、修改或删除等）其他用户产生的文件、目录和数据库记录等资源，查看是否成功，验证系统提供的剩余信息保护功能是否正确（确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除）。

结果判定

a) 如果测评实施中b）～c）缺少相关材料，则该项为否定；

b) 测评实施中b）～d）均为肯定，则信息系统符合本单元测评项要求。

7) 通信完整性(G4)

测评项

a) 应采用密码技术保证通信过程中数据的完整性。

测评方式

访谈，测评。

检查，测评对象

安全员，应用系统，设计/验收文档。

测评实施

a) 可访谈安全员，询问业务系统是否有数据在传输过程中进行完整性保证的操作，具体措施是什么；

b) 应检查设计/验收文档，查看其是否有通信完整性的说明，如果有则查看其是否有系统是根据校验码判断对方数据包的有效性的，用密码计算通信数据报文的报文验证码的描述；

c) 应测评应用系统，可通过获取通信双方的数据包，查看通信报文是否含有是否有验证码。

结果判定

a) 测评实施中b）～c）均为肯定，则信息系统符合本单元测评项要求。

8) 通信保密性(S4)

测评项

a) 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；

b) 应对通信过程中的**敏感数据**进行加密，**对于通过互联网对外提供服务的系统，应对通信过程中的整个报文或会话过程进行加密，如采用SSL协议，最低需达到128位的加密强度**；

c) 应基于硬件化的设备对重要通信过程进行加解密运算和密钥管理。

测评方式

访谈，检查，测评。

测评对象

安全员，应用系统，相关证明材料（证书）。

测评实施

a) 可访谈安全员，询问业务系统数据在存储和传输过程中是否采取保密措施（如在通信双方建立连接之前利用密码技术进行会话初始化验证，在通信过程中对敏感信息字段进行加密等），具体措施有哪些，是否所有应用系统的通信都采取了上述措施；

b) 应检查应用系统，查看其是否基于硬件化的设备，产生密钥，进行加解密运算；

c) 应检查相关证明材料（证书），查看主要应用系统采用的密码算法是否符合国家有关部门要求；

d) 应测评应用系统，查看当通信双方中的一方在一段时间内未作任何响应，另一方是否能自动结束会话；系统是否能在通信双方建立连接之前，利用密码技术进行会话初始化验证（如SSL建立加密通道前是否利用密码技术进行会话初始验证）；在通信过程中，是否对整个报文或会话过程进行加密；

e) 应测评应用系统，通过通信双方中的一方在一段时间内未作任何响应，查看另一方是否能自动结束会话，测评当通信双方中的一方在一段时间内未作任何响应，另一方是否能自动结束会话的功能是否有效；

f) 应测评应用系统，通过查看通信双方数据包的内容，查看系统在通信过程中，对整个报文或会话过程进行加密的功能是否有效。

结果判定

a) 如果测评实施中c）缺少相关材料，则该项为否定；

b) 测评实施中b）～f）均为肯定，则信息系统符合本单元测评项要求。

9) 抗抵赖(S4)

测评项

a) 应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能，**原发证据包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录，交易系统还应能够详细记录用户合规交易数据，如业务流水号、账户名、IP地址、交易指令等信息以供审计，并能够追溯到用户**；

b) 应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能，**接受证据应用系统操作与管理记录至少应包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录，交易系统还应能够详细记录用户合规交易数据，如业务流水号、账户名、IP地址、交易指令等信息以供审计，并能够追溯到用户。**

测评方式

访谈，测评。

测评对象

安全员，应用系统。

测评实施

a) 可访谈安全员，询问系统是否具有抗抵赖的措施，具体措施有哪些；

b) 应测评应用系统，通过双方进行通信，查看系统是否提供在请求的情况下为数据原发者或接收者提供数据原发证据的功能；系统是否提供在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

结果判定

a) 测评实施中b）为肯定，则信息系统符合本单元测评项要求。

10) 软件容错(A4)

测评项

a) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；

b) 应提供自动保护功能，当故障发生时自动保护当前所有状态；

c) 应提供自动恢复功能，当故障发生时立即自动启动新的进程，恢复原来的工作状态；

d) **应能够有效屏蔽系统技术错误信息，不将系统产生的错误信息直接反馈给客户。（F4）**

测评方式

访谈，检查，测评。

测评对象

系统管理员，应用系统。

测评实施

a) 可访谈系统管理员，询问业务系统是否有保证软件具有容错能力的措施（如对人机接口输入或通过通信接口输入的数据进行有效性检验等），具体措施有哪些；

b) 应检查应用系统，通过输入不同的数据格式或长度等进行验证，查看业务系统是否对人机接口输入（如用户界面的数据输入）或通信接口输入的数据进行有效性检验；是否允许按照操作的序列进行回退（如撤消操作）；是否在故障发生时继续提供一部分功能，确保能够实施必要的措施（如对重要数据的保存）；
c) 应检查应用系统，查看其是否具有状态监控能力，当故障发生时，是否能实时检测到故障状态并报警；系统是否具有自动保护能力，当故障发生时，是否能自动保护当前所有状态；
d) 应检查应用系统，查看其是否具有自动恢复能力，当故障发生时，是否能立即启动新的进程，恢复原来的工作状态；
e) 应测评应用系统，可通过输入的不同（如数据格式或长度等符合、不符合软件设定的要求），验证系统人机接口有效性检验功能是否正确；
f) 应测评应用系统，可通过多步操作，然后回退，验证系统能否按照操作的序列进行正确的回退；可通过给系统人为制造一些故障（如系统异常），验证系统能否在故障发生时继续提供一部分功能，并能实施必要的措施；
g) 应测评应用系统，通过制造异常事件，验证系统是否能实时检测到故障状态并报警，能否自动保护当前所有状态，是否具有自动恢复能力（当故障发生时，立即启动新的进程，恢复原来的工作状态）。

结果判定

a) 测评实施中b）-g）为肯定，则信息系统符合本单元测评项要求。

11) 资源控制(A4)

测评项

a) **对于有会话或短连接的应用系统**，当应用系统中的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；
b) 应能够对系统的最大并发会话连接数进行限制；
c) **对于有会话的应用系统，**应能够对单个帐户的多重并发会话进行限制；
d) 应能够对一个时间段内可能的并发会话连接数进行限制；
e) 宜能够对**系统占用的资源设定限额，超出限额时给出提示信息**；
f) 应能够对系统服务水平降低到预先规定的最小值进行检测和报警；
g) 应提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。

测评方式

访谈，检查，测评。

测评对象

系统管理员，应用系统。

测评实施

a) 可访谈系统管理员，询问业务系统是否有资源控制的措施（如对应用系统的最大并发会话连接数进行限制，是否禁止同一用户账号在同一时间内并发登录，是否对一个时间段内可能的并发会话连接数进行限制，对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额等），具体措施有哪些；
b) 应检查应用系统，查看是否有限制单个用户的多重并发会话；系统是否有最大并发会话连接数的限制，是否有对一个时间段内可能的并发会话连接数进行限制；是否能根据安全策略设定主体的服务优先级，根据优先级分配系统资源，保证优先级低的主体处理能力不会影响到优先级高的主体的处理能力；

c) 应检查应用系统，查看是否根据安全策略设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式；是否禁止同一用户账号在同一时间内并发登录；是否对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额；

d) 应检查应用系统，查看是否根据安全属性（用户身份、访问地址、时间范围等）允许或拒绝用户建立会话连接；查看是否有服务水平最小值的设定，当系统的服务水平降低到预先设定的最小值时，系统报警，是否对全部资源采用优先服务机制；

e) 应测评应用系统，可通过对系统进行超过单个用户的多重并发会话连接，验证系统能否正确地限制单个用户的多重并发会话数；可通过对系统进行超过最大并发会话连接数进行连接，验证系统能否正确地限制最大并发会话连接数；

f) 应测评应用系统，可通过在一个时间段内，用超过设定的并发连接数对系统进行连接，查看能否连接成功，验证系统对一个时间段内可能的并发会话连接数进行限制的功能是否正确；

g) 应测评应用系统，可通过设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式, 制造操作超时和鉴别失败，验证系统能否锁定，解锁或终止方式是否和设定的方式相同；

h) 应测评应用系统，可通过按照安全属性（用户身份、访问地址、时间范围等）设定允许或拒绝某个用户建立会话连接，然后用该用户进行对应的操作，验证查看系统能否正确地根据安全属性允许或拒绝用户建立会话连接；试图使服务水平降低到预先规定的最小值，验证系统能否正确检测并报警。

结果判定

a) 测评实施中b）~h）肯定，则信息系统符合本单元测评项要求。

在内容上，应用安全层面实施过程涉及 11 个工作单元，具体内容请参见附录 A.3.1.4。

7. 1. 3. 1. 5 数据安全及备份恢复

1) 数据完整性(S4)

测评项

a) 应能够检测到系统管理数据、鉴别信息和重要业务数据在**采集、传输、使用和存储过程**中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；

b) 应对**跨安全区域的**重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用通信协议的攻击破坏数据完整性。

测评方式

访谈，检查。

测评对象

系统管理员、网络管理员、安全员、数据库管理员，应用系统，设计/验收文档，相关证明性材料（如证书、检验报告等）。

测评实施

a) 可访谈安全员，询问业务系统数据在传输过程中是否有完整性保证措施，具体措施有哪些；在检测到完整性错误时是否能恢复，恢复措施有哪些；

b) 应访谈管理人员（系统管理员、网络管理员、安全员、数据库管理员），询问信息系统中的操作系统、网络设备、数据库管理系统和应用系统等是否为重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用通信协议的攻击，破坏数据的完整性；并询问具体的专用通信协议或安全通信协议服务是什么；

c) 应检查操作系统、网络设备、数据库管理系统的设计/验收文档或相关证明性材料（如证书、检验报告等）等，查看其是否有能检测/验证到系统管理数据（如WINDOWS域管理、目录管理数据）、鉴别信息（如用户名和口令）和用户数据（如用户数据文件）在传输过程中完整性受到破坏；能否检测到系统管理数据、身份鉴别信息和用户数据（如防火墙的访问控制规则）

在存储过程中完整性受到破坏；能否检测到重要系统完整性受到破坏；在检测到完整性错误时采取必要的恢复措施，具体的恢复措施有哪些；

d) 应检查应用系统，查看其是否配备检测/验证系统管理数据、鉴别信息和用户数据在传输过程中完整性受到破坏的功能；是否配备检测/验证系统管理数据、身份鉴别信息和用户数据在存储过程中完整性受到破坏的功能；是否配备检测/验证重要系统/模块完整性受到破坏的功能；在检测/验证到完整性错误时能采取的具体恢复措施有哪些；

e) 应检查操作系统、网络设备、数据库管理系统和应用系统中为重要通信提供的、**具体的专用通信协议或安全通信协议服务是否正在运行使用。**

结果判定

a) 如果操作系统、网络设备、数据库管理系统和应用系统中任意一种能为重要通信提供专用通信协议或安全通信协议服务（避免来自基于通用通信协议的攻击，破坏数据的完整性），则 b）为肯定；

b) 如果测评实施中 c）缺少相关材料，则该项为否定；

c) 测评实施中 b）~e）均为肯定，则信息系统符合本单元测评项要求。

2) 数据保密性(S4)

测评项

a) 应采用**硬件加密、点对点的数据加解密网络机制**或其他有效措施实现系统管理数据、鉴别信息和重要业务数据**采集、传输、使用和存储过程的**保密性；

b) 应对**跨安全区域的**重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用协议的攻击破坏数据保密性。

测评方式

访谈，检查，测评。

测评对象

系统管理员、网络管理员、安全员、数据库管理员，操作系统，网络设备，数据库管理系统，应用系统，设计/验收文档，相关证明性材料（如证书、检验报告等）。

测评实施

a) 可访谈网络管理员，询问信息系统中的网络设备的鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性；是否采用加密或其他保护措施实现存储保密性；

b) 可访谈系统管理员，询问信息系统中的操作系统的鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性；是否采用加密或其他保护措施实现存储保密性；

c) 可访谈数据库管理员，询问信息系统中的数据库管理系统的鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性；是否采用加密或其他保护措施实现存储保密性；

d) 可访谈安全员，询问信息系统中的应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性；是否采用加密或其他保护措施实现存储保密性；

e) 可访谈安全员，询问系统采用的密码算法和密钥是否符合国家密码管理规定；

f) 可访谈安全员，询问当使用便携式和移动式设备时，是否加密或者采用可移动磁盘存储敏感信息；

g) 应检查操作系统、网络设备、数据库管理系统、应用系统的设计/验收文档，查看其是否有关于应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据采用加密或其他有效措施实现传输保密性描述，是否有采用加密或其他保护措施实现存储保密性的描述；

h) 应检查相关证明性材料（如证书或其他相关材料等），查看其是否有特定业务通信的通信信道、密码算法和密钥符合相关国家规定的说明；

i) 应检查应用系统，查看其鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性描述，是否采用加密或其他保护措施实现存储保密性；

j) 应测评应用系统，通过用嗅探工具获取系统传输数据包，查看其是否采用了加密或其他有效措施实现传输保密性。

结果判定

a) 如果测评实施中 g）缺少相关材料，则该项为否定；

b) 如果没有相关证明性材料（如证书、检验报告等）测评实施中 h） 为否定；

c) 测评实施中 g）~ i）均为肯定，则信息系统符合本单元测评项要求。

3) 备份和恢复(A4)

测评项

a) 应提供本地数据备份与恢复功能，采取实时备份与异步备份或增量备份与完全备份的方式，**增量数据备份每天一次**，完全数据备份每周一次，备份介质场外存放，**数据保存期限至少15年；**

b) **数据备份存放方式应以多冗余方式，完全数据备份至少保证以一个月为周期的数据冗余；（F4）**

c) 应建立异地灾难备份中心，配备灾难恢复所需的通信线路、网络设备和数据处理设备，提供业务应用的实时无缝切换；

d) 应提供异地实时备份功能，利用通信网络将数据实时备份至灾难备份中心；

e) **对于同城数据备份中心，应与生产中心直线距离至少达到30公里，可以接管所有核心业务的运行；对于异地数据备份中心，应与生产中心直线距离至少达到100公里；（F4）**

f) **为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果；（F4）**

g) 应采用冗余技术设计网络拓扑结构，避免存在网络单点故障；

h) **异地备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，"就绪状态"指备份中心的所需资源(相关软硬件以及数据等资源)已完全满足但设备cpu还没有运行；"运行状态"指备份中心除所需资源完全满足要求外，cpu也在运行状态。（F4）**

测评方式

访谈，检查，测评。

测评对象

系统管理员、网络管理员、安全员、数据库管理员，操作系统，网络设备，数据库管理系统，业务系统，业务系统设计/验收文档。

测评实施

a) 可访谈网络管理员，询问信息系统中的网络设备是否提供自动备份机制对重要信息进行本地和异地备份功能；是否提供重要网络设备、通信线路和服务器的硬件冗余；是否提供自动机制在灾难发生时实现自动业务切换和恢复的功能；

b) 可访谈系统管理员，询问信息系统中的操作系统是否提供自动备份机制对重要信息进行本地和异地备份功能；是否提供自动机制在灾难发生时实现自动业务切换和恢复的功能；

c) 可访谈数据库管理员，询问信息系统中的数据库管理系统是否提供自动备份机制对重要信息进行本地和异地备份功能；是否提供重要业务系统的本地和异地系统级热备份；是否提供自动机制在灾难发生时实现自动业务切换和恢复的功能；

d) 应检查设计/验收文档，查看其是否有关于重要业务系统的本地和异地系统级热备份的描述；是否有关于在灾难发生时的业务自动切换和恢复功能的描述；

e) 应检查操作系统、网络设备、数据库管理系统、业务系统，查看其是否配备重要业务系统的本地和异地系统级热备份，配置是否正确；

f) 应检查重要网络设备、通信线路和服务器是否提供硬件冗余；
g) 应检查重要业务系统是否配备了本地系统级热备份的功能；是否配备自动机制在灾难发生时实现自动业务切换和恢复功能；
h) 应测评重要业务系统，验证其本地系统级热备份功能是否有效，在灾难发生时自动业务切换和恢复功能是否有效。

结果判定

a) 如果没有设计/验收文档，则测评实施中 d）为否定；
b) 测评实施中 d）～h）均为肯定，则信息系统符合本单元测评项要求。

数据安全层面分布在网络安全、主机安全和应用安全等层面进行测评，在内容上，数据安全层面实施过程涉及 3 个工作单元，具体内容请参见附录 A.3.1.5。

7.1.3.2 安全管理测评

7.1.3.2.1 安全管理制度

1) 管理制度(G4)

测评项

a) 应制定全机构范围信息安全工作的总体方针和安全策略，说明安全工作的总体目标、范围、原则和安全框架等，**并编制形成信息安全方针制度文件；**
b) 应建立全面的安全管理制度，能涵盖管理活动中的各类管理内容；
c) 应对科技管理人员或操作人员执行的日常管理操作建立操作规程；
d) 应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。

测评方式

访谈，检查。

测评对象

安全主管，总体方针、政策性文件和安全策略文件，安全管理制度清单，操作规程，评审记录。

测评实施

a) 应检查制度体系是否由安全政策、安全策略、管理制度、操作规程等构成，是否定期对安全管理制度体系进行评审，评审周期多长；
b) 应检查信息安全工作的总体方针、政策性文件和安全策略文件，查看文件是否明确机构安全工作的总体目标、范围、方针、原则、责任等，是否明确信息系统的安全策略；
c) 应检查安全管理制度清单，查看是否覆盖物理、网络、主机系统、数据、应用和管理等层面；
d) 应检查是否具有重要管理操作的操作规程，如系统维护手册和用户操作规程等；
e) 应检查是否具有安全管理制度体系的评审记录，查看记录日期与评审周期是否一致，是否记录了相关人员的评审意见。

结果判定

a) 测评实施中 a）～e）均为肯定，则信息系统符合本单元测评项要求。

2) 制定和发布(G4)

测评项

a) **由金融机构总部科技部门负责制定适用全机构范围的安全管理制度，各分支机构的科技部门负责制定适用辖内的安全管理制度；**
b) 安全管理制度应具有统一的格式，并进行版本控制；
c) 应组织相关人员对制定的安全管理制度进行论证和审定；
d) 安全管理制度应通过正式、有效的方式发布；
e) 安全管理制度应注明发布范围，并对收发文进行登记；
f) 有密级的安全管理制度，应注明安全管理制度密级，并进行密级管理。

测评方式

访谈，检查。

测评对象

安全主管，管理人员，制度制定和发布要求管理文档，评审记录，安全管理制度，收发登记记录。

测评实施

a) 应访检查安全管理制度是否在信息安全领导小组或委员会的总体负责下统一制定，参与制定人员有哪些；

b) 应访谈安全主管，询问安全管理制度的制定程序，是否对制定的安全管理制度进行论证和审定，论证和评审方式如何（如召开评审会、函审、内部审核等），是否按照统一的格式标准或要求制定，对有密级的管理制度如何控制使用，是否采取相应措施有效管理；

c) 应检查制度制定和发布要求管理文档，查看文档是否说明安全管理制度的制定和发布程序、格式要求、版本编号和密级标注等相关内容；

d) 应检查管理制度评审记录，查看是否有相关人员的评审意见；

e) 应检查安全管理制度的发布过程是否正式有效，并以某种方式发布到相关人员手中；

f) 应检查安全管理制度的收发登记记录，查看收发是否符合规定程序和发布范围要求。

结果判定

a) 测评实施中 a）~ f）均为肯定，则信息系统符合本单元测评项要求。

3) 评审和修订(G4)

测评项

a) 应由信息安全领导小组负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；

b) 应定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订；

c) 应明确需要定期修订的安全管理制度，并指定负责人或负责部门负责制度的日常维护；

d) **应该建立对门户网站内容发布的审核、管理和监控机制；（F4）**

e) 应根据安全管理制度的相应密级确定评审和修订的操作范围。

测评方式

访谈，检查。

测评对象

安全主管，管理人员，安全管理制度列表，评审记录，安全管理制度对应负责人或负责部门的清单。

测评实施

a) 应访谈安全主管，询问是否定期对安全管理制度进行评审，由何部门/何人负责；

b) 应访谈管理人员（负责定期评审、修订和日常维护的人员），询问定期对安全管理制度的评审、修订情况和日常维护情况，评审周期多长，评审、修订程序如何，维护措施如何；

c) 应访谈管理人员（负责人员），询问系统发生重大安全事故、出现新的安全漏洞以技术基础结构和组织机构结构等发生变更时是否对安全管理制度进行审定，对需要改进的制度是否进行修订；

d) 应访谈管理人员（负责定期评审、修订的人员），询问评审和修订有密级的安全管理制度时对参加评审和修订的人员是否考虑到相应保密要求；

e) 应检查安全管理制度评审记录，查看记录日期与评审周期是否一致；如果对制度做过修订，检查是否有修订版本的安全管理制度；

f) 应检查制度修订评审记录和需要定期评审的安全管理制度列表，查看列表是否注明评审周期；

g) 是否定期对安全管理制度进行评审，发现存在不足或需要改进的是否进行修订，评审周期多长，评审、修订程序如何，维护措施如何；

h) 应检查是否具有系统发生重大安全事故、出现新的安全漏洞以及技术基础结构等发生变更时对安全管理制度进行审定的记录；

i) 应检查是否具有所有安全管理制度对应相应负责人或者负责部门的清单。

结果判定

a) 测评实施中 a）～i）均为肯定，则信息系统符合本单元测评项要求。

安全管理制度测评对象主要为管理制度、制定和发布、评审和修订 3 个控制点相关的文件资料和工作记录。具体内容请参见附录 A.3.2.1。

7.1.3.2.2 安全管理机构

1) 岗位设置(G4)

测评项

a) **金融机构信息安全管理工作实行统一领导、分级管理，总部统一领导分支机构的信息安全管理，各机构负责本单位和辖内的信息安全管理；(F4)**

b) **应设立由本机构领导、业务与技术相关部门主要负责人组成的信息安全领导小组，负责协调本机构及辖内信息安全管理工作，决策本机构及辖内信息安全重大事宜；**

c) **应设立专门的信息科技风险审计岗位，负责信息科技审计制度和流程的实施，制订和执行信息科技审计计划，对信息科技整个生命周期和重大事件等进行审计；（F4）**

d) 应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；

e) 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责；

f) **除科技部门外，其他部门均应指定至少一名部门计算机安全员，具体负责本部门的信息安全管理工作，协同科技部门开展信息安全管理工作；（F4）**

g) **金融机构的主要负责人为本单位计算机信息系统安全保护工作的第一责任人。金融机构的计算机信息系统安全保护领导小组、专职部门和专(兼)职安全管理人员以及其他有关人员应当协助第一责任人组织落实有关规定；（F4）**

h) **应坚持三分离原则，实现前后台分离、开发与操作分离、技术与业务分离，信息技术人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务。（F4）**

测评方式

访谈，检查。

测评对象

安全主管，安全管理各个方面的负责人，领导小组日常管理工作的负责人，系统管理员，网络管理员，安全员，部门、岗位职责文件，委任授权书，工作记录。

测评实施

a) 应访谈安全主管，询问是否设立指导和管理信息安全工作的委员会或领导小组，其最高领导是否由单位主管领导委任或授权的人员担任；

b) 应访谈安全主管，询问是否设立专职的安全管理机构（即信息安全管理工作的职能部门）；机构内部门设置情况如何，是否明确各部门职责分工；

c) 应检查是否明确各个岗位（如安全主管、安全管理各个方面的负责人、机房管理员、系统管理员、网络管理员、安全员等重要岗位）的职责分工应访谈安全主管，询问是否设立安全管理各个方面的负责人，设置了哪些工作岗位（如安全主管、安全管理各个方面的负责人、机房管理员、系统管理员、网络管理员、安全员等重要岗位），是否明确各个岗位的职责分工；

d) 应访谈安全主管、安全管理各个方面的负责人、信息安全管理委员会或领导小组日常管理工作的负责人、系统管理员、网络管理员和安全员，询问其岗位职责包括哪些内容；

e) 应检查部门、岗位职责文件，查看文件是否明确安全管理机构的职责，是否明确机构内各部门的职责和分工，部门职责是否涵盖物理、网络和系统等各个方面；查看文件是否明确设置安全主管、安全管理各个方面的负责人、机房管理员、系统管理员、网络管理员、安全员等各个岗位，各个岗位的职责范围是否清晰，是否明确岗位人员应具有的技能要求，人员是否备案；
f) 应检查信息安全管理委员会或领导小组是否具有单位主管领导对其最高领导的委任授权书；
g) 应检查信息安全管理委员会职责文件，查看是否明确描述委员会的职责和其最高领导岗位的职责；
h) 应检查安全管理各部门和信息安全管理委员会或领导小组是否具有日常管理工作执行情况的文件或工作记录（如会议记录/纪要和信息安全工作决策文档等）。

结果判定

a) 如果测评实施中 d）被访谈人员表述与文件描述一致，则该项为肯定；
b) 测评实施中 a）~ h）均为肯定，则信息系统符合本单元测评项要求。

2) 人员配备(G4)

测评项

a) 应配备一定数量的系统管理员、网络管理员、安全管理员等；
b) 应配备专职信息安全管理人员，**实行A、B 岗制度，不可兼任；**
c) 关键事务岗位应配备多人共同管理；
d) **应定期或不定期对在信息技术重要岗位上的信息技术人员进行轮换。（F4）**

测评方式

访谈，检查。

测评对象

安全主管，人员配备要求的相关文档，管理人员名单。

测评实施

a) 应检查人员配备相关文档，查看岗位分工列表和定期轮岗情况（含轮岗周期、轮岗手续等）；
b) 应检查岗位分工名单，确认安全管理员是否是专职人员；
c) 应检查关键事务岗位多人管理情况（含定期轮岗情况、轮岗周期和轮岗手续等）；
d) 应访谈安全主管，询问各个安全管理岗位人员（按照岗位职责文件询问，包括机房管理员、系统管理员、数据库管理员、网络管理员和安全员等重要岗位人员）配备情况，包括数量、专职还是兼职等；
e) 应访谈安全主管，询问对哪些关键岗位实行定期轮岗（如中心机房的安全员和关键服务器的安全员等），定期轮岗情况如何，轮岗周期多长，轮岗手续如何；
f) 应访谈安全主管，询问其对关键区域或部位的安全员配备是否有一定条件要求（如中心机房的安全员、关键服务器的安全员、机密资料的管理员等），对关键事务的管理人员配备情况如何（如密钥管理等人员），是否配备2人或2人以上共同管理，相互监督和制约；
g) 应检查人员配备要求的相关文档，查看是否明确应配备哪些安全管理人员，是否包括机房管理员、系统管理员、数据库管理员、网络管理员和安全员等重要岗位人员并明确应配备专职的安全员；查看是否明确对哪些关键岗位（应有列表）实行定期轮岗并明确轮岗周期、轮岗手续等相关内容；查看是否明确对哪些关键区域或部位的安全员应按照机要人员的条件配备；查看是否明确对哪些关键事务的管理人员应配备2人或2人以上共同管理；
h) 应检查管理人员名单，查看其是否明确机房管理员、系统管理员、数据库管理员、网络管理员和安全员等重要岗位人员的信息，确认安全员是否是专职人员。

结果判定

a) 如果测评实施中 a）设置的安全员是专职的，则该项为肯定；
b) 测评实施中 a）~ h）均为肯定，则信息系统符合本单元测评项要求。

3) 授权和审批(G4)

测评项

a) 应根据各部门和岗位的的职责明确授权审批事项、审批部门和批准人等；

b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；

c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；

d) 应记录审批过程并保存审批文档；

e) **用户应被授予完成所承担任务所需的最小权限，重要岗位的员工之间应形成相互制约的关系。权限变更应执行相关审批流程，并有完整的变更记录；（F4）**

f) **应建立系统用户及权限清单，定期对员工权限进行检查核对，发现越权用户要查明原因并及时调整，同时清理过期用户权限，做好记录归档。（F4）**

测评方式

访谈，检查。

测评对象

安全主管，关键活动的批准人，授权管理文件，审批文档，审批记录，审查记录，消除授权记录。

测评实施

a) 应检查是否规定对信息系统中的关键活动进行审批；询问是否定期审查、更新审批项目，审查周期多长；

b) 应访谈关键活动的批准人，询问其对关键活动的审批范围包括哪些（如网络系统、应用系统、数据库管理系统、重要服务器和设备等重要资源的访问，重要管理制度的制定和发布，人员的配备、培训，产品的采购，第三方人员的访问、管理，与合作单位的合作项目等），审批程序如何；

c) 应检查授权管理文件，查看文件是否包含需审批事项列表，列表是否明确审批事项和双重审批事项、审批部门、批准人及审批程序等（如列表说明哪些事项应经过信息安全领导小组审批，哪些事项应经过安全管理机构审批，哪些关键活动应经过哪些部门双重审批等），文件是否说明应定期审查、更新需审批的项目和审查周期等是否建立针对系统变更、重要操作、物理访问和系统接入等事项的审批程序，按照审批程序执行审批过程；

d) 应检查经双重审批的文档，查看是否具有双重批准人的签字和审批部门的盖章；

e) 应检查关键活动的审批过程记录，查看记录的审批程序与文件要求是否一致；

f) 应检查审查记录，查看记录日期是否与审查周期一致；

g) 应检查是否具有对不再适用的权限及时取消授权的记录。

结果判定

a) 测评实施中 a）～g）均为肯定，则该测评项符合要求。

4) 沟通和合作(G4)

测评项

a) 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题，**并形成会议纪要**；

b) 应加强与兄弟单位、公安机关、电信公司的合作与沟通；

c) 应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通；

d) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；

e) 应聘请信息安全专家作为安全顾问，指导信息安全建设，参与安全规划和安全评审等。

测评方式

访谈，检查。

测评对象

安全主管，安全管理人员，会议文件，会议记录，外联单位说明文档，安全顾问名单。

测评实施

a) 应检查信息安全领导小组、部门间协调、安全检查等会议文件或会议记录，查看是否有会议内容、会议时间、参加人员、会议结果等的描述应访谈安全主管，询问是否建立与外单位（公安机关、电信公司、兄弟单位、供应商、业界专家、专业的安全公司、安全组织等），与组织机构内其它部门之间及内部各部门管理人员之间的沟通、合作机制，与外单位和其他部门有哪些合作内容，沟通、合作方式有哪些；

b) 应访谈安全主管，询问是否召开过部门间协调会议，组织其它部门人员共同协助处理信息系统安全有关问题，安全管理机构内部是否召开过安全工作会议部署安全工作的实施，参加会议的部门和人员有哪些，会议结果如何；信息安全领导小组或者安全管理委员会是否定期召开例会；

c) 应访谈安全主管，询问是否聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等；

d) 应访谈安全管理人员（从系统管理员和安全员等人员中抽查），询问其与外单位人员，与组织机构内其他部门人员，与内部各部门管理人员之间的沟通方式和主要沟通内容有哪些；

e) 应检查部门间协调会议文件或会议记录查看是否有会议内容、会议时间、参加人员、会议结果等的描述；

f) 应检查安全工作会议文件或会议记录，查看是否有会议内容、会议时间、参加人员、会议结果等的描述；

g) 应检查信息安全领导小组或者安全管理委员会定期例会会议文件或会议记录，查看是否有会议内容、会议时间、参加人员、会议结果等的描述；

h) 应检查外联单位列表，是否建立与外联单位（公安机关、电信公司、兄弟公司、供应商、业界专家、专业的安全公司和安全组织等）之间的沟通、合作机制，是否说明外联单位的联系人、联系方式等内容；

i) 应检查信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等相关记录文档。

结果判定

b) 测评实施中 a）~ i）均为肯定，则信息系统符合本单元测评项要求。

5) 审核和检查(G4)

测评项

a) 应制定安全审核和安全检查制度，规范安全审核和安全检查工作，按要求定期开展安全审核和安全检查活动；

b) 安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；

c) 应由内部人员或上级机构定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

d) 应制定安全检查表格，实施安全检查，汇总安全检查数据，形成安全检查报告，**要求限期整改的需要对相关整改情况进行后续跟踪，并将每次安全检查报告和整改落实情况整理汇总后，报上一级机构科技部门备案；**

e) **应制定违反和拒不执行安全管理措施规定的处罚细则。（F4）**

测评方式

访谈，检查。

测评对象

安全主管，安全员，安全检查制度，安全检查报告，审计分析报告，安全检查过程记录，安全检查表格。

测评实施

a) 应访谈安全主管，询问是否组织人员定期对信息系统进行安全检查，检查周期多长，是否定期分析、评审异常行为的审计记录；
b) 应访谈安全员，询问安全检查包含哪些内容，检查人员有哪些，检查程序是否按照系统相关策略和要求进行，是否制定安全检查表格实施安全检查，检查结果如何，是否对检查结果进行通报，通报形式、范围如何；
c) 应检查安全检查制度文档，查看文档是否规定检查内容、检查程序和检查周期等，检查内容是否包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等，内容是否包括用户账号情况、系统漏洞情况、系统审计情况等；
d) 应检查安全检查报告，查看报告日期与检查周期是否一致，报告中是否有检查内容、检查人员、检查数据汇总表、检查结果等的描述；
e) 应检查安全检查过程记录，查看记录的检查程序与文件要求是否一致；
f) 应查看报告日期与检查周期是否一致，报告中是否有分析人员、异常问题和分析结果等的描述，是否对发现的问题提出相应的措施；
g) 应检查是否具有安全检查表格。

结果判定

a) 测评实施中 a）～g）均为肯定，则信息系统符合本单元测评项要求。

安全管理机构测评对象主要为岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查 5 个控制点相关的文件资料和工作记录。具体内容请参见附录 A.3.2.2。

7.1.3.2.3 人员安全管理

1) 人员录用(G4)

测评项

a) 应指定或授权专门的部门或人员负责人员录用；
b) 应严格规范人员录用过程，对被录用人员的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；
c) 应与员工签署保密协议；
d) 应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议；
e) **对信息安全管理人员应实行备案管理，信息安全管理人员的配备和变更情况，应及时报上一级科技部门备案，金融机构总部信息管理人员在总部科技部门备案；（F4）**
f) **凡是因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员，不得从事信息安全管理工作。（F4）**

测评方式

访谈，检查。

测评对象

人事负责人，人事工作人员，人员录用要求管理文档，人员审查文档或记录，考核文档或记录，保密协议，岗位安全协议，审查记录。

测评实施

a) 应访谈人事负责人，询问在人员录用时对人员条件有哪些要求，目前录用的安全管理和技术人员是否有能力完成与其职责相对应的工作；
b) 应访谈人事工作人员，询问在人员录用时是否对被录用人的身份、背景、专业资格和资质进行审查，对技术人员的技术技能进行考核，录用后是否与其签署保密协议，是否对其说明工作职责；

c) 应访谈人事负责人，询问对从事关键岗位的人员是否从内部人员中选拔，是否要求其签署岗位安全安全协议，是否定期对关键岗位人员进行信用审查，审查周期多长；
d) 应检查人员录用要求管理文档，查看是否说明录用人员应具备的条件，如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等；
e) 应检查是否具有人员录用时对录用人身份、背景、专业资格和资质等进行审查的相关文档或记录，查看是否记录审查内容和审查结果等；
f) 应检查技能考核文档或记录，查看是否记录考核内容和考核结果等；
g) 应检查保密协议，查看是否有保密范围、保密责任、违约责任、协议的有效期限和责任人签字等内容；
h) 应检查岗位安全协议，查看是否有岗位安全责任、违约责任、协议的有效期限和责任人的签字等内容；
i) 应检查信用审查记录，查看是否记录了审查内容和审查结果等，查看审查时间与审查周期是否一致。

结果判定

a) 测评实施中 a）~ i）均为肯定，则信息系统符合本单元测评项要求。

2) 人员离岗(G4)

测评项

a) 应制定有关管理规范，严格规范人员离岗过程，及时终止离岗员工的所有访问权限；
b) 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
c) 应办理严格的调离手续,关键岗位人员离岗须承诺调离后的保密义务后方可离开，**并保证离岗人员负责的信息技术系统的口令必须立即更换**。

测评方式

访谈，检查。

测评对象

安全主管，人事工作人员，人员离岗要求文档，保密承诺文档，机要人员管理办法，执行记录。

测评实施

a) 应访谈安全主管，询问是否及时终止离岗人员所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备等；
b) 应访谈人事工作人员，询问调离手续包括哪些，对关键岗位的人员调离是否按照机要人员的有关管理办法执行，是否要求调离人员在脱密期满并承诺相关保密义务后方可离开；
c) 应检查人员离岗要求文档，查看是否规定了调离手续和离岗要求等；
d) 应检查是否具有交还身份证件和设备等的记录；
e) 应检查保密承诺文档，查看是否有调离人员的签字；
f) 应检查机要人员的有关管理办法，查看是否说明机要人员条件、机要人员调离手续等相关内容；
g) 应检查关键岗位人员调离的执行记录，查看记录与管理办法要求是否一致。

结果判定

b) 测评实施中 a）~ g）均为肯定，则信息系统符合本单元测评项要求。

3) 人员考核(G4)

测评项

a) 应定期对各个岗位的人员进行安全技能及安全认知的考核；
b) 应对关键岗位的人员进行全面、严格的安全审查和技能考核；
c) 应建立保密制度，并定期或不定期的对保密制度执行情况进行检查或考核；
d) 应对考核结果进行记录并保存。

测评方式

访谈，检查。

测评对象

安全主管，人事工作人员，人员考核记录。

测评实施

a) 应访谈安全主管，询问是否有人负责定期对各个岗位人员进行安全技能及安全知识的考核；
b) 应访谈人事工作人员，询问对各个岗位人员的考核情况，考核周期多长，考核内容有哪些；询问对人员的安全审查情况，审查人员是否包含所有岗位人员，审查内容有哪些（如操作行为、社会关系、社交活动等），是否全面；
c) 应访谈人事工作人员，询问对违背安全策略和规定的人员有哪些惩戒措施；
d) 应检查考核记录，查看记录的考核人员是否包括各个岗位的人员，考核内容是否包含安全知识、安全技能等；查看记录日期与考核周期是否一致。

结果判定

a) 如果测评实施中b）被访谈人员表述审查内容包含社会关系、社交活动、操作行为等各个方面，则该项为肯定；
b) 如果测评实施中c）被访谈人员表述与文件描述一致，则该项为肯定；
c) 测评实施中a）～d）均为肯定，则信息系统符合本单元测评项要求。

4) 安全意识教育和培训(G4)

测评项

a) 应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划；
b) **应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，普及信息安全基础知识、规范岗位操作、提高安全技能；**
c) **每年至少对信息安全管理人员进行一次信息安全培训；（F4）**
d) 应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒；
e) 应对安全教育和培训的情况和结果进行记录并归档保存。

测评方式

访谈，检查。

测评对象

安全主管，安全员，系统管理员，网络管理员，数据库管理员，培训计划，培训记录。

测评实施

a) 应检查是否制定安全教育和培训计划并按计划对各个岗位人员进行安全教育和培训；
b) 应检查安全责任和惩戒措施相关制度和惩戒记录；
c) 应检查安全教育和培训计划文档，查看是否具有不同岗位的培训计划；查看计划是否明确了培训目的、培训方式、培训对象、培训内容、培训时间和地点等，培训内容是否包含信息安全基础知识、岗位操作规程等；
d) 应检查是否具有安全教育和培训记录，查看记录是否有培训人员、培训内容、培训结果等的描述；查看记录与培训计划是否一致。

结果判定

a) 如果测评实施中b）访谈人员能够表述清楚询问内容，且安全职责、惩戒措施和岗位操作规程表述与文件描述一致，则该项为肯定；
b) 测评实施中a）～d）均为肯定，则信息系统符合本单元测评项要求。

5) 外部人员访问管理(G4)

测评项

a) **各机构指定责任部门负责非涉密计算机系统和网络相关的外部人员访问授权审批，批准后由专人全程陪同或监督，并登记备案；（F4）**

b) **应对允许被外部人员访问的金融机构计算机系统和网络资源，建立存取控制机制、认证机制，列明所有用户名单及其权限，其活动应受到监控；（F4）**

c) **获得外部人员访问授权的所有单位和个人应与金融机构签订安全保密协议，应严格遵守金融机构相关安全规定与操作规程，不得进行未授权的增加、删除、修改、查询数据操作，不得复制和泄漏金融机构的任何信息。（F4）**

测评方式

访谈，检查。

测评对象

安全主管，安全管理人员，安全责任合同书或保密协议，第三方人员访问管理文档，访问批准文档，登记记录。

测评实施

a) 应访谈安全主管，询问对第三方人员（如向系统提供服务的系统软、硬件维护人员，业务合作伙伴、评估人员等）的访问采取哪些管理措施，是否要求第三方人员访问前与机构签署安全责任合同书或保密协议；

b) 应访谈安全管理人员，询问对第三方人员访问重要区域（如访问主机房、重要服务器或设备、保密文档等）采取哪些措施，是否经有关负责人书面批准，是否由专人全程陪同或监督，是否进行记录并备案管理；

c) 应检查安全责任合同书或保密协议，查看是否有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等；

d) 应检查第三方人员访问管理文档，查看是否明确第三方人员包括哪些人员，允许第三方人员访问的范围（区域、系统、设备、信息等内容），第三方人员进入条件（对哪些重要区域的访问须提出书面申请批准后方可进入），第三方人员进入的访问控制（由专人全程陪同或监督等）和第三方人员的离开条件等；

e) 应检查第三方人员访问重要区域批准文档，查看是否有第三方人员访问重要区域的书面申请，是否有批准人允许访问的批准签字等；

f) 应检查第三方人员访问重要区域的登记记录，查看记录是否描述了第三方人员访问重要区域的进入时间、离开时间、访问区域、访问设备或信息及陪同人等信息。

结果判定

a) 测评实施中a）～f）均为肯定，则该测评项符合要求。

人员安全管理测评对象主要为人员录用、人员离岗、人员考核、安全意识教育培训和外部人员访问管理 5 个控制点相关的文件资料和工作记录。具体内容请参见附录 A.3.2.3。

7.1.3.2.4 系统建设管理

1) 系统定级(G4)

测评项

a) 应明确信息系统的边界和安全保护等级；

b) 应以书面的形式说明确定信息系统为某个安全保护等级的方法和理由；

c) 应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定；

d) 应确保信息系统的定级结果经过相关部门的批准。

测评方式

访谈，检查。

测评对象

安全主管，系统划分文档，系统定级文档，专家论证文档，系统属性说明文档。

测评实施

a) 应访谈安全主管，询问划分信息系统的方法和确定信息系统安全保护等级的方法是否参照定级指南的指导，是否对其进行明确描述；确定信息系统安全保护等级的方法是否参照定级指南的指导，是否组织相关部门和有关安全技术专家对定级结果进行论证和审定，定级结果是否获得了相关部门（如上级主管部门）的批准；
b) 应检查系统划分文档，查看文档是否明确描述信息系统划分的方法和理由；
c) 应检查系统定级文档，查看文档是否给出信息系统的安全保护等级，是否明确描述确定信息系统为某个安全保护等级的方法和理由，是否给出安全等级保护措施组成SxAyGz值；查看定级结果是否有相关部门的批准盖章；
d) 应检查专家论证文档，查看是否有专家对定级结果的论证意见；
e) 应检查系统属性说明文档，查看文档是否明确了系统使命、业务、网络、硬件、软件、数据、边界、人员等。

结果判定

a) 测评实施中a）没有上级主管部门的，如果有安全主管的批准，则该项为肯定；
b) 测评实施中b）～e）均为肯定，则信息系统符合本单元测评项要求。

2) 安全方案设计(G4)

测评项

a) 应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；
b) 使用上一级机构信息系统资源或对其他机构信息系统资源与配置造成影响的区域性建设项目，项目建设方案应分别通过上一级机构业务与科技部门的审核、批准；
c) 应根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施；
d) 应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划、安全性需求分析、和详细设计方案，并形成配套文件；
e) 应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、、安全性需求分析、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施；
f) 应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、安全性需求分析、详细设计方案等相关配套文件。

测评方式

访谈，检查。

测评对象

安全主管，系统建设负责人，总体安全策略文档，安全技术框架，安全管理策略文档，总体建设规划书，详细设计方案，专家论证文档，维护记录。

测评实施

a) 应访谈安全主管，询问是否授权专门的部门对信息系统的安全建设进行总体规划，有何部门/何人负责；
b) 应访谈系统建设负责人，询问是否制定近期和远期的安全建设工作计划，是否根据系统的安全级别选择基本安全措施，是否依据风险分析的结果补充和调整安全措施，做过哪些调整；
c) 应访谈系统建设负责人，询问是否根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等；
d) 应访谈系统建设负责人，询问是否组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略等相关配套文件进行论证和审定，并经过管理部门的批准；

e) 应访谈系统建设负责人，询问是否根据安全测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件，维护周期多长；

f) 应检查系统的安全建设工作计划，查看文件是否明确了系统的近期安全建设计划和远期安全建设计划；

g) 应检查系统总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等配套文件，查看各个文件是否有机构管理层的批准；

h) 应检查专家论证文档，查看是否有相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的论证意见；

i) 应检查是否具有总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的维护记录或修订版本，查看记录日期与维护周期是否一致。

结果判定

a) 测评实施中a）～i）均为肯定，则信息系统符合本单元测评项要求。

3) 产品采购(G4)

测评项

a) 应确保安全产品采购和使用符合国家的有关规定；

b) 应确保密码产品采购和使用符合国家密码主管部门的要求；

c) 应指定或授权专门的部门负责产品的采购，**设备采购应坚持公开、公平、公正的原则，宜采用招标、邀标等形式完成**；

d) **各机构购置扫描、检测类信息安全产品应报本科技主管部门批准、备案；（F4）**

e) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单；

f) 应对重要部位的产品委托专业测评单位进行专项测试；

g) **扫描、检测类信息安全产品仅限于本机构信息安全管理人员使用；（F4）**

h) **应定期查看各类信息安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取整改措施并按规定程序报告；（F4）**

i) **应定期对各类信息安全产品产生的日志和报表进行备份存档，至少保存6个月；（F4）**

j) **应及时升级维护信息安全产品，凡超过使用期限的或不能继续使用的信息安全产品，要按照固定资产报废审批程序处理；（F4）**

k) 应在本地配置信息安全产品。

测评方式

访谈，检查。

测评对象

安全主管，系统建设负责人，产品采购管理制度，产品选型测评结果记录，更新候选产品名单。

测评实施

a) 应访谈安全主管，询问是否有专门的部门负责产品的采购，由何部门负责；

b) 应访谈系统建设负责人，询问系统信息安全产品的采购情况，采购产品前是否预先对产品进行选型测评确定产品的候选范围，是否有产品采购清单指导产品采购，采购过程如何控制，是否定期审定和更新候选产品名单，审定周期多长；

c) 应访谈系统建设负责人，询问系统是否采用了密码产品，密码产品的使用是否符合国家密码主管部门的要求；

d) 应检查产品采购管理制度，查看内容是否明确采购过程的控制方法（如采购前对产品做选型测评，对重要部位的产品委托专业测评单位进行专项测评，明确需要的产品性能指标，确定产品的候选范围，通过招投标方式确定采购产品等）和人员行为准则；

e) 应检查系统使用的有关信息安全产品（边界安全设备、重要服务器操作系统、数据库等）是否符合国家的有关规定；

f) 应检查密码产品的使用情况是否符合密码产品使用、管理的相关规定（如《商用密码管理条例》规定任何单位只能使用经过国家密码管理机构认可的商用密码产品，商用密码产品发生故障，必须有国家密码管理机构指定的单位维修，报废商用密码产品应向国家密码管理机构备案等；《计算机信息系统保密工作暂行规定》规定涉密系统配置合格的保密专用设备，所采取的保密措施应与所处理信息的密级要求相一致等；

g) 应检查是否具有产品选型测评结果记录（包括对重要部位的产品委托专业测评单位进行专项测评的结果记录）、候选产品名单审定记录或更新的候选产品名单。

结果判定

a) 如果测评实施中c）访谈说明没有采用密码产品，则测评实施c）、f）为不适用；

b) 测评实施中a）～g）均为肯定，则信息系统符合本单元测评项要求。

4) 自行软件开发(G4)

测评项

a) **应制定软件开发管理制度和代码编写安全规范，明确说明开发过程的控制方法和人员行为准则，要求开发人员参照规范编写代码，不得在程序中设置后门或恶意代码程序；（F4）**

b) 应确保开发环境与实际运行环境物理分开，**应确保开发人员和测试人员分离，开发人员不能兼任系统管理员或业务操作人员，**确保测试数据和测试结果受到控制；

c) 应确保开发人员为专职人员，开发人员的开发活动受到控制、监视和审查；

d) 应确保提供软件设计的相关文档和使用指南，并由专人负责保管；

e) 应确保对程序资源库的修改、更新、发布进行授权和批准；

f) **在软件开发过程中，应同步完成相关文档手册的编写工作，保证相关资料的完整性和准确性（F4）。**

测评方式

访谈，检查。

测评对象

系统建设负责人，软件设计相关文档和使用指南，软件开发管理制度，审批文档或记录，文档使用控制记录，审查记录。

测评实施

a) 应访谈系统建设负责人，询问系统是否自主开发软件，是否对程序资源库的修改、更新、发布进行授权和批准，软件开发是否有相应的控制措施，是否要求开发人员不能做测评人员（即二者分离），开发人员有哪些人，是否是专职人员，软件开发是否在独立的模拟环境中编写、调试和完成；

b) 应访谈系统建设负责人，询问对开发人员的开发活动采取哪些控制措施，是否有专人监控、审查，系统开发文档是否由专人负责保管，负责人是何人，如何控制使用（如限制使用人员范围并做使用登记等），测评数据和测评结果是否受到控制；

c) 应检查是否具有软件设计的相关文档（应用软件设计程序文件、源代码文档等）和软件使用指南或操作手册和维护手册等；

d) 应检查软件开发环境与系统运行环境在物理上是否是分开的；

e) 应检查软件开发管理制度，查看文件是否明确软件设计、开发、测评、验收过程的控制方法和人员行为准则，是否明确哪些开发活动应经过授权、审批，是否明确软件开发相关文档的管理等；

f) 应检查对程序资源库的修改、更新、发布进行授权和审批的文档或记录，查看是否有批准人的签字；

g) 应检查是否具有系统软件开发相关文档（软件设计和开发程序文件、测评数据、测评结果、维护手册等）的使用控制记录；

h) 应检查对开发人员的审查记录，查看是否记录审查结果等。

结果判定

a) 测评实施中a）~ h）均为肯定，则信息系统符合本单元测评项要求。

5) 外包软件开发(G4)

测评项

a) 应根据开发需求检测软件质量；

b) 应在软件安装之前检测软件包中可能存在的恶意代码；

c) 应要求开发单位提供软件设计的相关文档和使用指南；

d) 应要求开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道；

e) **应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要；（F4）**

f) **应要求外包服务商每年至少开展一次信息安全风险评估并提交评估报告，应要求外包服务商聘请外部机构定期对其进行安全审计并提交审计报告，督促其及时整改发现的问题；（F4）**

g) **应禁止外包服务商转包并严格控制分包，保证外包服务水平；（F4）**

h) **应制定数据中心外包服务应急计划，制订供应商替换方案，以应对外包服务商破产、不可抗力或其它潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。（F4）**

测评方法

访谈，检查。

测评对象

系统建设负责人，软件开发安全协议，软件开发文档，软件培训文档，软件源代码文档。

测评实施

a) 应访谈系统建设负责人，询问在外包软件前是否对软件开发单位以书面文档形式（如软件开发安全协议）规范软件开发单位的责任、开发过程中的安全行为、开发环境要求、软件质量以及开发后的服务承诺等相关内容；

b) 应访谈系统建设负责人，询问是否具有能够独立的对软件进行日常维护和使用所需的文档，开发单位是否为软件的正常运行和维护提供过技术支持，以何种方式进行；

c) 应访谈系统建设负责人，询问软件交付前是否依据开发协议的技术指标对软件功能和性能等进行验收检测，验收检测是否是由开发商和委托方共同完成，软件安装之前是否检测软件中的恶意代码和可能的后门，检测工具是否是第三方的商业产品；

d) 应检查软件开发协议是否规定知识产权归属、安全行为等内容；查看是否具有需求分析说明书、软件设计说明书、软件操作手册、软件源代码文档等开发文档和用户培训计划、程序员培训手册等后期技术支持文档。

结果判定

a) 测评实施中 a）~ d）均为肯定，则信息系统符合本单元测评项要求

6) 工程实施(G4)

测评项

a) 应指定或授权专门的部门或人员负责工程实施过程的管理；

b) 应制定详细的工程实施方案控制实施过程，**并制定相关过程控制文档**，并要求工程实施单位能正式地执行安全工程过程；

c) 针对涉及到新旧数据系统切换的工程实施，应选择对客户影响较小的时间段进行。系统切换时间超过一个工作日，需至少提前5个工作日发布提示公告，并提供应急服务途径；

d) 应制定工程实施方面的管理制度明确说明实施过程的控制方法和人员行为准则；

e) 应通过第三方工程监理控制项目的实施过程；

f) **应制定灾难备份系统集成与测试计划并组织实施。通过技术和业务测试，确认灾难备份系统的功能与性能达到设计指标要求；（F4）**

g) **网络系统的建设、升级、扩充等工程应经过科学的规划、充分的论证和严格的技术审查，有关材料应妥善保存并接受主管部门的检查。（F4）**

测评方法

访谈，检查。

测评对象

系统建设负责人，工程安全建设协议，工程实施方案，工程实施管理制度，工程监理报告。

测评实施

a) 应访谈系统建设负责人，询问是否以书面形式（如工程安全建设协议）约束工程实施方的工程实施行为；

b) 应访谈系统建设负责人，询问是否指定专门人员或部门负责工程实施管理，是否由工程监理单位按照系统建设文档的要求对工程实施过程进行进度和质量控制，是否将控制方法和工程人员行为规范制度化，是否要求工程实施单位提供其能够安全实施系统建设的资质证明和能力保证；

c) 应检查工程安全建设协议，查看其内容是否规定工程实施方的责任、任务要求、质量要求等方面内容，约束工程实施行为；

d) 应检查工程实施管理制度，查看其是否规定实施过程的控制方法（如内部阶段性控制或外部监理单位控制）、实施参与人员的各种行为等方面内容，是否做过改进；

e) 应检查工程监理实施过程是否形成各种文档，如阶段性工程监理报告。

结果判定

a) 如果测评实施中 d）因没有出现过重大问题而没有做过制度内容的改进，则该项为不适用；

b) 测评实施中 a）~ e）均为肯定，则信息系统符合本单元测评项要求。

7) 测评验收(G4)

测评项

a) 应对系统测试验收的控制方法和人员行为准则进行书面规定；

b) **应由项目承担单位（部门）或公正的第三方制定安全测试方案，对系统进行安全性测试，出具安全性测试报告，并将测试报告报科技部门审查；**

c) 在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；

d) 应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作；

e) 应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认；

f) **新建应用系统投入生产运行前应进行不少于1个月的模拟运行和不少于3个月的试运行。（F4）**

测评方法

访谈，检查。

测评对象

系统建设负责人，测评方案，测评记录，测评报告，验收报告，验收测评管理制度。

测评实施

a) 应访谈系统建设负责人，询问在信息系统正式运行前，是否委托第三方测评机构根据设计方案或合同要求对信息系统进行独立的安全性测评；

b) 应访谈系统建设负责人，询问是否指定专门部门负责测评验收工作，由何部门负责，是否对测评过程（包括测评前、测评中和测评后）进行文档化和制度化要求；

c) 应访谈系统建设负责人，询问是否根据设计方案或合同要求组织相关部门和人员对测评报告进行符合性审定；
d) 应检查工程测评方案，查看其是否对参与测评部门、人员、现场操作过程等进行要求；查看测评记录是否详细记录了测评时间、人员、操作过程、测评结果等方面内容；查看测评报告是否提出存在问题及改进意见等；
e) 应检查是否具有系统验收报告；
f) 应检查验收测评管理制度是否对系统验收测评的过程控制、参与人员的行为等进行规定，是否根据实际工作中出现的问题而做过相应改进。

结果判定

a) 如果测评实施中 f）因没有出现过重大问题而没有做过制度内容的改进，则该项为不适用；
b) 测评实施中 a）—f）均为肯定，则信息系统符合本单元测评项要求。

8) 系统交付(G4)

测评项

a) 应对系统交付的控制方法和人员行为准则进行书面规定；
b) 应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
c) **系统建设单位应在完成建设任务后将系统建设过程文档和系统运维文档全部移交科技部门；（F4）**
d) 系统建设单位应对负责系统运行维护的技术人员进行相应的技能培训；
e) 应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作；
f) **外部建设单位应与金融机构签署相关知识产权保护协议和保密协议，不得将系统采用的关键安全技术措施和核心安全功能设计对外公开。（F4）**

测评方法

访谈，检查。

测评对象

系统建设负责人，系统交付清单，服务承诺书，系统培训记录，系统交付管理制度。

测评实施

a) 应访谈系统建设负责人，询问交接手续是什么，系统交接工作是否由专门部门按照该手续办理，是否根据交付清单对所交接的设备、文档、软件等进行清点，交付清单是否满足合同的有关要求；是否对交付工作的控制方法和人员行为准则进行制度化要求，交接工作是否由于出现管理上的问题而进行交接手续或制度要求的改进；
b) 应访谈系统建设负责人，询问目前的信息系统是否由内部人员独立运行维护，如果是，系统建设实施方是否对运维技术人员进行过培训，针对哪些方面进行过培训，是否以书面形式承诺对系统运行维护提供一定的技术支持服务，是否按照服务承诺书的要求进行过技术支持，以何形式进行，系统是否具有支持其独立运行维护所需的文档；
c) 应检查系统交付清单，查看其是否具有系统建设文档（如系统建设方案）、指导用户进行系统运维的文档（如服务器操作规程书）以及系统培训手册等文档名称；
d) 应检查是否具有系统建设方的服务承诺书和对系统进行的培训记录；
e) 应检查系统交付管理制度是否规定了交付过程的控制方法和对交付参与人员的行为限制等方面内容，是否做过改进；
f) 检查金融机构与外部建设单位签订的合同或协议，是否有相关约束条款来保证。系统采用的关键安全技术措施和核心安全功能设计不对外公开。

结果判定

a) 如果测评实施中 a）、d）中因没有出现交接工作中的问题而没有对相关文档做过改进，则以上两项不适用；
b) 测评实施中 a）～f）均为肯定，则信息系统符合本单元测评项要求。

9) 系统备案(G4)

测评项

a) 应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用；
b) 应将系统等级的相关材料报系统主管部门备案；
c) 应将系统等级及其他要求的备案材料报相应公安机关备案。

测评方式

访谈，检查。

测评对象

安全主管，文档管理员，备案记录。

测评实施

a) 应访谈安全主管，询问是否有专门的人员或部门负责管理系统定级、系统属性等文档，由何部门/何人负责；
b) 应访谈文档管理员，询问对系统定级、系统属性等文档备案采取哪些控制措施（如限制使用范围、使用登记记录等）；
c) 应检查是否具有将系统定级文档和系统属性说明文件等材料报主管部门备案的记录或备案文档；
d) 应检查是否具有将系统等级、系统属性和等级划分理由等备案材料报相应公安机关备案的记录或证明；
e) 应检查是否具有系统定级文档和系统属性说明文件等相关材料的使用控制记录。

结果判定

a) 测评实施中 c）～e）为肯定，则信息系统符合本单元测评项要求。

10) 等级测评(G4)

测评项

a) 在系统运行过程中，应至少每半年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改；
b) 应在系统发生变更时及时对系统进行等级测评。发现级别发生变化的及时调整级别并进行安全改造；发现不符合相应等级保护标准要求的及时整改；
c) 应选择具有**公安部认可的《全国等级保护测评机构推荐目录》中的**测评单位进行等级测评，并与测评单位签订安全保密协议；
d) 应选择具有国家相关技术资质和安全资质的测评单位进行等级测评；
e) 应指定或授权专门的部门或人员负责等级测评的管理。

测评方法

访谈、检查。

测评对象

系统建设负责人。

测评实施

a) 应访谈系统建设负责人，询问是否有等级测评相关的规范要求等文档。是否可按公安部对三级系统的要求进行每半年的等级测评并整改；
b) 应访谈系统建设负责人，询问当系统级别发生变化时，是否能及时调整相应的等级保护要求；
c) 应访谈系统建设负责人，询问是否有等级测评机构选择的相关规定，是否有相关留痕文档；
d) 应访谈系统建设负责人，询问是否有专门的部门或人员负责等级测评管理的工作。

结果判定

a) 测评实施中 a）~ d）为肯定，则信息系统符合本单元测评项要求。

11) 安全服务商选择(G4)

测评项

a) **选择信息安全服务提供商时应评估其资质、经营行为、业绩、服务体系和服务品质等要素；（F4）**

b) 应确保安全服务商的选择符合国家的有关规定；

c) 应与选定的安全服务商签订与安全相关的协议，明确约定相关责任；

d) 应确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同，**明确约定双方的权利和义务**。

测评方法

访谈、查阅文件。

测评对象

系统建设负责人。

测评实施

a) 应访谈系统建设负责人，询问对信息系统进行安全规划、设计、实施、维护、测评等服务的安全服务单位是否符合国家有关规定。

结果判定

a) 测评实施中a）为肯定，则信息系统符合本单元测评项要求。

系统建设管理测评对象主要为系统定级、安全方案设计、产品采购、自行软件开发、外包软件开发、工程实施、测评验收、系统交付、系统备案、等级测评和安全服务商选择 11 个控制点相关的文件资料和工作记录。具体内容请参见附录 A.3.2.4。

7. 1. 3. 2. 5 系统运维管理

1) 环境管理(G4)

测评项

a) 应建立集中的机房，统一为各信息系统提供运行环境。机房设施配备应符合国家计算机机房有关标准要求；

b) **机房应采用结构化布线系统，配线机柜内如果配备理线架，应做到跳线整齐，跳线与配线架统一编号，标记清晰；（F4）**

c) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；

d) 应指定部门负责机房安全，指派专人担任机房管理员，对机房的出入进行管理，**每天巡查机房运行状况，对机房供配电、空调、温湿度控制等设施进行维护管理，填写机房值班记录、巡视记录；（F4）**

e) **机房人员进出机房必须使用主管部门制发的证件；（F4）**

f) **机房管理员应经过相关培训，掌握机房各类设备的操作要领；（F4）**

g) **应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养；（F4）**

h) **机房所在区域应安装24小时视频监控录像装置，重要机房区域实行24小时警卫值班，机房实行封闭式管理，设置一个主出入口和一个或多个备用出入口,出入口控制、入侵报警和电视监控设备运行资料应妥善保管，保存期限不少于6个月，销毁录像等资料应经单位主管领导批准后实施；（F4）**

i) **应单独设置弱电井，并留有足够的可扩展空间；（F4）**

j) 应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等；

k) 应对机房和办公环境实行统一策略的安全管理，对出入人员进行相应级别的授权，对进入重要安全区域的活动行为实时监视和记录。

测评方式

访谈，检查。

测评对象

物理安全负责人，机房值守人员，工作人员，机房安全管理制度，办公环境管理文档，设备维护记录，机房进出登记表，机房电子门禁系统及其电子记录，摄像监控系统。

测评实施

a) 应访谈物理安全负责人，询问是否指定专人或部门对机房基本设施（如空调、供配电设备等）进行定期维护，由何部门/何人负责，维护周期多长；

b) 应访谈物理安全负责人，询问是否指定人员负责机房安全管理工作，对机房进出管理是否要求制度化和文档化；

c) 应访谈机房值守人员，询问对外来人员进出机房是否采用人工记录、电子记录和监控录像三重控制管理；

d) 应访谈物理安全负责人，询问办公环境是否和机房实行统一安全管理，出入是否要经过相应级别的授权控制；

e) 应访谈工作人员，询问对办公环境的保密性要求事项，其出入授权级别如何；

f) 应检查机房安全管理制度，查看其内容是否覆盖机房物理访问、物品带进、带出机房和机房环境安全等方面；

g) 应检查办公环境管理文档，查看其是否对工作人员离开座位后的保密行为（如清理桌面文件和屏幕锁定等）和人员调离办公室后的行为等方面作出规定；

h) 应检查机房进出登记表，查看是否记录外来人员进出时间、人员姓名、访问原因等内容；查看是否具有电子门禁系统和专职警卫值守，电子记录文档是否有时间和人员等信息；

i) 应检查机房基础设施维护记录，查看是否记录维护日期、维护人、维护设备、故障原因和维护结果等方面内容。

结果判定

a) 如果测评实施中 c）中访谈人员能够表述出针对办公环境保密性注意事项（如离开座位后应退出登录，并收好敏感性文件等），且其出入级别为相应级（如普通员工级）则该项为肯定；

b) 测评实施中 a）～i）均为肯定，则信息系统符合本单元测评项要求。

2) 资产管理(G4)

测评项

a) 应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；

b) 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为，包括资产领用、资产用途和安全授权、资产日常操作、资产维修、资产报废等；

c) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；

d) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

测评方式

访谈，检查。

测评对象

安全主管，物理安全负责人，资产管理员，资产清单，信息分类标识文档，资产安全管理制度，设备。

测评实施

a) 应访谈安全主管，询问是否指定资产管理的责任人员或部门,由何部门/何人负责；
b) 应访谈物理安全负责人，询问是否对资产管理要求文档化和制度化；
c) 应访谈资产管理员，询问是否根据资产清单定期对资产进行一致性清查，并对资产清单进行维护更新；是否对资产进行赋值和标识管理，不同类别的资产是否采取不同的管理措施；
d) 应访谈资产管理员，询问对信息的操作（包括信息使用、存储和传输等方面）是否要求进行标识；
e) 应检查资产清单，查看其内容是否覆盖资产责任人、所属级别、所处位置和所属部门等方面，清单内容是否因资产所属发生变化或资产增减而进行过改变；
f) 应检查资产安全管理制度，查看其内容是否覆盖了资产使用、借用、维护等方面；
g) 应检查信息分类文档，查看其是否规定了分类标识的原则和方法（如根据数据的重要程度、敏感程度或用途不同进行分类），是否根据分类文档所描述的信息种类规定不同信息的使用、传输、存储等方面内容；
h) 应检查资产清单中的设备，查看其是否具有相应标识。

结果判定

a) 如果测评实施中 c）中访谈人员能够描述出不同的资产管理措施，则该项为肯定；
b) 如果测评实施中 e）中因没有发生过资产变化而使资产清单没有改变，则该项为不适用；
c) 如果测评实施测评实施中 h）中设备标识与信息分类标识文档中所要求的一致，则该项为肯定；
d) 测评实施中 a）~h）均为肯定，则信息系统符合本单元测评项要求。

3) 介质管理(G4)

测评项

a) 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；
b) 应确保介质存放在安全的环境中，**并有明确标识，对各类介质进行控制和保护，**并实行存储环境专人管理；
c) **所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放；（F4）**
d) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行安全控制**，应选择安全可靠的传递、交接方式，做好防信息泄露控制措施；**
e) 应对介质归档和查询等进行登记记录，管理员应根据存档介质的目录清单定期盘点；
f) **对于重要文档，如是纸质文档则实行借阅登记制度，未经相关部门领导批准，任何人不得将文档转借、复制或对外公开，如是电子文档则应采用OA等电子化办公审批平台进行管理；（F4）**
g) **应按照统一格式对技术文档进行编写并及时更新，达到能够依靠技术文档恢复系统正常运行的要求；（F4）**
h) 应对带出工作环境的存储介质进行内容加密和监控管理；
i) 应对送出维修或销毁的介质应采用多次读写覆盖、清除敏感或秘密数据、对无法执行删除操作的受损介质必须销毁；
j) **对载有敏感信息存储介质的销毁，应报有关部门备案，由科技部门进行信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录，信息消除处理仅限于存储介质仍将在金融机构内部使用的情况，否则应进行信息的不可恢复性销毁；（F4）**
k) **应制定移动存储介质使用规范，并定期核查移动存储介质的使用情况；（F4）**
l) **应建立重要数据多重备份机制，其中至少1份备份介质应存放于科技部门指定的同城或异地安全区域；（F4）**
m) 应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理；

n) **应对技术文档实行有效期管理，对于超过有效期的技术文档降低保密级别，对已经失效的技术文档定期清理，并严格执行技术文档管理制度中的销毁和监销规定；（F4）**

o) **应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。（F4）**

测评方式

访谈，检查。

测评对象

资产管理员，介质管理记录，介质安全管理制度，各类介质，介质存放地，异地存放地。

测评实施

a) 应访谈资产管理员，询问介质的存放环境是否具有保护措施，防止其被盗、被毁、被未授权修改以及信息的非法泄漏，是否有专人管理；

b) 应访谈资产管理员，询问是否对介质的使用管理进行制度化和文档化，否根据介质的目录清单对介质的使用现状进行定期检查，是否对其完整性（数据是否损坏或丢失）和可用性（介质是否受到物理破坏）进行检查，是否根据所承载的数据和软件和重要性对介质进行分类和标识管理；

c) 应访谈资产管理员，询问对介质带出工作环境（如送出维修或销毁）和重要介质中的数据和软件是否进行保密性处理；对保密性较高的介质销毁前是否有领导批准，对介质的销毁和维修是否执行严格的控制（如双人在场，销毁过程进行记录，介质送出前要经过多次读写覆盖等）；询问对介质的物理传输过程是否要求选择可靠传输人员、严格介质的打包（如采用防拆包装置）、选择安全的物理传输途径、双方在场交付等环节的控制；

d) 应访谈资产管理员，询问是否对某些重要介质实行异地存储，异地存储环境是否与本地环境相同；

e) 应检查介质管理记录，查看其是否记录介质的存储、归档、借用等情况；

f) 应检查介质管理制度，查看其内容是否覆盖介质的存放环境、使用、维护和销毁等方面；是否具有介质销毁过程记录；

g) 应检查介质，查看是否对其进行了分类，并具有不同标识；

h) 应检查介质本地存放地的实际环境条件是否是安全的，异地存放地的环境要求和管理要求是否与本地相同，是否有专人对存放地进行管理。

结果判定

a) 测评实施中 a）～h）均为肯定，则信息系统符合本单元测评项要求。

4) 设备管理(G4)

测评项

a) 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；

b) 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等；

c) **设备确需送外单位维修时，应彻底清除所存的工作相关信息，必要时应与设备维修厂商签订保密协议，与密码设备配套使用的设备送修前必须请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息，并派专人在场监督；（F4）**

d) **制定规范化的故障处理流程，建立详细的故障日志(包括故障发生的时间、范围、现象、处理结果和处理人员等内容)；（F4）**

e) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；

f) **新购置的设备应经过测试测试合格后方能投入使用；（F4）**

g) **各机构科技部门负责对信息系统相关的各种设备（包括备份和冗余设备）、线路等进行维护管理；（F4）**

h) **应做好设备登记工作，制定设备管理规范，落实设备使用者的安全保护责任；（F4）**

i) **需要废止的设备，应由科技部门使用专用工具进行数据信息消除处理，如废止设备不再使用或调配到金融机构以外的单位，应由科技部门对其数据信息存储设备进行消磁或物理粉碎等不可恢复性销毁处理，同时备案；（F4）**

j) 应确保信息处理设备必须经过审批才能带离机房或办公地点。

测评方式

访谈，检查。

测评对象

资产管理员，系统管理员，审计员，设备操作规程，设备审批管理制度，设备使用管理文档，设备维护记录，软硬件维护制度，服务器操作日志，配置文档。

测评实施

a) 应访谈资产管理员，询问是否对各类设施、设备指定专人或专门部门进行定期维护，由何部门/何人维护，维护周期多长；

b) 应访谈资产管理员，询问是否对设备选用的各个环节（选型、采购、发放等）进行审批控制，是否对设备带离机构进行审批控制，设备的操作和使用是否要求规范化管理；

c) 应访谈系统管理员，询问其对服务器是否在统一安全策略下进行正确配置，对服务器的操作是否按操作规程进行；

d) 应访谈审计员，询问对服务器的操作是否建立日志，日志文件如何管理，是否定期检查管理情况；

e) 应检查设备审批、发放制度，查看其内容是否覆盖对设备选型、采购、发放以及带离机构等环节的申报和审批规定；查看是否具有对设备的选型、采购、发放等过程的申报材料和审批报告；

f) 应检查设备使用管理文档，查看其是否对终端计算机、便携机、网络设备等使用、操作原则、注意事项等方面作出规定；

g) 应检查服务器操作规程，查看其内容是否覆盖服务器如何启动、停止、加电、断电等操作；

h) 应检查软硬件维护制度，查看其是否覆盖维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等方面。

结果判定

a) 测评实施中a）～h）均为肯定，则信息系统符合本单元测评项要求。

5) 监控管理和安全管理中心(G4)

测评项

a) 应对通信线路、网络设备、主机和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存；

b) **应建立计算机系统运行监测周报、月报或季报制度，统计分析运行状况；（F4）**

c) 应定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，**发现重大隐患和运行事故应及时协调解决，并报上一级单位相关部门；**

d) 应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。

测评方式

访谈，检查。

测评对象

系统运维负责人，监控记录文档，安全管理中心。

测评实施

a) 应访谈系统运维负责人，询问其是否监视主要服务器的各项资源指标，如CPU、内存、进程和磁盘等使用情况；
b) 应访谈系统运维负责人，询问目前信息系统是否由机构自身负责运行维护，如果是，系统运行所产生的文档如何进行管理（责任书、授权书、许可证、各类策略文档、事故报告处理文档、安全配置文档、系统各类日志等）；
c) 应检查监控记录，查看是否记录监控对象、监控内容、监控的异常现象处理等方面；
d) 应访谈系统运维负责人，询问是否根据要求对运行安全保密问题开展过检查；
e) 应检查是否具有安全管理中心，对恶意代码、补丁和审计等进行集中管理。

结果判定

a) 测评实施中a）～e）均为肯定，则信息系统符合本单元测评项要求。

6) 网络安全管理(G4)

测评项

a) 应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；
b) 应建立网络安全运行管理制度，对网络安全配置(**最小服务配置**)、日志保存时间、安全策略、升级与打补丁、口令更新周期、**重要文件备份**等方面作出规定；
c) 应**定期检查网络日志，**检查违反规定拨号上网或其他违反网络安全策略的行为**，管理网络资源及其配置信息，建立网络安全运行维护记录，并有操作和复核人员的签名，维护记录应至少妥善保存6个月；**
d) 应严格控制网络管理用户的授权，授权程序中要求必须有两人在场，并经双重认可后方可操作，操作过程应保留不可更改的审计日志；
e) **网间互联由金融机构科技主管部门统一规划，按照相关标准组织实施，未经科技主管部门核准，任何机构不得自行与外部机构实施网间互联；（F4）**
f) **应制定网络接入管理规范，应禁止便携式和移动式设备接入网络，其他任何设备接入网络前，接入方案应经过科技部门的审核，审核批准后方可接入网络并分配相应的网络资源；**
g) **应制定远程访问控制规范，确因工作需要进行远程访问的，应由访问发起单位科技部门核准，提请被访问单位科技部门（岗）开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施；（F4）**
h) **各机构以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经科技主管部门批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用；（F4）**
i) **信息安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏才感信息，未经授权不得对外公开，未经科技主管部门授权，任何外部机构与人员不得检测或扫描机构内部网络；（F4）**
j) **所有网间互联应用系统和外联网络区应定期进行威胁评估和脆弱性评估并提供威胁和脆弱性评估报告；（F4）；**
k) **网络系统应采取定时巡检、定期检修和阶段性评估的措施，银行业务高峰时段和业务高峰日要加强巡检频度和力度，确保硬件可靠、运转正常；（F4）**
l) **金融业网间互联安全实行统一规范、分级管理、各负其责的安全管理模式,未经金融机构科技主管部门核准，任何机构不得自行与外部机构实施网间互联。（F4）**

测评方法

访谈，检查。

测评对象

安全主管，安全员，网络管理员，审计员，网络漏洞扫描报告，网络安全管理制度，系统外联授权书，网络审计日志。

测评实施

a) 应访谈安全主管，询问是否指定专人负责维护网络运行日志、监控记录和分析处理报警信息等网络安全管理工作；查阅网络安全管理制度，查看其内容是否覆盖网络安全配置（包括网络设备的安全策略、授权访问、最小服务、升级与打补丁）、审计日志保存时间、升级与打补丁等方面；
b) 应访谈安全员，询问是否对网络安全的管理工作（包括网络安全配置、网络用户、日志等方面）制度化；，查阅网络管理员分工，并调阅网络安全运行维护档案、网络日志；
c) 调阅网络管理员参加网络安全技术培训的文档，检查网间互联设备上配置，并与审批记录进行比对；
d) 应访谈安全员，询问网络的外联种类有哪些（互联网、合作伙伴企业网、上级部门网络等），是否都得到授权与批准，由何部门/何人批准；是否定期检查违规联网的行为；
e) 在相关网络设备上检查远程访问控制设置，并调阅远程访问审核记录；
f) 调阅非法外联监控系统的记录，并在国际互联网用机上检查是否存储有敏感工作信息；
g) 检查网络视频服务是否作了跨区域限制，如可以跨区域点播是否经科技部门批准；
h) 应访谈网络管理员，询问是否根据厂家提供的软件升级版本对网络设备进行过升级，目前的版本号为多少，升级前是否对重要文件（帐户数据和配置数据等）进行备份，采取什么方式进行；是否对网络设备进行过漏洞扫描，对扫描出的漏洞是否及时修补；
i) 检查网络设备的配置文件备份，检查网络设备的最小服务配置是如何实现的，调阅配置文件的离线备份；
j) 调阅网络变更记录中的审批、变更时间、配置参数备份；
k) 检查计算机接入国际互联网的申请记录上保密部门的授权；
l) 应访谈网络管理员，询问对网络管理用户的现场操作有何要求；
m) 应检查网络漏洞扫描报告，查看其内容是否覆盖网络存在的漏洞、严重级别、原因分析、改进意见等方面；
n) 应检查网络安全管理制度，查看其内容是否覆盖网络安全配置（包括网络设备的安全策略、授权访问、最小服务、升级与打补丁）、网络帐户（用户责任、义务、风险、权限审批、权限分配、帐户注销等）、审计日志以及配置文件的生成、备份、变更审批、符合性检查等方面；
o) 应检查是否具有内部网络所有外联的授权批准书，调阅计算机变更用途记录；
p) 对互联网上下载的信息进行病毒检测；
q) 应检查在规定的保存时间范围内是否存在网络审计日志。

结果判定

a) 如果测评实施中l）中有关现场操作的访谈回答为必须两人以上，经双重认可方能操作，并要形成审计日志，则该测评项为肯定；
b) 测评实施中a）~q）均为肯定，则信息系统符合本单元测评项要求。

7) 系统安全管理(G4)

测评项

a) 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定；
b) 应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则；

c) **系统管理员不得兼任业务操作人员，系统管理员不得对业务数据进行任何增加、删除、修改等操作，系统管理员确需对数据库系统进行业务数据维护操作的，应征得业务部门书面同意，并详细记录维护内容、人员、时间等信息；（F4）**

d) **信息安全管理员应每季度进行至少一次的漏洞扫描，对发现的系统安全漏洞及时进行修补，扫描结果应及时上报；（F4）**

e) 应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装，并**对系统变更进行记录；**

f) 系统管理员应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，**重要计算机系统的设置要求至少两人在场**，严禁进行未经授权的操作；

g) **系统管理员应对系统变更进行详细的记录；（F4）**

h) 应定期对运行日志和审计数据进行分析，以便及时发现异常行为；

i) 应对系统资源的使用进行预测，以确保充足的处理速度和存储容量，管理人员应随时注意系统资源的使用情况，包括处理器、存储设备和输出设备。

测评方法

访谈，检查。

测评对象

安全主管，安全员，系统管理员，系统审计员，系统安全管理制度，系统审计日志，系统漏洞扫描报告。

测评实施

a) 应访谈安全主管，询问是否指定专人负责系统安全管理；

b) 调阅人员分工表和岗位职责划定；

c) 调阅系统管理员维护操作记录；

d) 检查系统管理员对系统访问控制策略设置；

e) 应访谈系统管理员，询问对系统工具的使用（如脆弱性扫描工具）是否采取措施控制不同使用人员及数量；

f) 应访谈系统管理员，询问是否定期对系统安装安全补丁程序，是否在测评环境中测评其对应用系统的影响；在安装系统补丁前是否对重要文件（系统配置、系统用户数据等）进行备份，采取什么方式进行；是否对系统进行过漏洞扫描，发现漏洞是否进行及时修补；

g) 应访谈安全员，询问是否将系统安全管理工作（包括系统安全配置、系统帐户、审计日志等）制度化；

h) 应访谈系统管理员，询问对不常用的系统缺省用户是否采取了一定的处理手段阻止其继续使用（如删除或禁用）；是否对系统帐户安全管理情况是否定期进行检查和分析，发现问题如何处理；

i) 应访谈审计员，询问是否规定系统审计日志保存时间，多长时间；

j) 应检查在规定的保存时间范围内是否存在系统审计日志；

k) 应检查系统漏洞扫描报告，查看其内容是否覆盖系统存在的漏洞、严重级别、原因分析、改进意见等方面；

l) 应检查系统安全管理制度，查看其内容是否覆盖系统安全配置（包括系统的安全策略、授权访问、最小服务、升级与打补丁）、系统帐户（用户责任、义务、风险、权限审批、权限分配、帐户注销等）、审计日志以及配置文件的生成、备份、变更审批、符合性检查等方面。

结果判定

a) 测评实施中 a）～i）均为肯定，则信息系统符合本单元测评项要求。

8) 恶意代码防范管理(G4)

测评项

a) 应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取网络上接收文件或邮件之前，应先进行病毒检查，对存储设备接入网络系统之前也应进行病毒检查；

b) **金融机构客户端应统一安装病毒防治软件，设置用户密码和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序；（F4）**

c) 应指定专人对网络和主机进行恶意代码检测并保存检测记录；

d) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定；

e) 应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，对防病毒系统不能自动清除的计算机病毒，提出解决办法,并形成书面的报表和总结汇报。

测评方法

访谈，检查。

测评对象

安全员，恶意代码防范管理制度，恶意代码检测记录，升级记录，分析报告。

测评实施

a) 应访谈系统运维负责人，询问是否对员工进行基本恶意代码防范意识教育，如告知应及时升级软件版本，使用外来设备、网络上接收文件和外来计算机或存储设备接入网络系统之前应进行病毒检查；

b) 应访谈系统运维负责人，询问是否指定专人对恶意代码进行检测，并保存记录；

c) 应访谈安全员，询问是否将恶意代码防范管理工作（包括软件的授权使用、升级、情况汇报等）制度化，对其执行情况是否进行检查，检查周期多长；

d) 应访谈安全员，询问是否对恶意代码库的升级情况进行记录，对截获的危险病毒或恶意代码是否进行及时分析处理，并形成书面的报表和总结汇报；

e) 应访谈工作人员，询问其是否熟知恶意代码基本的防范手段，主要包括哪些；

f) 应检查恶意代码防范管理制度，查看其内容是否覆盖防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面；

g) 应检查是否具有恶意代码检测记录、恶意代码库升级记录和分析报告，查看升级记录是否记录升级时间、升级版本等内容；查看分析报告是否描述恶意代码的特征、修补措施等内容。

结果判定

a) 如果测评实施中 e）中访谈人员回答内容与测评实施 a）回答内容基本一致，则该项为肯定；

b) 测评实施中 a）～g）均为肯定，则信息系统符合本单元测评项要求。

9) 密码管理(G4)

测评项

a) 选用的密码产品和加密算法应符合国家相关密码管理政策规定**循金融业数据安全保密的国家标准和国际标准；**

b) **应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员必须是本机构在编的正式员工，并逐级进行备案，规范密钥管理；（F4）**

c) **主机管理员、数据库管理员、网络管理员、业务操作人员均须设置口令密码，至少每个月更换一次，口令密码的强度应满足不同安全性要求；（F4）**

d) **敏感计算机系统和设备的口令密码设置应在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经科技部门主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码使用后应立即更改并再次密封存放；（F4）**

e) **应根据实际情况在一定时限内妥善保管重要计算机系统升级改造前的口令密码；（F4）**

f) **密钥注入、密钥管理功能调试和密钥档案的保管应由专人负责。密钥资料须保存在保险柜内。保险柜钥匙由专人负责。使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录；（F4）**

g) **确因工作需要经授权可远程接入内部网络的用户，应妥善保管其身份认证介质及口令密码，不得转借他人使用。（F4）**

测评方法

访谈，检查。

测评对象

安全员，密码管理制度。

测评实施

a) 应访谈安全员，询问密码算法和密钥的使用是否遵照国家密码管理规定；

b) 应检查是否具有密码使用管理制度。

结果判定

a) 测评实施中 a）～b）均为肯定，则信息系统符合本单元测评项要求。

10) 变更管理(G4)

测评项

a) **变更管理应流程化、文档化和制度化，变更流程中应明确变更发起方、实施方的职责，应明确变更方案的测试、审批流程及实施策略，对有可能影响客户利益的变更应事先通知客户并得到客户的确认；（F4）**

b) 应确认系统中要发生的变更，并制定变更方案，**包括变更的组织结构与实施计划、操作步骤、应急及回退方案等，变更方案应经过测试，对于无法测试或不具备测试条件的变更，应得到充分论证和审批；**

c) 应建立变更管理制度，系统发生变更前，向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告；

d) 应建立变更控制的申报和审批文件化程序，控制系统所有的变更情况，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录；

e) 应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练；

f) 应定期检查变更控制的申报和审批程序的执行情况，评估系统现有状况与文档记录的一致性；

g) **变更前做好系统和数据的备份。风险较大的变更，应在变更后对系统的运行情况进行跟踪；（F4）**

h) **如果需要使用生产环境进行测试，应纳入变更管理，并制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划，确保生产系统的安全；（F4）**

i) **当生产中心发生变更时，应同步分析灾备系统变更需求并进行相应的变更，评估灾备恢复的有效性；应尽量减少紧急变更。（F4）**

测评方法

访谈，检查。

测评对象

系统运维负责人，系统变更申请书，变更方案，变更管理制度，变更申报和审批程序，变更失败恢复程序，变更评估报告，变更过程记录文档。

测评实施

a) 应访谈系统运维负责人，询问是否制定变更方案指导系统执行变更；目前系统发生过哪些变更，变更过程是否文档化并保存，是否修改相关的操作流程（如系统配置发生变更后，相应的操作流程是否修改）；

b) 应访谈系统运维负责人，询问重要系统变更前是否根据有关申报和审批程序得到有关领导的批准，由何人批准，对发生的变更情况是否通知了所有相关人员，以何种方式通知，是否按照申报和审批程序定期对系统变更情况进行一致性检查；
c) 应访谈系统运维负责人，询问变更失败后的恢复程序、工作方法和职责是否文档化，恢复过程是否经过演练；
d) 应检查重要系统的变更申请书，查看其是否有主管领导的批准；
e) 应检查系统变更方案，查看其是否对变更类型、变更原因、变更过程、变更前评估等方面进行规定；
f) 应检查变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容；
g) 应检查变更控制的申报、审批程序，查看其是否覆盖所有变更类型、申报流程、审批部门、批准人等方面内容；
h) 应检查变更失败恢复程序，查看其是否规定变更失败后的恢复流程；
i) 应检查是否具有变更过程记录文档和变更方案。

结果判定

a) 如果系统没有发生过变更，则测评实施中 i）不适用；
b) 测评实施中 a）~ i）均为肯定，则信息系统符合本单元测评项要求。

11) 备份与恢复管理(G4)

测评项

a) 应制定金融机构的数据备份与恢复相关安全管理制度，对备份信息的备份方式、备份频度、存储介质、保存期等进行规范；
b) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；
c) 应建立控制数据备份和恢复过程的程序，记录备份过程，对需要采取加密或数据隐藏处理的备份数据，进行备份和加密操作时要求两名工作人员在场，所有文件和记录应妥善保存；
d) **应每年至少进行一次重要信息系统专项灾备切换演练，每三年至少进行一次重要信息系统全面灾备切换演练，根据不同的应急恢复内容，确定演练的周期，并指定专人管理和维护应急预案，根据人员、信息资源等变动情况以及演练情况适时予以更新和完善，确保应急预案的有效性和灾难发生时的可获取性；（F4）**
e) **应定期对备份数据的有效性进行检查，每次抽检数据量不低于10%。备份数据要实行异地保存；（F4）**
f) **灾难恢复的需求应定期进行再分析，再分析周期最长为三年，当生产中心环境、生产系统或业务流程发生重大变更时，单位应立即启动灾难恢复需求再分析工作，依据需求分析制定灾难恢复策略；（F4）**
g) **恢复及使用备份数据时需要提供相关口令密码的，应把口令密码密封后与数据备份介质一并妥善保管；（F4）**
h) 应根据信息系统的备份技术要求，制定相应的灾难恢复计划，并对其进行测试以确保各个恢复规程的正确性和计划整体的有效性，测试内容包括运行系统恢复、人员协调、备用系统性能测试、通信连接等，根据测试结果，对不适用的规定进行修改或更新；
i) **应定期开展灾难恢复培训，在条件许可的情况下，由金融机构相关部门统一部署，至少每年进行一次灾难恢复演练，包括异地备份站点切换演练和本地系统灾难恢复演练；异地备份站点切换：在异地建立热备份站点，当主站点因发生灾难导致系统不可恢复时异地备份站点能承担起主站点的功能，本地系统灾难恢复：当本地系统发生异常中断时能够在短时间恢复和保障业务数据的可运行性；（F4）**

j) **金融机构应根据信息系统的灾难恢复工作情况，确定审计频率。单位应每年至少组织一次内部灾难恢复工作审计；（F4）**

k) **应安排专人负责灾难恢复预案的日常维护管理；（F4）**

l) **应建立灾难备份系统，主备系统实际切换时间应满足实时切换，灾备系统处理能力应不低于主用系统处理能力的50%，通信线路应分别接入主备系统。有条件时可采用主、备系统处理能力相同、轮换交替使用的双系统模式。（F4）**

测评方法

访谈，检查。

测评对象

系统管理员，数据库管理员，网络管理员，备份管理文档，备份和恢复策略文档，备份设备操作流程文档，备份和恢复程序，备份过程记录文档。

测评实施

a) 应访谈系统管理员、数据库管理员和网络管理员，询问是否识别出需要定期备份的业务信息、系统数据及软件系统，主要有哪些；对其的备份工作是否以文档形式规范了备份方式、频度、介质、保存期等内容，数据备份和恢复策略是否文档化，备份和恢复过程是否文档化，对特殊备份数据（如保密数据）的操作是否要求人员数量，过程是否记录备案；

b) 应访谈系统管理员、数据库管理员和网络管理员，询问其对备份及冗余设备的安装、配置和启动工作是否根据一定的流程进行，是否记录操作过程，是否保存记录文档，是否指定专人对备份设备的有效性定期维护和检查，多长时间检查一次；

c) 应访谈系统管理员、数据库管理员和网络管理员，询问是否定期执行恢复程序，周期多长，系统是否按照恢复程序完成恢复，如有问题，是否针对问题进行恢复程序的改进或调整其他因素；

d) 应检查是否具有规定备份方式、频度、介质、保存期的文档；

e) 应检查数据备份和恢复策略文档，查看其内容是否覆盖数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面；

f) 应检查备份设备操作流程文档，查看其是否规定备份及冗余设备的安装、配置、启动、关闭等操作流程；

g) 应检查备份过程记录文档，查看其内容是否覆盖备份时间、备份内容、备份操作、备份介质存放等内容；查看是否具有保密数据的备份过程记录文档。

结果判定

a) 测评实施中 a）～g）均为肯定，则信息系统符合本单元测评项要求。

12) 安全事件处置(G4)

测评项

a) 应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

b) 应制定安全事件报告和处置管理制度，明确安全事件类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；

c) 应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分；

d) 应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；

e) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；

f) 对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序；

g) 发生可能涉及国家秘密的重大失、泄密事件，应按照有关规定向公安、安全、保密等部门汇报；

h) 应严格控制参与涉及国家秘密事件处理和恢复的人员，重要操作要求至少两名工作人员在场并登记备案；

i) **应建立有效的技术保障机制，确保在安全事件处置过程中不会因技术能力缺乏而导致处置中断或延长应急处置时间。（F4）**

测评方法

访谈，检查。

测评对象

系统运维负责人，工作人员，安全事件报告和处置管理制度，安全事件记录文档，安全事件报告和处理程序文档。

测评实施

a) 应访谈系统运维负责人，询问是否告知用户在发现安全弱点和可疑事件时应及时报告，对重大的失、泄密事件是否向公安、安全、保密等国家部门汇报，安全事件的报告和响应处理过程是否制度化和文档化，不同安全事件是否采取不同的处理和报告程序，对涉密事件的处理是否要求现场人员数量；

b) 应访谈系统运维负责人，询问本系统已发生的和需要防止发生的安全事件主要有哪几类，对识别出的安全事件是否根据其对系统的影响程度划分不同等级，划分为几级，划分方法是否参照了国家相关管理部门的技术资料，主要参照哪些；

c) 应访谈工作人员，询问其发生安全事件时的报告流程；

d) 应检查安全事件报告和处置管理制度，查看其是否描述在安全事件处置、报告和恢复等工作中不同部门和人员的职责；

e) 应检查安全事件定级文档，查看其内容是否明确安全事件的定义、安全事件等级划分的原则、等级描述等方面内容；

f) 应检查安全事件记录分析文档，查看其是否记录引发安全事件的原因，是否记录事件处理过程，不同安全事件是否采取不同措施避免其再次发生；

g) 应检查安全事件报告和处理程序文档，查看其是否根据不同安全事件制定不同的处理和报告程序，是否明确具体报告方式、报告内容、报告人等方面内容。

结果判定

a) 如果测评实施中 a）中访谈回答为涉密事件的处理必须两人在现场，则该项为肯定；

b) 如果测评实施中 c）中访谈回答与 g）中描述一致，则该项为肯定；

c) 测评实施中 a）－g）为肯定，则信息系统符合本单元测评项要求。

13) 应急预案管理(G4)

测评项

a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括应急组织机构、启动应急预案的条件、应急处理流程、系统恢复流程、**事件信息收集、分析、报告制度、**事后教育和培训等内容，**业务处理系统应急预案的编制工作应由相关业务部门和科技部门共同完成，并由预案涉及的相关机构签字盖章；**

b) 应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；

c) 应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次；

d) **在与第三方合作的业务中，应建立并完善内部责任机制和与相关机构之间的协调机制，制定完整的应急预案及应急协调预案，并定期参加联合演练；（F4）**

e) **突发事件应急处置领导小组应统一领导计算机系统的应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业信息安全监管部门；（F4）**

f) **金融机构应急领导小组应及时向新闻媒体发布相关信息，严格按照行业、机构的相关规定和要求对外发布信息，机构内其它部门或者个人不得随意接受新闻媒体采访或对外发表个人看法；（F4）**

g) **实施报告制度和启动应急预案的单位应当实行重大突发事件24小时值班制度；（F4）**

h) **应定期对原有的应急预案重新评估，并根据安全评估结果，定期修订、演练，并进行专项内部审计；（F4）**

i) **应急演练结束后，金融机构应撰写应急演练情况总结报告，总结报告包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练结论；（F4）**

测评方法

访谈，检查。

测评对象

系统运维负责人，应急响应预案文档，应急预案培训记录，应急预案演练记录，应急预案审查记录，灾难恢复计划文档，应急预案测评方案，测评结果文档。

测评实施

a) 应访谈系统运维负责人，询问是否制定不同事件的应急预案和灾难恢复计划，是否对系统相关人员进行应急预案培训，培训内容是什么，多长时间举办一次，是否定期对应急预案进行演练，演练周期多长，是否对应急预案和灾难恢复计划进行测评并修改，是否对应急预案定期进行审查并更新，目前的预案文档为第几版；

b) 应访谈系统运维负责人，询问是否具有应急预案小组，是否具备应急设备并能正常工作，应急预案执行所需资金是否做过预算并能够落实；

c) 应检查应急响应预案和灾难恢复文档，查看其内容是否覆盖启动预案的条件、应急处理流程、系统恢复流程和事后教育等内容；

d) 应检查是否具有应急预案培训记录、演练记录和审查记录；

e) 应检查应急预案测评方案，查看其内容是否覆盖运行系统恢复、人员协调、备用系统性能测评、通信连接等方面；查看测评结果记录，是否记录测评出现的问题、原因分析和修改意见；

f) 调阅突发事件应急处置领导小组组织文件及职责；

g) 了解应急事件公告发布情况；

h) 调阅应急预案评估材料。

结果判定

a) 测评实施中 a）～h）均为肯定，则信息系统符合本单元测评项要求。

系统运维管理测评对象主要为环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置以及应急预案管理 13 个控制点相关的文件资料和工作记录。具体内容请参见附录 A.3.2.5。

7.2 整体测评

信息系统的整体测评，就是在单元测评的基础上，评价信息系统的整体安全保护能力有没有缺失，是否能够对抗相应等级的安全威胁。 信息系统整体测评应从安全控制点间、层面间和区域间等方面进行安全分析和测评，并最后从系统结构安全方面进行综合分析，对系统结构进行安全测评。 安全控制点间安全测评是指对同一区域同一层面内的两个或者两个以上不同安全控制点间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。 层面间安全测评是指对同一区域内的两个或者两个以上不同层面的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。 区域间安全测评是指对两个或者两个以上不同物理或逻辑区域间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

7.2.1 安全控制点间测评

安全控制间的安全测评主要考虑同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。安全功能上的增强和补充可以使两个不同强度、不同等级的安全控制发挥更强的综合效能，可以使单个的低等级安全控制在特定环境中达到高等级信息系统的安全要求。例如，可以通过物理层面上的物理访问控制来增强其安全防盗窃功能等。安全功能上的削弱会使一个安全控制的引入影响另一个安全控制的功能发挥或者给其带来新的脆弱性。例如，应用安全层面的代码安全与访问控制，如果代码安全没有做好，很可能会使应用系统的访问控制被旁路。

在测评安全控制间的增强和补充作用时，应先根据安全控制的具体实现和部署方式以及信息系统的实际环境，分析出物理安全、网络安全、主机系统安全、应用安全和数据安全等各自同一层面内的哪些安全技术控制间可能存在安全功能上的增强和补充作用，分析出处在安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等同一方面内的哪些安全管理控制间可能存在安全功能上的增强和补充作用。如果增强和补充作用是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断安全控制相互作用后，是否发挥出更强的综合效能，使其功能增强或得到补充。

在测评安全控制间的削弱作用时，应先根据安全控制的具体实现方式和部署方式以及信息系统的实际环境，分析物理安全、网络安全、主机系统安全、应用安全和数据安全同一层面内的哪些安全技术控制间可能会存在安全功能上的削弱作用，分析出处在安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等同一方面内的哪些安全管理控制间可能存在安全功能上的削弱作用。如果功能削弱是可以进行测评验证的，则应设计出具体测评过程进行测评验证。最后根据测评分析结果，综合判断安全控制相互作用后，一个安全控制是否影响另一个安全控制的功能发挥或者给其带来新的脆弱性，使其功能削弱。

如果安全控制间优势互补，使单个的低等级安全控制发挥的安全功能达到信息系统相应等级的安全要求，则可认为该安全控制没有影响信息系统的整体安全保护能力。如果安全控制间存在削弱作用，使某个安全控制的功能等级降低到其安全功能已不能达到信息系统相应等级的安全要求，则可认为该安全控制影响到信息系统的整体安全保护能力。

7.2.2 层面间安全测评

层面间的安全测评主要考虑同一区域内的不同层面之间存在的功能增强、补充和削弱等关联作用。安全功能上的增强和补充可以使两个不同层面上的安全控制发挥更强的综合效能，可以使单个的低等级安全控制在特定环境中达到高等级信息系统的安全要求。安全功能上的削弱会使一个层面上的安全控制影响另一个层面安全控制的功能发挥或者给其带来新的脆弱性。

在测评层面间的功能增强和补充作用时，应先根据层面的整合集成方式和信息系统的实际环境，重点研究不同层面上相同或相似的安全控制（如主机系统层面与应用层面上的身份鉴别之间的关系），以及技术与管理上各层面的关联关系，分析出哪些安全控制间可能会存在安全功能上的增强和补充作用。如果增强和补充作用是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断层面间整合后，是否发挥出更强的综合效能，使其功能增强或得到补充。

在测评层面间的功能削弱作用时，应先根据层面的整合集成方式和信息系统的实际环境，分析出哪些安全技术层面间和安全管理方面可能存在安全功能上的削弱作用。如果功能削弱是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断不同层面整合后，一个层面是否影响另一个层面安全功能的发挥或者给其带来新的脆弱性，使其功能削弱。

如果层面间安全功能增强或优势互补，使单个或部分低等级安全控制发挥的安全功能达到信息系统的安全要求，则可认为这些安全控制没有影响信息系统的整体安全保护能力。如果层面间存在削弱作用，使某个或某些安全控制的功能等级降低到其安全功能已不能满足信息系统相应等级的安全要求，则可认为这些安全控制影响到信息系统的整体安全保护能力。

7.2.3 区域间安全测评

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。例如，流入某个区域的所有网络数据都已经在另一个区域上做过网络安全审计，则可以认为该区域通过区域互连后具备网络安全审计功能。安全功能上的增强和补充可以使两个不同区域上的安全控制发挥更强的综合效能，可以使单个的低等级安全控制在特定环境中达到高等级信息系统的安全要求。安全功能上的削弱会使一个区域上的安全功能影响另一个区域安全功能的发挥或者给其带来新的脆弱性。

在测评区域间的功能增强和补充作用时，应先根据区域间互连互通的集成方式和信息系统的实际环境，特别是区域间的数据流流向和控制方式，分析出哪些区域间可能会存在安全功能上的增强和补充作用。如果增强和补充作用是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断区域间互连互通后，是否发挥出更强的综合效能，使其功能增强或得到补充。

在测评区域间的功能削弱作用时，应先根据区域间互连互通的集成方式和信息系统的实际环境，特别是区域间的数据流流向和控制方式，分析出哪些区域间可能会存在安全功能上的削弱作用。如果功能削弱是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断不同区域互连互通后，一个区域是否影响另一个区域安全功能的发挥或者给其带来新的脆弱性，使其功能削弱。

如果区域间安全功能增强或优势互补，使单个或部分低等级安全控制发挥的安全功能达到信息系统的安全要求，则可认为这些安全控制没有影响信息系统的整体安全保护能力。如果区域间存在削弱作用，使某个或某些安全控制的功能等级降低到其安全功能已不能满足信息系统相应等级的安全要求，则可认为这些安全控制影响到信息系统的整体安全保护能力。

7.2.4 系统结构安全测评

系统结构安全测评主要考虑信息系统整体结构的安全性和整体安全防范的合理性。例如，由于信息系统边界上的网络入侵防范设备的管理接口连接方式不当，可能使网络访问控制出现旁路，出现信息系统整体安全防范不当。测评分析信息系统整体结构的安全性，主要是指从信息安全的角度，分析信息系统的物理布局、网络结构和业务逻辑等在整体结构上是否合理、简单、安全有效。测评信息系统整体安全防范的合理性，主要是指从系统的角度，分析研究信息系统安全防范在整体上是否遵循纵深防御的思路，明晰系统边界，确定重点保护对象，在适当的位置部署恰当的安全技术和安全管理措施等。

在测评分析信息系统整体结构的安全性时，应掌握信息系统的物理布局、网络拓扑、业务逻辑（业务数据流）、系统实现和集成方式等各种情况，结合业务数据流分析物理布局与网络拓扑之间、网络拓扑与业务逻辑之间、物理布局与业务逻辑之间、不同信息系统之间存在的各种关系，明确物理、网络和业务系统等不同位置上可能面临的威胁、可能暴露的脆弱性等，考虑信息系统的实际情况，综合判定信息系统的整体布局是否合理、主要关系是否简单、整体是否安全有效等。

在测评分析信息系统整体安全防范的合理性时，应熟悉信息系统安全保护措施的具体实现方式和部署情况等，结合业务数据流分析不同区域和不同边界与安全保护措施的关系、重要业务和关键信息与安全保护措施的关系等，参照纵深防御的要求，识别信息系统的安全防范是否突出重点、层层深入，综合判定信息系统的整体安全防范是否恰当合理等。

8 分析与报告编制

8.1 单元测评结果判定

本任务主要是针对测评指标中的单个测评项，结合具体测评对象，客观、准确地分析测评证据，形成初步单项测评结果，单项测评结果是形成等级测评结论的基础。任务描述：

a）针对每个测评项，分析该测评项所对抗的威胁在被测系统中是否存在，如果不存在，则该测评项应标为不适用项。

b）如果测评证据表明所有要求内容与预期测评结果一致，则判定该测评项的单项测评结果为符合；

如果测评证据表明所有要求内容与预期测评结果不一致，判定该测评项的单项测评结果为不符合；否则判定该测评项的单项测评结果为部分符合。

8.2 单元测评结果汇总

一是以表格形式汇总测评结果。表格以不同颜色对测评结果进行区分，部分符合的安全子类采用黄色标识，不符合的安全子类采用红色标识，如表 6 所示。

表 6 测评指标符合情况表

序号	层面类	测评指标	符合情况			
			符合	部分符合	不符合	不适用
1	物理安全	物理位置的选择				
2		物理访问控制				
3		防盗窃和防破坏				
4		防雷击				
5		防火				
6		防水和防潮				
7		防静电				
8		温湿度控制				
9		电力供应				
10		电磁防护				
…	…		…	…	…	…
统计						

二是以柱状图形式统计不同设备和安全子类的测评结果。

三是以表格形式汇总信息系统中存在的安全问题。

8.3 整体测评结果汇总

从安全控制间、层面间、区域间和系统结构等方面对单元测评的结果进行验证、分析和整体评。

8.3.1 控制间安全测评

安全控制间的安全测评主要考虑同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。

例如，主机层面的身份鉴别与访问控制之间关系密切，应关注他们之间的关联互补作用。

例如，可以通过物理层面上的物理访问控制来增强其安全防盗窃功能等。安全功能上的削弱会使一个安全控制的引入影响另一个安全控制的功能发挥或者给其带来新的脆弱性。

例如，应用安全层面的代码安全与访问控制，如果代码安全没有做好，很可能会使应用系统的访问控制被旁路。

8.3.2 层面间安全测评

层面间的安全测评主要考虑同一区域内的不同层面之间存在的功能增强、补充和削弱等关联作。

实际环境，重点研究不同层面上相同或相似的安全控制(如主机系统层面与应用层面上的身份鉴别之间的关系)，以及技术与管理上各层面的关联关系，分析出哪些安全控制间可能会存在安全功能上的增强和补充作用。

8.3.3 区域间安全测评

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。

例如，流入某个区域的所有网络数据都已经在另一个区域上做过网络安全审计，则可以认为该区域通过区域互连后具备网络安全审计功能。

系统结构安全测评主要考虑信息系统整体结构的安全性和整体安全防范的合理性。

整体结构的安全性测评应从信息系统的物理布局、网络拓扑、业务逻辑（业务数据流）、系统实现和集成方式等入手，结合不同位置上可能面临的威胁、可能暴露的脆弱性等，综合判定信息系统的整体布局是否合理、整体是否安全有效等。

在检查信息系统安全保护措施的具体实现方式和部署情况后，结合其业务数据流分析不同区域和不同边界与安全保护措施的关系、重要业务和关键信息与安全保护措施的关系等，参照纵深防御的要求，识别信息系统的安全防范是否突出重点、层层深入，综合判定信息系统的整体安全防范是否恰当合理。

例如，由于信息系统边界上的网络入侵防范设备的管理接口连接方式不当，可能使网络访问控制出现旁路，出现信息系统整体安全防范不当。

8.4 风险分析和评价

依据等级保护的相关规范和标准，采用风险分析的方法分析信息系统等级测评结果中存在的安全问题（等级测评结果中部分符合项或不符合项的汇总结果）可能对信息系统安全造成的影响。

分析过程包括：

1）判断安全问题被威胁利用的可能性，可能性的取值范围为高、中和低；

2）判断安全问题被威胁利用后，对信息系统安全（业务信息安全和系统服务安全）造成的影响程度，影响程度取值范围为高、中和低；

3）综合 1）和 2）的结果对信息系统面临的安全风险进行赋值，风险值的取值范围为高、中和低；

4）结合信息系统的安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的风险。

以列表形式给出等级测评发现安全问题以及风险分析和评价情况。

表 7 系统安全问题风险分析和评价表

序号	问题描述	关联资产[1]	关联威胁[2]	风险值	风险评价
1					
2					
3					
…					

8.5 等级测评结论

综合第 3、4、5 章的测评与分析结果，对信息系统基本安全保护状态进行综合判断，并给出等级测评结论，应表述为“**符合**”、“**基本符合**”或者“**不符合**”。

测评结论的判别依据如表 8 所示。

表 8 测评结论判断依据

测评结论	判别依据
符合	等级测评结果中不存在部分符合项或不符合项
基本符合	等级测评结果中存在部分符合项或不符合项，但不会导致信息系统面临高等级安全风险

[1] 如风险值和评价相同，可填写多个关联资产。

[2] 对于多个关联的情况，应分别填写。

不符合	等级测评结果中存在部分符合项或不符合项，导致信息系统面临高等级安全风险

8.6 安全建设整改建议

应在报告中针对系统存在的主要安全问题提出安全建设和整改意见。并通过总结单元测评、整体测评、风险分析和评论中的相关缺陷，结合《技术指引》和《管理指引》的相关要求，提出切合工作实际的整改思路和方法。

附录 A
（资料性附录）
现场单元测评检查表

A.1 第二级信息系统等保检查表

A.1.1 技术类检查表

A.1.1.1 物理安全检查表

序号	类 别	测评要求	测评方法	结果记录	符合情况
1	物理位置的选择	a) 机房和办公场地应选择在具有防震、防雷击、防风和防雨等能力的建筑内；**应选择交通、通信便捷地区。**	检查机房和办公场地的设计/验收文档，检查机房和办公场地所在的建筑物，查看其是否具有防震(震级需根据机房所在地区的地质环境确定)、防雷击、防风和防雨等能力的基本条件。		
2	物理访问控制	**a)** 机房出入口应能控制、鉴别和记录进入的人员。	访谈物理安全负责人，了解具有哪些控制机房进出的机制，检查是否具有对进入机房人员的身份鉴别措施。		
		b) 需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。	检查机房安全管理制度，查看其是否具有关于外来人员出入机房方面的规定， 是否具有来访人员进入机房的审批记录。		
		c) 应对机房划分区域进行管理，如将机房划分为生产区、辅助区，其中生产区是指放置一般业务系统服务器、客户端（工作站）等设备的运行区域，辅助区是指放置供电、消防、空调等设备的区域。（F2）	访谈物理安全负责人，是否对机房进行了划分区域管理，是否对各个区域都有专门的管理要求；检查机房区域划分是否合理。		
3	防盗窃和防破坏	a) 应将主要设备放置在机房内。	检查主要设备是否都放置在机房内。		
		b) 应将设备或主要部件进行固定，并设置明显的不易除去的标记。	检查设备或设备主要部件的固定情况，是否不易被移动或被搬走，是否设置明显的不易除去的标记。		
		c) 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中。	检查通信线缆铺设是否在隐蔽处（如铺设在地下或管道中等）。		

序号	类 别	测评要求	测评方法	结果记录	符合情况
		d) 应对介质分类标识，存储在介质库或档案室中。	访谈资产管理员，是否对介质进行了分类标识，是否存放在介质库或档案室中；检查介质的管理情况。		
		e) 主机房应安装必要的防盗报警设施。	检查机房是否具有防盗报警设施，查看其是否正常运行。		
		f) 应建立机房设施与场地环境监控系统，对机房空调、消防、不间断电源（UPS）、供配电、门禁系统等重要设施实行全面监控。（F2）	检查机房设施与场地环境监控系统，是否对对机房空调、消防、不间断电源（UPS）、供配电、门禁系统等重要设施实行全面的监控。		
4	防雷击	a) 机房建筑应设置避雷装置。	访谈物理安全负责人，询问采取了哪些防雷措施，机房建筑是否设置了避雷装置，是否通过验收或国家有关部门的技术检测。		
		b) 机房应设置交流电源地线。	访谈物理安全负责人，询问机房计算机系统接地是否设置了交流电源地线；检查机房设计/验收文档，是否与实际情况一致。		
5	防火	**a) 机房应设置对计算机设备影响小的**气体灭火设备和火灾自动报警系统**。**	访谈物理安全负责人，询问机房采取了哪些防火措施；检查灭火设备摆放位置是否合理，有效期是否合格。		
		b) 机房内部通道设置、装饰材料、设备线缆等应满足消防要求，并通过消防验收。（F2）	机房是否设置二个以上消防逃生通道，同时能够保证机房内各分区到各消防通道的道路通畅，方便人员逃生时使用。在机房通道上是否设置显著的消防标志。		
6	防水和防潮	**a) 水管不宜穿过机房屋顶，但若有穿过地板应当采取保护防范措施。**	访谈物理安全负责人，询问机房内是否具有上下水管安装，如果有水管安装是否避免穿过屋顶，如果穿过活动地板是否采取保护措施。		
		b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。	检查机房是否具有对外开放的窗户，如果有窗户是否采取必要的防雨措施；在屋顶和墙壁等是否不存在漏水、渗透和返潮现象，机房及其环境是否不存在明显的漏水和返潮的威胁。		

序号	类 别	测评要求	测评方法	结果记录	符合情况
		c) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	检查机房是否具有除湿装置并能够正常运行，是否具有防止出现机房地下积水的转移与渗透的措施，是否与机房湿度记录情况一致。		
7	防静电	a) 关键设备应采用必要的接地防静电措施。	访谈物理安全负责人，询问机房是否存在静电问题或因静电引起的故障事件，采取了哪些有效防静电措施，主要设备是否采用必要的接地防静电措施；检查机房设计/验收文档，描述内容与实际情况是否一致。		
8	温湿度控制	a) 应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。	检查温、湿度自动调节系统是否能够正常运行。		
9	电力供应	a) 应在机房供电线路上设置稳压器和过电压防护设备。	访谈物理安全负责人，询问是否出现过电压不稳现象，计算机系统供电线路上是否设置了稳压器和过电压防护设备；检查机房，查看计算机系统供电线路上的稳压器、过电压防护设备是否正常运行，查看供电电压是否正常。		
		b) 应提供短期的备用电力供应，**备用供电措施(如蓄电池、发电机等)能提供超过1小时的供电时间。**	访谈物理安全负责人，是否设置了短期备用电力供应设备（如UPS），供电时间是否满足系统最低电力供应需求；检查短期备用电力供应设备是否工作正常。		
		c) 机房重要区域、重要设备应提供UPS单独供电。(F2)	检查机房重要区域、重要设备是否提供UPS单独供电。		
10	电磁防护	a) 电源线和通信线缆应隔离，避免互相干扰。	检查机房布线，查看是否做到电源线和通信线缆隔离。		

A.1.1.2 网络安全检查表

序号	类别	测评内容	测评方法	结果记录	符合情况

序号	类别	测评内容	测评方法	结果记录	符合情况
1	结构安全	a) 应保证关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要。	访谈网络管理员，询问信息系统边界设备和主要网络设备的处理性能能否满足目前业务高峰流量情况，询问采用何种手段对主要网络设备进行运行状况监控。		
		b) 应保证接入网络和核心网络部分的带宽满足业务高峰期需要。	访谈网络管理员，询问网络各个部分的带宽是否满足业务高峰的需要，如果无法满足，则需要在主要网络设备上进行带宽配置，若有网管系统或流量监控系统，查看网络和核心网络的带宽占用报表是否有达到或超过处理能力记录。		
		c) 应绘制与当前运行情况相符的网络拓扑结构图。	查看网络拓扑结构图与当前运行情况是否一致。		
		d) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素,划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；**生产网、互联网、办公网之间都应实现有效隔离。**	1、查网络设计/验收文档，查看是否有根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，2、登录核心交换机，show vlan brief 查看 vlan 划分、show int vlan X 详细查看某个具体 vlan 情况。		

序号	类别	测评内容	测评方法	结果记录	符合情况
2	访问控制	a) 应在网络边界部署访问控制设备，启用访问控制功能。	1)访谈并确定哪些设备是边界访问控制设备。 2)访谈并确定是否存在远程拨号用户，具体的远程拨号控制设备。		
		b) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为网段级。	1、查看客户端是否对重要网段、主机进行 arp 绑定，2、登录交换机，show run，查看是否对重要网段、主机采取静态 arp 绑定、端口与 mac 绑定措施，3、是否采取防火墙与代理服务等其他方式防止 arp 欺骗。		
		c) 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。	登录网络设备，show run，查看方位控制列表是否精确至 host。		
		d) 应限制具有拨号访问权限的用户数量。	登录网络设备，show run	b vty，查看 vty 用户数量是否限制。	

序号	类别	测评内容	测评方法	结果记录	符合情况
3	安全审计	a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。	登录网络设备，1、show snmp 查看是否配置 snmp 进行网络设备运行状况记录 ；、show logging 、2、show ip netflow export 查看是否配置网络流量记录；3、show aaa meth accounting 查看是否配置用户行为记录。		
		b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息,**保存时间不少于一个月。**	登录日志服务器为或 AAA 服务器，查看记录是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息，保存时间不少于一个月。		
4	边界完整性检查	a) 应能够对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查。	登录业务网非法外联监控管理服务器，查看是否有未安装非法外联客户端的计算机接入网络，若有是否采取进行定位、阻断。		
5	入侵防范	a) 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出、IP 碎片攻击和网络蠕虫攻击等。	查看其是否有在网络边界及核心业务网段处有对网络攻击采取相关措施。		

序号	类别	测评内容	测评方法	结果记录	符合情况
6	网络设备防护	a) 应对登录网络设备的用户进行身份鉴别。	是否对网络设备进行 AAA 认证或其他认证方式，若有登录 AAA 服务器，查看用户与管理员身份、权限是否匹配。		
		b) 应对网络设备的管理员登录地址进行限制。	登录网络设备，show run，查看是否在网络设备上是否采用相应 acl 限制管理员登录；2、登录 AAA 服务器，查看是否进行管理员地址限制。		
		c) 网络设备用户的标识应唯一。	访谈网络设备管理员，询问其各个网络设备用户的标识。		
		d) 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换。	应访谈网络管理员，询问网络设备的口令策略是什么。		
		e) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。	采用错误密码登录网络设备数次，观察是否结束会话、限制非法登录次数，并观察如果登录后长时间不操作会不会被系统退出。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		f） 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	远程登录网络设备，看是否采用22端口SSH方式或其他加密方式。		
		g） 应每月对网络设备的配置文件进行备份，发生变动时应及时备份。（F2）	应访谈网络管理员，询问网络设备配置文件如何进行备份。		
		h） 应定期对网络设备运行状况进行检查。（F2）	应查看检查记录，是否定期对网络设备运行状况进行检查。		
		i） 对网络设备系统自带的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端口开放审批制度。（F2）	应测评网络设备，是否关闭不必要的网络设备服务，并查看审批制度文件。		
		j） 应定期检验网络设备软件版本信息。（F2）	应查看检查表，是否定期检验网络设备软件版本信息。		
		k） 应建立网络设备的时钟同步机制。（F2）	应查看网络设备时钟设置情况。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		l） 应定期检查并锁定或撤销网络设备中多余的用户账号。（F2）	1、登录网络设备，show run ｜ b user，查看设立账户是否与管理员一一对应，2、若有网络日志服务器或 AAA 服务器，查看管理员变动相应时段是否有相关操作记录。		

A.1.1.3 主机安全检查表

序号	类别	测评项	测评方法	结果记录	符合情况
1	身份鉴别	a） 应对登录操作系统和数据库系统的用户进行身份标识和鉴别。	可访谈系统管理员/数据库管理员，询问操作系统的身份标识与鉴别机制采取何种措施实现，目前系统提供了哪些身份鉴别措施和鉴别失败处理措施。		
		b） 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，**关键系统的静态口令应在 6 位以上并由字母、数字、符号等混合组成并定期更换。**	应检查主要服务器操作系统和主要数据库管理系统，查看是否提供了身份鉴别措施（如用户名和口令等），其身份鉴别信息是否具有不易被冒用的特点，例如，口令足够长，口令复杂（如规定字符应混有大、小写字母、数字和特殊字符），口令生命周期，新旧口令的替换要求（如规定替换的字符数量）或为了便于记忆使用了令牌。		
		c） 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。	应检查主要服务器操作系统和主要数据库管理系统，查看是否已配置了鉴别失败处理功能，并设置了非法登录次数的限制值，对超过限制值的登录终止其鉴别会话或临时封闭帐号；查看是否设置网络登录连接超时，并自动退出；查看是否设置鉴别警示信息。		

序号	类别	测评项	测评方法	结果记录	符合情况
		d) 当通过互联网对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。	应检查主要服务器操作系统，查看服务器操作系统是否对与之相连的服务器或终端设备进行身份标识和鉴别并进行了相应的加密。		
		e) 应为操作系统和数据库的不同用户分配不同的用户名，确保用户名具有唯一性。	应测评主要服务器操作系统和主要数据库管理系统，添加一个新用户，其用户标识为系统原用户的标识（如用户名或UID），查看是否不会成功。		
2	访问控制	a) 应启用访问控制功能，依据安全策略控制用户对资源的访问。	应检查服务器操作系统和数据库管理系统的安全策略，查看是否明确主体（如用户）以用户和/或用户组的身份规定对客体（如文件或系统设备,目录表和存取控制表访问控制等）的访问控制，覆盖范围是否包括与信息安全直接相关的主体（如用户）和客体（如文件，数据库表等）及它们之间的操作（如读、写或执行）。		
		b) 应实现操作系统和数据库系统特权用户的权限分离。	应检查主要服务器操作系统和主要数据库管理系统，查看在系统管理员、安全管理员、安全审计员之间是否设置了相互制约关系（如系统管理员、安全管理员等不能对审计日志，安全审计员管理不了审计数据的开启、关闭、删除等重要事件的审计日志等）。		
		c) 应严格限制默认账户的访问权限，重命名系统默认账户，并修改这些账户的默认口令。	应查看主要服务器操作系统和主要数据库管理系统，查看匿名/默认用户的访问权限是否已被禁用或者严格限制（如限定在有限的范围内）。		
		d) 应及时删除多余的、过期的账户，避免共享账户的存在。	应查看是否有多余、过期、共享账户的存在。		
3	安全审计	a) 审计范围应覆盖到服务器上的每个操作系统用户和数据库用户。	可访谈安全审计员，询问主机系统是否设置安全审计；询问主机系统对事件进行审计的选择要求和策略是什么；对审计日志的处理方式有哪些。		

序号	类别	测评项	测评方法	结果记录	符合情况
		b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件。	应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、系统资源的异常使用、重要系统命令的使用（如删除客体）等。		
		c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。	应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容。		
		d) 应保护审计记录，避免受到未预期的删除、修改或覆盖等，**保存时间不少于一个月。**	应测评主要服务器操作系统、重要终端操作系统和主要数据库管理系统，在系统上以某个系统用户试图删除、修改或覆盖审计记录，测评安全审计的保护情况与要求是否一致。		
4	入侵防范	a) 操作系统遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器、系统软件预防性维护服务等方式保持系统补丁及时得到更新。	应与系统管理员访谈，询问入侵防范产品的厂家、版本和在主机系统中的安装部署情况；询问是否进行过部署的改进或者更换过产品，是否按要求（如定期或实时）进行产品升级。		
5	恶意代码防范	a) 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。	应访谈系统安全员，询问主机系统是否采取恶意代码实时检测与查杀措施，恶意代码实时检测与查杀措施的部署情况如何，因何改进过部署或者更换过产品，是否按要求（如定期或实时）进行产品升级。		
		b) 应支持恶意代码防范的统一管理。	应检查网络防恶意代码产品，查看厂家、版本号和恶意代码库名称等信息是否统一管理。		
6	资源控制	a) 应通过设定终端接入方式、网络地址范围等条件限制终端登录。	应检查主要服务器操作系统，查看是否限制单个用户的多重并发会话数量；查看是否设置登录终端的操作超时锁定和鉴别失败锁定，以及		

序号	类别	测评项	测评方法	结果记录	符合情况
			是否规定解锁或终止方式；查看是否配置了终端接入方式、网络地址范围等条件限制终端登录。		
		b） 应根据安全策略设置登录终端的操作超时锁定。	应测评主要服务器操作系统，任选一个用户，登录服务器，在一定时间内不进行任何动作，验证主要服务器操作系统能否对操作超时的终端进行锁定；任选一个用户，可通过多次失败登录服务器，验证服务器能否对鉴别失败的终端进行锁定，锁定后能否按照规定的解锁或终止方式进行解锁或终止。		
		c） 应限制单个用户对系统资源的最大或最小使用限度。	应检查主要服务器操作系统，查看是否在服务水平降低到预先规定的最小值时，能检测和报警，报警的方式有哪些，能否已根据安全策略设定主体（如进程）的服务优先级，并根据优先级分配系统资源，保证优先级低的主体处理能力不会影响到优先级高的主体的处理能力。		

A.1.1.4 应用安全检查表

序号	类别	测评项	测评方法	结果记录	符合情况
1	身份鉴别	a）应提供专用的登录控制模块对登录用户进行身份标识和鉴别。	1） 询问系统管理员，该系统是否提供专用的登录控制模块对登录的用户进行身份标识和鉴别，采用何种方式对用户进行身份标识和鉴别。 2） 检查应用系统，身份标识和鉴别的方式是否与管理员回答的一致。 3） 以某注册用户身份登录系统，查看登录是否成功；以非法用户身份登录系统，查看登录是否成功。		

序号	类别	测评项	测评方法	结果记录	符合情况
		b）应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。	1） 询问系统管理员，该系统的用户身份标识是否唯一。采取了什么措施防止身份鉴别信息被冒用。 2） 检查总体规划/设计文档，查看其是否有系统采取了唯一标识的说明。查看其身份鉴别信息是否具有不易被冒用的特点。 3） 询问系统管理员，该系统是否有专门的设置保证用户身份鉴别信息不易被冒用，如果应用系统采用口令进行身份鉴别，则查看是否有选项或设置强制要求口令长度、复杂度、定期修改等。 4） 如果应用系统式以用户名来保证用户身份标识的唯一性，则以已有的用户名重新注册，测试系统是否禁止该操作。 5） 扫描应用系统，测试其鉴别信息复杂度检查功能，检查系统是否不允许存在弱口令、空口令等。		
		c）应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。	1） 询问系统管理员，该系统是否具有登录失败处理的功能（如结束会话、限制非法登录次数，当登录连接超时，自动退出等），是如何进行处理的? 2） 如果有登录失败处理设置选项或模块，查看系统是否设置或选中了该功能。 3） 根据应用系统使用的登录失败处理方式，采用如下方法之一或全部进行测试： i. 以错误的用户名或密码登录系统，查看系统反应。 ii. 以超过系统规定的非法登录次数登录系统，查看系统反应。 iii. 登录系统连接超时，查看系统反应。		

序号	类别	测评项	测评方法	结果记录	符合情况
		d）应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。	1） 询问系统管理员，该系统的身份鉴别、身份标识唯一性检查、鉴别信息复杂度检查以及登录失败处理功能是否有专门的模块或选项，是否有相关参数需要配置。 2） 如果有参数需要配置，则查看实际配置情况，是否已经启用上述功能。		
2	访问控制	a）应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问。	1） 询问系统管理员，该系统是否提供访问控制功能，访问控制策略是什么？访问控制的粒度是否达到文件、数据库表？ 2） 检查应用系统的访问控制功能和策略配置是否与管理员回答的一致。 3） 以某一用户身份登录系统，依据安全策略对客体进行访问，测试是否成功。该用户不依据安全策略对客体进行访问，测试是否成功。		
		b）访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作。	1） 访谈系统管理员，询问系统访问控制策略是否覆盖到与信息安全直接相关的主体、客体及它们之间的操作？ 2） 检查应用系统的访问控制策略是否覆盖到与信息安全直接相关的所有主体、客体及它们之间的操作。		
		c）应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限。	1） 询问系统管理员，该系统是否有由授权主体配置访问控制策略的功能。 2） 如果系统有由授权主体配置访问控制策略的功能，则以该授权主体用户登录系统，查看某特定用户的权限。以该用户身份登录系统，进行在权限范围内和权限范围外的一些操作，查看是否成功。 3） 以该授权主体用户登录系统，修改上述特定用户的权限。以该用户身份登录系统，查看该用户的权限是否与刚修改过的权限保持一致，验证用户权限管理功能是否有效。		

序号	类别	测评项	测评方法	结果记录	符合情况
			4) 询问系统管理员，该系统是否有默认用户，如果有，是否限制了默认用户的访问权限。 5) 如果有默认帐户，以默认帐户（默认密码）登录系统，并进行合法及非法操作，测试系统是否对默认帐户访问权限进行了限制。		
		d）应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。	1) 访谈系统管理员，询问系统所有帐户是否只拥有完成自己承担任务所需的最小权限，相互之间是否形成相互制约关系。 2) 检查应用系统，查看不同帐户的权限是否分离（如管理员不能审计、审计员不能管理、安全员不能审计和管理等、审计员不能修改自己的行为日志等）。权限之间是否相互制约。 3) 以管理员身份进行审计操作，查看是否成功。以审计员身份进行删除/增加用户、设定用户权限的操作（也可进行一些其他管理员进行的操作），查看是否成功。 4) 以拥有其他权限的用户身份登录，查看其权限是否受到限制。		
		e）生产系统应建立关键账户与权限的关系表。（F2）	检查是否建立关键账户与权限的对应关系表，核实权限分配是否依据最小原则，是否相互制约。		
3	安全审计	a）应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计。	1) 访谈安全审计员，询问是否有安全审计功能，对事件进行审计的选择要求和策略是什么。 2) 检查应用系统的审计策略（审计记录），查看审计策略（或记录）是否覆盖到每个用户。都对哪些安全事件进行审计。 3) 多次以任意用户身份登录系统，进行一些操作，包括重要的安全相关操作或事件（如用户标识与鉴别、自主访问控制的所有操作记		

序号	类别	测评项	测评方法	结果记录	符合情况
			录（如用系统管理员身份改变用户权限，增加或删除用户），用户的行为（如删除数据、多次登录失败等））。 4） 用审计人员的身份登录系统，查看系统对上述用户的重要操作或事件是否进行审计。		
		b）应保证**不提供**删除、修改或覆盖审计记录**的功能**。	1） 访谈安全审计员，询问应用系统对审计日志的处理方式有哪些。 2） 以普通用户身份试图删除、修改或覆盖自身的审计记录，查看能否成功。试图删除、修改其他人的审计记录，查看能否成功。 3） 如果审计记录能够导入，则导出审计记录并进行修改后导入系统，查看能否覆盖以前的审计记录。		
		c）审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等，**保存时间不少于一个月。**	1） 以审计员身份登录系统，检查审计记录内容是否包括事件发生的日期、时间、发起者信息、事件类型、事件相关描述信息、事件的结果等。		
4	通信完整性	a）应采用校验码技术保证通信过程中数据的完整性。	1） 询问安全管理员应用系统是否有数据在传输过程中进行完整性保证的操作，具体采取什么措施。 2） 应检查设计/验收文档，查看其是否有通信完整性的说明，如果有则查看是否采用校验码技术保证通信完整性。		

序号	类别	测评项	测评方法	结果记录	符合情况
5	通信保密性	a）在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证。	1） 询问安全管理员系统在通信双方建立连接之前采用什么技术进行会话初始化验证。 2） 应检查设计/验收文档，查看其是否有通信保密性的说明，如果有则查看是否有利用密码技术进行通信会话初始化验证的说明。		
		b）应对通信过程中的敏感信息字段进行加密。	1） 询问安全管理员应用系统的敏感信息字段在通信过程中是否采取保密措施，具体采取什么措施。 2） 应检查设计/验收文档，查看其是否有通信保密性的说明，如果有则查看是否有对通信过程中的敏感信息字段进行加密的说明。		
6	软件容错	a）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。	1） 访谈管理员，询问是否有保证软件具有容错能力的措施，具体采取哪些措施。 2） 在应用终端输入不同（如数据格式或长度等符合、不符合软件设定的要求）的数据，包括登录标识与鉴别数据、其他操作数据等，查看系统的反应。		
		b）在故障发生时，应用系统应能够继续提供一部分功能，确保能够实施必要的措施。	访谈系统管理员，是否有保障系统在发生故障时继续提供服务的功能。		
		c）应能够有效屏蔽系统技术错误信息，不将系统产生的错误信息直接反馈给客户。（F2）	检查是否采取了屏蔽系统技术错误信息的措施，防止系统产生的错误信息直接反馈给客户。		

序号	类别	测评项	测评方法	结果记录	符合情况
7	资源控制	a）**对于有会话或短连接的应用系统**，当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话。	1） 询问业务系统是否有资源控制的措施，具体措施有哪些。 2） 登录应用系统服务器，查看应用系统属性是否设置了连接超时限制。		
		b）应能够对系统的最大并发会话连接数进行限制。	1） 询问管理员应用系统同时最多支持多少个并发会话连接？是否有限制？ 2） 登录应用系统服务器，查看系统是否设置了参数限制最大并发会话连接数。		
		c）**对于有会话的应用系统，**应能够对单个帐户的多重并发会话进行限制。	1） 询问管理员单个帐户同时可以发起多少个并发会话，是否有限制？ 2） 登录应用系统服务器，查看系统是否对单个帐户的多重并发会话进行限制。 3） 以超过单个帐户规定的并发会话连接数连接系统，测试能否成功。		

A.1.1.5 数据安全检查表

序号	类别	测评项	测评方法	结果记录	符合情况
1	数据完整性	a）应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏。	1） 询问安全管理员应用系统的鉴别信息和重要业务数据在传输过程中是否有完整性保证措施，具体措施有哪些。 2） 检查应用系统，查看其是否配备检测/验证鉴别信息和重要业务数据在传输过程中完整性受到破坏的功能。		

序号	类别	测评项	测评方法	结果记录	符合情况
2	数据保密性	a）应采用加密或其他保护措施实现鉴别信息数据存储保密性。	1） 询问安全管理员应用系统的鉴别信息和重要业务数据是否采用加密或其他有效措施实现存储保密性。 2） 检查应用系统设计/验收文档，查看其是否有关于其鉴别信息、敏感的用户数据采用加密或其他有效措施实现存储保密性的描述。 3） 检查应用系统，查看其鉴别信息和重要业务数据是否采用加密或其他有效措施实现存储保密性。		
3	备份和恢复	a） 应能够对重要信息进行备份和恢复。	1） 可访谈网络管理员，询问信息系统中的网络设备是否提供用户有选择的备份重要信息的功能；是否提供重要网络设备、通信线路和服务器的硬件冗余； 2） 可访谈系统管理员，询问信息系统中的操作系统是否提供用户有选择的备份重要信息的功能； 3） 可访谈数据库管理员，询问信息系统中的数据库管理系统是否提供用户有选择的备份重要信息的功能； 4） 应检查重要应用系统设计/验收文档，查看其是否有描述应用系统提供用户有选择的备份重要信息的功能的描述。		
		b） 应提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性。	1）应检查操作系统、网络设备、数据库管理系统、关键应用系统，查看其是否配置有选择的备份和恢复重要信息恢复的功能，其配置是否正确； 2） 应检查重要网络设备、通信线路和服务器是否提供硬件冗余。		

A.1.2 管理类检查表

A.1.2.1 安全管理制度

序号	类别	测评要求	测评方法	结果记录	符合情况

序号	类别	测评要求	测评方法	结果记录	符合情况
1	管理制度	a）应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等。	检查信息安全工作的总体方针和安全策略，查看文件是否明确机构安全工作的总体目标、范围、原则和安全框架等。		
		b）应对安全管理活动中重要的管理内容建立安全管理制度。	检查各项安全管理制度，查看是否覆盖系统建设、改造、升级、运行维护等方面。		
		c）应对安全管理人员或操作人员执行的日常管理操作建立操作规程。	检查是否具有对重要管理操作的操作规程，如系统维护手册和用户操作规程等。		
2	制定和发布	**a）由金融机构总部科技部门**负责制定适用全机构范围安全管理制度**，各分支机构的科技部门**负责制定适用辖内安全管理制度**。**	访谈安全主管，询问由何部门或人员负责安全管理制度的制定，参与制定人员有哪些。		
		b）应组织相关人员对制定的安全管理进行论证和审定。	访谈安全主管，询问安全管理制度的制定程序，是否对制定的安全管理制度进行论证和审定；检查管理制度评审记录，查看是否具有相关人员的评审意见。		
		c）应将安全管理制度以某种方式发布到相关人员手中。	应检查安全管理制度的发布过程是否正式有效，并以某种方式发布到相关人员手中。		
3	评审和修订	a）应定期对安全管理制度进行评审，对存在不足或需要改进的安全管理制度进行修订。	检查是否具有安全管理制度体系的评审记录，查看是否由信息安全领导小组负责，是否记录了相关人员的评审意见和修订记录。		

A.1.2.2 安全管理机构

序号	类别	测评要求	测评方法	结果记录	结果记录

序号	类别	测评要求	测评方法	结果记录	结果记录
1	岗位设置	**a）信息安全管理工作应实行统一领导、分级管理，总部统一领导分支机构的信息安全管理，各机构负责本单位和辖内的信息安全管理。(F2)**	检查金融行业信息安全管理工作是否实行统一领导、分级管理，总部和各分支机构在信息安全管理工作方面如何分配。		
		b）除科技部门外，其他部门均应指定至少一名部门计算机安全员，具体负责本部门的信息安全管理工作，协同科技部门开展信息安全管理工作。（F2）	检查是否具备信息安全管理人员名单，查看人员的配备和责任范围是否合理。		
		c）应设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。	检查部门、岗位职责文件，查看文件是否明确安全管理机构的职责，是否明确机构内各部门和各负责人的职责和分工。		
		d）应设立系统管理员、网络管理员、安全管理员岗位，并定义各个工作岗位的职责。	查看文件是否明确设置安全主管、安全管理各个方面的负责人、机房管理员、系统管理员、网络管理员、安全管理员等各个岗位，各个岗位的职责范围是否清晰、明确。		
2	人员配备	a）应配备一定数量的系统管理员、网络管理员、安全管理人员等。	检查管理人员名单，查看其是否明确哪些人员是机房管理员、系统管理员、网络管理员、安全管理员等重要岗位人员的信息。		
		b）安全管理人员不能兼任网络管理员、系统管理员、数据库管理员等。	检查管理人员名单，查看安全管理员是否兼职其他信息安全相关职位。		
3	授权和审批	a）应根据各个部门和岗位的职责明确授权审批部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批。	检查审批管理制度文档，查看文档中是否明确审批事项、审批部门和批准人等。		

序号	类别	测评要求	测评方法	结果记录	结果记录
		b）应针对关键活动建立审批流程，并由批准人签字确认。	检查审批管理制度文档，查看文档中是否明确审批程序等，是否审批确认。		
4	沟通和合作	a）应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通。	检查组织内部机构之间以及信息安全职能部门内部的安全工作会议文件或会议记录，查看是否具有会议内容、会议时间、参加人员和会议结果等描述；检查是否具有信息安全管理委员会或领导小组安全管理工作执行情况的文件或工作记录。		
		b）应加强与兄弟单位、公安机关、电信公司的合作与沟通。	检查外联单位联系列表，查看外联单位是否包含公安机关、电信公司、兄弟公司等，是否说明外联单位的名称、联系人、合作内容和联系方式等内容。		
5	审核和检查	a）安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	访谈安全主管，询问是否组织人员定期对信息系统进行安全检查，检查周期多长，检查内容是否包括系统日常运行、系统漏洞和数据备份等情况。		

A.1.2.3 人员安全管理

序号	类别	测评内容	测评方法	结果记录	符合情况
1	人员录用	a）应指定或授权专门的部门或人员负责人员录用。	访谈安全主管，询问是由何部门/何人负责安全管理和技术人员的录用工作。		
		b）应规范人员录用过程，对被录用人的身份、背景和专业资格和资质等进行审查，对其所具有的技术、技能进行考核。	检查人员录用要求管理文档，查看是否说明录用人员应具备的条件，如学历、学位要求等；检查技能考核文档或记录，查看是否记录考核内容和考核结果等。		
		c）应与从事关键岗位的人员签署保密协议。	访谈人事负责人，询问是否与录用后的关键岗位的人员签署保密协议；检查保密协议。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		d) 对信息安全管理人员应实行备案管理。信息安全管理人员的配备和变更情况，应及时报上一级科技部门备案，金融机构总部信息管理人员在总部科技部门备案。(F2)	检查对信息安全管理人员是否实行备案管理。信息安全管理人员的配备和变更情况，是否及时报上一级科技部门备案，金融机构总部信息管理人员是否在总部科技部门备案。		
		e)凡是因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员，不得从事信息安全管理工作。(F2)	检查相关人员档案背景，不得录用因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员。		
2	人员离岗	a）应规范人员离岗过程，及时终止即将离岗员工的所有访问权限。	访谈人事负责人，询问是否及时终止离岗人员的所有访问权限。		
		b）应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	检查是否具有交还身份证件和设备等的登记记录。		
		c）应办理严格的调离手续，并保证离岗人员负责的信息技术系统的口令必须立即更换。	检查人员离岗管理文档，查看是否规定了调离手续和离岗要求等。		
3	人员考核	a）应定期对各个岗位的人员进行安全技能及安全认知的考核。	访谈安全主管，询问对各个岗位人员是否定期进行考核，考核周期多长，考核内容有哪些；检查考核记录。		
4	安全意识教育和培训	a)应制定安全教育和培训计划。	检查安全教育和培训计划文档；查看计划是否明确了培训目的、培训方式、培训对象、培训内容、培训时间和地点等，培训内容是否包含信息安全基础知识、岗位操作规程等。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		b）应对各类人员进行安全意识教育、岗位技能和相关安全技术培训。	访谈安全主管，询问是否对各个岗位人员进行安全教育、岗位技能和安全技术培训，以什么形式进行，效果如何。		
		c)每年至少对信息安全管理人员进行一次信息安全培训。(F2)	检查各单位是否每年至少对信息安全管理人员进行一次信息安全培训。		
		d）应告知人员相关的安全责任和惩戒措施，对违反违背安全策略和规定的人员进行惩戒。	访谈安全管理员、系统管理员、网络管理员和数据库管理员，考查其是否了解与工作相关的安全责任和惩戒措施等；检查安全责任和惩戒措施管理文档。		
5	外部人员访问管理	**a）各机构指定责任部门负责非涉密计算机系统和网络相关的外部人员访问授权审批，批准后由专人全程陪同或监督，并登记备案。**	检查外部人员访问相关规定，检查外部人员访问重要区域批准文档和外部人员访问受控区域的登记记录。		
		b) 获得外部人员访问授权的所有单位和个人应与金融行业签订安全保密协议，不得进行未授权的增加、删除、修改、查询数据操作，不得复制和泄漏金融行业的任何信息。(F2)	检查获得外部人员访问授权的所有单位和个人是否与金融行业签订安全保密协议，是否进行未授权的增加、删除、修改、查询数据操作，是否发生过复制和泄漏金融行业的任何信息的事件。		
		c)外部人员进入金融机构进行现场实施时，应事先提交计划操作内容，金融机构人员应在现场陪同外部人员，核对操作内容并记录。(F2)	检查外部人员访问管理制度中是否规定外部人员进入金融机构进行现场实施时，应事先提交计划操作内容，金融机构人员应在现场陪同外部人员等内容。		

A.1.2.4 系统建设管理

序号	类别	测评内容	测评方法	结果记录	符合情况
1	系统定级	a）应明确信息系统的边界和安全保护等级。	检查系统定级说明文档，查看文档是否明确信息系统边界和安全保护等级。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		b）应以书面的形式说明确定信息系统为某个安全保护等级的方法和理由。	检查系统定级文档，查看文档是否明确信息系统的安全保护等级确定的方法和理由。		
		c）应确保信息系统的定级结果经过相关部门的批准。	检查系统定级文档，查看定级结果是否具有相关部门的批准盖章。		
2	安全方案设计	a）应根据系统的安全级别选择基本安全措施，依据风险分析的结果补充和调整安全措施。	访谈系统建设负责人，询问系统选择基本安全措施的依据，是否依据安全保护等级选择，是否依据风险分析的结果补充和调整安全措施，做过哪些调整。		
		b）应以书面形式描述对系统的安全保护要求、策略和措施等内容，形成系统的安全方案。	访谈安全主管，询问是否授权专门的部门对信息系统的安全建设进行总体规划，由何部门/何人负责；检查系统的安全建设工作计划。		
		c）应对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案。	访谈系统建设负责人，询问是否统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案等。		
		d）应组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。	访谈系统建设负责人，询问是否组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略等相关配套文件进行论证和审定。		
3	产品采购和使用	a）应确保安全产品的采购和使用符合国家的有关规定。	访谈系统建设负责人，询问系统信息安全产品的采购情况，是否按照国家的相关规定进行使用。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		b）应确保密码产品的采购和使用符合国家密码主管部门的要求。	访谈系统建设负责人，询问系统是否采用了密码产品，密码产品的使用是否符合国家密码主管部门的要求。		
		c）应指定或授权专门的部门负责产品的采购。	检查是否指定或授权专门的部门负责产品的采购。		
		d）购置扫描、检测类信息安全产品应报本机构科技主管部门批准、备案。(F2)	检查各单位购置扫描、检测类信息安全产品是否报本机构科技主管部门批准、备案。		
		e）应建立信息安全产品资产登记机制，建立信息安全类固定资产登记簿并由专人负责管理。(F2)	检查是否建立信息安全产品资产登记机制，是否建立信息安全类固定资产登记簿并由专人负责管理。		
		f）扫描、检测类信息安全产品仅限于本机构信息安全管理人员或经主管领导授权的网络管理员使用。(F2)	检查扫描、检测类信息安全产品是否仅限于本单位信息安全管理人员使用。		
		g）应定期检查各类信息安全产品相关日志和报表信息并定期汇总分析，若发现重大问题，立即采取控制措施并按规定程序报告。(F2)	检查是否随时检查各类信息安全产品使用情况，认真查看相关日志和报表信息并定期汇总分析，若发现重大问题，是否能立即采取控制措施并按规定程序报告。		
		h）应定期对各类信息安全产品的日志和报表进行备份存档。(F2)	检查是否具备信息安全产品备份的日志和报表，是否有备份记录。		
		i）应及时升级维护信息安全产品，凡超过使用期限的或不能继续使用的信息安全产品，要按照固定资产报废审批程序处理。(F2)	检查是否及时升级维护信息安全产品，凡超过使用期限的或不能继续使用的信息安全产品，是否按照固定资产报废审批程序处理。		

序号	类别	测评内容	测评方法	结果记录	符合情况
4	自行软件开发	a）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则。	检查是否具有软件开发管理制度。		
		b）应确保开发环境与实际运行环境物理分开。	检查开发环境环境和生产环境是否是物理隔离的。		
		c)应确保开发人员和测试人员分离，开发人员不能兼任系统管理员或业务操作人员，确保测试数据和测试结果受到控制。(F2)	访谈系统建设负责人，询问系统是否自主开发软件，是否在独立的开发环境中编写、调试和完成；是否要求开发人员不能做测试工作等。		
		d）应确保提供软件设计的相关文档和使用指南，并由专人负责保管。	访谈系统建设负责人，询问如何保管软件设计的相关文档，由何人负责保管；检查软件设计的相关文档（应用软件设计程序文件、源代码说明文档等）和软件使用指南或操作手册和维护手册等。		
5	外包软件开发	a）应根据开发需求检测软件质量。	访谈系统建设负责人，询问软件交付前是否依据开发协议的技术指标对软件功能和性能等进行验收检测。		
		b）应在软件安装之前检测软件包中可能存在的恶意代码。	访谈系统建设负责人，软件安装之前是否检测软件中的恶意代码，检测工具是否是第三方的商业产品。		
		c）应确保提供软件设计的相关文档和使用指南。	访谈系统建设负责人，询问是否具有软件设计的相关文档和使用指南；检查是否具有需求分析说明书、软件设计说明书、软件操作手册等开发文档。		
		d)应定期对外包服务活动和外包服务商的服务能力进行审核和评估。(F2)	访谈金融机构对外包服务活动和外包服务商服务能力进行审核和评估的频率，是否具有评估记录和报告。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		e）应要求开发单位提供软件源代码，并审查软件中可能存在的后门。	访谈系统建设负责人，询问开发单位是否提供了软件源代码，对其是否经过审查明确不存在后门。		
		f）应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。(F2)	访谈金融机构如何监督外包服务商的操作行为，是否保留外包服务商的操作痕迹、记录完整的日志。		
		g)应禁止外包服务商转包并严格控制分包，保证外包服务水平。(F2)	检查外包服务商的工作机制，是否存在分包、转包现象。		
		h）应制定数据中心外包服务应急计划，制订供应商替换方案，以应对外包服务商破产、不可抗力或其它潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。(F2)	检查是否具备关于外包服务的应急计划文档，文档中是否明确规定外包服务商的替换方案等。		
6	工程实施	a）应指定或授权专门的部门或人员负责工程实施过程的管理。	访谈系统建设负责人，询问是否指定专门部门或人员按照工程实施方案的要求对工程实施过程进行进度和质量控制。		
		b）应制定详细的工程实施方案，**并制定相关过程控制文档**，控制实施过程。	检查工程实施方案，查看其是否规定工程时间限制、进度、控制、质量控制等方面内容，工程实施过程是否按照实施方案形成各种文档，如阶段性工程进程汇报报告。		
7	测试验收	a）应对系统进行安全性测试验收。	检查是否具有第三方测试机构出示的系统安全性测试验收报告。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		b）在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告。	检查工程测试验收方案，查看其是否对参与验收部门、人员、现场操作过程等进行要求；查看测试记录是否详细记录了测试时间、人员、操作过程、测试结果等方面内容；查看测试报告是否提出存在问题及改进意见等。		
		c）应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。	访谈系统建设负责人，询问是否根据设计方案或合同要求组织相关部门和人员对测试报告进行符合性审定。		
		d）对于在生产系统上进行的测试工作，必须制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划，确保生产系统的安全。(F2)	对于需要在生产系统上就进行测试的工作，检查是否制定了详细的测试方案，包括系统数据备份、测试环境搭建、测试后数据恢复、系统审核等计划。		
8	系统交付	a）应制定系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。	检查是否具有系统交付清单，查看交付清单是否满足合同的有关要求。		
		b）系统建设单位应在完成建设任务后将系统建设过程文档和系统运维文档全部移交金融行业科技部门。	检查是否具有系统建设文档（如系统建设方案）、指导用户进行系统运维的文档（如服务器操作规程书）以及系统培训手册等文档。		
		c）外部建设单位应与金融机构签署相关知识产权保护协议和保密协议，不得将系统采用的关键安全技术措施和核心安全功能设计对外公开。(F2)	检查外部建设单位应与金融行业承担单位（部门）签署相关知识产权保护协议和保密协议，是否将系统采用的关键安全技术措施和核心安全功能设计对外公开。		
		d）应对负责系统运行维护的技术人员进行相应的技能培训。	访谈系统建设负责人，询问目前的信息系统是否由内部人员独立运行维护，如果是，系统建设实施方是否对运维技术人员进行过培训，针对哪些方面进行过培训。		

序号	类别	测评内容	测评方法	结果记录	符合情况
9	安全服务商选择	**a)选择信息安全服务提供商时应评估其资质、经营行为、业绩、服务体系和服务品质等要素。(F2)**	检查金融行业科技主管部门是否负责信息安全服务提供商的资质审查。		
		b）应确保安全服务商的选择符合国家的有关规定。	访谈系统建设负责人，询问对信息系统进行安全规划、设计、实施、维护、测评等服务的安全服务单位是否符合国家有关规定。		
		c）应与选定的安全服务商签订与安全相关的协议，明确约定相关责任。	检查是否具有与产品供应商、软件开发商、系统集成商、系统运维商和等级测评机构等相关安全服务商签订的协议。		
		d）应确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同。	访谈系统建设负责人，询问是否要求选定的安全服务商提供一定的技术培训和服务，以何种方式实现。		

A.1.2.5 系统运维管理

序号	类别	测评内容	测评方法	结果记录	符合情况
1	环境管理	a)应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定。	访谈物理安全负责人，询问是否配备机房安全管理工作，由何人、何部门负责。		
		b)机房应采用结构化布线系统，配线机柜内如果配备理线架，应做到跳线整齐，跳线与配线架统一编号，标记清晰。(F2)	访谈物理安全负责人，询问机房的布线方式，是否统一编号，标记是否清晰。		
		c)**应指定部门负责机房安全**，指派专人担任机房管理员，对机房的出入进行管理，定期巡查机房运行状况，对机房供配电、空调、温湿度控制等设施进行维护管理；**填写机房值班记录、巡视记**	访谈物理安全负责人，询问由何部门或何人对机房的基本设施（如空调、供配电设备等）进行定期维护；检查机房基础设施的维护记录。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		录。			
		d)机房人员进出机房必须使用主管部门制发的证件。(F2)	检查机房管理制度，是否对人员的进出进行规定，是否需要机房出入证。		
		e)机房管理员应经过相关培训，掌握机房各类设备的操作要领。(F2)	检查安全管理人员技能要求文档，查看是否要求机房管理员应具备掌握各类设备的操作要领，是否应经过相关培训。		
		f)应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养。(F2)	检查各单位是否定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养。		
		g)机房出入口和内部应安装7*24小时录像监控设施，录像至少保存一周。(F2)	查看机房出入口和内部是否安装7*24小时录像监控设施，录像是否至少保存一周。		
		h)机房应设置弱电井，并留有可扩展空间。（F2）	检查机房是否设置弱电井，询问其可扩展空间如何。		
		i)应加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等。	检查办公环境管理制度，查看是否对办公人员的相关行为进行规范。		
2	资产管理	a) 应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	检查资产清单，查看其内容是否覆盖资产责任人、所属级别、所处位置、所处部门等方面。		
		b) 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为。	检查资产管理制度，查看其内容是否覆盖资产使用、维护等方面，是否指定资产管理的责任部门或人员,由何部门/何人负责；		
3	介质管理	a) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理。	访谈资产管理员，询问介质存放于何种环境中，是否对存放环境实施专人管理。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		b） 所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放。(F2)	检查所有数据备份介质是否防磁、防潮、防尘、防高温、防挤压存放。		
		c） 应对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点。	访谈资产管理员，询问对介质的物理传输过程是否记录；是否对介质的使用情况进行登记管理，并定期盘点。		
		d） 对于重要文档，如是纸质文档则应实行借阅登记制度，未经科技部门领导批准，任何人不得将技术文档转借、复制或对外公开，如是电子文档则应采用 OA 等电子化办公审批平台进行管理。(F2)	检查纸质技术文档是否实行借阅登记制度，未经科技部门领导批准，是否将技术文档转借、复制或对外公开，电子文档是否实行 OA 等电子化办公审批平台管理。		
		e） 应对需要送出维修或销毁的介质，首先清除其中的敏感数据，防止信息的非法泄漏。	访谈资产管理员，询问对送出维修或销毁的介质如何管理，销毁前是否对数据进行净化处理。		
		f） 对载有敏感信息存储介质的销毁，应报科技相关部门备案，并进行统一销毁，由科技部门使用专用工具进行信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录。信息消除处理仅限于存储介质仍将在金融行业内部使用的情况，否则应进行信息的不可恢复性销毁。(F2)	检查对载有敏感信息存储介质的销毁，是否报保密部门备案，由科技部门使用专用工具进行信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录。信息消除处理仅限于存储介质仍将在金融行业内部使用的情况，是否进行信息的不可恢复性销毁。		
		g） 应按照统一格式对技术文档进行编写并及时更新，达到能够依靠技术文档恢复系统正常运行的要求。(F2)	检查技术文档的格式是否统一，内容是否具有参考性，是否达到能够依靠技术文档恢复系统正常运行的要求。		
		h） 应制定移动存储介质使用规范，并定期核查移动存储介质的使用情况。(F2)	检查各单位是否严格管理移动存储介质，是否定期核查所配发移动存储介质的在位使用情况，是否严禁违规使用移动存储介质。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		i） 应根据所承载数据和软件的重要程度对介质进行分类和标识管理。	访谈资产管理员，对介质是否根据重要性不同进行分类标识，并进行检查。		
		j） 应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。(F2)	检查是否定期对主要业务备份数据进行恢复性验证，是否及时转存介质中存储的数据。		
4	设备管理	a） 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理。	访谈资产管理员，询问是否对设备选用的各个环节（选型、采购、发放等）进行规范化管理，检查相应管理制度。		
		b） 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。	检查设备管理制度文档，查看其是否对设备的操作和使用了进行明确规定；检查设备操作手册，查看其内容是否覆盖设备启动、停止、加电、断电等操作。		
		c） 新购置的设备应经过测试，测试合格后方能投入使用。(F2)	检查是否具备新购设备的测试报告，是否测试合格后方可投入使用。		
		d） 各机构科技部门负责对信息系统相关的各种设备（包括备份和冗余设备）、线路等进行维护管理。(F2)	应访谈资产管理员，询问是否对各类设施、设备指定专人或专门部门进行定期维护，由何部门/何人维护。		
		e） 应做好设备登记工作，制定设备管理规范，落实设备使用者的安全保护责任。(F2)	检查各单位科技部门是否做好计算机设备登记工作，严格设备资产管理，落实计算机设备使用者的安全保护责任。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		f） 需要废止的设备，应由科技部门使用专用工具进行数据信息消除处理，如废止设备不再使用或调配到金融机构以外的单位，应由科技部门对其数据信息存储设备进行消磁或物理粉碎等不可恢复性销毁处理。(F2)	检查需要废止的计算机设备，是否由科技部门使用专用工具进行数据信息消除处理，如废止计算机设备不再使用或调配到金融行业以外的单位，是否由科技部门对其数据信息存储设备进行消磁或物理粉碎等不可恢复性销毁处理。		
		g） 设备确需送外单位维修时，应彻底清除所存的工作相关信息，并与设备维修厂商签订保密协议，与密码设备配套使用的设备送修前必须请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息。(F2)	检查计算机设备确需送外单位维修时，各单位科技部门是否彻底清除所存的工作相关信息，必要时应与设备维修厂商签订保密协议，与密码设备配套使用的计算机设备送修前必须请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息。		
		h） 应制定规范化的故障处理流程，建立详细的故障日志(包括故障发生的时间、范围、现象、处理结果和处理人员等内容)。(F2)	检查是否具备关于故障处理文档，文档中是否详细记录了处理流程，是否建立故障处理日志。		
		i） 应确保信息处理设备必须经过审批才能带离机房或办公地点。	访谈资产管理员，询问对带离机房的设备是否经过审批，由何人审批。		
5	网络安全管理	a)应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期、**重要文件备份**等方面作出规定。	检查网络安全管理制度，查看其内容是否覆盖网络安全配置（包括网络设备的安全策略、授权访问、最小服务、升级与打补丁）、审计日志保存时间、升级与打补丁等方面。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		b)应对网络环境运行状态进行巡检，巡检应保留记录，并有操作和复核人员的签名。(F2)	检查网络管理员是否定期对网络环境运行状态进行巡查，是否有巡查记录。		
		c)金融业网间互联安全实行统一规范、分级管理、各负其责的安全管理模式，未经金融行业科技主管部门核准，任何单位不得自行与外部机构实施网间互联。(F2)	询问管理员是否应定期检查违反规定拨号上网或其他违反网络安全策略的行为，金融行业内部网络与国际互联网实行安全隔离，所有接入金融行业内部网络或存储有敏感工作信息的计算机，不得接入国际互联网。		
		d)应制定远程访问控制规范，确因工作需要进行远程访问的，应由访问发起单位科技部门核准，提请被访问单位科技部门（岗）开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。(F2)	检查各单位是否严格远程访问控制，确因工作需要进行远程访问的，是否由访问发起单位科技部门核准，提请被访问单位科技部门（岗）开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。		
		e)各机构以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经金融行业科技主管部门批准，不得在金融行业内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。(F2)	检查各单位是否以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经金融行业科技主管部门批准，是否在金融行业内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。		
		f)信息安全管理人员经本部门主管领导批准后，有权对本单位或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不得对外公开，未经金融行业科技主管部门授权，任何外部单位与人员不得检测或扫描金融行业内部网络。	检查信息安全管理人员是否经本部门主管领导批准后，有权对本单位或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不得对外公开，未经金融行业科技主管部门授权，任何外部单位与人员不得检测或扫描金融行业内部网络。		
		g)应制定网络接入管理规范，任何设备接入网络前，接入方案应经过科技部门的审核，审核批准后方可接入网络并分配相应的网络资源。	检查是否制定网络接入管理规范，任何设备接入网络前的接入方案是否通过科技部门的批准。		

序号	类别	测评内容	测评方法	结果记录	符合情况
6	系统安全管理	a) 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定。	检查系统安全管理制度，查看其内容是否覆盖系统安全配置（包括系统的安全策略、授权访问、最小服务、升级与打补丁）、系统帐户（用户责任、义务、风险、权限审批、权限分配、帐户注销等）、审计日志以及配置文件的生成、备份、变更审批、符合性检查等方面。		
		b) 应根据业务需求和系统安全分析确定系统的访问控制策略。	访谈系统管理员，询问是否根据业务需求和系统安全分析确定系统的访问控制策略。		
		c) 系统管理员不得对业务数据进行任何增加、删除、修改、查询等操作，系统管理员确需对计算机系统数据库进行技术维护性操作的,应征得业务部门同意，并详细记录维护信息过程。(F2)	访谈系统管理员是否对业务数据进行任何增加、删除、修改、查询等操作，系统管理员确需对计算机系统数据库进行技术维护性操作的，是否征得业务部门同意，并详细记录维护信息。		
		d) 每年应进行至少一次漏洞扫描，对发现的系统安全漏洞及时进行修补。(F2)	访谈系统管理员，询问是否每年对系统进行漏洞扫描，发现漏洞是否进行了及时修补，检查系统漏洞扫描报告。		
		e) 应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装。	访谈系统管理员，询问在安装系统补丁程序前是否经过测试，并对重要文件进行备份。		
		f) 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作。	检查系统操作手册，查看其内容是否覆盖操作步骤、维护记录、参数配置等方面。		
		g) 应定期对运行日志和审计数据进行分析，以便及时发现异常行为。	访谈审计员，询问是否定期对系统审计日志进行分析。		

序号	类别	测评内容	测评方法	结果记录	符合情况
7	恶意代码防范管理	a) 应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。	访谈系统运维负责人，询问是否对员工进行基本恶意代码防范意识的教育，如告知应及时升级软件版本。		
		b) 金融机构客户端应统一安装病毒防治软件，设置用户密码和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序。(F2)	检查全行客户端是否统一安装病毒防治软件，设置用户密码和屏幕保护口令等安全防护措施，是否及时更新病毒特征码并安装必要的补丁程序。		
		c) 应指定专人对网络和主机进行恶意代码检测并保存检测记录。	访谈系统运维负责人，询问是否指定专人对恶意代码进行检测，并保存记录。		
		d) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。	检查恶意代码防范管理文档，查看其内容是否覆盖防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面。		
8	密码管理	a) 选用的密码产品和加密算法应符合国家相关密码管理政策规定。	访谈安全管理员，询问密码技术和产品的使用是否遵照国家密码管理规定。		
		b) 应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员必须是本机构在编的正式员工。(F2)	检查是否建立密钥管理体制，访谈密码管理人员是否是本单位在编的正式员工，并逐级进行备案，规范密钥管理。		
		c) 系统管理员、数据库管理员、网络管理员、业务操作人员均须设置口令密码，并定期更换，口令密码的强度应满足不同安全性要求。(F2)	访谈系统管理员、数据库管理员、网络管理员、业务操作人员是否均设置口令密码，并定期更换，检查口令密码的强度是否满足不同安全性要求。		

序号	类别	测评内容	测评方法	结果记录	符合情况
9	变更管理	a) 应确认系统中将发生的变更，并制定变更方案，**包括变更的组织结构与实施计划、操作步骤、影响分析等，以便于评估变更带来的风险**；系统发生重要变更前，应向主管领导申请，审批后方可实施变更，并在实施后向相关人员通告。	访谈系统运维负责人，询问是否制定变更方案指导系统执行变更；目前系统发生过哪些变更；检查系统变更方案。		
		b) 变更前应做好系统和数据的备份。风险较大的变更，应在变更后对系统的运行情况进行跟踪。(F2)	检查变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容；检查是否具有变更方案评审记录和变更过程记录文档。		
10	备份与恢复管理	a) 应对备份信息的备份方式、备份频度、存储介质、保存期等进行规范。	检查是否具有规定备份方式、频度、介质、保存期的安全管理制度。		
		b) 根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法。	检查数据备份和恢复策略文档，查看其内容是否覆盖数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面。		
		c) 灾难备份中心的选址应综合考虑生产中心与灾难备份中心交通和电讯的便利性与多样性，以及灾难备份中心当地的业务与技术支持能力、电讯资源、地理地质环境、公共资源与服务配套能力等外部支持条件。	访谈安全管理员，询问灾备中心的建设情况，选址是否合理、与生产中心设备是否一样、运行业务是否完全一致等情况。		
		d) 应识别需要定期备份的重要业务信息、系统数据及软件系统等。	访谈系统管理员、数据库管理员和网络管理员，询问需要定期备份的业务信息、系统数据及软件系统主要有哪些。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		e） 恢复及使用备份数据时需要提供相关口令密码的，应把口令密码密封后与数据备份介质 。(F2)	检查恢复及使用备份数据时是否需要提供相关口令密码的，是否把口令密码密封后与数据备份介质一并妥善保管。		
		f） 应建立灾难恢复计划，定期开展灾难恢复培训，并根据实际情况进行灾难恢复演练。(F2)	检查是否建立灾难恢复计划，检查定期开展灾难恢复培训、演练的记录。		
11	安全事件处置	a） 应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点。	访谈安全管理员，询问发现安全弱点和可疑事件的处理方式和处理流程。		
		b） 应制定安全事件报告和处置管理制度，明确安全事件类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责。	检查安全事件报告和处置管理制度，查看其是否明确与安全事件有关的工作职责，包括报告单位（人）、接报单位（人）和处置单位等职责。		
		c） 应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分。	访谈系统运维负责人，询问是否了解本系统已发生的和需要防止发生的安全事件，主要有哪几类，对识别出的安全事件是否根据其对系统的影响程度划分不同等级；检查安全事件定级文档。		
		d） 应记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生。	检查事件报告和响应处理程序，查看其内容是否包括事件的报告流程、响应处理方法等。		
		e） 应建立有效的技术保障机制，确保在安全事件处置过程中不会因技术能力缺乏而导致处置中断或延长应急处置时间。(F2)	检查金融机构是否建立了有效的技术保障机制，确保在安全事件处置过程中不会因技术能力缺乏而导致处置中断或延长应急处置时间。		

序号	类别	测评内容	测评方法	结果记录	符合情况
12	应急预案管理	a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容，**并由应急预案涉及的相关机构签字盖章。**	检查应急响应预案文档，查看其内容是否覆盖启动计划的条件、应急处理流程、系统恢复流程和事后教育等内容。		
		b) 应对系统相关的人员进行应急预案培训，对应急预案的培训应至少每年举办一次。	访谈系统运维负责人，询问是否制定不同事件的应急预案，是否对系统相关人员进行应急预案培训，培训内容是什么，多长时间举办一次；检查应急预案培训记录、演练记录和审查记录。		
		c) 金融机构应急领导小组应严格按照行业、机构的相关规定和要求对外发布信息，机构内其它部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。(F2)	访谈是否由金融行业负责统一向社会发布应急事件公告，其他任何单位或个人不得向社会发布应急事件公告。		
		d) 突发事件应急处置领导小组统一领导计算机系统的应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业信息安全监管部门。(F2)	检查各单位突发事件应急处置领导小组是否统一领导计算机系统的应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源。		
		e) 应定期对原有的应急预案重新评估，并根据安全评估结果，定期修订、演练，并进行专项内部审计。(F2)	检查金融机构是否对应急预案进行定期重新评估、修订和演练，是否有修订和演练记录，是否有评估报告。		

A.2 第三级信息系统等保检查表

A.2.1 技术类检查表

A.2.1.1 物理安全检查表

序号	类 别	测评要求	测评方法	结果记录	符合情况
1	物 理 位 置	a)机房和办公场地应选择在具有防震、防雷击、**承重**、防风和防	检查机房和办公场地的设计/验收文档，检查机房和办公场地所在的		

序号	类 别	测评要求	测评方法	结果记录	符合情况
	的 选 择	雨等能力的建筑内，**应选择交通、通信便捷地区。**	建筑物，查看其是否具有防震(震级需根据机房所在地区的地质环境确定)、防风和防雨等能力的基本条件。		
		b)机房场地应避免设在建筑物的顶层或地下室，以及用水设备的下层或隔壁。	检查机房场地是否避免在建筑物的高层或地下室，以及用水设备的下层或隔壁。		
		c)机房应避开火灾危险程度高的区域，周围 100 米内不得有加油站、煤气站等危险建筑和重要军事目标。(F3)	检查机房是否避开火灾危险程度高的区域，周围一定距离是否有加油站、煤气站等危险建筑。		
2	物 理 访 问 控制	a)机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。	访谈物理安全负责人，了解具有哪些控制机房进出的机制，检查是否具有对进入机房人员的身份鉴别措施。		
		b)需进入机房的来访人员应经过申请和审批流程，**由金融机构专人陪同**，并限制和监控其活动范围,**对于重要区域还应限制来访人员携带的随身物品。**	检查机房安全管理制度，查看其是否具有关于外来人员出入机房方面的规定， 是否具有来访人员进入机房的审批记录。		
		c）应对机房划分区域进行管理，如将机房划分为核心区、生产区、辅助区，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域，**其中核心区是指装有关键业务系统服务器、主要通信设备、网络控制器、通讯保密设备和（或）系统打印设备的要害区域，生产区是指放置一般业务系统服务器、客户端（工作站）等设备的运行区域，辅助区是指放置供电、消防、空调等设备的区域。**	访谈物理安全负责人，是否对机房进行了划分区域管理，是否对各个区域都有专门的管理要求；检查机房区域划分是否合理。		
		d）重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。	检查是否具有电子门禁系统，是否正常工作（不考虑断电后的工作情况），是否能够鉴别和记录进入人员身份。		
3	防 盗 窃 和 防 破 坏	a)应将主要设备放置在机房内。	检查主要设备是否都放置在机房内。		
		b)应将设备或主要部件放入机柜中进行固定放置，并设置明显的标签，标注不易除去的标记。	检查设备或设备主要部件的固定情况，是否不易被移动或被搬走，是否设置明显的不易除去的标记。		

序号	类 别	测评要求	测评方法	结果记录	符合情况
		c)应将通信线缆铺设在隐蔽处，可架空铺设在地板下或置于管道中，**强弱电需隔离铺设并进行统一标识。**	检查通信线缆铺设是否在隐蔽处（如铺设在地下或管道中等）。		
		d)应对磁带、光盘等介质分类标识，存储在介质库或档案室的金属防火柜中。	检查磁带、光盘等介质是否有分类标识，并检查是否存储在介质库或档案室的金属防火柜中。		
		e)应建立机房设施与场地环境监控系统，进行24小时连续监视，并对监视录像进行记录，监控对象包括机房空调、消防、不间断电源（UPS）、门禁系统等重要设施，监控记录至少保存3个月。(F3)	检查是否有机房设施与场地环境监控系统，是否能够进行 24 小时连续监视，并能够对监视录像进行记录，监控对象是否包括机房空调、消防、不间断电源（UPS）、供配电、门禁系统等重要设施。		
		f)机房主要设备工作间安装红外线探测设备等光电防盗设备，一旦发现有破坏性入侵即时显示入侵部位，并驱动声光报警装置。(F3)	检查机房主要设备工作间是否安装红外线探测设备等光电防盗设备，发现有破坏性入侵是否能够即时显示入侵部位，并驱动声光报警装置。		
4	防 雷 击	a)机房建筑应设置避雷针等避雷装置。	访谈物理安全负责人，询问采取了哪些防雷措施，机房建筑是否设置了避雷装置，是否通过验收或国家有关部门的技术检测。		
		b)应设置**通过国家认证的**防雷保安器，防止感应雷。	检查是否在电源和信号线上增加有资质的防雷保安器，以避免感应雷击。		
		c)机房应设置交流电源地线。	访谈物理安全负责人，询问机房计算机系统接地是否设置了交流电源地线；检查机房设计/验收文档，是否与实际情况一致。		
5	防火	a)机房应设置有效的自动灭火系统，**能够通过在机房内、基本工作房间内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位应设置烟感、温感等多种方式自动检测火情、自动报警。**	访谈物理安全负责人，询问机房采取了哪些防火措施；检查灭火设备摆放位置是否合理，有效期是否合格。检查机房内、基本工作房间内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位是否设置烟感探测器、温感探测器。		
		b)机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。	检查机房设计/验收文档，查看是否说明机房及相关的工作房间和辅助房间的建筑材料具有相应的耐火等级。		
		c)机房应采取区域隔离防火措	检查机房是否采取区域隔离防火措		

序号	类 别	测评要求	测评方法	结果记录	符合情况
		施，将重要设备与其他设备隔离开。	施，将重要设备与其他设备隔离开。		
		d)机房应设置自动消防报警系统，并备有一定数量的对计算机设备影响小的气体灭火器。消防报警系统应具有与空调系统、新风系统、门禁系统联动的功能，一般工作状态为手动触发。(F3)	检查机房是否设置自动消防报警系统，是否备有一定数量的对计算机设备影响小的气体灭火器。消防报警系统是否有与空调系统、新风系统、门禁系统、UPS 联动的功能，工作状态是否为手动触发。		
		e)机房内所使用的设备线缆应符合消防要求，纸张，磁带和胶卷等易燃物品，要放置于金属制的防火柜内。(F3)	检查机房内所使用的纸张，磁带和胶卷等易燃物品，是否放置于金属制的防火柜内，设备线缆是否符合消防要求。		
		f)采用管网式洁净气体灭火系统或高压细水雾灭火系统的主机房，应同时设置两种火灾探测器，且火灾报警系统应与灭火系统联动；凡设置洁净气体灭火系统的主机房，应配置专用空气呼吸器或氧气呼吸器。(F3)	检查采用管网式洁净气体灭火系统或高压细水雾灭火系统的主机房，是否同时设置两种火灾探测器，且火灾报警系统应与灭火系统联动；凡设置洁净气体灭火系统的主机房，是否配置专用空气呼吸器或氧气呼吸器。		
		g)应定期检查消防设施，每半年至少组织一次消防演练。(F3)	检查是否定期检查消防设施，是否每半年至少组织一次消防演练。		
		h)机房应设置二个以上消防逃生通道，同时应保证机房内各分区到各消防通道的道路通畅，方便人员逃生时使用。在机房通道上应设置显著的消防标志。(F3)	检查机房是否设置二个以上消防逃生通道，机房内各分区到各消防通道的道路是否通畅，是否方便人员逃生时使用，在机房通道上是否设置显著的消防标志 。		
6	防水和防潮	a）**水管不宜穿过机房屋顶，但若有穿过地板应当采取保护防范措施。**	访谈物理安全负责人，询问机房内是否具有上下水管安装，如果有水管安装是否避免穿过屋顶，如果穿过活动地板是否采取保护防范措施。		
		b)应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。	检查机房是否具有对外开放的窗户，如果有窗户是否采取必要的防雨措施；在屋顶和墙壁等是否不存在漏水、渗透和返潮现象，机房及其环境是否不存在明显的漏水和返潮的威胁。		
		c）为便于地下积水的转移，漏水隐患区域地面周围应设排水沟和地漏，当采用吊顶上布置空调风口时，风口位置不宜设置在设备正上方防止水蒸气结露和渗透。	检查机房是否具有除湿装置并能够正常运行，是否具有防止出现机房地下积水的转移与渗透的措施，是否与机房湿度记录情况一致。		

序号	类 别	测评要求	测评方法	结果记录	符合情况
		d)应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。	检查是否设置水敏感的检测仪表或元件，对机房进行防水检测和报警，查看该仪表或元件是否正常运行。		
7	防静电	a)主要设备应采用必要的接地防静电措施。	访谈物理安全负责人，询问机房是否存在静电问题或因静电引起的故障事件，采取了哪些有效防静电措施，主要设备是否采用必要的接地防静电措施；检查机房设计/验收文档，描述内容与实际情况是否一致。		
		b）机房应采用防静电地板。	检查机房是否不存在明显的静电现象；是否铺设了防静电地板。		
		c)主机房和辅助区内的工作台面宜采用导静电或静电耗散材料。(F3)	检查主机房和辅助区内的工作台面是否采用导静电或静电耗散材料。		
8	温湿度控制	**a）设备开机时主机房的温、湿度应执行 A 级，基本工作间可根据设备要求按 A，B 两级执行，其他辅助房间应按设备要求确定。**	检查设备开机时主机房的温、湿度是否执行 A 级； 检查基本工作间主机房是否根据设备要求按 A，B 两级执行，其他辅助房间是否按照设备要求确定温度。 A 级：夏天温度 23±1℃、冬天温度 20 ± 2 ℃ ； 夏 冬 开 机 相 对 湿 度 40%~55%；夏冬温湿度变化率< 5℃/h 并不得结露； B 级：全年温度 18~28℃、全年开机相对湿度 35%~75%、全年温度变化率< 10℃/h 并不得结露。		
		b）机房应采用专用空调设备，空调机应带有通信接口，通信协议应满足机房监控系统的要求。(F3)	检查机房是否采用专用空调设备，空调机是否带有通信接口，通信协议是否满足机房监控系统的要求，显示屏是否有汉字显示。		
		c） 空调系统的主要设备应有备份，空调设备在容量上应有一定的余量。(F3)	空调系统的主要设备是否有备份，空调设备在容量上是否有一定的余量。		
		d)安装在活动地板上及吊顶上的送风口、回风口应采用难燃材料或非燃材料。(F3)	检查安装在活动地板上及吊顶上的送风口、回风口是否采用难燃材料或非燃材料。		
		e）采用空调设备时，应设置漏水报警装置，并设置防水小堤，还应注意冷却塔、泵、水箱等供水设备的防冻、防火措施。(F3)	检查采用空调设备时，是否设置漏水报警装置，是否设置防水小堤，查看了解冷却塔、泵、水箱等供水设备的防冻、防火措施。		
9	电 力供应	a)应在机房供电线路上配置稳压器和过电压防护设备。	访谈物理安全负责人，询问是否出现过电压不稳现象，计算机系统供		

序号	类 别	测评要求	测评方法	结果记录	符合情况
			电线路上是否设置了稳压器和过电压防护设备；检查机房，查看计算机系统供电线路上的稳压器、过电压防护设备是否正常运行，查看供电电压是否正常。		
		b)应按照双路供电的原则设置冗余或并行的电力电缆线路为计算机系统供电。	访谈物理安全负责人,询问是否安装了冗余或并行的电力电缆线路（如双路供电方式），如何进行双路供电切换，切换时是否能够对计算机系统正常供电。		
		c)应建立发电机等备用供电系统（如备用发电机），以备供电系统临时停电时启用，并确保备用供电系统能在UPS供电时间内到位，每年需进行备用供电系统的模拟演练，并定期对备用电力供应设备进行检修和维护，确保其能正常使用。	访谈物理安全负责人,是否建立备用供电系统（如备用发电机）。		
		d)UPS供电系统的冗余方式应采用N+1、N+2、2N、2(N+1) 等方式。没有建立柴油发电机应急供电系统的单位，UPS后备时间至少2小时。(F3)	1.检查 UPS 供电系统是否为采用 N+1、N+2、2N、2(N+1) 等方式，并检查是否通过两路独立市电提供 UPS 输入。 2.对于没有建立柴油发电机应急供电系统的单位，UPS 后备时间至少 2 小时。		
		e)机房内要求采用机房专用插座，机房内分别设置维修和测试用电源插座，两者应有明显区别标志。市电、UPS电源插座分开，满足负荷使用要求。(F3)	检查机房内是否采用机房专用插座，机房内是否设置维修和测试用电源插座，两者是否有明显区别标志。市电、UPS 电源插座是否分开，是否满足负荷使用要求。		
		f)计算机系统应选用铜芯电缆，避免铜、铝混用。若不能避免时，应采用铜铝过渡头连接。(F3)	计算机系统是否选用铜芯电缆，避免铜、铝混用。若不能避免时，是否采用铜铝过渡头连接。		
		g)机房应设置应急照明和安全出口指示灯，供配电柜（箱）和分电盘内各种开关、手柄、按钮应标志清晰，防止误操作。(F3)	检查机房是否设置应急照明和安全出口指示灯，供配电柜（箱）和分电盘内各种开关、手柄、按钮是否标志清晰，是否可以防止误操作。		
10	电 磁防护	a)应采用接地方式防止外界电磁干扰和设备寄生耦合干扰。	访谈物理安全负责人，询问是否具有防止外界电磁干扰和设备寄生耦合干扰的措施，是否出现过因电磁防护问题引发的安全事件，检查机房设备外壳是否具有安全接地。		

序号	类 别	测评要求	测评方法	结果记录	符合情况
		b）电源线和通信线缆应隔离，避免互相干扰。	检查机房布线，查看是否做到电源线和通信线缆隔离。		
		c）应对关键设备和磁介质实施电磁屏蔽。	访谈物理安全负责人，询问是否具有处理或者存储秘密级信息的设备或介质，设备是否为低辐射设备，设备与磁介质是否采取了必要的电磁屏蔽措施。检查关键设备与磁介质是否存放在具有电磁屏蔽功能的容器中。		
		d)计算机系统设备网络布线不得与空调设备、电源设备的无电磁屏蔽的布线平行；交叉时，应尽量以接近于垂直的角度交叉，并采取防延燃措施。(F3)	计算机系统设备网络布线是否与空调设备、电源设备的无电磁屏蔽的布线平行；交叉时，是否尽量以接近于垂直的角度交叉，是否采取防延燃措施。		

A.2.1.2 网络安全检查表

序号	类别	测评内容	测评方法	结果记录	符合情况
1	结构安全	a)应保证主要网络设备和通信线路冗余，主要网络设备业务处理能力能满足业务高峰期**需要的1倍以上，双线路设计时，宜由不同的服务商提供。**	访谈网络管理员，询问信息系统边界设备和主要网络设备的处理性能能否满足目前业务高峰流量情况，询问采用何种手段对主要网络设备进行运行状况监控。		
		b)应保证网络各个部分的带宽满足业务高峰期需要。	访谈网络管理员，询问网络各个部分的带宽是否满足业务高峰的需要，如果无法满足，则需要在主要网络设备上进行带宽配置，若有网管系统或流量监控系统，查看网络和核心网络的带宽占用报表是否有达到或超过处理能力记录。		
		c)应在业务终端与业务服务器之间进行路由控制建立安全的访问路径。	业务终端 trace 业务服务器地址，查看访问路径所经节点是否安全可靠。		
		d)应绘制与当前运行情况相符的网络拓扑结构图。	查看网络拓扑结构图与当前运行情况是否一致。		
		e)应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段，**生产网、互联网、办公网之间都应实现有效隔离。**	1、查网络设计/验收文档，查看是否有根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段；2、登录核心交换机，show vlan brief 查看 vlan 划分、show int vlan X 详细查看某个具体 vlan 情况。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		f)应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段。	检查是否将重要网段部署至网络边界与外部信息系统直连，重要网段与其他网段间是否使用防火墙、访问控制等手段隔离。		
		g)应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。	1、登录下联路由器，show run，查看是否有 qos 策略并应用到相应端口； 2、登录交换机，show run，查看是否有 acl 对流量分类、是否对分类流量打标、是否应用到相应端口。		
2	访问控制	a)应在网络边界部署访问控制设备，启用访问控制功能。	登录网络设备，show run，查看是否有相应访问控制列表。		
		b)应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。	登录网络设备，show run，查看方位控制列表是否精确至端口。		
		c)应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制。	登录边界网络设备（业务网纵向防火墙和金融城市网防火墙），查看是否对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制。		
		d)应在会话处于非活跃一定时间或会话结束后终止网络连接。	登录网络设备，show run，查看 vty 下是否有 exec-timeout X X，X 不可为均为 0。		
		e)应在网络区域边界(互联网区域边界、外部区域边界和内部区域边界)对网络最大流量数及网络并发连接数进行监控。	查看是否有端口带宽限制，防火墙是否监控网络并发连接数和流量。。		
		f)重要网段应采取技术手段防止地址欺骗。	1、查看客户端是否对重要网段、主机进行 arp 绑定，2、登录交换机，show run，查看是否对重要网段、主机采取静态 arp 绑定、端口与 mac 绑定措施，3、是否采取防火墙与代理服务等其他方式防止 arp 欺骗。		
		g)应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。	登录网络设备，show run，查看方位控制列表是否精确至 host。		
		h)应对拨号接入用户采用数字证书认证机制，并限制具有拨号访问权限的用户数量。	登录网络设备，show run	b vty，查看 vty 用户数量是否限制。		
		i)网络设备应按最小安全访问原	访谈网络管理员，询问网络设备的		

序号	类别	测评内容	测评方法	结果记录	符合情况
		则设置访问控制权限。(F3)	配置原则如何设置，是否是最小原则。		
3	安全审计	a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。	登录网络设备，1、show snmp 查看是否配置 snmp 进行网络设备运行状况记录 、show logging 、2、show ip netflow export 查看是否配置网络流量记录；3、show aaa meth accounting 查看是否配置用户行为记录。		
		b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	查看是否有相关的审计信息，是否包括事件的日期和时间、用户、事件类型、事件是否成功。		
		c)应能够根据记录数据进行分析，并生成审计报表。	询问日志服务器或 AAA 服务器是够具备生成报表功能，若有登录并现场生成。		
		d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等，**保存时间不少于半年。**	登录日志服务器为或 AAA 服务器，查看记录是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息，保存时间不少于半年。		
4	边界完整性检查	a)应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。	登录业务网非法外联监控管理服务器，查看是否有未安装非法外联客户端的计算机接入网络，若有是否采取进行定位、阻断。		
		b)应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。	登录业务网非法外联监控管理服务器，查看客户端覆盖情况、与上下级服务器连接是否正常、策略是否及时更新。		
5	入侵防范	a)应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、注入式攻击、IP 碎片攻击和网络蠕虫攻击等；	查看其是否有在网络边界及核心业务网段处有对网络攻击采取相关措施。		
		b)当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。	1)查看对网络攻击事件是否采用报警。 2)采用何种报警方式。		
6	恶意代码防	a)应在**与外单位和互联网连接的**网络边界处对恶意代码进行检测和清除。	登录边界网络设备，查看是否根据恶意代码特征采取措施从网络层进行检测和清除。		

序号	类别	测评内容	测评方法	结果记录	符合情况
	范	b) 应定期对恶意代码防护设备进行代码库升级和系统更新。	登录防病毒服务器，查看病毒库升级情况、客户端病毒定义码升级情况。		
7	网络设备防护	a)应对登录网络设备的用户进行身份鉴别。	是否对网络设备进行 AAA 认证或其他认证方式,若有登录 AAA 服务器，查看用户与管理员身份、权限是否匹配。		
		b)应对网络设备的管理员登录地址进行限制。	登录网络设备，show run，查看是否在网络设备上是否采用相应 acl 限制管理员登录；2、登录 AAA 服务器，查看是否进行管理员地址限制。		
		c)网络设备用户的标识应唯一。	访谈网络设备管理员，询问其各个网络设备用户的标识信息。		
		d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。	查看登录网络设备的认证方式的种类，一般有用户名和密码组合认证、动态口令、指纹识别认证、数字证书认证等，要求两种或两种以上。		
		e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换。	应访谈网络管理员，询问网络设备的口令策略是什么。		
		f)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。	采用错误密码登录网络设备数次，观察是否结束会话、限制非法登录次数，并观察如果登录后长时间不操作会不会被系统退出。		
		g)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	远程登录网络设备，看是否采用 22 端口 SSH 方式或其他加密方式。		
		h)应实现设备特权用户的权限分离。	登录网络设备，show run｜b user，查看定义只有查看权限 level 3 的审计用户和具有管理权限的 level 15 用户。		
		i)应定期对网络设备的配置文件进行备份，发生变动时应及时备份。(F3)	查阅文件、上机查阅备份文件。		
		j)应定期对网络设备运行状况进行检查。(F3)	检查是否每天对运行状况进行检查。		
		k) 对网络设备系统自带的的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端口开放审批制度。(F3)	检查网络设备是否关闭不必要的网络设备服务端口，并查看审批制度文件。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		l)应定期检验网络设备软件版本信息，避免使用软件版本中出现安全隐患。(F3)	检查网络设备是否定期检验网络设备软件版本信息。		
		m)应建立网络设备的时钟同步机制。(F3)	访谈网络管理员，询问是否建立了网络设备的时钟同步机制。		
		n)应定期检查并锁定或撤销网络设备中不必要的用户账号。(F3)	1、登录网络设备，show run | b user，查看设立账户是否与管理员一一对应，2、若有网络日志服务器或AAA服务器，查看管理员变动相应时段是否有相关操作记录。		

A.2.1.3 主机安全检查表

序号	类别	测评项	测评方法	结果记录	符合情况
1	身份鉴别	a) 应为操作系统和数据库的不同用户分配不同的用户名,确保用户名具有唯一性。	应测评主要服务器操作系统和主要数据库管理系统，添加一个新用户，其用户标识为系统原用户的标识（如用户名或UID），查看是否不会成功。		
		b) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别。	可访谈系统管理员/数据库管理员，询问操作系统的身份标识与鉴别机制采取何种措施实现，目前系统提供了哪些身份鉴别措施和鉴别失败处理措施.		
		c) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点,**系统的静态口令应在7位以上并由字母、数字、符号等混合组成并每三个月更换口令。**	应检查主要服务器操作系统和主要数据库管理系统，查看是否提供了身份鉴别措施（如用户名和口令等），其身份鉴别信息是否具有不易被冒用的特点，例如，口令足够长，口令复杂（如规定字符应混有大、小写字母、数字和特殊字符），口令生命周期，新旧口令的替换要求(如规定替换的字符数量）或为了便于记忆使用了令牌。		
		d) 应启用登录失败处理功能，可采取结束会话、限制登录间隔、限制非法登录次数和自动退出等措施。	应检查主要服务器操作系统和主要数据库管理系统，查看是否已配置了鉴别失败处理功能，并设置了非法登录次数的限制值，对超过限制值的登录终止其鉴别会话或临时封闭帐号；查看是否设置网络登录连接超时，并自动退出；查看是否设置鉴别警示信息。		

序号	类别	测评项	测评方法	结果记录	符合情况
		e）主机系统应对与之相连的服务器或终端设备进行身份标识和鉴别，当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。（F3）	应检查主要服务器操作系统，查看服务器操作系统是否对与之相连的服务器或终端设备进行身份标识和鉴别并进行了相应的加密。		
		f）宜采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别，**例如以密钥证书、动态口令卡、生物特征等作为身份鉴别信息。**	应检查主要服务器操作系统和主要数据库管理系统，查看身份鉴别是否采用两个及两个以上身份鉴别技术的组合来进行身份鉴别（如采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技术和数字证书方式的身份鉴别技术中的任意两个组合）。		
2	访问控制	a）应启用访问控制功能，依据安全策略控制用户对资源的访问。	应检查服务器操作系统和数据库管理系统的安全策略，查看是否明确主体（如用户）以用户和/或用户组的身份规定对客体（如文件或系统设备，目录表和存取控制表访问控制等）的访问控制，覆盖范围是否包括与信息安全直接相关的主体（如用户）和客体（如文件，数据库表等）及它们之间的操作（如读、写或执行）。		
		b） 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。	应检查主要服务器操作系统和主要数据库管理系统，查看特权用户的权限是否进行分离，如可分为系统管理员、安全管理员、安全审计员等；查看是否采用最小授权原则（如系统管理员只能对系统进行维护，安全管理员只能进行策略配置和安全设置，安全审计员只能维护审计信息等）。		
		c）应实现操作系统和数据库系统特权用户的权限分离。	应检查主要服务器操作系统和主要数据库管理系统，查看在系统管理员、安全管理员、安全审计员之间是否设置了相互制约关系（如系统管理员、安全管理员等不能对审计日志，安全审计员管理不了审计数据的开启、关闭、删除等重要事件的审计日志等）。		
		d） 应禁用或严格限制默认帐户的访问权限，重命名系统默认帐	应查看主要服务器操作系统和主要数据库管理系统，查看匿名/默认用		

序号	类别	测评项	测评方法	结果记录	符合情况
		户，修改这些帐户的默认口令。	户的访问权限是否已被禁用或者严格限制（如限定在有限的范围内）。		
		e）应及时删除多余的、过期的账户，避免共享账户的存在。	应查看是否有多余、过期、共享账户的存在。		
		f）应对重要信息资源设置敏感标记。	应检查服务器操作系统和数据库管理系统的安全策略，查看是否明确主体（如用户）具有非敏感标记（如角色），并能依据非敏感标记规定对客体的访问。		
		g）应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	应检查主要服务器操作系统和主要数据库管理系统，查看是否能对重要信息资源和访问重要信息资源的所有主体设置敏感标记，这些敏感标记是否构成多级安全模型的属性库，主体和客体的敏感标记是否以默认方式生成或由安全员建立、维护和管理。		
3	安全审计	a)审计应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。	可访谈安全审计员，询问主机系统是否设置安全审计；询问主机系统对事件进行审计的选择要求和策略是什么；对审计日志的处理方式有哪些。		
		b）审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用、**账号的分配、创建与变更、审计策略的调整、审计系统功能的关闭与启动**等系统内重要的安全相关事件。	应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、系统资源的异常使用、重要系统命令的使用（如删除客体）等。		
		c）审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等，**并定期备份审计记录，涉及敏感数据的记录保存时间不少于半年。**	应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容。		
		d)应能够根据记录数据进行分析，	应检查主要服务器和重要终端操作		

序号	类别	测评项	测评方法	结果记录	符合情况
		并生成审计报表；	系统，查看是否为授权用户浏览和分析审计数据提供专门的审计工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表。		
		e）应保护审计进程，避免受到未预期的中断。	应测评主要应用系统，可通过非法终止审计功能或修改其配置，验证审计功能是否受到保护。		
		f）应保护审计记录，避免受到未预期的删除、修改或覆盖等。	应测评主要服务器操作系统、重要终端操作系统和主要数据库管理系统，在系统上以某个系统用户试图删除、修改或覆盖审计记录，测评安全审计的保护情况与要求是否一致。		
4	剩余信息保护	a）应保证操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他使用人员前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。	应与系统管理员/数据库管理员访谈，询问操作系统用户/数据库管理员用户的鉴别信息存储空间，被释放或再分配给其他用户前是否得到完全清除；系统内的文件、目录等资源所在的存储空间，被释放或重新分配给其他用户前是否得到完全清除。		
		b）应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他使用人员前得到完全清除。	应检查主要操作系统和主要数据库管理系统维护操作手册，查看是否明确用户的鉴别信息存储空间，被释放或再分配给其他用户前的处理方法和过程；文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前的处理方法和过程。		
5	入侵防范	a）应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。	应与系统管理员访谈，询问主机系统是否采取入侵防范措施，入侵防范内容是否包括主机运行监视、资源使用超过值报警、特定进程监控、入侵行为检测、完整性检测等方面内容。		

序号	类别	测评项	测评方法	结果记录	符合情况
		b）应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施或**在检测到完整性即将受到破坏时进行事前阻断。**	应测评主要服务器系统，试图破坏重要程序（如执行系统任务的重要程序）的完整性，验证主机能否检测到重要程序的完整性受到破坏。		
		c）操作系统遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器、系统软件预防性维护服务等方式保持系统补丁及时得到更新。	应与系统管理员访谈，询问入侵防范产品的厂家、版本和在主机系统中的安装部署情况；询问是否进行过部署的改进或者更换过产品，是否按要求（如定期或实时）进行产品升级。		
6	恶意代码防范	**a）应安装国家安全部门认证的正版防恶意代码软件，对于依附于病毒库进行恶意代码查杀的软件应及时更新防恶意代码软件版本和恶意代码库，对于非依赖于病毒库进行恶意代码防御的软件，如主动防御类软件，应保证软件所采用的特征库有效性与实时性，对于某些不能安装相应软件的系统可以采取其他安全防护措施来保证系统不被恶意代码攻击。**	应访谈系统安全员，询问主机系统是否采取恶意代码实时检测与查杀措施或其他安全防护措施，恶意代码实时检测与查杀措施的部署情况如何，因何改进过部署或者更换过产品，是否按要求（如定期或实时）进行产品升级，其他安全防护措施是如何防范恶意代码攻击的。		
		b)主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库。	检查主机和网络是否具备恶意代码产品，以及其各自的恶意代码库是否一样，是否是最新代码库。		
		c）应支持恶意代码防范的统一管理。	应检查网络防恶意代码产品，查看厂家、版本号和恶意代码库名称等信息是否统一管理。		
		d)应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。(F3)	检查如何对网络内计算机病毒进行监控，是否建立了病毒监控中心。		
7	资源控制	a）应通过设定终端接入方式、网络地址范围等条件限制终端登录。	应检查主要服务器操作系统，查看是否限制单个用户的多重并发会话数量；查看是否设置登录终端的操作超时锁定和鉴别失败锁定，以及是否规定解锁或终止方式；查看是否配置了终端接入方式、网络地址范围等条件限制终端登录。		

序号	类别	测评项	测评方法	结果记录	符合情况
		b）应根据安全策略设置登录终端的操作超时锁定。	应测评主要服务器操作系统，任选一个用户，登录服务器，在一定时间内不进行任何动作，验证主要服务器操作系统能否对操作超时的终端进行锁定；任选一个用户，可通过多次失败登录服务器，验证服务器能否对鉴别失败的终端进行锁定，锁定后能否按照规定的解锁或终止方式进行解锁或终止。		
		c）应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况。	应检查主要服务器操作系统，查看是否对一个时间段内可能的并发会话连接数进行限制，是否禁止同一用户账号在同一时间内并发登录，是否限制单个用户对系统资源（如CPU、内存和硬盘等）的最大或最小使用限度。		
		d）应限制单个用户对系统资源的最大或最小使用限度。	应检查主要服务器操作系统，查看是否在服务水平降低到预先规定的最小值时，能检测和报警，报警的方式有哪些，能否已根据安全策略设定主体（如进程）的服务优先级，并根据优先级分配系统资源，保证优先级低的主体处理能力不会影响到优先级高的主体的处理能力。		
		e）应定期对系统的性能和容量进行规划，能够对系统的服务水平降低到预先规定的最小值进行检测和报警。	应测评主要服务器操作系统，试图使服务水平降低到预先规定的最小值，验证系统能否正确检测和报警。		
		f)所有的服务器应全部专用化，不使用服务器进行收取邮件、浏览互联网操作。(F3)	检查所有服务器是否是全部专用化，是否使用服务器进行收取邮件、浏览互联网操作。		

A.2.1.4 应用安全检查表

序号	类别	测评项	测评方法	结果记录	符合情况
1	身份鉴别	a)应提供专用的登录控制模块对登录用户进行身份标识和鉴别。	1） 询问系统管理员，该系统是否提供专用的登录控制模块对登录的用户进行身份标识和鉴别，采用何种方式对用户进行身份标识和鉴别？ 2） 检查应用系统，身份标识和鉴		

序号	类别	测评项	测评方法	结果记录	符合情况
			别的方式是否与管理员回答的一致。 3) 以某注册用户身份登录系统，查看登录是否成功；以非法用户身份登录系统，查看登录是否成功。		
		b)应对同一用户的关键操作采用两种或两种以上组合的鉴别技术实现用户身份鉴别；**如使用磁卡、IC 卡、动态密码卡、动态口令设备、手机短信动态密码、指纹识别等方式加强鉴别。**	1）询问系统管理员，该系统是否采用了两个及两个以上身份鉴别技术的组合来进行身份鉴别。 2）如果是，查看身份鉴别技术是什么？是否与回答一致。		
		c)应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。	1) 询问系统管理员，该系统的用户身份标识是否唯一。采取了什么措施防止身份鉴别信息被冒用。 2) 检查总体规划/设计文档，查看其是否有系统采取了唯一标识的说明。查看其身份鉴别信息是否具有不易被冒用的特点。 3) 询问系统管理员，该系统是否有专门的设置保证用户身份鉴别信息不易被冒用，如果应用系统采用口令进行身份鉴别，则查看是否有选项或设置强制要求口令长度、复杂度、定期修改等。 4) 如果应用系统式以用户名来保证用户身份标识的唯一性，则以已有的用户名重新注册，测试系统是否禁止该操作。 5) 扫描应用系统，测试其鉴别信息复杂度检查功能，检查系统是否不允许存在弱口令、空口令等。		
		d)应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。	1) 询问系统管理员，该系统是否具有登录失败处理的功能（如结束会话、限制非法登录次数，当登录连接超时，自动退出等），是如何进行处理的? 2) 如果有登录失败处理设置选项或模块，查看系统是否设置或选中了该功能。 3) 根据应用系统使用的登录失败处理方式，采用如下方法之一或全部进行测试：		

序号	类别	测评项	测评方法	结果记录	符合情况
			i. 以错误的用户名或密码登录系统，查看系统反应。 ii. 以超过系统规定的非法登录次数登录系统，查看系统反应。 iii. 登录系统连接超时，查看系统反应。		
		e)应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。	1) 询问系统管理员，该系统的身份鉴别、身份标识唯一性检查、鉴别信息复杂度检查以及登录失败处理功能是否有专门的模块或选项，是否有相关参数需要配置。 2) 如果有参数需要配置，则查看实际配置情况，是否已经启用上述功能。		
		f)应用软件应能在指定的闲置时间间隔到期后，自动锁定客户端的使用。(F3)	检测应用软件客户端在指定闲置时间到期后是否自动锁定。		
		g)对于系统自动分配或者预设的强度较弱的初始密码，系统应强制用户首次登录时修改初始密码。(F3)	应测评系统初始密码是否在首次登录时被要求强制修改。		
		h) 修改密码时，不允许新设定的密码与旧密码相同。(F3)	应测评修改密码是否不能修改成上次相同的密码。		
2	访问控制	a)应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问。	1) 询问系统管理员，该系统是否提供访问控制功能，访问控制策略是什么？访问控制的粒度是否达到文件、数据库表？ 2) 检查应用系统的访问控制功能和策略配置是否与管理员回答的一致。 3) 以某一用户身份登录系统，依据安全策略对客体进行访问，测试是否成功。该用户不依据安全策略对客体进行访问，测试是否成功。		

序号	类别	测评项	测评方法	结果记录	符合情况
		b)访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作。	1) 访谈系统管理员，询问系统访问控制策略是否覆盖到与信息安全直接相关的主体、客体及它们之间的操作？ 2) 检查应用系统的访问控制策略是否覆盖到与信息安全直接相关的所有主体、客体及它们之间的操作。		
		c)应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限。	1) 询问系统管理员，该系统是否有由授权主体配置访问控制策略的功能。 2) 如果系统有由授权主体配置访问控制策略的功能，则以该授权主体用户登录系统，查看某特定用户的权限。以该用户身份登录系统，进行在权限范围内和权限范围外的一些操作，查看是否成功。 3) 以该授权主体用户登录系统，修改上述特定用户的权限。以该用户身份登录系统，查看该用户的权限是否与刚修改过的权限保持一致，验证用户权限管理功能是否有效。 4) 询问系统管理员，该系统是否有默认用户，如果有，是否限制了默认用户的访问权限。 5) 如果有默认帐户，以默认帐户（默认密码）登录系统，并进行合法及非法操作，测试系统是否对默认帐户访问权限进行了限制。		
		d)应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。	1) 访谈系统管理员，询问系统所有帐户是否只拥有完成自己承担任务所需的最小权限，相互之间是否形成相互制约关系。 2) 检查应用系统，查看不同帐户的权限是否分离（如管理员不能审计、审计员不能管理、安全员不能审计和管理等、审计员不能修改自己的行为日志等）。权限之间是否相互制约。 3) 以管理员身份进行审计操作，查看是否成功。以审计员身份进行		

序号	类别	测评项	测评方法	结果记录	符合情况
			删除/增加用户、设定用户权限的操作（也可进行一些其他管理员进行的操作），查看是否成功。 4) 以拥有其他权限的用户身份登录，查看其权限是否受到限制。		
		e)应有生产系统关键账户与权限的关系表。(F3)	检查是否建立账户权限关系表，是否明确说明账户类别以及其具有的权限范围。		
		f)**宜**具有对重要信息资源设置敏感标记的功能。	检查目标系统，查看系统是否具有对重要信息资源设置敏感标记的功能？如果有，则验证该功能是否有效。		
		g)**宜**依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	检查目标系统，如果具有对重要信息资源设置敏感标记的功能，则查看系统是否依据安全策略控制用户对有敏感标记重要信息资源的操作。		
3	安全审计	a)应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计。	1) 访谈安全审计员，询问是否有安全审计功能，对事件进行审计的选择要求和策略是什么。 2) 检查应用系统的审计策略（审计记录），查看审计策略（或记录）是否覆盖到每个用户。都对哪些安全事件进行审计。 3) 多次以任意用户身份登录系统，进行一些操作，包括重要的安全相关操作或事件（如用户标识与鉴别、自主访问控制的所有操作记录（如用系统管理员身份改变用户权限，增加或删除用户），用户的行为（如删除数据、多次登录失败等））。 4) 用审计人员的身份登录系统，查看系统对上述用户的重要操作或事件是否进行审计。		

序号	类别	测评项	测评方法	结果记录	符合情况
		b)应保证无法单独中断审计进程，**不提供**删除、修改或覆盖审计记录**的功能**。	1) 访谈安全审计员，询问应用系统对审计日志的处理方式有哪些。 2) 以普通用户身份试图删除、修改或覆盖自身的审计记录，查看能否成功。试图删除、修改其他人的审计记录，查看能否成功。 3) 如果审计记录能够导入，则导出审计记录并进行修改后导入系统，查看能否覆盖以前的审计记录。		
		c)审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等，**并定期备份审计记录，保存时间不少于半年。**	以审计员身份登录系统，检查审计记录内容是否包括事件发生的日期、时间、发起者信息、事件类型、事件相关描述信息、事件的结果等。		
		d)应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。	1) 检查应用系统，查看其是否为授权用户浏览和分析审计数据提供专门的审计工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等）。 2) 检查应用系统是否能够生成审计报表。		
		e) 对于从互联网客户端登陆的应用系统，应在每次用户登录时提供用户上一次成功登录的日期、时间、方法、位置等信息，以便用户及时发现可能的问题。(F3)	检查客户端登录时是否可以提供户上一次成功登录的日期、时间、方法、位置、错误登录等信息。		
4	剩余信息保护	a)应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。	访谈系统管理员，询问系统是否采取措施保证对存储介质中的残余信息进行删除，采取什么具体措施。		
		b)应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。	如果鉴别信息存放在文件中，则用另一个用户登录查看能否读取用户信息。如果用户的鉴别信息存放在数据库中，则通过用户界面或其他方式能否获取系统鉴别信息。		

序号	类别	测评项	测评方法	结果记录	符合情况
5	通信完整性	a)应采用密码技术保证通信过程中**关键**数据的完整性。	1) 询问安全管理员应用系统是否有数据在传输过程中进行完整性保证的操作，具体采取什么措施。 2) 应检查设计/验收文档，查看其是否有通信完整性的说明，如果有则查看是否采用校验码技术保证通信完整性。		
6	通信保密性	a)在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证。	1) 询问安全管理员系统在通信双方建立连接之前采用什么技术进行会话初始化验证。 2) 应检查设计/验收文档，查看其是否有通信保密性的说明，如果有则查看是否有利用密码技术进行通信会话初始化验证的说明。		
		b)**对于通过互联网对外提供服务的系统，在**通信过程中的整个报文或会话过程，**应通过专用的通信协议或加密的方式保证通信过程的机密性**进行加密。	1) 询问安全管理员应用系统的敏感信息字段在通信过程中是否采取保密措施，具体采取什么措施。 2) 应检查设计/验收文档，查看其是否有通信保密性的说明，如果有则查看是否有对通信过程中的敏感信息字段进行加密的说明。		
7	抗抵赖	a)应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能，**原发证据包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录，交易系统还应能够详细记录用户合规交易数据，如业务流水号、账户名、IP 地址、交易指令等信息以供审计，并能够追溯到用户。**	1) 访谈安全员，询问系统是否具有抗抵赖的措施，具体措施有哪些。 2) 测试应用系统，通过双方进行通信，查看系统是否提供在请求的情况下为数据原发者提供数据原发证据的功能。		
		b)应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能，**接受证据应用系统操作与管理记录至少应包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录，交易系统还应能够详细记录用户合规交易数据，如业务流水号、账户名、IP 地址、交易指令等信息以供审计，并能够追溯**	1) 访谈安全员，询问系统是否具有抗抵赖的措施，具体措施有哪些。 2) 测试应用系统，通过双方进行通信，查看系统是否提供在请求的情况下为数据接收者提供数据原发证据的功能。		

序号	类别	测评项	测评方法	结果记录	符合情况
		到用户。			
8	软件容错	a)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。	1） 访谈管理员，询问是否有保证软件具有容错能力的措施，具体采取哪些措施。 2） 在应用终端输入不同（如数据格式或长度等符合、不符合软件设定的要求）的数据，包括登录标识与鉴别数据、其他操作数据等，查看系统的反应。		
		b)应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。	1） 询问管理员应用系统是否发生过故障，故障发生时是否能够继续提供一部分功能保证实施必要的措施。		
		c)应能够有效屏蔽系统技术错误信息，不将系统产生的错误信息直接反馈给客户。(F3)	检查是否能够有效屏蔽系统技术错误信息，不将系统产生的错误信息直接反馈给客户。		
9	资源控制	a） **对于有会话或短连接的应用系统**，当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话。	1） 询问业务系统是否有资源控制的措施，具体措施有哪些。 2） 登录应用系统服务器，查看应用系统属性是否设置了连接超时限制。		
		b)应能够对系统的最大并发会话连接数进行限制。	1） 询问管理员应用系统同时最多支持多少个并发会话连接？是否有限制？ 2） 登录应用系统服务器，查看系统是否设置了参数限制最大并发会话连接数。		
		c） **对于有会话的应用系统，**应能够对单个帐户的多重并发会话进行限制。	1） 询问管理员单个帐户同时可以发起多少个并发会话，是否有限制？ 2） 登录应用系统服务器，查看系统是否对单个帐户的多重并发会话进行限制。 3） 以超过单个帐户规定的并发会话连接数连接系统，测试能否成功。		
		d)应能够对一个时间段内可能的并发会话连接数进行限制。	1） 询问管理员是否对一个时间段内可能的会话连接数进行限制 2） 检查应用系统是否有对一段时间内可能的并发会话连接数进行限制。 3） 在一个时间段内以超过设定		

序号	类别	测评项	测评方法	结果记录	符合情况
			的并发会话连接数连接系统，测试能否连接成功。		
		e)宜能够对**系统占用的资源设定限额，超出限额时给出提示信息**；	a) 访谈管理员，询问应用系统是否对访问用户或请求进程占用的资源分配最大和最小限额。 b) 检查应用系统，是否对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额。		
		f)应能够对系统服务水平降低到预先规定的最小值进行检测和报警。	检查应用系统，查看是否有服务水平最小值的设定（当系统的服务水平降低到预先设定的最小值时，系统是否报警）。		
		g）应提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。	访谈管理员，询问应用系统是否能根据安全策略设定主体的服务优先级，根据优先级分配系统资源，保证优先级低的主体处理能力不会影响到优先级高的主体的处理能力。		

A.2.1.5 数据安全检查表

序号	类别	测评项	测评方法	结果记录	符合情况
1	数据完整性	a)应能够检测到系统管理数据、鉴别信息和重要业务数据在**采集、传输、使用和存储过程**中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。	1) 询问安全管理员应用系统的鉴别信息和重要业务数据在传输、存储过程中是否有完整性保证措施，具体措施有哪些。 2) 检查应用系统，查看其是否配备检测/验证鉴别信息和重要业务数据在传输、存储过程中完整性受到破坏的功能。		
2	数据保密性	a)应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据**采集、传输、使用和存储过程**的保密性。	1) 询问安全管理员应用系统的鉴别信息和重要业务数据是否采用加密或其他有效措施实现传输保密性。 2) 检查应用系统设计/验收文档，查看其是否有关于其鉴别信息、敏感的用户数据采用加密或其他有效措施实现传输、存储等密性的描述。 3) 检查应用系统，查看其鉴别信息和重要业务数据是否采用加密或其他有效措施实现传输、存储等保密性。		
3	备份	a) 应提供本地数据备份与恢复功	1) 询问安全管理员应用系统是		

序号	类别	测评项	测评方法	结果记录	符合情况
	和恢复	能，采取实时备份与异步备份或增量备份与完全备份的方式，增量数据备份每天一次，完全数据备份每周一次，备份介质场外存放，**数据保存期限依照国家相关规定。**	否具有对重要信息进行备份的功能，配置如何。是否提供对重要信息进行恢复的功能。 2) 检查应用系统设计/验收文档，查看其是否有描述应用系统提供用户备份和恢复重要信息的功能的描述。 3) 检查应用系统，查看其是否提供对重要信息进行备份和恢复的功能，其配置是否正确。		
		b)应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地。	1) 询问系统管理员是否有异地数据备份，备份方法和备份方式。 2) 检查异地备份的设备和线路。		
		c) 对于同城数据备份中心，应与生产中心直线距离至少达到 30 公里，可以接管所有核心业务的运行；对于异地数据备份中心，应与生产中心直线距离至少达到 100 公里。(F3)	访谈安全管理员关于灾备中心的建设情况，检查灾备中心是同城灾备，还是不同城市的异地灾备，是否可以接管所有核心业务的运行。		
		d)为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果。(F3)	询问系统管理员是否采用相关技术避免关键节点存在的单点故障。		
		e)数据备份存放方式应以多冗余方式，至少保证以一个星期为周期的数据冗余。	检查数据备份存放方式是否实现以一个星期为周期的数据冗余。		
		f)异地备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，"就绪状态"指备份中心的所需资源(相关软硬件以及数据等资源)已完全满足但设备 cpu 还没有运行；"运行状态"指备份中心除所需资源完全满足要求外，cpu 也在运行状态。(F3)	访谈安全管理员，询问异地备份中心是否配备恢复所需的全部运行环境，并处于就绪状态或运行状态。		

A.2.2 管理类检查表

A.2.2.1 安全管理制度

序号	类别	测评要求	测评方法	结果记录	符合情况

序号	类别	测评要求	测评方法	结果记录	符合情况
1	管理制度	a)应制定信息安全工作的总体方针和安全策略，说明安全工作的总体目标、范围、原则和安全框架等，**并编制形成信息安全方针制度文件。**	检查信息安全工作的总体方针和安全策略，查看文件是否明确机构安全工作的总体目标、范围、原则和安全框架等。		
		b)应对安全管理活动中各类管理内容建立安全管理制度。	检查是否依据各项管理内容建立各项安全管理制度。		
		c)应对科技管理人员或操作人员执行的日常管理操作建立操作规程。	检查是否具有对重要管理操作的操作规程，如系统维护手册和用户操作规程等。		
		d) 应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。	访谈安全主管，询问机构是否形成全面的信息安全管理制度体系，制度体系是否由安全政策、管理制度、操作规程等构成。		
2	制定和发布	**a）由金融机构总部科技部门负责制定适用全机构范围的安全管理制度，各分支机构的科技部门负责制定适用辖内的安全管理制度。(F3)**	访谈安全主管，询问由何部门或人员负责安全管理制度的制定，参与制定人员有哪些。		
		b）安全管理制度应具有统一的格式，并进行版本控制。	检查安全管理制度制定和发布要求管理文档，查看文档是否说明安全管理制度的格式要求、版本编号，并检查安全管理制度文档，查看是否具有版本标识，查看各项制度文档格式是否统一。		
		c）应组织相关人员对制定的安全管理进行论证和审定。	访谈安全主管，询问安全管理制度的制定程序，是否对制定的安全管理制度进行论证和审定；检查管理制度评审记录，查看是否具有相关人员的评审意见。		
		d）安全管理制度应通过正式、有效的方式发布。	检查安全管理制度制定和发布要求管理文档，查看文档是否说明安全管理制度的制定、发布程序和发布范围等各项要求。		

序号	类别	测评要求	测评方法	结果记录	符合情况
		e）安全管理制度应注明发布范围，并对收发文进行登记。	检查安全管理制度的收发登记记录，查看收发是否通过正式、有效的方式（如正式发文、领导签署和单位盖章等），是否注明管理制度的发布范围。		
3	评审和修订	a）信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定。	检查是否具有安全管理制度体系的评审记录，查看是否由信息安全领导小组负责，是否记录了相关人员的评审意见。		
		b）应该建立对门户网站内容发布的审核、管理和监控机制。（F3）	检查是否建立管理制度对门户网站内容发布的审核、管理和监控进行规定。		
		c）应定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。	检查是否具有定期对安全管理制度进行修订的记录；检查是否具有系统发生重大安全事故、出现新的安全漏洞以及技术基础结构发生变更时对安全管理制度进行修订的记录。		

A.2.2.2 安全管理机构

序号	类别	测评要求	测评方法	结果记录	结果记录
1	岗位设置	**a）金融机构信息安全管理工作实行统一领导、分级管理，总部统一领导分支机构的信息安全管理，各机构负责本单位和辖内的信息安全管理。(F3)**	检查金融行业信息安全管理工作是否实行统一领导、分级管理，金融行业统一领导分支机构和直属企事业单位的信息安全管理，负责金融行业机关的信息安全管理，分支机构负责本单位和辖内的信息安全管理，各直属企事业单位负责本单位的信息安全管理。		
		b）应设立由本机构领导、业务与技术相关部门主要负责人组成的信息安全领导小组，负责协调本机构及辖内信息安全管理工作，决策本机构及辖内信息安全重大事宜。	应访谈安全主管，询问是否设立专职的安全管理机构（即信息安全管理工作的职能部门）；机构内部门设置情况如何，是否明确各部门职责分工。		

序号	类别	测评要求	测评方法	结果记录	结果记录
		c）应设立专门的信息科技风险审计岗位，负责信息科技审计制度和流程的实施，制订和执行信息科技审计计划，对信息科技整个生命周期和重大事件等进行审计。(F3)	检查信息安全岗位制度，是否规定设立专门的信息科技风险审计岗位，负责信息科技审计制度和流程的实施，制订和执行信息科技审计计划，对信息科技整个生命周期和重大事件等进行审计。		
		d)应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。	检查部门、岗位职责文件，查看文件是否明确安全管理机构的职责，是否明确机构内各部门和各负责人的职责和分工。		
		e)应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责。	查看文件是否明确设置安全主管、安全管理各个方面的负责人、机房管理员、系统管理员、网络管理员、安全管理员等各个岗位，各个岗位的职责范围是否清晰、明确。		
		f)金融机构的主要负责人为本单位计算机信息系统安全保护工作的第一责任人。金融机构的计算机信息系统安全保护领导小组、专职部门和专(兼)职安全管理人员以及其他有关人员应当协助第一责任人组织落实有关规定。(F3)	检查金融机构相关部门的岗位职责制度文件，是否规定金融机构的主要负责人为本单位计算机信息系统安全保护工作的第一责任人，信息系统安全保护领导小组、专职部门和专(兼)职安全管理人员以及其他有关人员应当协助第一责任人组织落实有关规定。		
		g)应坚持三分离原则，实现前后台分离、开发与操作分离、技术与业务分离，信息技术人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务。(F3)	检查岗位设置相关文档，是否规定了实现前后台分离、开发与操作分离、技术与业务分离原则。		
		h)除科技部门外，其他部门均应指定至少一名部门计算机安全员，具体负责本部门的信息安全管理工作，协同科技部门开展信息安全管理工作。(F3)	检查除科技部门外，各单位其他部门是否均指定至少 1 名部门计算机安全员，具体负责本部门的信息安全管理工作，协同科技部门开展信息安全管理工作。		
2	人员配备	a）应配备一定数量的系统管理员、网络管理员、安全管理员等。	检查管理人员名单，查看其是否明确哪些人员是机房管理员、系统管理员、网络管理员、安全管理员等重要岗位人员的信息。		

序号	类别	测评要求	测评方法	结果记录	结果记录
		b）**应**配备专职安全管理员，**实行A、B 岗制度，**不可兼任。	检查管理人员名单，查看安全管理员是否是专职人员。		
		c）关键事务岗位应配备多人共同管理。	访谈安全主管，询问哪些关键事物需要配备2人或2人以上共同管理，人员具体配备情况如何；检查人员配备要求管理文档。		
3	授权和审批	a）应根据各部门和岗位的的职责明确授权审批事项、审批部门和批准人等。	检查审批管理制度文档，查看文档中是否明确审批事项、审批部门和批准人等。		
		b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度。	检查审批管理制度文档，查看文档中是否明确审批程序等，是否明确对重要活动进行逐级审批，由哪些部门/人员逐级审批；检查经逐级审批的文档。		
		c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。	检查审批管理文件，查看文件是否明确需定期审查、更新审批的项目、审批部门、审批人和审查周期等。		
		d）应记录审批过程并保存审批文档。	检查关键活动的审批过程记录，查看记录的审批程序与文件要求是否一致。		
		e）用户应被授予完成所承担任务所需的最小权限，重要岗位的员工之间应形成相互制约的关系。权限变更应执行相关审批流程，并有完整的变更记录。(F3)	访谈安全管理员，询问用户权限的分配原则，查看权限关系表，用户是否应被授予完成所承担任务所需的最小权限，重要岗位的员工之间应形成相互制约的关系。		
		f)应建立系统用户及权限清单，定期对员工权限进行检查核对，发现越权用户要查明原因并及时调整，同时清理过期用户权限，做好记录归档。(F3)	检查用户权限清单是否合理，是否定期对用户权限清单进行审查和清理，是否有记录并归档。		

序号	类别	测评要求	测评方法	结果记录	结果记录
4	沟通和合作	a）应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题，**并形成会议纪要。**	检查组织内部机构之间以及信息安全职能部门内部的安全工作会议文件或会议记录，查看是否具有会议内容、会议时间、参加人员和会议结果等描述；检查是否具有信息安全管理委员会或领导小组安全管理工作执行情况的文件或工作记录。		
		b）应加强与兄弟单位、公安机关、电信公司的合作与沟通。	检查外联单位联系列表，查看外联单位是否包含公安机关、电信公司、兄弟公司等，是否说明外联单位的名称、联系人、合作内容和联系方式等内容。		
		c）应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通。	检查外联单位联系列表，查看外联单位是否包含供应商、业界专家、专业的安全公司和安全组织等，是否说明外联单位的名称、联系人、合作内容和联系方式等内容。		
		d）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	检查外联单位联系列表，查看外联单位是否包含公安机关、电信公司、兄弟公司、供应商、业界专家、专业的安全公司和安全组织等，是否说明外联单位的名称、联系人、合作内容和联系方式等内容。		
		e）应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。	检查是否有聘请信息安全专家作为常年的安全顾问的证明文档。		
5	审核和检查	a）应制定安全审核和安全检查制度规范安全审核和安全检查工作，按要求定期开展安全审核和安全检查活动。	检查安全检查制度文档，查看文档是否规定检查内容、检查程序和检查周期等，检查内容是否包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。		
		b）安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	访谈安全主管，询问是否组织人员定期对信息系统进行安全检查，检查周期多长，检查内容是否包括系统日常运行、系统漏洞和数据备份等情况。		

序号	类别	测评要求	测评方法	结果记录	结果记录
		c）应由内部人员或上级机构定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。	访谈安全管理员，询问是否定期进行全面安全检查，检查周期多长，安全检查包含哪些内容，检查人员有哪些，检查程序是否按照相关策略和要求进行；检查安全检查过程记录，查看记录的检查程序与文件要求是否一致。		
		d）应制定安全检查表格，实施安全检查，汇总安全检查数据，形成安全检查报告，**要求限期整改的需要对相关整改情况进行后续跟踪，并将每次安全检查报告和整改落实情况整理汇总后，报上一级机构科技部门备案。**	检查是否具有安全检查表格；检查安全检查报告，查看报告日期与检查周期是否一致。		
		e)应制定违反和拒不执行安全管理措施规定的处罚细则。(F3)	检查是否制定违反和拒不执行安全管理措施规定的处罚细则。		

A.2.2.3 人员安全管理

序号	类别	测评内容	测评方法	结果记录	符合情况
1	人员录用	a）应指定或授权专门的部门或人员负责人员录用。	访谈安全主管，询问是由何部门/何人负责安全管理和技术人员的录用工作。		
		b）应严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核。	检查人员录用要求管理文档，查看是否说明录用人员应具备的条件，如学历、学位要求等；检查技能考核文档或记录，查看是否记录考核内容和考核结果等。		
		c）应与员工签署保密协议。	访谈人事负责人，询问是否与录用后的技术人员签署保密协议；检查保密协议。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		d）应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。	访谈人员录用负责人员，询问哪些岗位是比较关键的岗位，对从事关键岗位的人员是否从内部人员中选拔，是否要求其签署岗位安全协议；检查岗位安全协议。		
		e)对信息安全管理人员应实行备案管理。信息安全管理人员的配备和变更情况，应及时报上一级科技部门备案，金融机构总部信息管理人员在总部科技部门备案。(F3)	检查对信息安全管理人员是否实行备案管理。信息安全管理人员的配备和变更情况，是否及时报上一级科技部门备案，金融机构总部信息管理人员是否在总部科技部门备案。		
		f）凡是因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员，不得从事信息安全管理工作。(F3)	检查相关人员档案背景，不得录用因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员。		
2	人员离岗	a）应严格规范人员离岗过程，及时终止离岗员工的所有访问权限。	访谈人事负责人，询问是否及时终止离岗人员的所有访问权限。		
		b）应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	检查是否具有交还身份证件和设备等的登记记录。		
		c)应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开，**并保证离岗人员负责的信息技术系统的口令必须立即更换。**	检查人员离岗管理文档，查看是否规定了调离手续和离岗要求等；检查保密承诺文档，查看是否具有调离人员签字。		
3	人员考核	a）应定期对各个岗位的人员进行安全技能及安全认知的考核。	访谈安全主管，询问对各个岗位人员是否定期进行考核，考核周期多长，考核内容有哪些；检查考核记录。		
		b)应对关键岗位的人员进行全面、严格的安全审查和技能考核。	访谈人员录用负责人员，询问对关键岗位人员的安全审查和考核与一般岗位人员有何不同，内容有哪些，		

序号	类别	测评内容	测评方法	结果记录	符合情况
			审查内容是否包括操作行为和社会关系等。		
		c）应对考核结果进行记录并保存。	检查是否具有各岗位人员考核记录，查看考核内容是否包含安全知识、安全技能等；查看记录日期与考核周期是否一致。		
4	安全意识教育和培训	a）应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划。	访谈安全主管，询问是否对各个岗位人员进行安全教育、岗位技能和安全技术培训，以什么形式进行，效果如何。		
		b）应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，**普及信息安全基础知识、规范岗位操作、提高安全技能。**	应检查安全教育和培训计划文档，查看是否具有不同岗位的培训计划；查看计划是否明确了培训目的、培训方式、培训对象、培训内容、培训时间和地点等，培训内容是否包含信息安全基础知识、岗位操作规程等。		
		c)每年至少对信息安全管理人员进行一次信息安全培训。(F3)	检查金融机构是否每年至少对信息安全管理人员进行一次信息安全培训，是否有培训记录。		
		d）应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒。	访谈安全管理员、系统管理员、网络管理员和数据库管理员，考查其是否了解与工作相关的安全责任和惩戒措施等；检查安全责任和惩戒措施管理文档。		
		e）应对安全教育和培训的情况和结果进行记录并归档保存。	检查是否具有安全教育和培训的结果记录，查看记录中是否具有培训人员、培训内容、培训结果等的描述；查看记录与培训计划是否一致。		
5	外部人员访问管理	**a)各机构指定责任部门负责非涉密计算机系统和网络相关的外部人员访问授权审批，批准后由专人全程陪同或监督，并登记备案。**	检查外部人员访问相关规定，检查外部人员访问重要区域批准文档和外部人员访问重要区域的登记记录。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		b）允许被外部人员访问的金融行业计算机系统和网络资源应建立存取控制机制、认证机制，列明所有用户名单及其权限，其活动应受到监控。	检查外部人员访问相关规定，查看是否对允许外部人员访问的区域、系统、设备和信息等进行明确规定。		
		c)获得外部人员访问授权的所有单位和个人应与金融机构签订安全保密协议，不得进行未授权的增加、删除、修改、查询数据操作，不得复制和泄漏金融机构的任何信息。(F3)	检查获得外部人员访问授权的所有单位和个人是否与金融行业签订安全保密协议，是否进行未授权的增加、删除、修改、查询数据操作，不得复制和泄漏金融行业的任何信息。		

A.2.2.4 系统建设管理

序号	类别	测评内容	测评方法	结果记录	符合情况
1	系统定级	a）应明确信息系统的边界和安全保护等级。	检查系统定级说明文档，查看文档是否明确信息系统边界和安全保护等级。		
		b）应以书面的形式说明确定信息系统为某个安全保护等级的方法和理由。	检查系统定级文档，查看文档是否明确信息系统的安全保护等级确定的方法和理由。		
		c）应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定。	访谈安全主管，询问是否组织相关部门和有关安全技术专家对定级结果进行论证和审定；检查定级结果论证文档。		
		d）应确保信息系统的定级结果经过相关部门的批准。	检查系统定级文档，查看定级结果是否具有相关部门的批准盖章。		
2	安全方案设计	a）应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划。	检查是否有对金融机构范围信息系统的安全建设进行总体规划，是否制定了近期和远期的安全建设工作计划，金融机构的科技部门对本单位的安全建设是否进行规划，是否制定近期和远期的安全建设工作计		

序号	类别	测评内容	测评方法	结果记录	符合情况
			划。		
		b）应根据系统的安全级别选择基本安全措施，依据风险分析的结果补充和调整安全措施。	访谈系统建设负责人，询问系统选择基本安全措施的依据，是否依据安全保护等级选择，是否依据风险分析的结果补充和调整安全措施，做过哪些调整。		
		c）应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件。	访谈系统建设负责人，询问是否根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案等。		
		d）应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。	访谈系统建设负责人，询问是否组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略等相关配套文件进行论证和审定。		
		e）应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。	访谈系统建设负责人，询问总体安全策略、安全技术框架、安全管理策略等相关配套文件是否定期进行调整和修订，依据什么原则。		
3	产品采购和使用	a）应确保安全产品的采购和使用符合国家的有关规定。	访谈系统建设负责人，询问系统信息安全产品的采购情况，是否按照国家的相关规定进行使用。		
		b）应确保密码产品的采购和使用符合国家密码主管部门的要求。	访谈系统建设负责人，询问系统是否采用了密码产品，密码产品的使用是否符合国家密码主管部门的要求。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		c)应指定或授权专门的部门负责产品的采购，**设备采购应坚持公开、公平、公正的原则，宜采用招标、邀标等形式完成。**	访谈系统建设负责人，询问是否具有专门的部门负责产品的采购，由何部门负责。		
		d）各机构购置扫描、检测类信息安全产品应报科技主管部门批准、备案。(F3)	检查各单位购置扫描、检测类信息安全产品是否报金融行业科技主管部门批准、备案。		
		e）应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。	访谈系统建设负责人，询问系统信息安全产品的采购情况，检查是否具有产品选型测试结果记录和候选产品名单。		
		f)扫描、检测类信息安全产品仅限于本机构信息安全管理人员或经主管领导授权的网络管理员使用。(F3)	检查扫描、检测类信息安全产品使用记录表，验证是否仅限于本单位信息安全管理人员使用。		
		g）应定期查看各类信息安全产品相关日志和报表信息并定期汇总分析，若发现重大问题，立即采取控制措施并按规定程序报告。(F3)	检查是否随时检查各类信息安全产品使用情况，认真查看相关日志和报表信息并定期汇总分析，若发现重大问题，是否立即采取控制措施并按规定程序报告。		
		h)应定期对各类信息安全产品产生的日志和报表进行备份存档，至少保存 3 个月。(F3)	检查各类信息安全产品在使用中产生的日志和报表信息等重要技术资料，是否备份存档至少 3 个月。		
		i）应及时升级维护信息安全产品，凡超过使用期限的或不能继续使用的信息安全产品，要按照固定资产报废审批程序处理。(F3)	检查是否及时升级维护信息安全产品，凡超过使用期限的或不能继续使用的信息安全产品，是否按照固定资产报废审批程序处理。		
4	自行软件开发	**a）应制定软件开发管理制度和代码编写安全规范，明确说明开发过程的控制方法和人员行为准则，要求开发人员参照规范编写代码，不得在程序中设置后门或恶意代码程序。(F3)**	检查是否具有软件开发管理制度，检查是否具有代码编写安全规范。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		b）应确保开发环境与实际运行环境物理分开，**应确保开发人员和测试人员分离，开发人员不能兼任系统管理员或业务操作人员，**确保测试数据和测试结果受到控制。	访谈系统建设负责人，询问系统是否自主开发软件，是否在独立的开发环境中编写、调试和完成；是否要求开发人员不能做测试工作。		
		c）应确保提供软件设计的相关文档和使用指南，并由专人负责保管。	检查是否提供软件设计的相关文档和使用指南，是否由专人负责保管。		
		d）应确保对程序资源库的修改、更新、发布进行授权和批准。	检查对程序资源库的修改、更新、发布是否进行授权和批准。		
		e)在软件开发过程中，应同步完成相关文档手册的编写工作，保证相关资料的完整性和准确性。(F3)	检查软件是否具备需求说明书、详细设计说明书、安装手册、用户操作手册等文档，文档是否完整、规范和准确。		
5	外包软件开发	a）应根据开发需求检测软件质量。	检查是否根据开发需求检测软件质量。		
		b）应在软件安装之前检测软件包中可能存在的恶意代码。	检查在软件安装之前是否检测软件包中可能存在的恶意代码。		
		c）应要求开发单位提供软件设计的相关文档和使用指南。	检查开发单位是否提供了软件设计的相关文档和使用指南。		
		d）应要求开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。	检查开发单位提供的软件源代码，审查软件中是否存在后门。		
		e)应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。(F3)	检查外包人员进入金融行业进行现场实施时，是否事先提交计划操作内容并留有记录，金融行业人员是否在现场陪同外包人员，核对操作内容并准确记录实际操作内容，涉及敏感操作（如输入用户口令等）是否由金融行业人员进行操作。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		f)应要求外包服务商每年至少开展一次信息安全风险评估并提交评估报告，应要求外包服务商聘请外部机构定期对其进行安全审计并提交审计报告，督促其及时整改发现的问题。(F3)	检查外包服务商是否每年至少开展一次内部或聘请外部机构的安全评估工作，是否具有评估报告。		
		g)应禁止外包服务商转包并严格控制分包，保证外包服务水平。(F3)	检查外包服务商的工作机制，是否存在分包、转包现象。		
		h）应制定数据中心外包服务应急计划，制订供应商替换方案，以应对外包服务商破产、不可抗力或其它潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。(F3)	检查是否具备关于外包服务的应急计划文档，文档中是否明确规定外包服务商的替换方案等。		
6	工程实施	a）应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则。	检查是否制定工程实施方面的管理制度，是否明确说明实施过程的控制方法和人员行为准则。		
		b）应指定或授权专门的部门或人员负责工程实施过程的管理。	检查是否指定或授权专门的部门或人员负责工程实施过程的管理。		
		c）应制定详细的工程实施方案控制实施过程，并制定相关过程控制文档，并要求工程实施单位能正式地执行安全工程过程。	检查是否制定详细的工程实施方案控制实施过程，检查工程实施单位是否能正式地执行安全工程过程。		
		d)应制定灾难备份系统集成与测试计划并组织实施。通过技术和业务测试，确认灾难备份系统的功能与性能达到设计指标要求。(F3)	检查是否建立灾难备份系统集成和测试的计划文档，是否组织计划实施验证灾难备份系统的功能与性能达到设计指标要求。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		e)网络系统的建设、升级、扩充等工程应经过科学的规划、充分的论证和严格的技术审查，有关材料应妥善保存并接受主管部门的检查。(F3)	检查网络系统的建设、升级、扩充等工程是否经过科学的规划、充分的论证和严格的技术审查，有关材料是否妥善保存并接受主管部门的检查。		
7	测试验收	a）应对系统测试验收的控制方法和人员行为准则进行书面规定。	检查科技部门是否对系统测试验收的控制方法和人员行为准则进行书面规定。		
		b）应由项目承担单位（部门）或公正的第三方制定安全测试方案，对系统进行安全性测试，并出具安全性测试报告，测试报告报科技部门审查。(F3)	检查项目承担单位（部门）或公正的第三方制定安全测试方案，是否对系统进行安全性测试，是否出具安全性测试报告，测试报告是否报科技部门审查。		
		c）在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告。	检查在测试验收前是否根据设计方案或合同要求等制订测试验收方案，在测试验收过程中是否详细记录测试验收结果，是否形成测试验收报告。		
		d）应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作。	检查是否指定或授权专门的部门负责系统测试验收的管理，是否按照管理规定的要求完成系统测试验收工作。		
		e）应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。	检查是否组织相关部门和相关人员对系统测试验收报告进行审定，是否签字确认。		
		f)新建应用系统投入生产运行前应进行不少于1个月的模拟运行和不少于3个月的试运行。(F3)	检查新建应用系统投入生产运行前是否进行模拟试运行测试，模拟和试运行的时间是多少。		

序号	类别	测评内容	测评方法	结果记录	符合情况
8	系统交付	a）应对系统交付的控制方法和人员行为准则进行书面规定。	科技部门是否对系统交付的控制方法和人员行为准则进行书面规定。		
		b）应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。	检查是否制定详细的系统交付清单，是否根据交付清单对所交接的设备、软件和文档等进行清点。		
		c）系统建设单位应在完成建设任务后将系统建设过程文档和系统运维文档全部移交科技部门。(F3)	系统建设单位检查是否在完成建设任务后将系统建设过程中的文档和指导用户进行系统运行维护的文档全部移交金融行业科技部门。		
		d）系统建设单位应对负责系统运行维护的技术人员进行相应的技能培训。	系统建设单位检查是否对负责系统运行维护的技术人员进行相应的技能培训。		
		e）应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。	检查是否指定或授权专门的部门负责系统交付的管理工作，是否按照管理规定的要求完成系统交付工作。		
		f)外部建设单位应与金融机构签署相关知识产权保护协议和保密协议，不得将系统采用的关键安全技术措施和核心安全功能设计对外公开。(F3)	检查金融机构与外部建设单位签订的合同或协议，是否有相关约束条款来保证。系统采用的关键安全技术措施和核心安全功能设计不对外公开。		
9	系统备案	a）应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用。	检查是否指定专门的部门或人员负责管理系统定级的相关材料，是否控制这些材料的使用。		
		b）应将系统等级及相关材料报系统主管部门备案。	检查是否将系统等级及相关材料报系统主管部门备案。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		c）应将系统等级及其他要求的备案材料报相应公安机关备案。	检查是否将系统等级及其他要求的备案材料报相应公安机关备案。		
10	等级测评	a）在系统运行过程中，应至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改。	在系统运行过程中，是否每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的是否及时整改。		
		b）应在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改。	检查是否在系统发生变更时及时对系统进行等级测评，发现级别发生变化的是否及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的是否及时整改。		
		c)应选择具有**公安部认可的《全国等级保护测评机构推荐目录》中**的测评单位进行等级测评，并与测评单位签订安全保密协议。	检查是否选择具有国家相关技术资质和安全资质的测评单位进行等级测评，测评单位是否签订安全保密协议。		
		d）应指定或授权专门的部门或人员负责等级测评的管理。	检查是否指定或授权专门的部门或人员负责等级测评的管理。		
11	安全服务商选择	**a)选择信息安全服务提供商时应评估其资质、经营行为、业绩、服务体系和服务品质等要素。(F3)**	金融行业科技主管部门是否将信息安全服务提供商的资质进行审查。		
		b）应确保安全服务商的选择符合国家的有关规定。	检查安全服务商的选择是否符合国家的有关规定，涉密计算机系统集成商是否具有国家相关部门颁发的涉密系统集成资质证书的单位。		
		c）应与选定的安全服务商签订与安全相关的协议，明确约定相关责任。	检查是否与选定的安全服务商签订与安全相关的协议，是否与涉密计算机系统集成商签订严格的保密协议，是否明确约定相关责任。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		d）应确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同。	检查选定的安全服务商提供技术培训和服务承诺，是否与其签订服务合同。		

A.2.2.5 系统运维管理

序号	类别	测评内容	测评方法	结果记录	符合情况
1	环境管理	a)应建立集中的机房，统一为各信息系统提供运行环境。机房设施配备应符合国家计算机机房有关标准要求。	检查机房配备的实施是否符合国家计算机机房的有关标准要求。		
		b)机房应采用结构化布线系统，配线机柜内如果配备理线架，应做到跳线整齐，跳线与配线架统一编号，标记清晰。(F3)	访谈物理安全负责人，询问机房的布线方式，是否统一编号，标记是否清晰。		
		c)应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定。	检查机房安全管理制度，查看其内容是否覆盖机房物理访问、物品带进、带出机房和机房环境安全等方面。		
		d)**应指定部门负责机房安全**，指派专人担任机房管理员，对机房的出入进行管理，定期巡查机房运行状况，对机房供配电、空调、温湿度控制等设施进行维护管理，**填写机房值班记录、巡视记录。**	访谈物理安全负责人，询问由何部门或何人对机房的基本设施（如空调、供配电设备等）进行定期维护；检查机房基础设施的维护记录。		
		e)机房管理员应经过相关专业培训，掌握机房各类设备的操作要领。(F3)	检查机房管理员是否经过相关专业培训，是否掌握机房各类设备的操作要领；。		
		f)应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养。(F3)	检查各单位应定期对机房设施是否进行维修保养，加强对易损、易失效设备或部件的维护保养。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		g)机房人员进出机房必须使用主管部门制发的证件。(F3)	检查机房管理制度，是否对人员的进出进行规定，是否需要机房出入证。		
		h）应单独设置弱电井，并留有足够的可扩展空间。（F3）	检查是否设置弱电井，询问其可扩展空间如何。		
		i)机房所在区域应安装24小时视频监控录像装置，重要机房区域实行24小时警卫值班，机房实行封闭式管理，设置一个主出入口和一个或多个备用出入口，出入口控制、入侵报警和电视监控设备运行资料应妥善保管，保存期限不少于3个月，销毁录像等资料应经机构主管领导批准后实施。(F3)	询问管理员是否出入口控制、入侵报警和电视监控设备运行资料应妥善保管，保存期限不少于 3 个月；销毁录像等资料应经机构主管领导批准后实施。		
		j)应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。	检查办公环境管理制度，查看是否对办公人员的相关行为进行规范。		
2	资产管理	a)应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	检查资产清单，查看其内容是否覆盖资产责任人、所属级别、所处位置、所处部门等方面。		
		b)应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为。	检查资产管理制度，查看其内容是否覆盖资产使用、维护等方面，是否指定资产管理的责任部门或人员,由何部门/何人负责。		
		c)应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施。	检查资产清单中的设备，查看其是否具有相应标识，标识是否能表明资产的重要程度。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		d)应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。	检查信息分类文档，查看其内容是否规定了分类标识的原则和方法（如根据信息的重要程度、敏感程度或用途不同进行分类）。		
3	介质管理	a)应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定。	检查介质管理制度，查看其内容是否覆盖介质的使用、维修、销毁等过程的操作。		
		b)应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理。	访谈资产管理员，询问介质存放于何种环境中，是否对存放环境实施专人管理。		
		c)所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放。(F3)	检查所有数据备份介质是否防磁、防潮、防尘、防高温、防挤压存放。		
		d)应对介质在物理传输过程中的人员选择、打包、交付等情况进行安全控制，**应选择安全可靠的传递、交接方式，做好防信息泄露控制措施。**	访谈资产管理员，询问对介质的物理传输过程是否要求选择可靠传输人员、严格介质的打包（如采用防拆包装置）、选择安全的物理传输途径、双方在场交付等环节的控制；是否对介质的使用情况进行登记管理，并定期盘点。		
		e)应对介质归档和查询等进行登记记录，管理员应根据存档介质的目录清单定期盘点。	询问管理员是否应根据存档介质的目录清单并定期盘点。		
		f）对于重要文档，如是纸质文档则应实行借阅登记制度，未经相关部门领导批准，任何人不得将文档转借、复制或对外公开，如是电子文档则应采用 OA 等电子化办公审批平台进行管理。(F3)	检查纸质技术文档是否实行借阅登记制度，未经科技部门领导批准，是否有人将技术文档转借、复制或对外公开，电子文档是否采用 OA 等电子化办公审批平台进行管理。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		g)应按照统一格式对技术文档进行编写并及时更新，达到能够依靠技术文档恢复系统正常运行的要求。(F3)	检查技术文档的格式是否统一，内容是否具有参考性，是否达到能够依靠技术文档恢复系统正常运行的要求。		
		h)应对带出工作环境的存储介质进行内容加密和监控管理。	询问管理员是否对带出工作环境的存储介质进行内容加密和监控管理。		
		i)应对送出维修的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁。	访谈资产管理员，询问对送出维修或销毁的介质如何管理，销毁前是否对数据进行净化处理。		
		j)对载有敏感信息存储介质的销毁，应报有关部门备案，由科技部门进行信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录，信息消除处理仅限于存储介质仍将在金融机构内部使用的情况，否则应进行信息的不可恢复性销毁。(F3)	检查需要废止的计算机设备，是否由科技部门使用专用工具进行数据信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录，信息消除处理仅限于存储介质仍将在金融行业内部使用的情况，否则应进行信息的不可恢复性销毁处理。		
		k)应制定移动存储介质使用规范，并定期核查移动存储介质的使用情况。(F3)	检查各单位是否严格管理移动存储介质，定期核查所配发移动存储介质的在位使用情况，是否违规使用移动存储介质的情况。		
		l)应建立重要数据多重备份机制，其中至少1份备份介质应存放于科技部门指定的同城或异地安全区域。(F3)	访谈资产管理员，询问是否对某些重要介质(至少一份)实行异地存储，异地存储环境是否与本地环境相同，检查介质本地存放的实际环境的安全性。		
		m)应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。	访谈资产管理员，对重要介质中的数据和软件是否进行保密性处理，对介质是否根据重要性不同进行分类标识，并进行检查。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		n)应对技术文档实行有效期管理，对于超过有效期的技术文档降低保密级别，对已经失效的技术文档定期清理，并严格执行技术文档管理制度中的销毁和监销规定。(F3)	检查技术文档的有效期时间和密级级别是否一致、合理，对于过期的技术文档的销毁是否遵循文档制度中的毁和监销规定。		
		o)应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。(F3)	检查是否定期对主要业务备份数据进行恢复性验证，是否及时转存介质中存储的数据。		
4	设备管理	a)应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理。	访谈资产管理员，询问是否对设备选用的各个环节（选型、采购、发放等）进行规范化管理，检查相应管理制度。		
		b)应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等。	检查设备维护管理文档，看其是否覆盖维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等方面。		
		c)设备确需送外单位维修时，应彻底清除所存的工作相关信息，并与设备维修厂商签订保密协议，与密码设备配套使用的设备送修前必须请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息，并派专人在场监督。(F3)	检查计算机设备确需送外单位维修时，各单位科技部门是否彻底清除所存的工作相关信息，必要时应与设备维修厂商签订保密协议，与密码设备配套使用的计算机设备送修前必须请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息。		
		d)制定规范化的故障处理流程，建立详细的故障日志(包括故障发生的时间、范围、现象、处理结果和处理人员等内容)。(F3)	检查是否具备关于故障处理文档，文档中是否详细记录了处理流程，是否建立故障处理日志。		
		e)应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。	检查设备管理制度文档，查看其是否对设备的操作和使用了进行明确规定；检查设备操作手册，查看其内容是否覆盖设备启动、停止、加电、断电等操作。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		f)各机构科技部门负责对信息系统相关的各种设备（包括备份和冗余设备）、线路等进行维护管理。(F3)	应访谈资产管理员，询问是否对各类设施、设备指定专人或专门部门进行定期维护，由何部门/何人维护。		
		g)新购置的设备应经过测试，测试合格后方能投入使用。(F3)	检查是否具备新购设备的测试报告，是否测试合格后方可投入使用。		
		h)应做好设备登记工作，制定设备管理规范，落实设备使用者的安全保护责任。(F3)	检查各单位科技部门是否做好计算机设备登记工作，严格设备资产管理，落实计算机设备使用者的安全保护责任。		
		i)需要废止的设备，应由科技部门使用专用工具进行数据信息消除处理，如废止设备不再使用或调配到金融行业以外的单位，应由科技部门备案并对其数据信息存储设备进行消磁或物理粉碎等不可恢复性销毁处理，同时备案。(F3)	检查需要废止的计算机设备，是否由科技部门使用专用工具进行数据信息消除处理，如废止计算机设备不再使用或调配到金融行业以外的单位，是否由科技部门对其数据信息存储设备进行消磁或物理粉碎等不可恢复性销毁处理。		
		j)应确保信息处理设备必须经过审批才能带离机房或办公地点。	访谈资产管理员，询问对带离机房的设备是否经过审批，由何人审批。		
5	监控管理和安全管理中心	a)应对通信线路、网络设备、主机和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存。	访谈系统运维负责人，询问其是否监控主机、网络设备和应用系统的运行状况等，采用何种方式进行监控。		
		b)应建立计算机系统运行监测周报、月报或季报制度，统计分析运行状况。(F3)	检查各单位科技部门是否建立计算机系统运行监测周报、月报或季报制度，统计分析运行状况。		
		c)应定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，**发现重大隐患和运行事故应及时协调解决，并报上一级单位相关部门。**	访谈系统运维负责人，询问是否定期对监控记录进行分析、评审。检查各单位是否及时预警、响应和处置运行监测中发现的问题，发现重大隐患和运行事故应及时协调解决，是否并报上一级单位相关部门。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		d)应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。	访谈系统运维负责人，询问是否建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等相关事项进行集中管理。		
6	网络安全管理	a)应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作，**并有操作和复核人员的签名，维护记录应至少妥善保存3 个月。**	访谈安全主管，询问是否指定专人负责维护网络安全管理工作。		
		b)应建立网络安全运行管理制度，对网络安全配置(**最小服务配置**)、日志保存时间、安全策略、升级与打补丁、口令更新周期、**重要文件备份**等方面作出规定。	检查网络安全管理制度，查看其内容是否覆盖网络安全配置（包括网络设备的安全策略、授权访问、最小服务、升级与打补丁）、审计日志保存时间、升级与打补丁等方面。		
		c)应制定网络接入管理规范，任何设备接入网络前，接入方案应经过科技部门的审核，审核批准后方可接入网络并分配相应的网络资源。	询问系统管理员是否制定网络接入管理规范，接入方案应经过科技部门的审核，审核批准后方可接入网络并分配相应的网络资源。		
		d)应制定远程访问控制规范，确因工作需要进行远程访问的，应由访问发起机构科技部门核准，提请被访问机构科技部门（岗）开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。(F3)	检查各单位是否严格远程访问控制，确因工作需要进行远程访问的，应由访问发起单位科技部门核准，提请被访问单位科技部门（岗）开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。		
		e)各机构以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经科技主管部门批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。(F3)	检查各单位以不影响正常网络传输为原则，是否合理控制多媒体网络应用规模和范围，未经金融行业科技主管部门批准，不得在金融行业内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。		
		f)信息安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不	询问信息安全管理人员经本部门主管领导批准后，有权对本单位或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不		

序号	类别	测评内容	测评方法	结果记录	符合情况
		得对外公开，未经科技主管部门授权，任何外部机构与人员不得检测或扫描机构内部网络。(F3)	得对外公开，未经金融行业科技主管部门授权，任何外部单位与人员不得检测或扫描金融行业内部网络。		
		g)金融业网间互联安全实行统一规范、分级管理、各负其责的安全管理模式，未经金融机构科技主管部门核准，任何机构不得自行与外部机构实施网间互联。(F3)	询问管理员是否应定期检查违反规定拨号上网或其他违反网络安全策略的行为，金融行业内部网络与国际互联网实行安全隔离，所有接入金融行业内部网络或存储有敏感工作信息的计算机，不得接入国际互联网。		
		h)所有网间互联应用系统和外联网络区应定期进行威胁评估和脆弱性评估并提供威胁和脆弱性评估报告。(F3)	访谈安全管理员，询问是否对所有网间互联应用系统和外联网络区进行威胁评估和脆弱性评估，评估的频率以及是否具有评估报告。		
7	系统安全管理	a)应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定。	检查系统安全管理制度，查看其内容是否覆盖系统安全配置（包括系统的安全策略、授权访问、最小服务、升级与打补丁）、系统帐户（用户责任、义务、风险、权限审批、权限分配、帐户注销等）、审计日志以及配置文件的生成、备份、变更审批、符合性检查等方面。		
		b)应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则。	访谈系统管理员，询问是否指定专人负责系统管理工作，是否对系统账户进行分类管理，权限设定是否遵循最小授权原则。		
		c)系统管理员不得兼任业务操作人员，系统管理员不得对业务数据进行任何增加、删除、修改、查询等操作，系统管理员确需对计算机系统数据库进行业务数据维护操作的，应征得业务部门书面同意，并详细记录维护内容、人员、时间等信息。(F3)	检查系统管理员不得兼任业务操作人员，系统管理员不得对业务数据进行任何增加、删除、修改、查询等操作，系统管理员确需对计算机系统数据库进行业务数据维护操作的，检查是否征得业务部门书面同意，并详细记录维护内容、人员、时间等信息。		
		d)应每半年至少进行一次漏洞扫描，对发现的系统安全漏洞及时进行修补，扫描结果应及时上报。(F3)	访谈系统管理员，询问是否每半年对系统进行漏洞扫描，发现漏洞是否进行了及时修补，检查系统漏洞扫描报告。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		e)系统管理员应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装，并对系统变更进行记录。	访谈系统管理员，询问在安装系统补丁程序前是否经过测试，并对重要文件进行备份。		
		f)系统管理员应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，**重要计算机系统的系统设置要求至少两人在场。**	检查系统操作手册，查看其内容是否覆盖操作步骤、维护记录、参数配置等方面。访谈系统管理员，询问是否指定专人负责系统管理工作，是否对系统账户进行分类管理，权限设定是否遵循最小授权原则。		
		g)应定期对运行日志和审计数据进行分析，以便及时发现异常行为。	访谈审计员，询问是否定期对系统审计日志进行分析，以便及时发现异常行为。		
		h)系统用户权限变更应以书面记录，并经相关管理层批准。(F3)	检查系统管理员是否对系统变更进行详细的记录。		
8	恶意代码防范管理	a)应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。	访谈系统运维负责人，询问是否对员工进行基本恶意代码防范意识的教育，如告知应及时升级软件版。		
		b)金融机构客户端应统一安装病毒防治软件，设置用户密码和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序。(F3)	检查全行客户端是否统一安装病毒防治软件，设置用户密码和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序。		
		c)应指定专人对网络和主机进行恶意代码检测并保存检测记录。	访谈系统运维负责人，询问是否指定专人对恶意代码进行检测，并保存记录。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		d)应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。	检查恶意代码防范管理文档，查看其内容是否覆盖防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面。		
		e)应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，对防病毒系统不能自动清除的计算机病毒，提出解决办法，并形成书面的报表和总结汇报。	访谈安全管理员，询问是否对恶意代码库的升级情况进行记录，对各类防病毒产品上截获的恶意代码是否进行分析并汇总上报；是否出现过大规模的病毒事件，如何处理；检查恶意代码检测记录、恶意代码库升级记录和分析报告检查恶意代码防范管理文档，查看其内容是否覆盖防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面。		
9	密码管理	a)选用的密码产品和加密算法应符合国家相关密码管理政策规定。	访谈安全管理员，询问密码技术和产品的使用是否金融行业的《含有密码技术的信息产品政府采购规定》中的安全要求,使用符合国家密码管理规定的密码技术和产品。		
		b）应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员必须是本机构在编的正式员工，并逐级进行备案，规范密钥管理。(F3)	访谈安全管理员，是否建立密码使用管理制度，并符合要求。		
		c)主机管理员、数据库管理员、网络管理员、业务操作人员均须设置口令密码，至少每 3 个月更换一次，口令密码的强度应满足不同安全性要求。(F3)	检查各单位系统管理员、数据库管理员、网络管理员、业务操作人员是否均设置口令密码，并至少每 3 个月更换一次，口令密码的强度是否满足不同安全性要求。检查各类密钥是否定期更换，对已泄漏或怀疑泄漏的密钥是否做到及时废除，过期密钥是否安全归档或定期销毁。		
		d)敏感计算机系统和设备的口令密码设置应在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经科技部门主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码	检查敏感计算机系统和设备的口令密码设置是否在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经科技部门主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密		

序号	类别	测评内容	测评方法	结果记录	符合情况
		使用后应立即更改并再次密封存放。(F3)	码使用后是否做到了立即更改并再次密封存放。检查各单位系统管理员、数据库管理员、网络管理员、业务操作人员是否均设置口令密码，并至少每 3 个月更换一次，口令密码的强度是否满足不同安全性要求。		
		e)密钥注入、密钥管理功能调试和密钥档案的保管应由专人负责。密钥资料须保存在保险柜内。保险柜钥匙由专人负责。使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录。(F3)	检查密钥注入、管理功能调试和档案保管是否是专人负责；密钥资料保存在何处，以及是否具备管理制度来规定密钥的使用和销毁，是否有使用记录和销毁记录。		
		f)确因工作需要经授权可远程接入内部网络的用户，应妥善保管其身份认证介质及口令密码，不得转借他人使用。(F3)	确因工作需要经授权可远程接入内部网络的用户，检查是否妥善保管其身份认证介质及口令密码，查看是否转借他人使用。		
10	变更管理	**a)变更管理应流程化、文档化和制度化，变更流程中应明确变更发起方、实施方的职责，应明确变更方案的测试、审批流程及实施策略，对有可能影响客户利益的变更应事先通知客户并得到客户的确认。(F3)**	检查是否具备变更管理制度明确规定变更流程，明确变更发起方、实施方的职责，明确变更方案的测试、审批流程及实施策略，对有可能影响客户利益的变更是否具备变更客户通知确认程序。		
		b)应确认系统中要发生的变更，并制定变更方案，**包括变更的组织结构与实施计划、操作步骤、应急及回退方案等，变更方案应经过测试，对于无法测试或不具备测试条件的变更，应得到充分论证和审批。**	访谈系统运维负责人，询问是否制定变更方案指导系统执行变更；目前系统发生过哪些变更；检查系统变更方案。		
		c)应建立变更管理制度，重要系统变更前，应向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告。	检查变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容；检查是否具有变更方案评审记录和变更过程记录文档访谈系统运维负责人，询问是否制定变更方案指导系统执行变更；目前系统发生过哪些变更；检查系统变更方案。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		d)应建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录。	检查变更控制的申报、审批程序，查看其是否规定需要申报的变更类型、申报流程、审批部门、批准人等方面内容。检查变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容；检查是否具有变更方案评审记录和变更过程记录文档。		
		e)应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。	检查中止变更并从失败变更中恢复的文件化程序，是否明确过程控制方法和人员职责，必要时对恢复过程进行演练。		
		f)变更前做好系统和数据的备份。风险较大的变更，应在变更后对系统的运行情况进行跟踪。(F3)	检查变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容；检查是否具有变更方案评审记录和变更过程记录文档。		
		g)如果需要使用生产环境进行测试，应纳入变更管理，并制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划，确保生产系统的安全。(F3)	访谈安全管理员，是否需要使用生产环境进行测试，如果需要是否纳入变更管理中，是否制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划。		
		h)当生产中心发生变更时，应同步分析灾备系统变更需求并进行相应的变更，评估灾备恢复的有效性；应尽量减少紧急变更。(F3)	检查灾备中心是否在生产系统发生变更时也同步进行变更，是否有相关的变更记录。		
11	备份与恢复管理	a)应制定数据备份与恢复相关安全管理制度，对备份信息的备份方式、备份频度、存储介质、保存期等进行规范。	检查是否根据金融行业的统一规定建立自己的备份与恢复管理的相关制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范，同时根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		b)应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法。	检查数据备份和恢复策略文档，查看其内容是否覆盖数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面。检查是否具有规定备份方式、频度、介质、保存期的安全管理制度。		
		c)应建立控制数据备份和恢复过程的程序，记录备份过程，对需要采取加密或数据隐藏处理的备份数据，进行备份和加密操作时要求两名工作人员在场，所有文件和记录应妥善保存。	检查数据备份恢复管理制度，是否明确记录备份过程，是否要求对要采取加密或数据隐藏处理的备份数据，进行备份和加密操作时要求两名工作人员在场，是否具备备份恢复记录等所有文件。		
		d)应每年至少进行一次重要信息系统专项灾备切换演练，每三年至少进行一次重要信息系统全面灾备切换演练，根据不同的应急恢复内容，确定演练的周期，并指定专人管理和维护应急预案，根据人员、信息资源等变动情况以及演练情况适时予以更新和完善，确保应急预案的有效性和灾难发生时的可获取性。（F3）	查看是否应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期，定期组织应急预案的演练，并指定专人管理和维护应急预案，根据人员、信息资源等变动情况以及演练情况适时予以更新和完善，确保应急预案的有效性和灾难发生时的可获取性。		
		e)应定期对备份数据的有效性进行检查，每次抽检数据量不低于5%。备份数据要实行异地保存。(F3)	访谈安全管理员，询问是否对备份数据进行有效性验证，验证时间间隔为多长时间，验证的备份数据的比例为多少，是否进行异地保存。		
		f)恢复及使用备份数据时需要提供相关口令密码的，应把口令密码密封后与数据备份介质一并妥善保管。(F3)	检查数据备份恢复口令的存放管理制度，以及是否口令与数据备份介质均进行有效管理。		
		g)灾难恢复的需求应定期进行再分析，再分析周期最长为三年，当生产中心环境、生产系统或业务流程发生重大变更时，单位应立即启动灾难恢复需求再分析工作，依据需求分析制定灾难恢复策略。(F3)	访谈安全管理员，询问是否对灾难恢复的需求进行定期分析，尤其在发生变更时是否进行灾难恢复需求的再分析工作，再分析的周期是多少。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		h)应建立健全灾难恢复计划，恢复计划至少要包括灾难恢复范围和目标、灾难切换规程、灾后重续运行操作指引、各系统灾难切换操作手册。(F3)	检查是否具备灾难恢复计划，计划中是否包括灾难恢复范围和目标、灾难切换规程、灾后重续运行操作指引等内容。		
		i)金融机构应根据信息系统的灾难恢复工作情况，确定审计频率。单位应每年至少组织一次内部灾难恢复工作审计。(F3)	检查是否定期对信息系统的灾难恢复工作进行审计，以及审计频率是否是至少一年进行一次。		
		j)应定期开展灾难恢复培训，并根据实际情况进行灾难恢复演练。(F3)	应检查是否有灾难恢复培训记录，是否有相关的灾难恢复演练及其记录。		
		k)应建立灾难备份系统，主备系统实际切换时间应少于60分钟，灾备系统处理能力应不低于主用系统处理能力的50%，通信线路应分别接入主备系统，有条件时可采用主、备系统处理能力相同、轮换交替使用的双系统模式。(F3)	检查金融机构是否建立灾难备份系统，主备系统实际切换时间是否少于 60 分钟，灾备系统处理能力是否不低于主用系统处理能力的 50%。		
12	安全事件处置	a)应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点。	访谈系统运维负责人，询问是否告知用户在发现安全弱点和可疑事件时应进行及时报告。		
		b)应制定安全事件报告和处置管理制度，明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责。	访谈系统运维负责人，询问是否了解本系统已发生的和需要防止发生的安全事件，主要有哪几类，对识别出的安全事件是否根据其对系统的影响程度划分不同等级；检查安全事件定级文档。		
		c)应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分。	检查是否按照信息安全报告制度进行信息通报，一般信息安全事件应逐级通报，发生因人为、自然原因等造成的信息系统瘫痪以及利用计算机实施犯罪等影响和损失较大的信息安全事件(以下简称重大信息安全事件)应直接报金融行业突发事件应急处置指挥部，同时抄报科技主管部门。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		d)应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等。	检查是否在重大信息安全事件发生后，按照金融行业信息安全报告制度报上一级科技部门，并按照相关规定由上级科技部门或本单位决定是否发布预警信息或启动应急预案。		
		e)应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存。	检查安全事件记录分析文档，查看其是否记录引发安全事件的系统弱点，是否分析不同安全事件发生的原因。检查事件报告和响应处理程序，查看其内容是否包括事件的报告流程、响应处理方法等。		
		f)对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。	访谈工作人员，询问其不同安全事件的报告流程；检查安全事件报告和处理程序文档。检查安全事件记录分析文档，查看其是否记录引发安全事件的系统弱点，是否分析不同安全事件发生的原因。		
		g)应建立有效的技术保障机制，确保在安全事件处置过程中不会因技术能力缺乏而导致处置中断或延长应急处置时间。(F3)	访谈安全管理员，检查技术保障机制是否充足、有效，是否可以保障安全事件的处置的顺利进行。		
13	应急预案管理	a)应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括应急组织机构、启动应急预案的条件、应急处理流程、系统恢复流程、**事件信息收集、分析、报告制度**、事后教育和培训等内容，**业务处理系统应急预案的编制工作应由相关业务部门和科技部门共同完成，并由预案涉及的相关机构签字盖章。**	检查应急响应预案文档，查看其内容是否覆盖启动计划的条件、应急处理流程、系统恢复流程和事后教育等内容。访谈工作人员，询问其不同安全事件的报告流程；检查安全事件报告和处理程序文档。		
		b)应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障。	访谈询问金融机构的人力、设备、技术和财力等各方面是否可以有效保障应急预案的执行。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		c)应对系统相关的人员进行应急预案培训，对应急预案的培训应至少每年举办一次。	访谈系统运维负责人，询问是否制定不同事件的应急预案，是否对系统相关人员进行应急预案培训，培训内容是什么，多长时间举办一次；检查应急预案培训记录、演练记录和审查记录。		
		d)在与第三方合作的业务中，应建立并完善内部责任机制和与相关机构之间的协调机制，制定完整的应急预案及应急协调预案，并定期参加联合演练。	检查是否在与第三方合作的业务中，应建立并完善内部责任机制和与相关机构之间的协调机制，制定完整的应急预案及应急协调预案，并定期参加联合演练。		
		e)突发事件应急处置领导小组应统一领导计算机系统的应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业信息安全监管部门。(F3)	检查是否有突发事件应急处置领导小组并统一领导计算机系统的应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源。		
		f)金融机构应急领导小组应及时向新闻媒体发布相关信息，严格按照行业、机构的相关规定和要求对外发布信息，机构内其它部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。(F3)	检查是否金融行业办公厅负责统一向社会发布应急事件公告，其他任何单位或个人不得向社会发布应急事件公告。		
		g)实施报告制度和启动应急预案的单位应当实行重大突发事件 24 小时值班制度。(F3)	实施报告制度和启动应急预案的单位检查是否实行重大突发事件 24 小时值班制度。		
		h)应定期对原有的应急预案重新评估，并根据安全评估结果，定期修订、演练，并进行专项内部审计。(F3)	检查随着信息系统的变更定期对原有的应急预案重新评估的证明文件，以及根据安全评估结果，定期修订完善机房环境、网络和计算机系统等应急预案。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		i)应急演练结束后，金融机构应撰写应急演练情况总结报告，总结报告包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练结论。(F3)	检查金融机构是否定期进行应急演练，是否具有演练记录和演练总结报告，报告的内容是否涵盖演练的人员、演练过程、存在问题和改进措施等内容。		

A.3 第四级信息系统等保检查表

A.3.1 技术类检查表

A.3.1.1 物理安全检查表

序号	类别	测评要求	测评方法	结果记录	符合情况
1	物理位置的选择	a）机房应选择在具有防震、防雷击、**承重**、防风和防雨等能力的建筑内，**应选择交通、通信便捷地区。**	检查机房和办公场地的设计/验收文档，检查机房和办公场地所在的建筑物，查看其是否具有防震(震级需根据机房所在地区的地质环境确定)、防风和防雨等能力的基本条件。		
		b）机房应避开火灾危险程度高的区域，周围100米内不得有加油站、煤气站等危险建筑和重要军事目标。(F4)	1.检查机房是否避开火灾危险程度高的区域， 2.检查机房周围 100 米内是否有加油站、煤气站等危险建筑。		
		c）机房场地应避免设在建筑物的顶层或地下室，以及用水设备的下层或隔壁。	检查机房场地是否避免在建筑物的高层或地下室，以及用水设备的下层或隔壁。		
2	物理访问控制	a）机房出入口应安排专人值守并配置电子门禁系统，控制、鉴别和记录进入的人员。	访谈物理安全负责人，了解具有哪些控制机房进出的机制和电子门禁心态等，检查是否具有对进入机房人员的身份鉴别措施。		
		b）需进入机房的来访人员应经过申请和审批流程，由金融机构专人陪同，并限制和监控其活动范围，**对于重要区域还应限制来访人员携带的随身物品。**	检查机房安全管理制度，查看其是否具有关于外来人员出入机房方面的规定，是否具有来访人员进入机房的审批记录。		

序号	类别	测评要求	测评方法	结果记录	符合情况
		c）应对机房划分区域进行管理，如将机房划分为核心区、生产区、辅助区，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域，**其中核心区是指装有关键业务系统服务器、主要通信设备、网络控制器、通讯保密设备和（或）系统打印设备的要害区域，生产区是指放置一般业务系统服务器、客户端（工作站）等设备的运行区域，辅助区是指放置供电、消防、空调等设备的区域。**	访谈物理安全负责人，是否对机房进行了划分区域管理，是否对各个区域都有专门的管理要求；检查机房区域划分是否合理。		
		d）重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员。	检查是否具有第二道电子门禁系统，是否正常工作（不考虑断电后的工作情况），是否能够鉴别和记录进入人员身份。		
3	防盗窃和防破坏	a）应将主要设备放置在机房内。	检查主要设备是否都放置在机房内。		
		b）应将设备或主要部件放入机柜中进行固定放置并配备安全锁，并设置明显的标签，标注不易除去的标记。	检查设备或设备主要部件的固定情况，是否不易被移动或被搬走，是否设置明显的不易除去的标记。		
		c）应将通信线缆铺设在隐蔽处，可架空铺设在地板下或置于管道中，**强弱电需隔离铺设并进行统一标识。**	检查通信线缆铺设是否在隐蔽处（如铺设在地下或管道中等）。		
		d）应对磁带、光盘等介质分类标识，存储在介质库或档案室的金属防火柜中。	访谈资产管理员，是否对介质进行了分类标识，是否存放在介质库或档案室中；检查介质的管理情况。		
		e）应利用光、电等技术设置机房防盗报警系统，如**安装红外线探测设备等光电防盗设备，一旦发现有破坏性入侵即时显示入侵部位，并驱动声光报警装置。**	检查机房是否具有防盗报警设施，查看其是否正常运行。		
		f）应建立机房设施与场地环境监控系统，进行 24 小时连续监视，并对监视录像进行记录，监控对象包括机房空调、消防、不间断电源（UPS）、门禁系统等重要设备、设施及其所在区域，监控记录至少保	检查机房是否具有摄像、传感等监控报警系统，查看其是否正常运行。		

序号	类别	测评要求	测评方法	结果记录	符合情况
		存 3 个月。(F4)			
4	防雷击	a）机房建筑应设置避雷针等避雷装置。	访谈物理安全负责人，询问采取了哪些防雷措施，机房建筑是否设置了避雷装置，是否通过验收或国家有关部门的技术检测。		
		b）应设置**通过国家认证的**防雷保安器，防止感应雷。	检查是否在电源和信号线上增加有资质的防雷保安器，以避免感应雷击。		
		c）机房应设置交流电源地线。	访谈物理安全负责人，询问机房计算机系统接地是否设置了交流电源地线；检查机房设计/验收文档，是否与实际情况一致。		
5	防火	a）机房应设置有效的自动灭火系统，**能够通过在机房内、基本工作房间内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位应设置烟感、温感等多种方式**自动检测火情、自动报警。	访谈物理安全负责人，询问机房采取了哪些防火措施；检查灭火设备摆放位置是否合理，有效期是否合格。检查机房内、基本工作房间内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位是否设置烟感探测器、温感探测器。		
		b）机房应备有对计算机设备影响小的气体灭火器。(F4)	检查机房是否备有对计算机设备影响小的气体灭火器。		
		c）机房及相关的工作房间和辅助房应采用至少2级耐火等级的建筑材料。(F4)	检查机房及相关的工作房间和辅助房应是否采用至少 2 级耐火等级的建筑材料。		
		d）机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。	检查机房是否采取区域隔离防火措施，将重要设备与其他设备隔离开。		
		e）机房应设置自动消防报警系统（自动和手动两种触发装置齐全），并备有灭火器。消防报警系统应具有与空调系统、新风系统、门禁系统联动的功能，一般工作状态为手动触发。(F4)	检查机房是否设置自动消防报警系统，是否备有一定数量的对计算机设备影响小的气体灭火器。消防报警系统是否有与空调系统、新风系统、门禁系统、UPS 联动的功能，工作状态是否为手动触发。		
		f）机房内所使用的设备线缆应符合消防要求，纸张，磁带和胶卷等易燃物品，要放置于金属制的防火柜内。(F4)	检查机房内所使用的纸张，磁带和胶卷等易燃物品，是否放置于金属制的防火柜内，设备线缆是否符合消防要求。		

序号	类别	测评要求	测评方法	结果记录	符合情况
		g）采用管网式洁净气体灭火系统或高压细水雾灭火系统的主机房，应同时设置两种火灾探测器，且火灾报警系统应与灭火系统联动；凡设置洁净气体灭火系统的主机房，应配置专用空气呼吸器或氧气呼吸器。(F4)	检查采用管网式洁净气体灭火系统或高压细水雾灭火系统的主机房，是否同时设置两种火灾探测器，且火灾报警系统应与灭火系统联动；凡设置洁净气体灭火系统的主机房，是否配置专用空气呼吸器或氧气呼吸器。		
		h）应定期检查消防设施，每半年至少组织一次消防演练。(F4)	检查是否定期检查消防设施，是否每半年至少组织一次消防演练。		
		i）机房应设置二个以上消防逃生通道，同时应保证机房内各分区到各消防通道的道路通畅，方便人员逃生时使用，在机房通道上应设置显著的消防标志。(F4)	检查机房是否设置二个以上消防逃生通道，机房内各分区到各消防通道的道路是否通畅，是否方便人员逃生时使用。在机房通道上是否设置显著的消防标志。		
6	防水和防潮	a）**水管不宜穿过机房屋顶，但若有穿过地板应当采取保护防范措施。**	访谈物理安全负责人，询问机房内是否具有上下水管安装，如果有水管安装是否避免穿过屋顶，如果穿过活动地板是否采取保护防范措施。		
		b）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。	检查机房是否具有对外开放的窗户，如果有窗户是否采取必要的防雨措施；在屋顶和墙壁等是否不存在漏水、渗透和返潮现象，机房及其环境是否不存在明显的漏水和返潮的威胁。		
		c）为便于地下积水的转移，漏水隐患区域地面周围应设排水沟和地漏，当采用吊顶上布置空调风口时，风口位置不宜设置在设备正上方防止水蒸气结露和渗透。	检查机房是否具有除湿装置并能够正常运行，是否具有防止出现机房地下积水的转移与渗透的措施，是否与机房湿度记录情况一致。		
		d）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。	检查是否设置水敏感的检测仪表或元件，对机房进行防水检测和报警，查看该仪表或元件是否正常运行。		
7	防静电	a）设备应采用必要的接地防静电措施。	访谈物理安全负责人，询问机房是否存在静电问题或因静电引起的故障事件，采取了哪些有效防静电措施，主要设备是否采用必要的接地防静电措施；检查机房设计/验收文档，描述内容与实际情况是否一致。		

序号	类别	测评要求	测评方法	结果记录	符合情况
		b）机房应采用防静电地板。	检查机房是否不存在明显的静电现象；是否铺设了防静电地板。		
		c）进入机房应准备鞋套，减少带人机房的灰尘。(F4)	检查进入机房是否准备鞋套。		
		d）应采用静电消除器等装置，减少静电的产生。	如果在静电较强的地区，应检查机房是否了采用了如防静电地板、防静电工作台、以及静电消除剂和静电消除器等措施；应查看使用静电消除剂或静电消除器等的除湿操作记录。		
		e）主机房和辅助区内的工作台面宜采用导静电或静电耗散材料。(F4)	检查主机房和辅助区内的工作台面是否采用导静电或静电耗散材料。		
8	温湿度控制	**a）设备开机时主机房的温、湿度应执行 A 级，基本工作间可根据设备要求按 A，B 两级执行，其他辅助房间应按设备要求确定。**	检查设备开机时主机房的温、湿度是否执行 A 级； 检查基本工作间主机房是否根据设备要求按 A，B 两级执行，其他辅助房间是否按照设备要求确定温度。 A 级：夏天温度 23±1℃、冬天温度 20 ± 2 ℃ ； 夏 冬 开 机 相 对 湿 度 40%~55%；夏冬温湿度变化率< 5℃/h 并不得结露； B 级：全年温度 18~28℃、全年开机相对湿度 35%~75%、全年温度变化率< 10℃/h 并不得结露。		
		b）机房应采用专用空调设备，空调机应带有通信接口，通信协议应满足机房监控系统的要求。(F4)	检查机房是否采用专用空调设备，空调机是否带有通信接口，通信协议是否满足机房监控系统的要求，显示屏是否有汉字显示。		
		c）空调设备中安装的电加热器和电加湿器应有防火护衬，并尽可能使电加热器远离用易燃材料制成的空气过滤器。(F4)	检查空调设备中安装的电加热器和电加湿器是否有防火护衬，是否使电加热器远离用易燃材料制成的空气过滤器。		
		d）安装在活动地板上及吊顶上的送风口、回风口应采用难燃材料或非燃材料。(F4)	检查安装在活动地板上及吊顶上的送风口、回风口是否采用难燃材料或非燃材料。		
		e）采用空调设备时，应设置漏水报警装置，并设置防水小堤，还应注意冷却塔、泵、水箱等供水设备的防冻、防火措施。(F4)	检查采用空调设备时，是否设置漏水报警装置，是否设置防水小堤，查看了解冷却塔、泵、水箱等供水设备的防冻、防火措施。		

序号	类别	测评要求	测评方法	结果记录	符合情况
9	电力供应	**a）计算机系统供电应与其他供电分开。(F4)**	检查计算机系统供电是否与其他供电分开。		
		b）应在机房供电线路上设置稳压器和过电压防护设备。	访谈物理安全负责人，询问是否出现过电压不稳现象，计算机系统供电线路上是否设置了稳压器和过电压防护设备；检查机房，查看计算机系统供电线路上的稳压器、过电压防护设备是否正常运行，查看供电电压是否正常。		
		c）应按照双路供电的原则设置冗余或并行的电力电缆线路为计算机系统供电。	访谈物理安全负责人,询问是否安装了冗余或并行的电力电缆线路（如双路供电方式),如何进行双路供电切换，切换时是否能够对计算机系统正常供电。		
		d）应建立发电机等备用供电系统（如备用发电机），以备临时供电系统停电时启用，并确保备用供电系统能在UPS供电时间内到位，每年需进行备用供电系统的模拟演练，并定期对备用电力供应设备进行检修和维护，确保其能正常使用。	访谈物理安全负责人,是否建立备用供电系统（如备用发电机)。		
		e）UPS供电系统的冗余方式应采用N+1、N+2、2N、2(N+1) 等方式，负载功率小于单机UPS额定功率的80%，并通过两路独立市电提供UPS输入，UPS后备时间至少2小时。核心区域、重要设备应由不同的UPS提供双回路供电。(F4)	1.检查UPS供电系统是否采用N+1、N+2、2N、2(N+1) 等方式，负载功率是否小于单机 UPS 额定功率的65%，并检查是否通过两路独立市电提供UPS输入。 2.对于没有建立柴油发电机应急供电系统的单位，UPS后备时间至少2小时。 3.机房核心区域、重要设备应由不同的UPS提供双回路供电。		
		f）机房内要求采用机房专用插座，机房内分别设置维修和测试用电源插座，两者应有明显区别标志。市电、UPS 电源插座分开，满足负荷使用要求。(F4)	检查机房内是否采用机房专用插座，机房内是否设置维修和测试用电源插座，两者是否有明显区别标志。市电、UPS电源插座是否分开，是否满足负荷使用要求。		
		g）计算机系统应选用铜芯电缆，避免铜、铝混用。若不能避免时，应采用铜铝过渡头连接。(F4)	计算机系统是否选用铜芯电缆，避免铜、铝混用。若不能避免时，是否采用铜铝过渡头连接。		

序号	类别	测评要求	测评方法	结果记录	符合情况
		h）机房应设置应急照明和安全出口指示灯，供配电柜（箱）和分电盘内各种开关、手柄、按钮应标志清晰，防止误操作。(F4)	检查机房是否设置应急照明和安全出口指示灯，供配电柜（箱）和分电盘内各种开关、手柄、按钮是否标志清晰，是否可以防止误操作。		
10	电磁防护	a）应采用接地方式防止外界电磁干扰和设备寄生耦合干扰。	访谈物理安全负责人，询问是否具有防止外界电磁干扰和设备寄生耦合干扰的措施，是否出现过因电磁防护问题引发的安全事件，检查机房设备外壳是否具有安全接地。		
		b）电源线和通信线缆应隔离，避免互相干扰。	检查机房布线，查看是否做到电源线和通信线缆隔离。		
		c）应对关键区域**和重要设备**以及磁介质实施电磁屏蔽。	访谈物理安全负责人，询问是否具有处理或者存储秘密级信息的设备或介质，设备是否为低辐射设备，设备与磁介质是否采取了必要的电磁屏蔽措施。检查关键设备与磁介质是否存放在具有电磁屏蔽功能的容器中。 如对关键区域采用了电子屏蔽，应检查其设备运行时是否开启了电子屏蔽装置；如果安装了屏蔽机房，应检查进入机房的电源线和非光纤通信线是否经过滤波器，光纤通信线是否经过波导管，机房门是否及时关闭，屏蔽机房是否定期测试电磁泄露，应查看电磁泄露测试报告。		
		d）计算机系统设备网络布线不得与空调设备、电源设备的无电磁屏蔽的布线平行；交叉时，应尽量以接近于垂直的角度交叉，并采取防延燃措施。(F4)	计算机系统设备网络布线是否与空调设备、电源设备的无电磁屏蔽的布线平行；交叉时，是否尽量以接近于垂直的角度交叉，是否采取防延燃措施。		

A.3.1.2 网络安全检查表

序号	类别	测评内容	测评方法	结果记录	符合情况
1	结构安全	a）应保证**主要网络设备和通信线路**冗余，**主要网络设备业务处理能力**能满足业务高峰期**需要的2倍以上，双线路设计时，宜由不同的服务商提供。**	访谈网络管理员，询问信息系统网络设备的处理性能能否满足目前业务高峰流量情况，询问采用何种手段对主要网络设备进行运行状况监控。		
		b）应保证网络各个部分的带宽满	访谈网络管理员，询问网络各个部		

序号	类别	测评内容	测评方法	结果记录	符合情况
		足业务高峰期需要。	分的带宽是否满足业务高峰的需要，如果无法满足，则需要在主要网络设备上进行带宽配置，若有网管系统或流量监控系统，查看网络和核心网络的带宽占用报表是否有达到或超过处理能力记录。		
		c）应在业务终端与业务服务器之间进行路由控制建立安全的访问路径。	业务终端 trace 业务服务器地址，查看访问路径所经节点是否安全可靠。		
		d）应绘制与当前运行情况相符的网络拓扑结构图。	查看网络拓扑结构图与当前运行情况是否一致。		
		e）应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段，**生产网、互联网、办公网之间都应实现有效隔离。**	1、查网络设计/验收文档，查看是否有根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，2、登录核心交换机，show vlan brief 查看 vlan 划分、show int vlan X 详细查看某个具体 vlan 情况。		
		f）应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段。	检查是否将重要网段部署至网络边界与外部信息系统直连，重要网段与其他网段间是否使用防火墙、访问控制等手段隔离。		
		g）应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。	1、登录下联路由器，show run，查看是否有 qos 策略并应用到相应端口；2、登录交换机，show run，查看是否有 acl 对流量分类、是否对分类流量打标、是否应用到相应端口。		
		h）应使用前置设备实现跨行联网系统与入网银行业务主机系统的隔离，防止外部系统直接对入网银行业务主机的访问和操作。(F4)	检查是否使用前置设备实现跨行联网系统与入网银行业务主机系统的隔离，防止外部系统直接对入网银行业务主机的访问和操作。		
		i）应使用专用网络用于入网银行与信息交换中心的联网，与公用数据网络隔离。(F4)	检查是否采用专用网络用于入网银行与信息交换中心的联网，与公用数据网络隔离。		
		j)机构应至少通过两条主干链路接入跨行交易交换网络，并可根据实际情况选择使用专用的通信链路。两条主干链路应具有不同的路由，当一条链路发生异常时，另一条链路应能承载全部的交易数据。(F4)	1.检查被测机构是否通过两条主干链路接入跨行交易交换网络，并根据实际情况选择使用 DDN、FR 或其它方式的通信链路。 2.检查两条主干链路是否具有不同的路由，当一条链路发生异常时，另一条链路能承载全部的交易		

序号	类别	测评内容	测评方法	结果记录	符合情况
			数据。		
2	访问控制	a) 应在网络边界部署访问控制设备，启用访问控制功能。	登录网络设备，show run，查看是否有相应访问控制列表。		
		b) 应不允许数据带通用协议通过。	应测试边界和主要网络设备，可通过发送带通用协议的数据（如使用http隧道工具），测试访问控制措施是否有效阻断这种连接。		
		c) 应根据数据的敏感标记允许或拒绝数据通过。	访谈网络管理员，是否对敏感标记的数据有相关的访问控制策略。		
		d)应不开放远程拨号访问功能。	应检查是否屏蔽了远程拨号访问功能。		
		e) 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。	登录网络设备，show run，查看方位控制列表是否精确至host。		
		f) 应在网络区域边界(互联网区域边界、外部区域边界和内部区域边界)**对**网络最大流量数**及网络并发连接数进行监控。**	查看是否有端口带宽限制，防火墙是否设置最大并发连接数。		
		g) 网络设备应按最小安全访问原则设置访问控制权限。(F4)	访谈网络管理员，询问网络设备的配置原则如何设置，是否是最小原则。		
3	安全审计	a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。	登录网络设备，1、show snmp 查看是否配置 snmp 进行网络设备运行状况记录 ；、show logging 、2、show ip netflow export 查看是否配置网络流量记录；3、show aaa meth accounting 查看是否配置用户行为记录。		
		b)审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	登录日志服务器为或AAA服务器，查看记录是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。		
		c)应能够根据记录数据进行分析，并生成审计报表。	询问日志服务器或 AAA 服务器是够具备生成报表功能，若有登录并现场生成。		
		d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等，**保存时间不少于一年**。	应检查边界和主要网络设备，查看其审计跟踪设置是否定义了审计跟踪极限的阈值，当存储空间被耗尽时，能否采取必要的保护措施，例如，是否报警并导出、丢弃未记录的审计信息、暂停审计或覆盖以		

序号	类别	测评内容	测评方法	结果记录	符合情况
			前的审计记录等。		
		e)应定义审计跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施，防止审计数据丢失。	应检查边界和主要网络设备，查看其存储空间被耗尽时是否可终止审计事件的发生。		
		f)应根据信息系统的统一安全策略，实现集中审计，时钟保持与时钟服务器同步。	应访谈安全管理员和系统管理员，是否有统一安全策略，是否有集中审计功能且时钟应与时钟服务器保持同步。		
4	边界完整性检查	a)应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。	登录业务网非法外联监控管理服务器，查看是否有未安装非法外联客户端的计算机接入网络，若有是否采取进行定位、阻断。		
		b)应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。	登录业务网非法外联监控管理服务器，查看是否有非法外联行为记录，若有是否采取措施进行定位、阻断。		
5	入侵防范	a)应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、注入式攻击、IP 碎片攻击和网络蠕虫攻击等。	查看其是否有在网络边界及核心业务网段处有对网络攻击采取相关措施。		
		b)当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警及自动采取相应动作。	1)查看对网络攻击事件是否采用报警。 2)采用何种报警方式。		
		c)入侵检测的管理系统应做到分级管理，对系统的部署做到逐级分布。(F4)	检查入侵检测的管理系统是如何管理的，对系统的部署是否逐步分布。		
6	恶意代码防范	a)应在**与外单位与互联网连接的**网络边界处对恶意代码进行检测和清除。	登录边界网络设备，查看是否根据恶意代码特征采取措施从网络层进行检测和清除。		
		b) 应定期对恶意代码防护设备进行代码库升级和系统更新。	登录防病毒服务器，查看病毒库升级情况、客户端病毒定义码升级情况。		
7	网络设备防护	a)应对登录网络设备的用户进行身份鉴别。	是否对网络设备进行 AAA 认证或其他认证方式，若有登录 AAA 服务器，查看用户与管理员身份、权限是否匹配。		
		b)应对网络设备的管理员登录地址进行限制。	登录网络设备，show run，查看是否在网络设备上是否采用相应 acl 限制管理员登录；2、登录 AAA 服务器，查看是否进行管理员地址限		

序号	类别	测评内容	测评方法	结果记录	符合情况
			制。		
		c)网络设备用户的标识应唯一。	访谈网络设备管理员，询问其各个网络设备用户的标识信息。		
		d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。	查看登录网络设备的认证方式的种类，一般有用户名和密码组合认证、动态口令、指纹识别认证、数字证书认证等，要求两种或两种以上。		
		e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换。	应访谈网络管理员，询问网络设备的口令策略是什么。		
		f)网络设备用户的身份鉴别信息至少应有一种是不可伪造的。	访谈网络设备管理员并查看是否有 2 种身份鉴别信息，且至少有一项是不可伪造的。		
		g)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。	采用错误密码登录网络设备数次，观察是否结束会话、限制非法登录次数，并观察如果登录后长时间不操作会不会被系统退出。		
		h)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	远程登录网络设备，看是否采用 22 端口 SSH 方式或其他加密方式。		
		i)应实现设备特权用户的权限分离。	登录网络设备，show run｜b user，查看定义只有查看权限 level 3 的审计用户和具有管理权限的 level 15 用户。		
		j)对网络设备系统自带的的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端口开放审批制度。(F4)	检查网络设备是否关闭不必要的网络设备服务端口，并查看审批制度文件。		
		k) 应每季度检验网络设备软件版本信息，并通过有效测试验证进行相应的升级。(F4)	检查网络设备是否每周检验网络设备软件版本信息。		
		l) 应建立网络设备的时钟同步机制。(F4)	访谈网络管理员，询问是否建立了网络设备的时钟同步机制。		
		m) 应每月对网络设备的配置文件进行备份，发生变动时应及时备份。(F4)	访谈网络管理员，询问对网络设备配置是否进行备份，备份的周期和方式是什么。		
		n)应每季度检查并锁定或撤销网络设备中多余的用户账号。(F4)	1 登录网络设备，show run ｜ b user，查看设立账户是否与管理员一一对应； 2 若有网络日志服务器或 AAA 服务器，查看管理员变动相应时段是否		

序号	类别	测评内容	测评方法	结果记录	符合情况
			有相关操作记录。		

A.3.1.3 主机安全检查表

序号	类别	测评项	测评方法	结果记录	符合情况
1	身份鉴别	a）应对登录操作系统和数据库系统的用户进行身份标识和鉴别。	可访谈系统管理员/数据库管理员，询问操作系统的身份标识与鉴别机制采取何种措施实现，目前系统提供了哪些身份鉴别措施和鉴别失败处理措施。		
		b）操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，系统的静态口令应在8位以上并由字母、数字、符号等混合组成，至少每月更换口令一次。	应检查主要服务器操作系统和主要数据库管理系统，查看是否提供了身份鉴别措施（如用户名和口令等），其身份鉴别信息是否具有不易被冒用的特点，例如，口令足够长，口令复杂（如规定字符应混有大、小写字母、数字和特殊字符），口令生命周期，新旧口令的替换要求（如规定替换的字符数量）或为了便于记忆使用了令牌。		
		c）应启用登录失败处理功能，可采取结束会话、限制登录间隔、限制非法登录次数和自动退出等措施。	应检查主要服务器操作系统和主要数据库管理系统，查看是否已配置了鉴别失败处理功能，并设置了非法登录次数的限制值，对超过限制值的登录终止其鉴别会话或临时封闭帐号；查看是否设置网络登录连接超时，并自动退出；查看是否设置鉴别警示信息。		
		d）应设置鉴别警示信息，当出现越权访问或尝试非法访问时，系统会自动提示未授权访问。	应检查主要服务器操作系统和主要数据库管理系统，查看其是否设置警示信息。		
		e）主机系统应对与之相连的服务器或终端设备进行身份标识和鉴别，当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。(F4)	应检查主要服务器操作系统，查看服务器操作系统是否对与之相连的服务器或终端设备进行身份标识和鉴别并进行了相应的加密。		
		f）应为操作系统和数据库的不同用户分配不同的用户名，确保用户名具有唯一性。	应测评主要服务器操作系统和主要数据库管理系统，添加一个新用户，其用户标识为系统原用户的标识（如用户名或UID），查看是否不会		

序号	类别	测评项	测评方法	结果记录	符合情况
		数据库管理员只具备数据库的运维管理权限。	是否设置了相互制约关系（如系统管理员、安全管理员等不能对审计日志，安全审计员管理不了审计数据的开启、关闭、删除等重要事件的审计日志等）。		
		e） 应禁用或严格限制默认账户的访问权限，重命名系统默认账户，并修改这些账户的默认口令。	应查看主要服务器操作系统和主要数据库管理系统，查看匿名/默认用户的访问权限是否已被禁用或者严格限制（如限定在有限的范围内）。		
		f）应及时删除多余的、过期的账户，避免共享账户的存在。	应查看是否有多余、过期、共享账户的存在。		
4	可信路径	a）**对通过互联网远程访问操作系统、数据库系统的用户进行身份鉴别时，**系统与用户之间应能够建立一条安全的信息传输路径。	应访问系统管理员和安全管理员，在系统对用户进行身份鉴别时是否在系统与用户之间建立了安全的信息传输路径。		
		b）在用户**通过互联网远程访问操作系统、数据库系统时**，系统与用户之间应能够建立一条安全的信息传输路径。	应访问系统管理员和安全管理员，在用户对系统进行身份鉴别时是否在系统与用户之间建立了安全的信息传输路径。		
5	安全审计	a)审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。	可访谈安全审计员，询问主机系统是否设置安全审计；询问主机系统对事件进行审计的选择要求和策略是什么；对审计日志的处理方式有哪些。		
		b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用、**账号的分配、创建与变更、审计策略的调整、审计系统功能的关闭与启动**等系统内重要的安全相关事件。	应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、系统资源的异常使用、重要系统命令的使用（如删除客体）等。		
		c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等，**并定期备份审计记录，保存时间不少于一年。**	应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）、事件的结果		

序号	类别	测评项	测评方法	结果记录	符合情况
			等内容。		
		d）应能够根据记录数据进行分析，并生成审计报表。	应检查主要服务器和重要终端操作系统，查看是否为授权用户浏览和分析审计数据提供专门的审计工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表。		
		e）应保护审计进程，避免受到未预期的中断。	应测评主要服务器操作系统、重要终端操作系统和主要数据库管理系统，可通过非法终止审计功能或修改其配置，验证审计功能是否受到保护。		
		f）应保护审计记录，避免受到未预期的删除、修改或覆盖等。	应测评主要服务器操作系统、重要终端操作系统和主要数据库管理系统，在系统上以某个系统用户试图删除、修改或覆盖审计记录，测评安全审计的保护情况与要求是否一致。		
		g）应能够根据信息系统的统一安全策略，实现集中审计。	应与系统管理员/数据库管理员访谈，并检查是否有统一的安全策略，是否实现了集中审计。		
6	剩余信息保护	a）应保证操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他**使用人员**前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。	应与系统管理员/数据库管理员访谈，询问操作系统用户/数据库管理员用户的鉴别信息存储空间，被释放或再分配给其他用户前是否得到完全清除；系统内的文件、目录等资源所在的存储空间，被释放或重新分配给其他用户前是否得到完全清除。		
		b）应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他**使用人员**前得到完全清除。	应检查主要操作系统和主要数据库管理系统维护操作手册，查看是否明确用户的鉴别信息存储空间，被释放或再分配给其他用户前的处理方法和过程；文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前的处理方法和过程。		

序号	类别	测评项	测评方法	结果记录	符合情况
7	入侵防范	a）应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。	应与系统管理员访谈，询问主机系统是否采取入侵防范措施，入侵防范内容是否包括主机运行监视、资源使用超过值报警、特定进程监控、入侵行为检测、完整性检测等方面内容。		
		b）应能够对重要程序完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施**或在检测到完整性即将受到破坏时进行事前阻断。**	应测评主要服务器系统，试图破坏重要程序（如执行系统任务的重要程序）的完整性，验证主机能否检测到重要程序的完整性受到破坏。		
		c）操作系统遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器、系统软件预防性维护服务等方式保持系统补丁及时得到更新。	应与系统管理员访谈，询问入侵防范产品的厂家、版本和在主机系统中的安装部署情况；询问是否进行过部署的改进或者更换过产品，是否按要求（如定期或实时）进行产品升级。		
8	恶意代码防范	a）应安装**国家安全部门认证的正版**防恶意代码软件，**对于依附于病毒库进行恶意代码查杀的软件**应及时更新防恶意代码软件版本和恶意代码库，**对于非依赖于病毒库进行恶意代码防御的软件，如主动防御类软件，应保证软件所采用的特征库有效性与实时性，对于某些不能安装相应软件的系统可以采取其他安全防护措施来保证系统不被恶意代码攻击。**	应访谈系统安全员，询问主机系统是否采取恶意代码实时检测与查杀措施，恶意代码实时检测与查杀措施的部署情况如何，因何改进过部署或者更换过产品，是否按要求（如定期或实时）进行产品升级，是否采取其他安全防护措施保证系统不被恶意代码攻击。		
		b)主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库。	应检查主要服务器系统和主要终端系统，查看是否安装实时检测与查杀恶意代码的软件产品，查看实时检测与查杀恶意代码的软件产品是否支持恶意代码防范的统一管理功能，查看检测与查杀恶意代码软件产品的厂家、版本号和恶意代码库名称。		

序号	类别	测评项	测评方法	结果记录	符合情况
		c）应支持恶意代码防范的统一管理。	应检查网络防恶意代码产品，查看厂家、版本号和恶意代码库名称等信息是否统一管理。		
		d）应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。(F4)	检查如何对网络内计算机病毒进行监控，是否建立了病毒监控中心。		
9	资源控制	a）应通过设定终端接入方式、网络地址范围等条件限制终端登录。	应检查主要服务器操作系统，查看是否限制单个用户的多重并发会话数量；查看是否设置登录终端的操作超时锁定和鉴别失败锁定，以及是否规定解锁或终止方式；查看是否配置了终端接入方式、网络地址范围等条件限制终端登录。		
		b）应根据安全策略设置登录终端的操作超时锁定。	应测评主要服务器操作系统，任选一个用户，登录服务器，在一定时间内不进行任何动作，验证主要服务器操作系统能否对操作超时的终端进行锁定；任选一个用户，可通过多次失败登录服务器，验证服务器能否对鉴别失败的终端进行锁定，锁定后能否按照规定的解锁或终止方式进行解锁或终止。		
		c）应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况。	应检查主要服务器操作系统，查看是否对一个时间段内可能的并发会话连接数进行限制，是否禁止同一用户账号在同一时间内并发登录，是否限制单个用户对系统资源（如CPU、内存和硬盘等）的最大或最小使用限度。		
		d）应限制单个用户对系统资源的最大或最小使用限度。	应检查主要服务器操作系统，查看是否在服务水平降低到预先规定的最小值时，能检测和报警，报警的方式有哪些，能否已根据安全策略设定主体（如进程）的服务优先级，并根据优先级分配系统资源，保证优先级低的主体处理能力不会影响到优先级高的主体的处理能力。		
		e）**应定期对系统的性能和容量进行规划**，能够对系统的服务水平降低到预先规定的最小值进行检测	应测评主要服务器操作系统，试图使服务水平降低到预先规定的最小值，验证系统能否正确检测和报警。		

序号	类别	测评项	测评方法	结果记录	符合情况
		和报警。			
		f）所有的服务器应全部专用化，不使用服务器进行收取邮件、浏览互联网操作。(F4)	检查所有服务器是否是全部专用化，是否使用服务器进行收取邮件、浏览互联网操作。		

A.3.1.4 应用安全检查表

序号	类别	测评项	测评方法	结果记录	符合情况
1	身份鉴别	a）应提供专用的登录控制模块对登录用户进行身份标识和鉴别。	询问系统管理员，该系统是否提供专用的登录控制模块对登录的用户进行身份标识和鉴别，采用何种方式对用户进行身份标识和鉴别。 检查应用系统，身份标识和鉴别的方式是否与管理员回答的一致。 以某注册用户身份登录系统，查看登录是否成功；以非法用户身份登录系统，查看登录是否成功。		
		b）应对同一用户**的关键操作**采用两种或两种以上组合的鉴别技术实现用户身份鉴别其中一种是不可伪造的；**如使用磁卡、IC 卡、动态密码卡、动态口令设备、手机短信动态密码、指纹识别等方式加强鉴别。**	询问系统管理员，该系统是否采用了两个及两个以上身份鉴别技术的组合来进行身份鉴别。 如果是，查看身份鉴别技术是什么？是否与回答一致。		
		c)应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。	询问系统管理员，该系统的用户身份标识是否唯一。采取了什么措施防止身份鉴别信息被冒用。 检查总体规划/设计文档，查看其是否有系统采取了唯一标识的说明。 查看其身份鉴别信息是否具有不易被冒用的特点。 询问系统管理员，该系统是否有专门的设置保证用户身份鉴别信息不易被冒用，如果应用系统采用口令进行身份鉴别，则查看是否有选项或设置强制要求口令长度、复杂度、定期修改等。 如果应用系统式以用户名来保证用户身份标识的唯一性，则以已有的用户名重新注册，测试系统是否禁		

序号	类别	测评项	测评方法	结果记录	符合情况
			止该操作。 扫描应用系统，测试其鉴别信息复杂度检查功能，检查系统是否不允许存在弱口令、空口令等。		
		d)应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。	询问系统管理员，该系统是否具有登录失败处理的功能（如结束会话、限制非法登录次数，当登录连接超时，自动退出等），是如何进行处理的? 如果有登录失败处理设置选项或模块，查看系统是否设置或选中了该功能。 根据应用系统使用的登录失败处理方式，采用如下方法之一或全部进行测试： 以错误的用户名或密码登录系统，查看系统反应。 以超过系统规定的非法登录次数登录系统，查看系统反应。 登录系统连接超时，查看系统反应。		
		e)应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。	询问系统管理员，该系统的身份鉴别、身份标识唯一性检查、鉴别信息复杂度检查以及登录失败处理功能是否有专门的模块或选项，是否有相关参数需要配置。 如果有参数需要配置，则查看实际配置情况，是否已经启用上述功能。		
		f)应用软件应能在指定的闲置时间间隔到期后，自动锁定客户端的使用。(F4)	检测应用软件客户端在指定闲置时间到期后是否自动锁定。		
		g)系统应强制客户首次登录时修改初始密码。(F4)	应测评系统初始密码是否在首次登录时被要求强制修改。		

序号	类别	测评项	测评方法	结果记录	符合情况
		h) 修改密码时，不允许新设定的密码与旧密码相同。(F4)	应测评修改密码是否不能修改成与前次相同的密码。		
2	安全标记	**应**提供为主体和客体设置安全标记的功能并在安装后启用。	应访谈系统管理员并检查，是否设置了主体和客体的安全标记，是否已经启用了安全标记的相关功能。		
3	访问控制	a)应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问。	询问系统管理员，该系统是否提供访问控制功能，访问控制策略是什么？访问控制的粒度是否达到文件、数据库表？ 检查应用系统的访问控制功能和策略配置是否与管理员回答的一致。 以某一用户身份登录系统，依据安全策略对客体进行访问，测试是否成功。该用户不依据安全策略对客体进行访问，测试是否成功。		
		b)自主访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作。	访谈系统管理员，询问系统访问控制策略是否覆盖到与信息安全直接相关的主体、客体及它们之间的操作？ 检查应用系统的访问控制策略是否覆盖到与信息安全直接相关的所有主体、客体及它们之间的操作。		
		c)应由授权主体配置访问控制策略，并禁止默认帐户的访问。	询问系统管理员，该系统是否有由授权主体配置访问控制策略的功能。 如果系统有由授权主体配置访问控制策略的功能，则以该授权主体用户登录系统，查看某特定用户的权限。以该用户身份登录系统，进行在权限范围内和权限范围外的一些操作，查看是否成功。 以该授权主体用户登录系统，修改上述特定用户的权限。以该用户身份登录系统，查看该用户的权限是否与刚修改过的权限保持一致，验证用户权限管理功能是否有效。 询问系统管理员，该系统是否有默		

序号	类别	测评项	测评方法	结果记录	符合情况
			认用户，如果有，是否禁止了默认账户。		
		d)应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。	访谈系统管理员，询问系统所有帐户是否只拥有完成自己承担任务所需的最小权限，相互之间是否形成相互制约关系。 检查应用系统，查看不同帐户的权限是否分离（如管理员不能审计、审计员不能管理、安全员不能审计和管理等、审计员不能修改自己的行为日志等）。权限之间是否相互制约。 以管理员身份进行审计操作，查看是否成功。以审计员身份进行删除/增加用户、设定用户权限的操作（也可进行一些其他管理员进行的操作），查看是否成功。 以拥有其他权限的用户身份登录，查看其权限是否受到限制。		
		e）应有生产系统内关键账户与权限的关系表。(F4)	检查是否建立账户权限关系表，是否明确说明账户类别以及其具有的权限范围。		
		f） **宜**具有对重要信息资源设置敏感标记的功能。	检查目标系统，查看系统是否具有对重要信息资源设置敏感标记的功能？如果有，则验证该功能是否有效。		
		g)**宜**通过比较安全标记来确定是授予还是拒绝主体对客体的访问。	访谈系统管理员，并检查是否对主体和客体的安全标记有相关的访问控制列表等控制策略。		
4	可信路径	a)在应用系统对用户进行身份鉴别时，应能够建立一条安全的信息传输路径。	应检查应用系统文档，查看系统提供了哪些可信路径功能； 应检查应用系统，查看文档声称的可信路径功能是否有效； 应访谈安全管理员，询问在什么情况下起用可信路径进行初始登录和/或鉴别；目前系统提供了哪些可信路径。		

序号	类别	测评项	测评方法	结果记录	符合情况
		b)在用户通过应用系统对资源进行访问时，应用系统应保证在被访问的资源与用户之间应能够建立一条安全的信息传输路径。	应检查数据库管理系统文档，查看系统提供了哪些可信路径功能； 应检查主要数据库管理系统，查看文档声称的可信路径功能是否有效。		
5	安全审计	a)应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计。	访谈安全审计员，询问是否有安全审计功能，对事件进行审计的选择要求和策略是什么。 检查应用系统的审计策略（审计记录），查看审计策略（或记录）是否覆盖到每个用户。都对哪些安全事件进行审计。 多次以任意用户身份登录系统，进行一些操作，包括重要的安全相关操作或事件（如用户标识与鉴别、自主访问控制的所有操作记录（如用系统管理员身份改变用户权限，增加或删除用户），用户的行为（如删除数据、多次登录失败等））。 用审计人员的身份登录系统，查看系统对上述用户的重要操作或事件是否进行审计。		
		b)应保证无法单独中断审计进程，**不提供**删除、修改或覆盖审计记录**的功能**。	访谈安全审计员，询问应用系统对审计日志的处理方式有哪些。 以普通用户身份试图删除、修改或覆盖自身的审计记录，查看能否成功。试图删除、修改其他人的审计记录，查看能否成功。 如果审计记录能够导入，则导出审计记录并进行修改后导入系统，查看能否覆盖以前的审计记录。		
		c)审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等，**并定期备份审计记录，保存时间不少于一年。**	以审计员身份登录系统，检查审计记录内容是否包括事件发生的日期、时间、发起者信息、事件类型、事件相关描述信息、事件的结果等。		
		d)应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。	检查应用系统，查看其是否为授权用户浏览和分析审计数据提供专门的审计工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等）。 检查应用系统是否能够生成审计报表。		

序号	类别	测评项	测评方法	结果记录	符合情况
		e)应根据系统统一安全策略，提供集中审计接口。	检查系统是否依据统一的安全策略提供审计功能。 检查系统是否对审计功能进行集中审计。		
		f）对于从互联网客户端登陆的应用系统，应在每次用户登录时提供用户上一次成功登录的日期、时间、方法、位置等信息，以便用户及时发现可能的问题。(F4)	检查客户端登录时是否可以提供户上一次成功登录的日期、时间、方法、位置、错误登录等信息。		
6	剩余信息保护	a)应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。	访谈系统管理员，询问系统是否采取措施保证对存储介质中的残余信息进行删除，采取什么具体措施。		
		b)应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。	如果鉴别信息存放在文件中，则用另一个用户登录查看能否读取用户信息。如果用户的鉴别信息存放在数据库中，则通过用户界面或其他方式能否获取系统鉴别信息。		
7	通信完整性	a)应采用密码技术保证通信过程中数据的完整性。	询问安全管理员应用系统是否有数据在传输过程中进行完整性保证的操作，具体采取什么措施。 应检查设计/验收文档，查看其是否有通信完整性的说明，如果有则查看是否采用校验码技术保证通信完整性。		
8	通信保密性	a)在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证。	询问安全管理员系统在通信双方建立连接之前采用什么技术进行会话初始化验证。 应检查设计/验收文档，查看其是否有通信保密性的说明，如果有则查看是否有利用密码技术进行通信会话初始化验证的说明。		

序号	类别	测评项	测评方法	结果记录	符合情况
		b)应对通信过程中的**敏感数据**进行加密，**对于通过互联网对外提供服务的系统，应对通信过程中的整个报文或会话过程进行加密，如采用 SSL 协议，最低需达到 128 位的加密强度。**	询问安全管理员应用系统的敏感信息字段在通信过程中是否采取保密措施，具体采取什么措施。 应检查设计/验收文档，查看其是否有通信保密性的说明，如果有则查看是否有对通信过程中的敏感信息字段进行加密的说明。		
		c)应基于硬件化的设备对重要通信过程进行加解密运算和密钥管理。	检查是否采用硬件设备对重要通信进行加解密以及密钥管理。		
9	抗抵赖	a)应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能，**原发证据包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录，交易系统还应能够详细记录用户合规交易数据，如业务流水号、账户名、IP 地址、交易指令等信息以供审计，并能够追溯到用户。**	访谈安全员，询问系统是否具有抗抵赖的措施，具体措施有哪些。 测试应用系统，通过双方进行通信，查看系统是否提供在请求的情况下为数据原发者提供数据原发证据的功能。		
		b)应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能，**接受证据应用系统操作与管理记录至少应包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录，交易系统还应能够详细记录用户合规交易数据，如业务流水号、账户名、IP 地址、交易指令等信息以供审计，并能够追溯到用户。**	访谈安全员，询问系统是否具有抗抵赖的措施，具体措施有哪些。 测试应用系统，通过双方进行通信，查看系统是否提供在请求的情况下为数据接收者提供数据原发证据的功能。		
10	软件容错	a)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。	访谈管理员，询问是否有保证软件具有容错能力的措施，具体采取哪些措施。 在应用终端输入不同（如数据格式或长度等符合、不符合软件设定的要求）的数据，包括登录标识与鉴别数据、其他操作数据等，查看系统的反应。		

序号	类别	测评项	测评方法	结果记录	符合情况
		b)应提供自动保护功能，当故障发生时自动保护当前所有状态。	询问管理员应用系统是否发生过故障，故障发生时是否能够继续提供一部分功能保证实施必要的措施。		
		c)应提供自动恢复功能，当故障发生时立即自动启动新的进程，恢复原来的工作状态。	检查系统是否有自动恢复功能，当系统出错时能自动启动进程恢复原来的工作状态。		
		d）应能够有效屏蔽系统技术错误信息，不将系统产生的错误信息直接反馈给客户。(F4)	检查是否能够有效屏蔽系统技术错误信息，不将系统产生的错误信息直接反馈给客户。		
11	资源控制	a） **对于有会话或短连接的应用系统**，当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话。	询问业务系统是否有资源控制的措施，具体措施有哪些。 登录应用系统服务器，查看应用系统属性是否设置了连接超时限制。		
		b)应能够对系统的最大并发会话连接数进行限制。	询问管理员应用系统同时最多支持多少个并发会话连接？是否有限制? 登录应用系统服务器，查看系统是否设置了参数限制最大并发会话连接数。		
		c） **对于有会话的应用系统，**应能够对单个帐户的多重并发会话进行限制。	询问管理员单个帐户同时可以发起多少个并发会话，是否有限制? 登录应用系统服务器，查看系统是否对单个帐户的多重并发会话进行限制。 以超过单个帐户规定的并发会话连接数连接系统，测试能否成功。		

序号	类别	测评项	测评方法	结果记录	符合情况
		d）应能够对一个时间段内可能的并发会话连接数进行限制。	询问管理员是否对一个时间段内可能的会话连接数进行限制 检查应用系统是否有对一段时间内可能的并发会话连接数进行限制。 在一个时间段内以超过设定的并发会话连接数连接系统，测试能否连接成功。		
		e)宜能够对**系统占用的资源设定限额，超出限额时给出提示信息**。	访谈管理员，询问应用系统是否对访问用户或请求进程占用的资源分配最大和最小限额。 检查应用系统，是否对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额。		
		f)应能够对系统服务水平降低到预先规定的最小值进行检测和报警。	检查应用系统，查看是否有服务水平最小值的设定（当系统的服务水平降低到预先设定的最小值时，系统是否报警）。		
		g)应提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。	访谈管理员，询问应用系统是否能根据安全策略设定主体的服务优先级，根据优先级分配系统资源，保证优先级低的主体处理能力不会影响到优先级高的主体的处理能力。		

A.3.1.5 数据安全检查表

序号	类别	测评项	测评方法	结果记录	符合情况
1	数据完整性	a） 应能够检测到系统管理数据、鉴别信息和重要业务数据在**采集、传输、使用和存储过程**中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。	1） 询问安全管理员应用系统的鉴别信息和重要业务数据在传输过程中是否有完整性保证措施，具体措施有哪些。 2） 检查应用系统，查看其是否配备检测/验证鉴别信息和重要业务数据在传输过程中完整性受到破坏的功能。		
		b)应对**跨安全区域的**重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用通信协议的攻击破坏数据完整性。	1） 考虑相同的安全区域内有网络安全技术保证安全域内的信息安全，考察跨安全域的重要通信是否采用了专用的通讯协议或使用了安全的通信协议服务对数据进行完整性校验。		
2	数据	a)应采用**硬件加密、点对点的数据**	1） 询问安全管理员应用系统的		

序号	类别	测评项	测评方法	结果记录	符合情况
	保密性	**加密网络机制**或其他有效措施实现系统管理数据、鉴别信息和重要业务数据**采集、传输、使用和存储过程的**保密性。	鉴别信息和重要业务数据是否采用加密或其他有效措施实现传输保密性。 2) 检查应用系统设计/验收文档，查看其是否有关于其鉴别信息、敏感的用户数据采用加密或其他有效措施实现传输保密性的描述。 3) 检查应用系统，查看其鉴别信息和重要业务数据是否采用加密或其他有效措施实现传输保密性。		
		b)应对**跨安全区域的**重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用协议的攻击破坏数据保密性。	1) 考虑相同的安全区域内有网络安全技术保证安全域内的信息安全，考察跨安全域的重要通信是否采用了专用的通讯协议或使用了安全的通信协议服务对数据进行加密传输。		
3	备份和恢复	a) 应提供本地数据备份与恢复功能，采取实时备份与异步备份或增量备份与完全备份的方式，**增量数据备份每天一次**，完全数据备份每周一次，备份介质场外存放，**数据保存期限至少 15 年。**	1) 询问安全管理员应用系统是否具有对重要信息进行备份的功能，配置如何。是否提供对重要信息进行恢复的功能； 2) 检查应用系统设计/验收文档，查看其是否有描述应用系统提供用户备份和恢复重要信息的功能的描述； 3) 检查应用系统，查看其是否提供对重要信息进行备份和恢复的功能，其配置是否正确。		
		b)数据备份存放方式应以多冗余方式，完全数据备份至少保证以一个月为周期的数据冗余。(F4)	检查数据备份存放方式是否实现以一个月为周期的数据冗余。		
		c)应建立异地灾难备份中心，配备灾难恢复所需的通信线路、网络设备和数据处理设备，提供业务应用的实时无缝切换。	1) 询问系统管理员是否有异地数据备份，备份方法和备份方式。 2) 检查异地备份的设备和线路。 3) 业务实时无缝切换功能是否定期检查，演练，功能是否可用。		
		d)应提供异地实时备份功能，利用通信网络将数据实时备份至灾难备份中心。	1) 检查异地备份功能是否有效。 2) 是否通过网络将数据实时备份至灾难备份中心。		
		e) 对于同城数据备份中心，应与生产中心直线距离至少达到 30 公里，可以接管所有核心业务的运行；对于异地数据备份中心，应与	访谈安全管理员关于灾备中心的建设情况，检查灾备中心是同城灾备，还是不同城市的异地灾备，是否可以接管所有核心业务的运行。		

序号	类别	测评项	测评方法	结果记录	符合情况
		生产中心直线距离至少达到100公里。(F4)			
		f)为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果。(F4)	询问系统管理员是否采用相关技术避免关键节点存在的单点故障。		
		g)应采用冗余技术设计网络拓扑结构，避免存在网络单点故障。	询问系统管理员是否采用相关技术避免关键节点存在的单点故障。		
		h)异地备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，"就绪状态"指备份中心的所需资源(相关软硬件以及数据等资源)已完全满足但设备 cpu 还没有运行；"运行状态"指备份中心除所需资源完全满足要求外，cpu 也在运行状态。(F4)	询问系统管理员是否定期验证备份数据的可用性？查看相关文档，检查是否具有验证备份数据可用性的记录。		

A.3.2 管理类检查表

A.3.2.1 安全管理制度

序号	类别	测评要求	测评方法	结果记录	符合情况
1	管理制度	a)应制定全机构范围信息安全工作的总体方针和安全策略，说明安全工作的总体目标、范围、原则和安全框架等，**并编制形成信息安全方针制度文件。**	检查信息安全工作的总体方针和安全策略，查看文件是否明确机构安全工作的总体目标、范围、原则和安全框架等。		
		b)应建立安全管理制度，能涵盖管理活动中的给类管理内容。	检查是否依据各项管理内容建立各项安全管理制度。		
		c)应对科技管理人员或操作人员执行的日常管理操作建立操作规程。	检查是否具有对重要管理操作的操作规程，如系统维护手册和用户操作规程等。		
		d) 应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。	访谈安全主管，询问机构是否形成全面的信息安全管理制度体系，制度体系是否由安全政策、管理制度、操作规程等构成。		

序号	类别	测评要求	测评方法	结果记录	符合情况
2	制定和发布	**a）由金融机构总部科技部门负责制定适用全机构范围的安全管理制度，各分支机构的科技部门负责制定适用辖内的安全管理制度。**	访谈安全主管，询问由何部门或人员负责安全管理制度的制定，参与制定人员有哪些。		
		b）安全管理制度应具有统一的格式，并进行版本控制。	检查安全管理制度制定和发布要求管理文档，查看文档是否说明安全管理制度的格式要求、版本编号，并检查安全管理制度文档，查看是否具有版本标识，查看各项制度文档格式是否统一。		
		c）应组织相关人员对制定的安全管理进行论证和审定。	访谈安全主管，询问安全管理制度的制定程序，是否对制定的安全管理制度进行论证和审定；检查管理制度评审记录，查看是否具有相关人员的评审意见。		
		d）安全管理制度应通过正式、有效的方式发布。	检查安全管理制度制定和发布要求管理文档，查看文档是否说明安全管理制度的制定、发布程序和发布范围等各项要求。		
		e）安全管理制度应注明发布范围，并对收发文进行登记。	检查安全管理制度的收发登记记录，查看收发是否通过正式、有效的方式（如正式发文、领导签署和单位盖章等），是否注明管理制度的发布范围。		
		f)有密级的安全管理制度，应注明安全管理制度密级，并进行密级管理。	检查金融机构是否制定密级安全管理制度，是否按照密级管理制度注明密级，并进行密级管理。		
3	评审和修订	a）应由信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定。	检查是否具有安全管理制度体系的评审记录，查看是否由信息安全领导小组负责，是否记录了相关人员的评审意见。		
		b）应定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。	检查是否具有定期对安全管理制度进行修订的记录；检查是否具有系统发生重大安全事故、出现新的安全漏洞以及技术基础结构发生变更时对安全管理制度进行修订的记录。		

序号	类别	测评要求	测评方法	结果记录	符合情况
		c)应明确需要定期修订的安全管理制度，并指定负责人或负责部门负责制度的日常维护。	检查金融机构是否定期修订安全管理制度，是否指定负责人或负责部门负责制度的日常维护。		
		d）应该建立对门户网站内容发布的审核、管理和监控机制。(F4)	检查是否建立管理制度对门户网站内容发布的审核、管理和监控进行规定。		
		e）应根据安全管理制度的相应密级确定评审和修订的操作范围。	检查是否根据安全管理制度的相应密级确定评审和修订的操作范围。		

A.3.2.2 安全管理机构

序号	类别	测评要求	测评方法	结果记录	结果记录
1	岗位设置	**a）金融机构信息安全管理工作实行统一领导、分级管理，总部统一领导分支机构的信息安全管理，各机构负责本单位和辖内的信息安全管理。(F4)**	检查金融行业信息安全管理工作是否实行统一领导、分级管理，金融行业统一领导分支机构和直属企事业单位的信息安全管理，负责金融行业机关的信息安全管理，分支机构负责本单位和辖内的信息安全管理，各直属企事业单位负责本单位的信息安全管理。		
		b）应设立由本机构领导、业务与技术相关部门主要负责人组成的信息安全领导小组，负责协调本机构及辖内信息安全管理工作，决策本机构及辖内信息安全重大事宜。	应访谈安全主管，询问是否设立专职的安全管理机构（即信息安全管理工作的职能部门）；机构内部门设置情况如何，是否明确各部门职责分工。		
		c）应设立专门的信息科技风险审计岗位，负责信息科技审计制度和流程的实施，制订和执行信息科技审计计划，对信息科技整个生命周期和重大事件等进行审计。(F4)	检查信息安全岗位制度，是否规定设立专门的信息科技风险审计岗位，负责信息科技审计制度和流程的实施，制订和执行信息科技审计计划，对信息科技整个生命周期和重大事件等进行审计。		

序号	类别	测评要求	测评方法	结果记录	结果记录
		d)应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。	检查部门、岗位职责文件，查看文件是否明确安全管理机构的职责，是否明确机构内各部门和各负责人的职责和分工。		
		e)应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责。	查看文件是否明确设置安全主管、安全管理各个方面的负责人、机房管理员、系统管理员、网络管理员、安全管理员等各个岗位，各个岗位的职责范围是否清晰、明确。		
		f)除科技部门外，其他部门均应指定至少一名部门计算机安全员，具体负责本部门的信息安全管理工作，协同科技部门开展信息安全管理工作。(F4)	检查除科技部门外，各单位其他部门是否均指定至少 1 名部门计算机安全员，具体负责本部门的信息安全管理工作，协同科技部门开展信息安全管理工作。		
		g)金融机构的主要负责人为本单位计算机信息系统安全保护工作的第一责任人。金融机构的计算机信息系统安全保护领导小组、专职部门和专(兼)职安全管理人员以及其他有关人员应当协助第一责任人组织落实有关规定。(F4)	检查金融机构相关部门的岗位职责制度文件，是否规定金融机构的主要负责人为本单位计算机信息系统安全保护工作的第一责任人，信息系统安全保护领导小组、专职部门和专(兼)职安全管理人员以及其他有关人员应当协助第一责任人组织落实有关规定。		
		h)应坚持三分离原则，实现前后台分离、开发与操作分离、技术与业务分离，信息技术人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务。(F4)	检查岗位设置相关文档，是否规定了实现前后台分离、开发与操作分离、技术与业务分离原则。		
2	人员配备	a）应配备一定数量的系统管理员、网络管理员、安全管理员等。	检查管理人员名单，查看其是否明确哪些人员是机房管理员、系统管理员、网络管理员、安全管理员等重要岗位人员的信息。		
		b)应配备专职安全管理员，**实行 A、B 岗制度，不可兼任。**	检查管理人员名单，查看安全管理员是否是专职人员。		

序号	类别	测评要求	测评方法	结果记录	结果记录
		c）关键事务岗位应配备多人共同管理。	访谈安全主管，询问哪些关键事物需要配备2人或2人以上共同管理，人员具体配备情况如何；检查人员配备要求管理文档。		
		d)应定期或不定期对在信息技术重要岗位上的信息技术人员进行轮换。(F4)	访谈安全主管，询问是否对重要岗位的信息技术人员进行轮换； 查看管理制度是否已明文说明轮换。		
3	授权和审批	a）应根据各部门和岗位的的职责明确授权审批事项、审批部门和批准人等。	检查审批管理制度文档，查看文档中是否明确审批事项、审批部门和批准人等。		
		b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度。	检查审批管理制度文档，查看文档中是否明确审批程序等，是否明确对重要活动进行逐级审批，由哪些部门/人员逐级审批；检查经逐级审批的文档。		
		c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。	检查审批管理文件，查看文件是否明确需定期审查、更新审批的项目、审批部门、审批人和审查周期等。		
		d）应记录审批过程并保存审批文档。	检查关键活动的审批过程记录，查看记录的审批程序与文件要求是否一致。		
		e）用户应被授予完成所承担任务所需的最小权限，重要岗位的员工之间应形成相互制约的关系。权限变更应执行相关审批流程，并有完整的变更记录。(F4)	访谈安全管理员，询问用户权限的分配原则，查看权限关系表，用户是否应被授予完成所承担任务所需的最小权限，重要岗位的员工之间应形成相互制约的关系。		
		f)应建立系统用户及权限清单，定期对员工权限进行检查核对，发现越权用户要查明原因并及时调整，同时清理过期用户权限，做好记录归档。(F4)	检查用户权限清单是否合理，是否定期对用户权限清单进行审查和清理，是否有记录并归档。		

序号	类别	测评要求	测评方法	结果记录	结果记录
4	沟通和合作	a）应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题，**并形成会议纪要。**	检查组织内部机构之间以及信息安全职能部门内部的安全工作会议文件或会议记录，查看是否具有会议内容、会议时间、参加人员和会议结果等描述；检查是否具有信息安全管理委员会或领导小组安全管理工作执行情况的文件或工作记录		
		b）应加强与兄弟单位、公安机关、电信公司的合作与沟通。	检查外联单位联系列表，查看外联单位是否包含公安机关、电信公司、兄弟公司等，是否说明外联单位的名称、联系人、合作内容和联系方式等内容。		
		c）应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通。	检查外联单位联系列表，查看外联单位是否包含供应商、业界专家、专业的安全公司和安全组织等，是否说明外联单位的名称、联系人、合作内容和联系方式等内容。		
		d）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	检查外联单位联系列表，查看外联单位是否包含公安机关、电信公司、兄弟公司、供应商、业界专家、专业的安全公司和安全组织等，是否说明外联单位的名称、联系人、合作内容和联系方式等内容。		
		e）应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。	检查是否有聘请信息安全专家作为常年的安全顾问的证明文档。		
5	审核和检查	a）应制定安全审核和安全检查制度规范安全审核和安全检查工作，按要求定期开展安全审核和安全检查活动。	检查安全检查制度文档，查看文档是否规定检查内容、检查程序和检查周期等，检查内容是否包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。		
		b）安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	访谈安全主管，询问是否组织人员定期对信息系统进行安全检查，检查周期多长，检查内容是否包括系统日常运行、系统漏洞和数据备份等情况。		

序号	类别	测评要求	测评方法	结果记录	结果记录
		c）应由内部人员或上级机构定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。	访谈安全管理员，询问是否定期进行全面安全检查，检查周期多长，安全检查包含哪些内容，检查人员有哪些，检查程序是否按照相关策略和要求进行；检查安全检查过程记录，查看记录的检查程序与文件要求是否一致。		
		d）应制定安全检查表格，实施安全检查，汇总安全检查数据，形成安全检查报告，**要求限期整改的需要对相关整改情况进行后续跟踪，并将每次安全检查报告和整改落实情况整理汇总后，报上一级机构科技部门备案。**	检查是否具有安全检查表格；检查安全检查报告，查看报告日期与检查周期是否一致。		
		e)应制定违反和拒不执行安全管理措施规定的处罚细则。(F4)	检查是否制定违反和拒不执行安全管理措施规定的处罚细则。		

A.3.2.3 人员安全管理

序号	类别	测评内容	测评方法	结果记录	符合情况
1	人员录用	a）应指定或授权专门的部门或人员负责人员录用。	访谈安全主管，询问是由何部门/何人负责安全管理和技术人员的录用工作。		
		b）应严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核。	检查人员录用要求管理文档，查看是否说明录用人员应具备的条件，如学历、学位要求等；检查技能考核文档或记录，查看是否记录考核内容和考核结果等。		
		c）应与员工签署保密协议。	访谈人事负责人，询问是否与录用后的技术人员签署保密协议；检查保密协议。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		d）应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。	访谈人员录用负责人员，询问哪些岗位是比较关键的岗位，对从事关键岗位的人员是否从内部人员中选拔，是否要求其签署岗位安全协议；检查岗位安全协议。		
		e)对信息安全管理人员应实行备案管理。信息安全管理人员的配备和变更情况，应及时报上一级科技部门备案，金融机构总部信息管理人员在总部科技部门备案。(F4)	检查对信息安全管理人员是否实行备案管理。信息安全管理人员的配备和变更情况，是否及时报上一级科技部门备案，金融机构总部信息管理人员是否在总部科技部门备案。		
		f）凡是因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员，不得从事信息安全管理工作。(F4)	检查相关人员档案背景，不得录用因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员。		
2	人员离岗	a）应制定有关管理规范，严格规范人员离岗过程，及时终止离岗员工的所有访问权限。	访谈人事负责人，询问是否及时终止离岗人员的所有访问权限。		
		b）应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	检查是否具有交还身份证件和设备等的登记记录。		
		c)应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开，**并保证离岗人员负责的信息技术系统的口令必须立即更换。**	检查人员离岗管理文档，查看是否规定了调离手续和离岗要求等；检查保密承诺文档，查看是否具有调离人员签字。		
3	人员考核	a）应定期对各个岗位的人员进行安全技能及安全认知的考核。	访谈安全主管，询问对各个岗位人员是否定期进行考核，考核周期多长，考核内容有哪些；检查考核记录。		
		b）应对关键岗位的人员进行全面、严格的安全审查和技能考核。	访谈人员录用负责人员，询问对关键岗位人员的安全审查和考核与一般岗位人员有何不同，内容有哪些，		

序号	类别	测评内容	测评方法	结果记录	符合情况
			审查内容是否包括操作行为和社会关系等。		
		c）应建立保密制度，并定期或不定期的对保密制度执行情况进行检查或考核。	检查是否建立保密制度，是否对保密制度执行情况进行检查和考核，检查和考核的频率是多少。		
		d）应对考核结果进行记录并保存。	检查是否具有各岗位人员考核记录，查看考核内容是否包含安全知识、安全技能等；查看记录日期与考核周期是否一致。		
4	安全意识教育和培训	a）应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划。	访谈安全主管，询问是否对各个岗位人员进行安全教育、岗位技能和安全技术培训，以什么形式进行，效果如何。		
		b） 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，**普及信息安全基础知识、规范岗位操作、提高安全技能。**	应检查安全教育和培训计划文档，查看是否具有不同岗位的培训计划；查看计划是否明确了培训目的、培训方式、培训对象、培训内容、培训时间和地点等，培训内容是否包含信息安全基础知识、岗位操作规程等。		
		c)每年至少对信息安全管理人员进行一次信息安全培训。（F4）	检查金融机构是否每年至少对信息安全管理人员进行一次信息安全培训，是否有培训记录。		
		d）应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒。	访谈安全管理员、系统管理员、网络管理员和数据库管理员，考查其是否了解与工作相关的安全责任和惩戒措施等；检查安全责任和惩戒措施管理文档。		
		e）应对安全教育和培训的情况和结果进行记录并归档保存。	检查是否具有安全教育和培训的结果记录，查看记录中是否具有培训人员、培训内容、培训结果等的描述；查看记录与培训计划是否一致。		
5	外部人员访问管理	**a)各机构**指定责任**部门负责非涉密计算机系统和网络相关的外部人员访问授权审批，批准后由专人全程陪同或监督，并登记备案。**	检查外部人员访问相关规定，检查外部人员访问重要区域批准文档和外部人员访问重要区域的登记记录。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		（F4）			
		b）应对允许被外部人员访问的金融行业计算机系统和网络资源应建立存取控制机制、认证机制，列明所有用户名单及其权限，其活动应受到监控。（F4）	检查外部人员访问相关规定，查看是否对允许外部人员访问的区域、系统、设备和信息等进行明确规定。		
		c)获得外部人员访问授权的所有单位和个人应与金融机构签订安全保密协议，不得进行未授权的增加、删除、修改、查询数据操作，不得复制和泄漏金融机构的任何信息。（F4）	检查获得外部人员访问授权的所有单位和个人是否与金融行业签订安全保密协议，是否进行未授权的增加、删除、修改、查询数据操作，不得复制和泄漏金融行业的任何信息。		

A.3.2.4 系统建设管理

序号	类别	测评内容	测评方法	结果记录	符合情况
1	系统定级	a）应明确信息系统的边界和安全保护等级。	检查系统定级说明文档，查看文档是否明确信息系统边界和安全保护等级。		
		b）应以书面的形式说明确定信息系统为某个安全保护等级的方法和理由。	检查系统定级文档，查看文档是否明确信息系统的安全保护等级确定的方法和理由。		
		c）应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定。	访谈安全主管，询问是否组织相关部门和有关安全技术专家对定级结果进行论证和审定；检查定级结果论证文档。		
		d）应确保信息系统的定级结果经过相关部门的批准。	检查系统定级文档，查看定级结果是否具有相关部门的批准盖章。		

序号	类别	测评内容	测评方法	结果记录	符合情况
2	安全方案设计	a）应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划。	检查是否有对金融机构范围信息系统的安全建设进行总体规划，是否制定了近期和远期的安全建设工作计划，金融机构的科技部门对本单位的安全建设是否进行规划，是否制定近期和远期的安全建设工作计划。		
		b)使用上一级机构信息系统资源或对其他机构信息系统资源与配置造成影响的区域性建设项目，项目建设方案应分别通过上一级机构业务与科技部门的审核、批准。	审查区域性建设项目是都经过上一级机构业务与科技部门的审核、批准。		
		c）应根据系统的安全级别选择基本安全措施，依据风险分析的结果补充和调整安全措施。	访谈系统建设负责人，询问系统选择基本安全措施的依据，是否依据安全保护等级选择，是否依据风险分析的结果补充和调整安全措施，做过哪些调整。		
		d）应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件。	访谈系统建设负责人，询问是否根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案等。		
		e）应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。	访谈系统建设负责人，询问是否组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略等相关配套文件进行论证和审定。		
		f）应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。	访谈系统建设负责人，询问总体安全策略、安全技术框架、安全管理策略等相关配套文件是否定期进行调整和修订，依据什么原则。		
3	产品采购和使用	a）应确保安全产品的采购和使用符合国家的有关规定。	访谈系统建设负责人，询问系统信息安全产品的采购情况，是否按照国家的相关规定进行使用。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		b）应确保密码产品的采购和使用符合国家密码主管部门的要求。	访谈系统建设负责人，询问系统是否采用了密码产品，密码产品的使用是否符合国家密码主管部门的要求。		
		c)应指定或授权专门的部门负责产品的采购，**设备采购应坚持公开、公平、公正的原则，宜采用招标、邀标等形式完成。**	访谈系统建设负责人，询问是否具有专门的部门负责产品的采购，由何部门负责。		
		d）各机构购置扫描、检测类信息安全产品应报科技主管部门批准、备案。（F4）	检查各单位购置扫描、检测类信息安全产品是否报金融行业科技主管部门批准、备案。		
		e）应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。	访谈系统建设负责人，询问系统信息安全产品的采购情况，检查是否具有产品选型测试结果记录和候选产品名单。		
		f）应对重要部位的产品委托专业测评单位进行专项测试。	检查是否具有对委托专业测评单位进行专项测试报告。		
		g)扫描、检测类信息安全产品仅限于本机构信息安全管理人员或经主管领导授权的网络管理员使用。（F4）	检查扫描、检测类信息安全产品使用记录表，验证是否仅限于本单位信息安全管理人员使用		
		h）应定期查看各类信息安全产品相关日志和报表信息并定期汇总分析，若发现重大问题，立即采取控制措施并按规定程序报告。(F4)	检查是否随时检查各类信息安全产品使用情况，认真查看相关日志和报表信息并定期汇总分析，若发现重大问题，是否立即采取控制措施并按规定程序报告。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		i)应定期对各类信息安全产品产生的日志和报表进行备份存档，至少保存 6 个月。（F4）	检查各类信息安全产品在使用中产生的日志和报表信息等重要技术资料，是否备份存档至少 6 个月。		
		j)应及时升级维护信息安全产品，凡超过使用期限的或不能继续使用的信息安全产品，要按照固定资产报废审批程序处理。（F4）	检查是否及时升级维护信息安全产品，凡超过使用期限的或不能继续使用的信息安全产品，是否按照固定资产报废审批程序处理。		
		k）应在本地配置信息安全产品。	访谈信息安全主管，并现场检查本地信息安全产品配置情况。		
4	自行软件开发	**a）应制定软件开发管理制度和代码编写安全规范，明确说明开发过程的控制方法和人员行为准则，要求开发人员参照规范编写代码，不得在程序中设置后门或恶意代码程序。（F4）**	检查是否具有软件开发管理制度，检查是否具有代码编写安全规范。		
		b）应确保开发环境与实际运行环境物理分开，**应确保开发人员和测试人员分离，开发人员不能兼任系统管理员或业务操作人员，**确保测试数据和测试结果受到控制。	访谈系统建设负责人，询问系统是否自主开发软件，是否在独立的开发环境中编写、调试和完成；是否要求开发人员不能做测试工作。		
		c）应确保开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。	访谈信息安全主管，询问开发人员是否为专职人员，并查看是否具有对开发活动控制。件事和审查的相关记录。		
		d）应确保提供软件设计的相关文档和使用指南，并由专人负责保管。	检查是否提供软件设计的相关文档和使用指南，是否由专人负责保管。		
		e）应确保对程序资源库的修改、更新、发布进行授权和批准。	检查对程序资源库的修改、更新、发布是否进行授权和批准。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		f)在软件开发过程中，应同步完成相关文档手册的编写工作，保证相关资料的完整性和准确性。（F4）	查看是否具备软件开发相关文档手册，是否已保证相关资料的完整性和准确性。		
5	外包软件开发	a）应根据开发需求检测软件质量。	检查是否根据开发需求检测软件质量。		
		b）应在软件安装之前检测软件包中可能存在的恶意代码。	检查在软件安装之前是否检测软件包中可能存在的恶意代码。		
		c）应要求开发单位提供软件设计的相关文档和使用指南。	检查开发单位是否提供了软件设计的相关文档和使用指南。		
		d）应要求开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。	检查开发单位提供的软件源代码，审查软件中是否存在后门。		
		e)应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。（F4）	检查外包人员进入金融行业进行现场实施时，是否事先提交计划操作内容并留有记录，金融行业人员是否在现场陪同外包人员，核对操作内容并准确记录实际操作内容，涉及敏感操作（如输入用户口令等）是否由金融行业人员进行操作。		
		f)应要求外包服务商每年至少开展一次信息安全风险评估并提交评估报告，应要求外包服务商聘请外部机构定期对其进行安全审计并提交审计报告，督促其及时整改发现的问题。（F4）	检查外包服务商是否每年至少开展一次内部或聘请外部机构的安全评估工作，是否具有评估报告。		
		g)应禁止外包服务商转包并严格控制分包，保证外包服务水平。（F4）	检查外包服务商的工作机制，是否存在分包、转包现象。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		h）应制定数据中心外包服务应急计划，制订供应商替换方案，以应对外包服务商破产、不可抗力或其它潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。（F4）	检查是否具备关于外包服务的应急计划文档，文档中是否明确规定外包服务商的替换方案等。		
6	工程实施	a）应指定或授权专门的部门或人员负责工程实施过程的管理。	检查是否指定或授权专门的部门或人员负责工程实施过程的管理。		
		b）应制定详细的工程实施方案控制实施过程，**并制定相关过程控制文档**，并要求工程实施单位能正式地执行安全工程过程。	检查是否制定详细的工程实施方案控制实施过程，检查工程实施单位是否能正式地执行安全工程过程。		
		c）针对涉及到新旧数据系统切换的工程实施，应选择对客户影响较小的时间段进行。系统切换时间超过一个工作日，需至少提前 5 个工作日发布提示公告，并提供应急服务途径。	查看是否已建立针对新旧系统切换的相关制度，并检查制度内容是否与测评项要求相符。		
		d）应制定工程实施方面的管理制度明确说明实施过程的控制方法和人员行为准则。	检查是否制定工程实施方面的管理制度，是否明确说明实施过程的控制方法和人员行为准则。		
		e）应通过第三方工程监理控制项目的实施过程。	检查相关第三方工程监理合同，查看合同条款。		
		f）应制定灾难备份系统集成与测试计划并组织实施。通过技术和业务测试，确认灾难备份系统的功能与性能达到设计指标要求。（F4）	检查是否已制定灾难备份系统集成与测试计划；是否具有灾难备份系统功能与性能设计指标要求。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		g)网络系统的建设、升级、扩充等工程应经过科学的规划、充分的论证和严格的技术审查，有关材料应妥善保存并接受主管部门的检查。（F4）	访谈科技主管部门负责人，是否对网络系统工程有详细的规则制度，并对相关材料进行妥善保存。		
7	测试验收	a）应对系统测试验收的控制方法和人员行为准则进行书面规定。	检查科技部门是否对系统测试验收的控制方法和人员行为准则进行书面规定。		
		b）应由项目承担单位（部门）或公正的第三方制定安全测试方案，对系统进行安全性测试，并出具安全性测试报告，测试报告报科技部门审查。	检查项目承担单位（部门）或公正的第三方制定安全测试方案，是否对系统进行安全性测试，是否出具安全性测试报告，测试报告是否报科技部门审查。		
		c）在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告。	检查在测试验收前是否根据设计方案或合同要求等制订测试验收方案，在测试验收过程中是否详细记录测试验收结果，是否形成测试验收报告。		
		d）应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作。	检查是否指定或授权专门的部门负责系统测试验收的管理，是否按照管理规定的要求完成系统测试验收工作。		
		e）应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。	检查是否组织相关部门和相关人员对系统测试验收报告进行审定，是否签字确认。		
		f)新建应用系统投入生产运行前应进行不少于 1 个月的模拟运行和不少于 3 个月的试运行。（F4）	检查新建应用系统投入生产运行前是否进行模拟试运行测试，模拟和试运行的时间是多少。		

序号	类别	测评内容	测评方法	结果记录	符合情况
8	系统交付	a）应对系统交付的控制方法和人员行为准则进行书面规定。	科技部门是否对系统交付的控制方法和人员行为准则进行书面规定。		
		b）应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。	检查是否制定详细的系统交付清单，是否根据交付清单对所交接的设备、软件和文档等进行清点。		
		c）系统建设单位应在完成建设任务后将系统建设过程文档和系统运维文档全部移交科技部门。(F4)	系统建设单位检查是否在完成建设任务后将系统建设过程中的文档和指导用户进行系统运行维护的文档全部移交金融行业科技部门。		
		d）系统建设单位应对负责系统运行维护的技术人员进行相应的技能培训。	系统建设单位检查是否对负责系统运行维护的技术人员进行相应的技能培训。		
		e）应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。	检查是否指定或授权专门的部门负责系统交付的管理工作，是否按照管理规定的要求完成系统交付工作。		
		f)外部建设单位应与金融机构签署相关知识产权保护协议和保密协议，不得将系统采用的关键安全技术措施和核心安全功能设计对外公开。(F4)	检查金融机构与外部建设单位签订的合同或协议，是否有相关约束条款来保证系统采用的关键安全技术措施和核心安全功能设计不对外公开。		
9	系统备案	a）应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用。	检查是否指定专门的部门或人员负责管理系统定级的相关材料，是否控制这些材料的使用。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		b）应将系统等级及相关材料报系统主管部门备案。	检查是否将系统等级及相关材料报系统主管部门备案。		
		c）应将系统等级及其他要求的备案材料报相应公安机关备案。	检查是否将系统等级及其他要求的备案材料报相应公安机关备案。		
10	等级测评	a）在系统运行过程中，应至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改。	在系统运行过程中，是否每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的是否及时整改。		
		b）应在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改。	检查是否在系统发生变更时及时对系统进行等级测评，发现级别发生变化的是否及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的是否及时整改。		
		c)应选择具有**公安部认可的《全国等级保护测评机构推荐目录》中的**测评单位进行等级测评，并与测评单位签订安全保密协议。	检查是否选择具有国家相关技术资质和安全资质的测评单位进行等级测评，测评单位是否签订安全保密协议。		
		d）应指定或授权专门的部门或人员负责等级测评的管理。	检查是否指定或授权专门的部门或人员负责等级测评的管理。		
		e）应指定或授权专门的部门或人员负责等级测评的管理。	检查是否指定或授权专门的部门或人员负责等级测评的管理。		
11	安全服务商选	**a)选择信息安全服务提供商时应评估其资质、经营行为、业绩、服务体系和服务品质等要素。（F4）**	金融行业科技主管部门是否将信息安全服务提供商的资质进行审查。		

序号	类别	测评内容	测评方法	结果记录	符合情况
	择	b）应确保安全服务商的选择符合国家的有关规定。	检查安全服务商的选择是否符合国家的有关规定，涉密计算机系统集成商是否具有国家相关部门颁发的涉密系统集成资质证书的单位。		
		c）应与选定的安全服务商签订与安全相关的协议，明确约定相关责任。	检查是否与选定的安全服务商签订与安全相关的协议，是否与涉密计算机系统集成商签订严格的保密协议，是否明确约定相关责任。		
		d）应确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同，**明确约定双方的权利和义务。**	检查选定的安全服务商提供技术培训和服务承诺，是否与其签订服务合同。		

A.3.2.5 系统运维管理

序号	类别	测评内容	测评方法	结果记录	符合情况
1	环境管理	a)应建立集中的机房，统一为各信息系统提供运行环境。机房设施配备应符合国家计算机机房有关标准要求。	检查机房配备的实施是否符合国家计算机机房的有关标准要求。		
		b)机房应采用结构化布线系统，配线机柜内如果配备理线架，应做到跳线整齐，跳线与配线架统一编号，标记清晰。（F4）	访谈物理安全负责人，询问机房的布线方式，是否统一编号，标记是否清晰。		
		c)应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定。	检查机房安全管理制度，查看其内容是否覆盖机房物理访问、物品带进、带出机房和机房环境安全等方面。		
		d)应指定部门负责机房安全，指派专人担任机房管理员，对机房的出入进行管理，**每天巡查机房运行状况，对机房供配电、空调、温湿度控制等设施进行维护管理，填写机房值班记录、巡视记录。**	访谈物理安全负责人，询问由何部门或何人对机房的基本设施（如空调、供配电设备等）进行定期维护；检查机房基础设施的维护记录。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		e)机房人员进出机房必须使用主管部门制发的证件。（F4）	检查机房管理制度，是否对人员的进出进行规定，是否需要机房出入证。		
		f)机房管理员应经过相关专业培训，掌握机房各类设备的操作要领。（F4）	检查机房管理员是否经过相关专业培训，是否掌握机房各类设备的操作要领；。		
		g)应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养。（F4）	检查各单位应定期对机房设施是否进行维修保养，加强对易损、易失效设备或部件的维护保养。		
		h)机房所在区域应安装24小时视频监控录像装置，重要机房区域实行24小时警卫值班，机房实行封闭式管理，设置一个主出入口和一个或多个备用出入口，出入口控制、入侵报警和电视监控设备运行资料应妥善保管，保存期限不少于6个月，销毁录像等资料应经机构主管领导批准后实施。（F4）	询问管理员是否出入口控制、入侵报警和电视监控设备运行资料应妥善保管，保存期限不少于 6 个月；销毁录像等资料应经机构主管领导批准后实施。		
		i）应单独设置弱电井，并留有足够的可扩展空间。（F4）	检查是否设置弱电井，询问是否留有足够的可扩展空间。		
		j)应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。	检查办公环境管理制度，查看是否对办公人员的相关行为进行规范。		
		k） 应对机房和办公环境实行统一策略的安全管理，对出入人员进行相应级别的授权，对进入重要安全区域的活动行为实时监视和记录。	访谈机房负责人是否对出入机房人员进行相应级别的授权管理，并对重要安全区域的活动实时监视和记录。		

序号	类别	测评内容	测评方法	结果记录	符合情况
2	资产管理	a)应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	检查资产清单，查看其内容是否覆盖资产责任人、所属级别、所处位置、所处部门等方面。		
		b)应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为，包括资产领用、资产用途和安全授权、资产日常操作、资产维修、资产报废等。	检查资产管理制度，查看其内容是否覆盖资产使用、维护等方面，是否指定资产管理的责任部门或人员,由何部门/何人负责。		
		c)应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施。	检查资产清单中的设备，查看其是否具有相应标识，标识是否能表明资产的重要程度。		
		d)应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。	检查信息分类文档，查看其内容是否规定了分类标识的原则和方法（如根据信息的重要程度、敏感程度或用途不同进行分类）。		
3	介质管理	a)应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定。	检查介质管理制度，查看其内容是否覆盖介质的使用、维修、销毁等过程的操作。		
		b)应确保介质存放在安全的环境中，**并有明确标识，**对各类介质进行控制和保护，并实行存储环境专人管理。	访谈资产管理员，询问介质存放于何种环境中，是否对存放环境实施专人管理。		
		c)所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放。（F4）	检查所有数据备份介质是否防磁、防潮、防尘、防高温、防挤压存放。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		d)应对介质在物理传输过程中的人员选择、打包、交付等情况进行安全控制，**应选择安全可靠的传递、交接方式，做好防信息泄露控制措施。**	访谈资产管理员，询问对介质的物理传输过程是否要求选择可靠传输人员、严格介质的打包（如采用防拆包装置）、选择安全的物理传输途径、双方在场交付等环节的控制；是否对介质的使用情况进行登记管理，并定期盘点。		
		e)应对介质归档和查询等进行登记记录，管理员应根据存档介质的目录清单定期盘点。	询问管理员是否应根据存档介质的目录清单并定期盘点。		
		f)对于重要文档，如是纸质文档则应实行借阅登记制度，未经相关部门领导批准，任何人不得将文档转借、复制或对外公开，如是电子文档则应采用 OA 等电子化办公审批平台进行管理。（F4）	检查纸质技术文档是否实行借阅登记制度，未经科技部门领导批准，是否有人将技术文档转借、复制或对外公开，电子文档是否采用 OA 等电子化办公审批平台进行管理。		
		g)应按照统一格式对技术文档进行编写并及时更新，达到能够依靠技术文档恢复系统正常运行的要求。（F4）	检查技术文档的格式是否统一，内容是否具有参考性，是否达到能够依靠技术文档恢复系统正常运行的要求。		
		h)应对带出工作环境的存储介质进行内容加密和监控管理。	询问管理员是否对带出工作环境的存储介质进行内容加密和监控管理。		
		i)应对送出维修或销毁的介质应采用多次读写覆盖、清除敏感或秘密数据，对无法执行删除操作的受损介质必须销毁。	访谈资产管理员，询问对送出维修或销毁的介质如何管理，销毁前是否对数据进行净化处理。		
		j)对载有敏感信息存储介质的销毁，应报有关部门备案，由科技部门进行信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录，信息消除处理仅限于存储介质仍将在金融机构内部使用的情况，否则应进行信息的不可恢复性销毁。（F4）	检查需要废止的计算机设备，是否由科技部门使用专用工具进行数据信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录，信息消除处理仅限于存储介质仍将在金融行业内部使用的情况，否则应进行信息的不可恢复性销毁处理。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		k)应制定移动存储介质使用规范，并定期核查移动存储介质的使用情况。（F4）	检查各单位是否严格管理移动存储介质，定期核查所配发移动存储介质的在位使用情况，是否违规使用移动存储介质的情况。		
		l)应建立重要数据多重备份机制，其中至少 1 份备份介质应存放于科技部门指定的同城或异地安全区域。（F4）	访谈资产管理员，询问是否对某些重要介质(至少一份)实行异地存储，异地存储环境是否与本地环境相同，检查介质本地存放的实际环境的安全性。		
		m)应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。	访谈资产管理员，对重要介质中的数据和软件是否进行保密性处理，对介质是否根据重要性不同进行分类标识，并进行检查。		
		n)应对技术文档实行有效期管理，对于超过有效期的技术文档降低保密级别，对已经失效的技术文档定期清理，并严格执行技术文档管理制度中的销毁和监销规定。(F4)	检查技术文档的有效期时间和密级级别是否一致、合理，对于过期的技术文档的销毁是否遵循文档制度中的毁和监销规定。		
		o)应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。（F4）	检查是否定期对主要业务备份数据进行恢复性验证，是否及时转存介质中存储的数据。		
4	设备管理	a)应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理。	访谈资产管理员，询问是否对设备选用的各个环节（选型、采购、发放等）进行规范化管理，检查相应管理制度。		
		b)应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等。	检查设备维护管理文档，看其是否覆盖维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等方面。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		c)设备确需送外单位维修时，应彻底清除所存的工作相关信息，并与设备维修厂商签订保密协议，与密码设备配套使用的设备送修前必须请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息，并派专人在场监督。（F4）	检查计算机设备确需送外单位维修时，各单位科技部门是否彻底清除所存的工作相关信息，必要时应与设备维修厂商签订保密协议，与密码设备配套使用的计算机设备送修前必须请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息。		
		d)制定规范化的故障处理流程，建立详细的故障日志(包括故障发生的时间、范围、现象、处理结果和处理人员等内容)。（F4）	检查是否具备关于故障处理文档，文档中是否详细记录了处理流程，是否建立故障处理日志。		
		e)应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。	检查设备管理制度文档，查看其是否对设备的操作和使用了进行明确规定；检查设备操作手册，查看其内容是否覆盖设备启动、停止、加电、断电等操作。		
		f)新购置的设备应经过测试，测试合格后方能投入使用。（F4）	检查是否具备新购设备的测试报告，是否测试合格后方可投入使用。		
		g)各机构科技部门负责对信息系统相关的各种设备(包括备份和冗余设备）、线路等进行维护管理。（F4）	应访谈资产管理员，询问是否对各类设施、设备指定专人或专门部门进行定期维护，由何部门/何人维护。		
		h)应做好设备登记工作，制定设备管理规范，落实设备使用者的安全保护责任。（F4）	检查各单位科技部门是否做好计算机设备登记工作，严格设备资产管理，落实计算机设备使用者的安全保护责任。		
		i)需要废止的设备，应由科技部门使用专用工具进行数据信息消除处理，如废止设备不再使用或调配到金融行业以外的单位，应由科技部门备案并对其数据信息存储设备进行消磁或物理粉碎等不可恢复性销毁处理，同时备案。（F4）	检查需要废止的计算机设备，是否由科技部门使用专用工具进行数据信息消除处理，如废止计算机设备不再使用或调配到金融行业以外的单位，是否由科技部门对其数据信息存储设备进行消磁或物理粉碎等不可恢复性销毁处理。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		j)应确保信息处理设备必须经过审批才能带离机房或办公地点。	访谈资产管理员，询问对带离机房的设备是否经过审批，由何人审批。		
5	监控管理和安全管理中心	a)应对通信线路、网络设备、主机和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存。	访谈系统运维负责人，询问其是否监控主机、网络设备和应用系统的运行状况等，采用何种方式进行监控。		
		b)应建立计算机系统运行监测周报、月报或季报制度，统计分析运行状况。（F4）	检查各单位科技部门是否建立计算机系统运行监测周报、月报或季报制度，统计分析运行状况。		
		c)应定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，**发现重大隐患和运行事故应及时协调解决，并报上一级单位相关部门。**	访谈系统运维负责人，询问是否定期对监控记录进行分析、评审。检查各单位是否及时预警、响应和处置运行监测中发现的问题，发现重大隐患和运行事故应及时协调解决，是否并报上一级单位相关部门。		
		d)应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。	访谈系统运维负责人，询问是否建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等相关事项进行集中管理。		
6	网络安全管理	a)应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作。	访谈安全主管，询问是否指定专人负责维护网络安全管理工作。		
		b)应建立网络安全运行管理制度，对网络安全配置**(最小服务配置)**、日志保存时间、安全策略、升级与打补丁、口令更新周期、**重要文件备份**等方面作出规定。	检查网络安全管理制度，查看其内容是否覆盖网络安全配置（包括网络设备的安全策略、授权访问、最小服务、升级与打补丁）、审计日志保存时间、升级与打补丁等方面。		
		c)应**定期检查网络日志**，检查违反规定拨号上网或其他违反网络安全策略的行为，**管理网络资源及其配置信息，建设网络安全运行维护记录，并有操作和复核人员的签名，维护记录应至少妥善保存6 个月。**	访谈安全主管，询问是否指定专人负责维护网络安全管理工作。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		d)应严格控制网络管理用户的授权，授权程序中要求必须有两人在场，并经双重认可后方可操作，操作过程应保留不可更改的审计日志。	访谈信息安全负责人，了解网络管理用户授权流程，并确保操作过程已保留不可更改的审计日志。		
		e)网间互联由金融机构科技主管部门统一规划，按照相关标准组织实施，未经科技主管部门核准，任何机构不得自行与外部机构实施网间互联。（F4）	访谈科技主管，是否已建立网间互联相关标准组织实施，检查内容是否与测评项要求相符。		
		f)应制定网络接入管理规范，应禁止便携式和移动式设备接入网络，**其他任何设备接入网络前，接入方案应经过科技部门的审核，审核批准后方可接入网络并分配相应的网络资源。**	询问系统管理员是否制定网络接入管理规范，接入方案应经过科技部门的审核，审核批准后方可接入网络并分配相应的网络资源。		
		g)应制定远程访问控制规范，确因工作需要进行远程访问的，应由访问发起机构科技部门核准，提请被访问机构科技部门（岗）开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。（F4）	检查各单位是否严格远程访问控制，确因工作需要进行远程访问的，应由访问发起单位科技部门核准，提请被访问单位科技部门（岗）开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。		
		h)各机构以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经科技主管部门批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。（F4）	检查各单位以不影响正常网络传输为原则，是否合理控制多媒体网络应用规模和范围，未经金融行业科技主管部门批准，不得在金融行业内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。		
		i)信息安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不得对外公开，未科技主管部门授权，任何外部机构与人员不得检测或扫描机构内部网络。（F4）	询问信息安全管理人员经本部门主管领导批准后，有权对本单位或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不得对外公开，未经金融行业科技主管部门授权，任何外部单位与人员不得检测或扫描金融行业内部网络。		
		j)所有网间互联应用系统和外联网络区应定期进行威胁评估和脆弱性评估并提供威胁和脆弱性评估报告。（F4）	访谈安全管理员，询问是否对所有网间互联应用系统和外联网络区进行威胁评估和脆弱性评估，评估的频率以及是否具有评估报告。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		k)网络系统应采取定时巡检、定期检修和阶段性评估的措施，银行业务高峰时段和业务高峰日要加强巡检频度和力度，确保硬件可靠、运转正常。（F4）	访谈网络系统管理员，是否存在网络系统定期巡检、检修和阶段性评估流程，并根据实际情况加强巡检频度和力度。		
		l)金融业网间互联安全实行统一规范、分级管理、各负其责的安全管理模式，未经金融机构科技主管部门核准，任何机构不得自行与外部机构实施网间互联。（F4）	询问管理员是否应定期检查违反规定拨号上网或其他违反网络安全策略的行为，金融行业内部网络与国际互联网实行安全隔离，所有接入金融行业内部网络或存储有敏感工作信息的计算机，不得接入国际互联网。		
7	系统安全管理	a)应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定。	检查系统安全管理制度，查看其内容是否覆盖系统安全配置（包括系统的安全策略、授权访问、最小服务、升级与打补丁）、系统帐户（用户责任、义务、风险、权限审批、权限分配、帐户注销等）、审计日志以及配置文件的生成、备份、变更审批、符合性检查等方面。		
		b)应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则。	访谈系统管理员，询问是否指定专人负责系统管理工作，是否对系统账户进行分类管理，权限设定是否遵循最小授权原则。		
		c)系统管理员不得兼任业务操作人员，系统管理员不得对业务数据进行任何增加、删除、修改、查询等操作，系统管理员确需对计算机系统数据库进行业务数据维护操作的，应征得业务部门书面同意，并详细记录维护内容、人员、时间等信息。（F4）	检查系统管理员不得兼任业务操作人员，系统管理员不得对业务数据进行任何增加、删除、修改、查询等操作，系统管理员确需对计算机系统数据库进行业务数据维护操作的，检查是否征得业务部门书面同意，并详细记录维护内容、人员、时间等信息。		
		d)信息安全管理员应每季度至少进行一次漏洞扫描，对发现的系统安全漏洞及时进行修补，扫描结果应及时上报。（F4）	访谈信息安全管理员，询问是否每季度对系统进行漏洞扫描，发现漏洞是否进行了及时修补，检查系统漏洞扫描报告。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		e)系统管理员应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装，**并对系统变更进行记录。**	访谈系统管理员，询问在安装系统补丁程序前是否经过测试，并对重要文件进行备份。		
		f)系统管理员应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，**重要计算机系统的系统设置要求至少两人在场，**严禁进行未经授权的操作。	检查系统操作手册，查看其内容是否覆盖操作步骤、维护记录、参数配置等方面。访谈系统管理员，询问是否指定专人负责系统管理工作，是否对系统账户进行分类管理，权限设定是否遵循最小授权原则。		
		g)系统管理员应对系统变更进行详细的记录。（F4）	访谈系统管理员了解系统变更流程，查看系统变更记录。		
		h)应定期对运行日志和审计数据进行分析，以便及时发现异常行为。	访谈审计员，询问是否定期对系统审计日志进行分析，以便及时发现异常行为。		
		i) 应对系统资源的使用进行预测，以确保充足的处理速度和存储容量，管理人员应随时注意系统资源的使用情况，包括处理器、存储设备和输出设备。	访谈系统管理员如何确保系统资源得到充足的使用，查看管理人员是否实时注意资源使用情况。		
8	恶意代码防范管理	a)应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。	访谈系统运维负责人，询问是否对员工进行基本恶意代码防范意识的教育，如告知应及时升级软件版。		
		b)金融机构客户端应统一安装病毒防治软件，设置用户密码和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序。（F4）	检查全行客户端是否统一安装病毒防治软件，设置用户密码和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		c)应指定专人对网络和主机进行恶意代码检测并保存检测记录。	访谈系统运维负责人，询问是否指定专人对恶意代码进行检测，并保存记录。		
		d)应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。	检查恶意代码防范管理文档，查看其内容是否覆盖防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面。		
		e)应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，对防病毒系统不能自动清除的计算机病毒，提出解决办法，并形成书面的报表和总结汇报。	访谈安全管理员，询问是否对恶意代码库的升级情况进行记录，对各类防病毒产品上截获的恶意代码是否进行分析并汇总上报；是否出现过大规模的病毒事件，如何处理；检查恶意代码检测记录、恶意代码库升级记录和分析报告检查恶意代码防范管理文档，查看其内容是否覆盖防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面。		
9	密码管理	a)选用的密码产品和加密算法应符合国家相关密码管理政策规定**循金融业数据安全保密的国家标准和国际标准。**	访谈安全管理员，询问密码技术和产品使用是否符合金融业数据安全保密的国家标准和国际标准。		
		b)应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员必须是本机构在编的正式员工，并逐级进行备案，规范密钥管理。（F4）	访谈安全管理员，询问密码技术和产品的使用是否金融行业的《含有密码技术的信息产品政府采购规定》中的安全要求,使用符合国家密码管理规定的密码技术和产品,应建立密码使用管理制度。		
		c)主机管理员、数据库管理员、网络管理员、业务操作人员均须设置口令密码，至少每月更换一次，口令密码的强度应满足不同安全性要求。（F4）	检查各单位系统管理员、数据库管理员、网络管理员、业务操作人员是否均设置口令密码，并至少每3个月更换一次，口令密码的强度是否满足不同安全性要求。检查各类密钥是否定期更换，对已泄漏或怀疑泄漏的密钥是否做到及时废除，过期密钥是否安全归档或定期销毁。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		d)敏感计算机系统和设备的口令密码设置应在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经科技部门主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码使用后应立即更改并再次密封存放。（F4）	检查敏感计算机系统和设备的口令密码设置是否在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经科技部门主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码使用后是否做到了立即更改并再次密封存放。检查各单位系统管理员、数据库管理员、网络管理员、业务操作人员是否均设置口令密码，并至少每 3 个月更换一次，口令密码的强度是否满足不同安全性要求。		
		e)应根据实际情况在一定时限内妥善保管重要计算机系统升级改造前的口令密码。（F4）	访谈安全管理员是否已建立在系统升级前保管重要计算机口令密码等相关规定。		
		f)密钥注入、密钥管理功能调试和密钥档案的保管应由专人负责。密钥资料须保存在保险柜内。保险柜钥匙由专人负责。使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录。（F4）	检查密钥注入、管理功能调试和档案保管是否是专人负责；密钥资料保存在何处，以及是否具备管理制度来规定密钥的使用和销毁，是否有使用记录和销毁记录。		
		g)确因工作需要经授权可远程接入内部网络的用户，应妥善保管其身份认证介质及口令密码，不得转借他人使用。（F4）	确因工作需要经授权可远程接入内部网络的用户，检查是否妥善保管其身份认证介质及口令密码，查看是否转借他人使用。		
10	变更管理	**a)变更管理应流程化、文档化和制度化，变更流程中应明确变更发起方、实施方的职责，应明确变更方案的测试、审批流程及实施策略，对有可能影响客户利益的变更应事先通知客户并得到客户的确认。（F4）**	检查是否具备变更管理制度明确规定变更流程，明确变更发起方、实施方的职责，明确变更方案的测试、审批流程及实施策略，对有可能影响客户利益的变更是否具备变更客户通知确认程序。		
		b)应确认系统中要发生的变更，并制定变更方案，**包括变更的组织结构与实施计划、操作步骤、应急及回退方案等，变更方案应经过测试，对于无法测试或不具备测试条件的变更，应得到充分论证和审批。**	访谈系统运维负责人，询问是否制定变更方案指导系统执行变更；目前系统发生过哪些变更；检查系统变更方案。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		c)应建立变更管理制度，重要系统变更前，应向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告。	检查变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容；检查是否具有变更方案评审记录和变更过程记录文档访谈系统运维负责人，询问是否制定变更方案指导系统执行变更；目前系统发生过哪些变更；检查系统变更方案。		
		d)应建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录。	检查变更控制的申报、审批程序，查看其是否规定需要申报的变更类型、申报流程、审批部门、批准人等方面内容。检查变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容；检查是否具有变更方案评审记录和变更过程记录文档。		
		e)应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。	检查中止变更并从失败变更中恢复的文件化程序，是否明确过程控制方法和人员职责，必要时对恢复过程进行演练。		
		f)应定期检查变更控制的申报和审批程序的执行情况，评估系统现有状况与文档记录的一致性。	检查变更控制记录，评估系统现有状态与变更控制记录的是否一致。		
		g)变更前做好系统和数据的备份。风险较大的变更，应在变更后对系统的运行情况进行跟踪。（F4）	检查变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容；检查是否具有变更方案评审记录和变更过程记录文档。		
		h)如果需要使用生产环境进行测试，应纳入变更管理，并制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划，确保生产系统的安全。（F4）	访谈安全管理员，是否需要使用生产环境进行测试，如果需要是否纳入变更管理中，是否制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		i)当生产中心发生变更时，应同步分析灾备系统变更需求并进行相应的变更，评估灾备恢复的有效性；应尽量减少紧急变更。（F4）	检查灾备中心是否在生产系统发生变更时也同步进行变更，是否有相关的变更记录。		
11	备份与恢复管理	a)应制定金融机构的数据备份与恢复相关安全管理制度，对备份信息的备份方式、备份频度、存储介质、保存期等进行规范。	检查是否根据金融行业的统一规定建立自己的备份与恢复管理的相关制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范，同时根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法。		
		b)应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法。	检查数据备份和恢复策略文档，查看其内容是否覆盖数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面。检查是否具有规定备份方式、频度、介质、保存期的安全管理制度。		
		c)应建立控制数据备份和恢复过程的程序，记录备份过程，对需要采取加密或数据隐藏处理的备份数据，进行备份和加密操作时要求两名工作人员在场，所有文件和记录应妥善保存。	检查数据备份恢复管理制度，是否明确记录备份过程，是否要求对要采取加密或数据隐藏处理的备份数据，进行备份和加密操作时要求两名工作人员在场，是否具备备份恢复记录等所有文件。		
		d)应每年至少进行一次重要信息系统专项灾备切换演练，每三年至少进行一次重要信息系统全面灾备切换演练，根据不同的应急恢复内容，确定演练的周期，并指定专人管理和维护应急预案，根据人员、信息资源等变动情况以及演练情况适时予以更新和完善，确保应急预案的有效性和灾难发生时的可获取性。	查看是否应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期，定期组织应急预案的演练，并指定专人管理和维护应急预案，根据人员、信息资源等变动情况以及演练情况适时予以更新和完善，确保应急预案的有效性和灾难发生时的可获取性。		
		e)应定期对备份数据的有效性进行检查，每次抽检数据量不低于10%。备份数据要实行异地保存。（F4）	访谈安全管理员，询问是否对备份数据进行有效性验证，验证时间间隔为多长时间，验证的备份数据的比例为多少，是否进行异地保存。		

序号	类别	测评项	测评方法	结果记录	符合情况
			成功。		
		g）应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别，并且身份鉴别信息至少有一种是不可伪造的，**例如以密钥证书、动态口令卡、生物特征等作为身份鉴别信息。(F4)**	应检查主要服务器操作系统和主要数据库管理系统，查看身份鉴别是否采用两个及两个以上身份鉴别技术的组合来进行身份鉴别（如采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技术和数字证书方式的身份鉴别技术中的任意两个组合）。并且有一种是不易伪造的（如数字证书或生物识别技术）。		
2	安全标记	a）应对所有主体和客体设置敏感标记。	应访谈系统管理员、并检查系统主体和客体是否分级进行敏感标记。		
3	访问控制	a）应依据安全策略和所有主体和客体设置的敏感标记控制主体对客体的访问。	应检查主要服务器操作系统和主要数据库管理系统，查看是否能对重要信息资源和访问重要信息资源的所有主体设置敏感标记，这些敏感标记是否构成多级安全模型的属性库，主体和客体的敏感标记是否以默认方式生成或由安全员建立、维护和管理。		
		b)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表、记录和字段级。	应检查服务器操作系统和数据库管理系统的安全策略，查看是否明确主体（如用户）具有非敏感标记（如角色），并能依据非敏感标记规定对客体的访问。验证访问控制粒度是否达到主体为用户级或进程级，客体为文件、数据库表、记录和字段级。		
		c） 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。	应检查主要服务器操作系统和主要数据库管理系统，查看特权用户的权限是否进行分离，如可分为系统管理员、安全管理员、安全审计员等；查看是否采用最小授权原则（如系统管理员只能对系统进行维护，安全管理员只能进行策略配置和安全设置，安全审计员只能维护审计信息等）。		
		d）应实现操作系统和数据库系统特权用户的权限分离，系统管理员只具备操作系统的运维管理权限，	应检查主要服务器操作系统和主要数据库管理系统，查看在系统管理员、安全管理员、安全审计员之间		

序号	类别	测评内容	测评方法	结果记录	符合情况
		f）灾难恢复的需求应定期进行再分析，再分析周期最长为三年，当生产中心环境、生产系统或业务流程发生重大变更时，单位应立即启动灾难恢复需求再分析工作，依据需求分析制定灾难恢复策略。(F4)	访谈安全管理员，询问是否对灾难恢复的需求进行定期分析，尤其在发生变更时是否进行灾难恢复需求的再分析工作，再分析的周期是多少。		
		g)恢复及使用备份数据时需要提供相关口令密码的，应把口令密码密封后与数据备份介质一并妥善保管。（F4）	检查数据备份恢复口令的存放管理制度，以及是否口令与数据备份介质均进行有效管理。		
		h）应根据信息系统的备份技术要求，制定相应的灾难恢复计划，并对其进行测试以确保各个恢复规程的正确性和计划整体的有效性，测试内容包括运行系统恢复、人员协调、备用系统性能测试、通信连接等，根据测试结果，对不适用的规定进行修改或更新。	查看灾难恢复计划，以及相关测试记录，确保测试内容与检测项内容一致，并根据测试结果对不适用的规定进行修改或更新。		
		i)应定期开展灾难恢复培训，在条件许可的情况下，由金融机构相关部门统一部署，至少每年进行一次灾难恢复演练，包括异地备份站点切换演练和本地系统灾难恢复演练，异地备份站点切换：在异地建立热备份站点，当主站点因发生灾难导致系统不可恢复时异地备份站点能承担起主站点的功能，本地系统灾难恢复：当本地系统发生异常中断时能够在短时间恢复和保障业务数据的可运行性。（F4）	检查灾难恢复培训计划，查看是否每年进行一次灾难恢复演练，包括异地备份站点切换演练和本地系统灾难恢复演练。		
		j)金融机构应根据信息系统的灾难恢复工作情况，确定审计频率。单位应每年至少组织一次内部灾难恢复工作审计。（F4）	检查是否定期对信息系统的灾难恢复工作进行审计，以及审计频率是否是至少一年进行一次。		
		k）应安排专人负责灾难恢复预案的日常维护管理。（F4）	询问安全管理员是否安排专人负责灾难恢复预案的日常维护管理。		
		l）应建立灾难备份系统，主备系统实际切换时间应满足实时切换，灾备系统处理能力应不低于主用系统处理能力的50%，通信线路应	检查金融机构是否建立灾难备份系统，主备系统实际切换时间是否少于 60 分钟，灾备系统处理能力是否不低于主用系统处理能力的 50%。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		分别接入主备系统。有条件时可采用主、备系统处理能力相同、轮换交替使用的双系统模式。（F4）			
12	安全事件处置	a)应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点。	访谈系统运维负责人，询问是否告知用户在发现安全弱点和可疑事件时应进行及时报告。		
		b)应制定安全事件报告和处置管理制度，明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责。	访谈系统运维负责人，询问是否了解本系统已发生的和需要防止发生的安全事件，主要有哪几类，对识别出的安全事件是否根据其对系统的影响程度划分不同等级；检查安全事件定级文档。		
		c)应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分。	检查是否按照信息安全报告制度进行信息通报，一般信息安全事件应逐级通报，发生因人为、自然原因等造成的信息系统瘫痪以及利用计算机实施犯罪等影响和损失较大的信息安全事件（以下简称重大信息安全事件）应直接报金融行业突发事件应急处置指挥部，同时抄报科技主管部门。		
		d)应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等。	检查是否在重大信息安全事件发生后，按照金融行业信息安全报告制度报上一级科技部门，并按照相关规定由上级科技部门或本单位决定是否发布预警信息或启动应急预案。		
		e)应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存。	检查安全事件记录分析文档，查看其是否记录引发安全事件的系统弱点，是否分析不同安全事件发生的原因。检查事件报告和响应处理程序，查看其内容是否包括事件的报告流程、响应处理方法等。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		f)对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。	访谈工作人员，询问其不同安全事件的报告流程；检查安全事件报告和处理程序文档。检查安全事件记录分析文档，查看其是否记录引发安全事件的系统弱点，是否分析不同安全事件发生的原因。		
		g)发生可能涉及国家秘密的重大失、泄密事件，应按照有关规定向公安、安全、保密等部门汇报。	访谈安全管理员，是否已建立重大失、泄密事件处理流程及相关制度。		
		h)应严格控制参与涉及国家秘密事件处理和恢复的人员，重要操作要求至少两名工作人员在场并登记备案。	访谈安全管理员，是否已建立重大失、泄密事件处理流程及相关制度。		
		i)应建立有效的技术保障机制，确保在安全事件处置过程中不会因技术能力缺乏而导致处置中断或延长应急处置时间。（F4）	访谈安全管理员，检查技术保障机制是否充足、有效，是否可以保障安全事件的处置的顺利进行。		
13	应急预案管理	a)应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括应急组织机构、启动应急预案的条件、应急处理流程、系统恢复流程、**事件信息收集、分析、报告制度、**事后教育和培训等内容，**业务处理系统应急预案的编制工作应由相关业务部门和科技部门共同完成，并由预案涉及的相关机构签字盖章。**	检查应急响应预案文档，查看其内容是否覆盖启动计划的条件、应急处理流程、系统恢复流程和事后教育等内容。访谈工作人员，询问其不同安全事件的报告流程；检查安全事件报告和处理程序文档。		
		b)应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障。	访谈询问金融机构的人力、设备、技术和财力等各方面是否可以有效保障应急预案的执行。		
		c)应对系统相关的人员进行应急预案培训，对应急预案的培训应至少每年举办一次。	访谈系统运维负责人，询问是否制定不同事件的应急预案，是否对系统相关人员进行应急预案培训，培训内容是什么，多长时间举办一次；检查应急预案培训记录、演练记录和审查记录。		

序号	类别	测评内容	测评方法	结果记录	符合情况
		d)在与第三方合作的业务中，应建立并完善内部责任机制和与相关机构之间的协调机制，制定完整的应急预案及应急协调预案，并定期参加联合演练。（F4）	检查是否在与第三方合作的业务中，应建立并完善内部责任机制和与相关机构之间的协调机制，制定完整的应急预案及应急协调预案，并定期参加联合演练。		
		e)突发事件应急处置领导小组应统一领导计算机系统的应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业信息安全监管部门。（F4）	检查是否有突发事件应急处置领导小组并统一领导计算机系统的应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源。		
		f)金融机构应急领导小组应及时向新闻媒体发布相关信息，严格按照行业、机构的相关规定和要求对外发布信息，机构内其它部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。（F4）	检查是否金融行业办公厅负责统一向社会发布应急事件公告，其他任何单位或个人不得向社会发布应急事件公告。		
		g)实施报告制度和启动应急预案的单位应当实行重大突发事件 24 小时值班制度。（F4）	实施报告制度和启动应急预案的单位检查是否实行重大突发事件 24 小时值班制度。		
		h)应定期对原有的应急预案重新评估，并根据安全评估结果，定期修订、演练，并进行专项内部审计。（F4）	检查随着信息系统的变更定期对原有的应急预案重新评估的证明文件，以及根据安全评估结果，定期修订完善机房环境、网络和计算机系统等应急预案。		
		i)应急演练结束后，金融机构应撰写应急演练情况总结报告，总结报告包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练结论。（F4）	检查金融机构是否定期进行应急演练，是否具有演练记录和演练总结报告，报告的内容是否涵盖演练的人员、演练过程、存在问题和改进措施等内容。		

参考文献

[1] 全国人民代表大会常务委员会 《中华人民共和国标准化法》 （1988 年月中华人民共和国主席令第 11 号）

[2] GB/T 1.1-2000 标准化工作导则 第 1 部分：标准的结构和起草规则

[3] GB/T 10112-1999 术语工作 原则与方法

[4] GB/T 16785-1997 术语工作 概念与术语的协调

[5] GB/T 20001.1-2001 标准编写规则 第 1 部分：术语

[6] GB/T 22240-2008 信息系统安全等级保护定级指南

[7] GB/T 25070-2010 信息系统等级保护安全设计技术要求

[8] JR/T 0060 证券期货业信息系统安全等级保护基本要求

[9] JR/T 0067 证券期货业信息系统安全等级保护测评要求