ICS 03.060
A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0071—2012

金融行业信息系统信息安全等级保护实施指引

Implementation 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”系列标准中的第一项标准。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。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。

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实施指引

1 范围

本标准依据国家《信息系统安全等级保护基本要求》和《信息系统等级保护安全设计技术要求》标准，结合金融行业特点以及信息系统安全建设需要，对金融行业的信息安全体系架构采用分区分域设计、对不同等级的应用系统进行具体要求，以保障将国家等级保护要求行业化，具体化，提高我行重要网络和信息系统信息安全防护水平。

本标准适用于金融机构（包括其分支机构）的系统规划建设部门（业务与技术）、应用开发部门、系统运行部门、安全管理部门、系统使用部门、内部监察、审计等部门。也可作为信息安全职能部门进行监督、检查和指导的依据。随着内容的补充和丰富，为等级保护工作的开展提供指导。

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

GB/T 25069　信息安全技术 术语

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 术语和定义

GB/T 25069 确立的以及下列术语和定义适用于本文件。

3.1 **敏感数据** sensitive data

敏感数据是指一旦泄露可能会对用户或金融机构造成损失的数据，包括但不限于：

a) 用户敏感数据，如用户口令、密钥等；
b) 系统敏感数据，如系统的密钥、关键的系统管理数据；
c) 其他需要保密的敏感业务数据；
d) 关键性的操作指令；
e) 系统主要配置文件；
f) 其他需要保密的数据。

3.2 **风险** risk

某种威胁存在利用一种资产或若干资产的脆弱性使这些资产损失或破坏的可能性。

3.3 **安全策略** security policy

主要指为信息系统安全管理制定的行动方针、路线、工作方式、指导原则或程序。

3.4 **安全需求** security requirement

为使设备、信息、应用及设施符合安全策略的要求而需要采取的保护类型及保护等级。

3.5 **完整性** integrity

包括数据完整性和系统完整性。数据完整性表征数据所具有的特征，即无论数据形式作何变化，数据的准确性和一致性均保持不变的程度；系统完整性表征系统在防止非授权用户修改或使用资源和防止授权用户不正确地修改或使用资源的情况下，系统能履行其操作目的的品质。

3.6 **可用性** availability

表征数据或系统根据授权实体的请求可被访问与使用程度的安全属性。

3.7 **弱口令** weak password

指在计算机使用过程中，设置的过于简单或非常容易被破解的口令或密码。

4 指引编制策略

4.1 国家等级保护要求

国家针对等级保护制定了一系列的法规和标准，这些法规和标准是建设等级保护系统的依据。目前，我国共制定了和发布了约50余个相关国标、行标以及已报批标准，初步形成了信息安全等级保护标准体系。这些标准分别从基础、设计、实施、管理、制度等各个方面对信息安全等级保护提出了要求和建议，为信息系统的使用者、设计者、建设者提供了管理规范和技术标准，如图1所示。

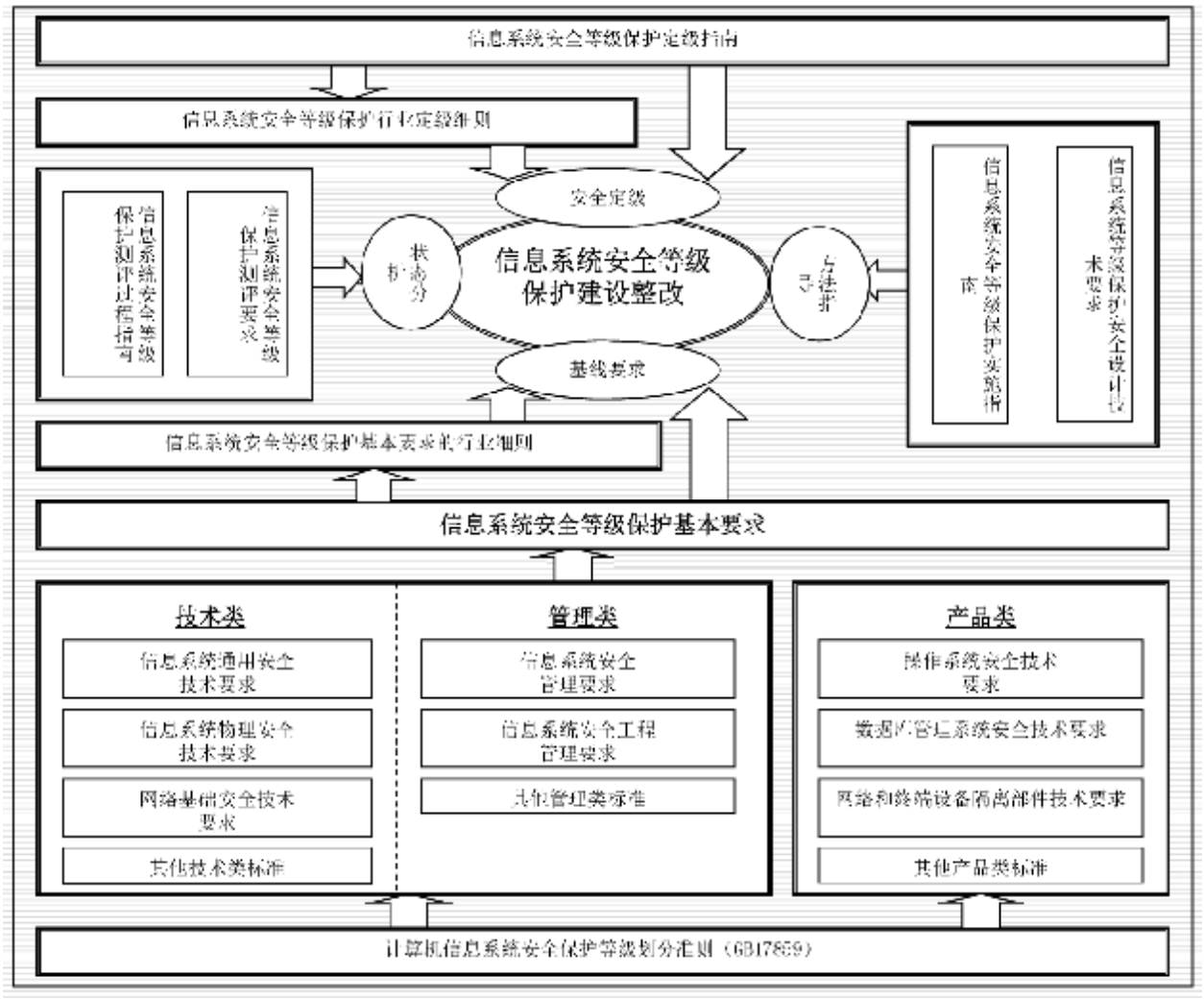

图 1 信息系统安全等级保护整体要求

4.1.1 基本要求

信息系统应依据信息系统的安全保护等级情况，保证它们具有相应等级的基本安全保护能力，不同安全保护等级的信息系统应具有不同的安全保护能力。

《信息安全技术 信息系统安全等级保护基本要求》(GB/T 22239-2008)(以下简称《基本要求》)是针对不同安全保护等级信息系统应该具有的基本安全保护能力提出的安全要求。根据实现方式的不同，基本安全要求分为基本技术要求和基本管理要求两大类，用于指导不同安全保护等级信息系统的安全建设和监督管理，如图2所示。技术类安全要求与信息系统提供的技术安全机制有关，主要通过在信息系统中部署软硬件并正确的配置其安全功能来实现;管理类安全要求与信息系统中各种角色参与的活动有关，主要通过控制各种角色的活动，从政策、制度、规范、流程以及记录等方面做出规定来实现。

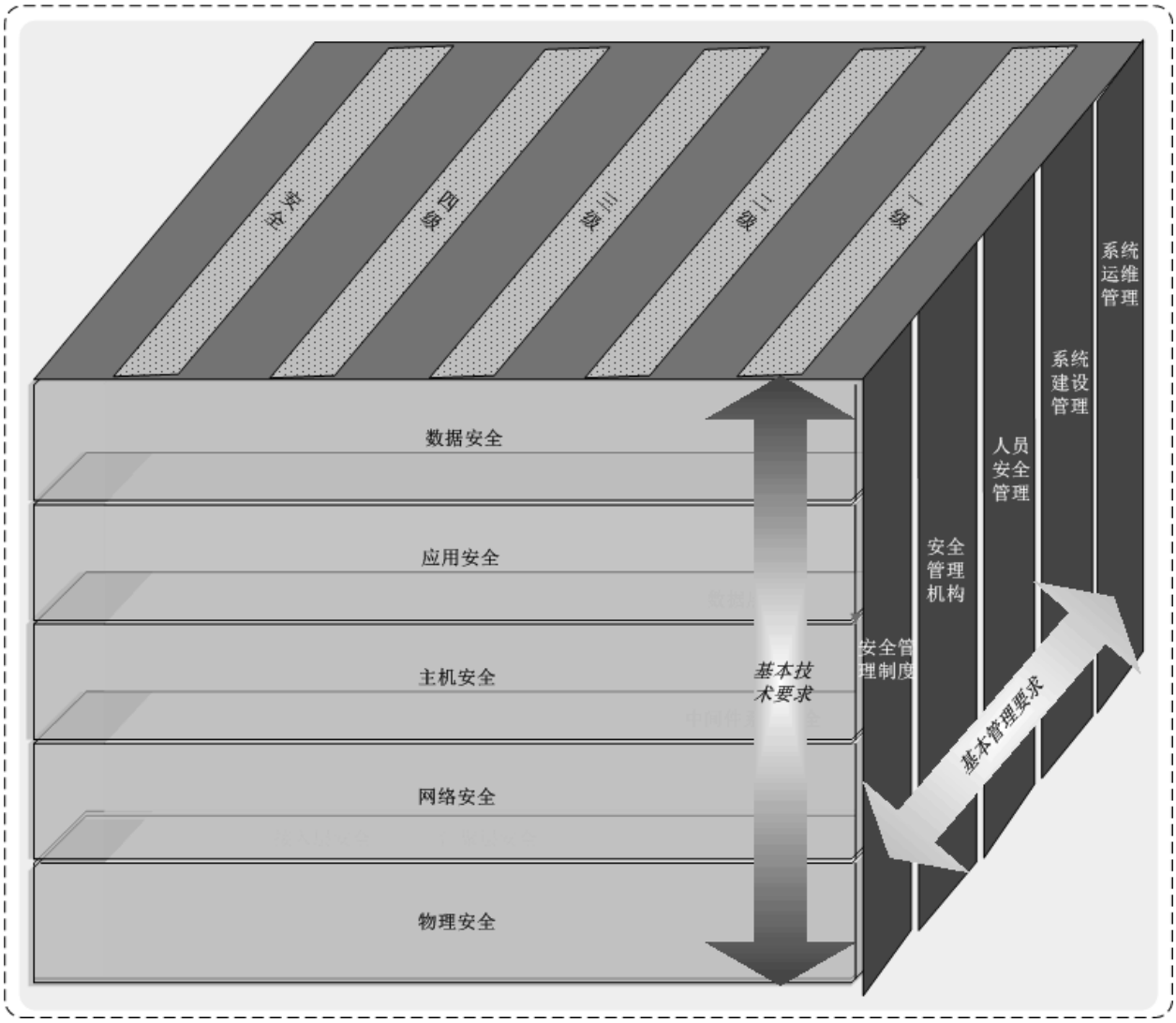

图 2 信息系统安全等级保护基本要求框架

其中，基本技术要求从物理安全、网络安全、主机安全、应用安全和数据安全几个层面提出；基本管理要求从安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理几个方面提出，基本技术要求和基本管理要求是确保信息系统安全不可分割的两个部分。

《基本要求》从各个层面或方面提出了系统的每个组件应该满足的安全要求，信息系统具有的整体安全保护能力通过不同组件实现基本安全要求来保证。除了保证系统的每个组件满足基本安全要求外，还要考虑组件之间的相互关系，来保证信息系统的整体安全保护能力。

4.1.2 设计要求

《信息安全技术 信息系统等级保护安全设计技术要求》(GB/T 25070-2010)(以下简称《设计要求》)是进行等级保护建设的直接指导，在《基本要求》的基础之上，采用了系统化的设计方法，引入了深度防御的保护理念，提出了“一个中心，三重防护”的保障框架，形成了在安全管理中心统一管理下安全计算环境、安全区域边界、安全通信网络层层防护的综合保障技术体系，规范了信息系统等级保护安全设计技术要求，包括第一级至第五级系统安全保护环境以及定级系统互联的设计技术要求，为信息系统的等级保护建设提供了科学、合理、有效的方法和指导。进行安全技术设计时，要根据信息系统定级情况，确定相应安全策略，采取相应级别的安全保护措施。

《设计要求》中明确指出信息系统等级保护安全技术设计包括各级系统安全保护环境的设计及其安全互联的设计，如图3所示。各级系统安全保护环境由相应级别的安全计算环境、安全区域边界、安全通信网络和（或）安全管理中心组成。定级系统互联由安全互联部件和跨定级系统安全管理中心组成。

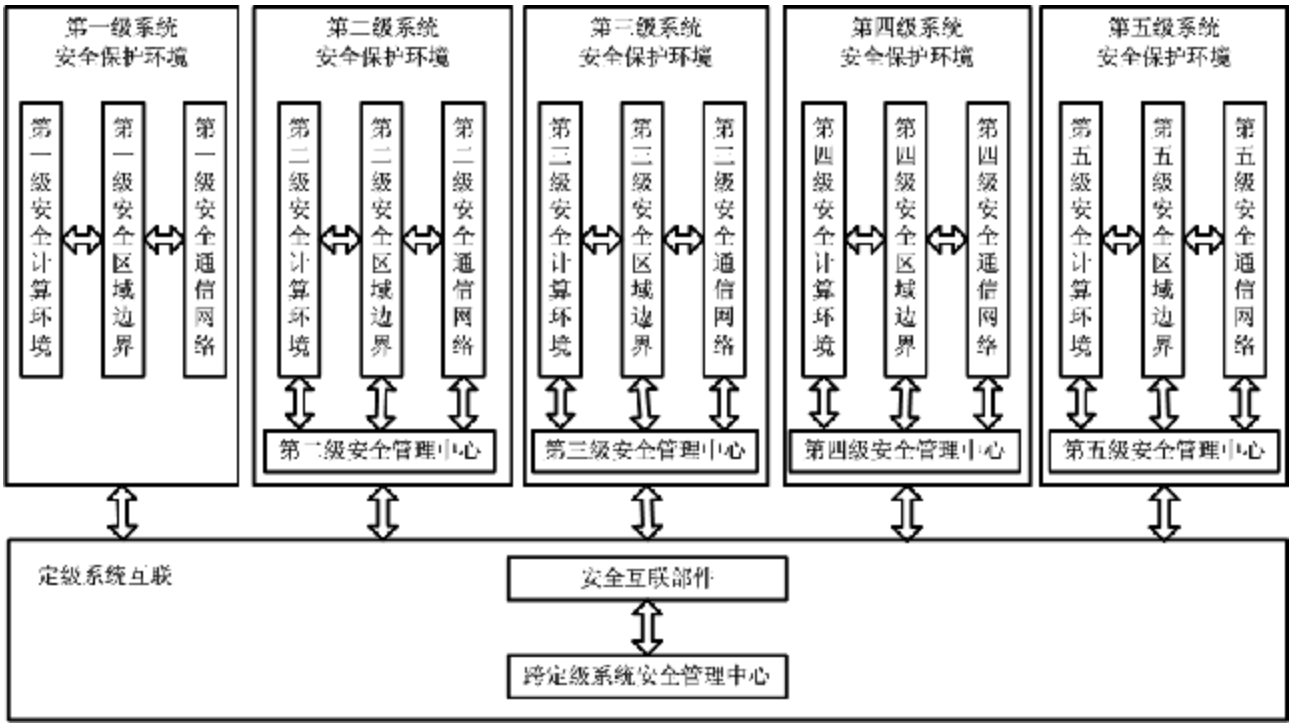

图 3 信息系统等级保护安全技术设计框架

4.2 指导思想

结合金融机构特点落实等级保护相关要求，指导思想可以通过图4进行说明：

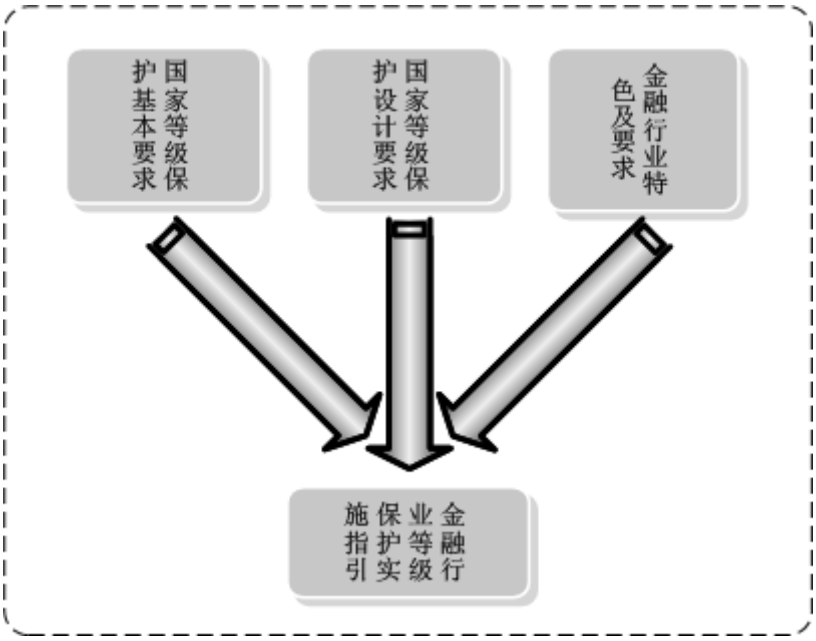

图 4 实施指引示意图

等级保护要求与金融机构系统特色相结合的指导思想，主要通过以下四个方面来体现：

a) 符合国家等级保护基本要求；

本标准依据国家等级保护基本要求中的技术要求和管理要求，分别对物理、网络、主机、人员、机构等10项内容进行规范，从而保障定级系统的安全。

b) 借鉴等级保护安全设计技术要求；

结合金融机构的安全体系架构，借鉴等级保护安全设计技术要求的体系化设计思路，设计出一套适合于金融行业的安全体系架构，从而保障同级系统、跨级系统互联乃至整个体系的安全。

c) 将等级保护基本要求给出具体的实施、配置措施；

针对等级保护基本要求，本标准将给出具体的实施、配置措施建议见附录A，以保证将等级保护的基本要求在金融机构实施。

d) 适用于金融机构特色的等级保护实施指引。

本标准新增“**金融行业增强安全保护类（F类）**”要求见附录B，该类要求是在结合等级保护及金融行业相关规定的基础上进行补充和完善。使得本标准更贴近金融行业的特点及需求，更容易理解和落实。

4.2.1 纵深防御设计的必要性

采用纵深防御的安全体系架构能够提供进行多层保护的框架，以此防范计算机威胁。该方法能够使攻破一层或一类的保护的攻击行为无法破坏整个信息系统基础设施。通过对网络基础设施、区域边界、计算环境、支撑性基础设施4个区域实施保护来实现纵深防御的目标。在纵深防御战略中，人、技术和操作是三个核心因素，要保障信息及信息系统的安全，三者缺一不可。人即管理，管理在信息安全保障体系建设中同样起到了十分关键的作用，可以说技术是安全的基础，管理是安全的根本。信息系统的安全稳定运行是与这三者密不可分的，因此，要保证信息系统的安全稳定运行，必须从技术、管理，单个系统、整个生产体系等多个维度进行设计和要求。

4.2.2 基本要求与纵深防御设计结合的意义

《基本要求》是等级保护建设的要求，《设计要求》是等级保护设计和实施的方法，《设计要求》提出的“一个中心，三重防护”的体系架构为等级保护的实施提供了科学、有效的方法，从系统化的角度、工程化的思想落实《基本要求》。因此将《基本要求》和《设计要求》进行有机结合保障整个体系的安全才是将等级保护的要求由点到面的落实和执行。

通过以下三个阶段保证将等级保护的要求由点到面的落实和执行。

a) 单个系统的安全：针对等级保护要求逐项建设落实；

b) 多个系统的安全：根据共同访问路径原则，划分子域；

c) 整个体系的安全：构建安全体系架构、安全防护体系。

5 信息安全保障框架

5.1 概述

《实施指引》以国家等级保护要求为原则，以金融行业特点为基础，形成了兼顾技术与管理、以《基本要求》为根本、以《设计要求》为基本方法设计的金融行业信息安全保障总体框架，如图 5 所示。

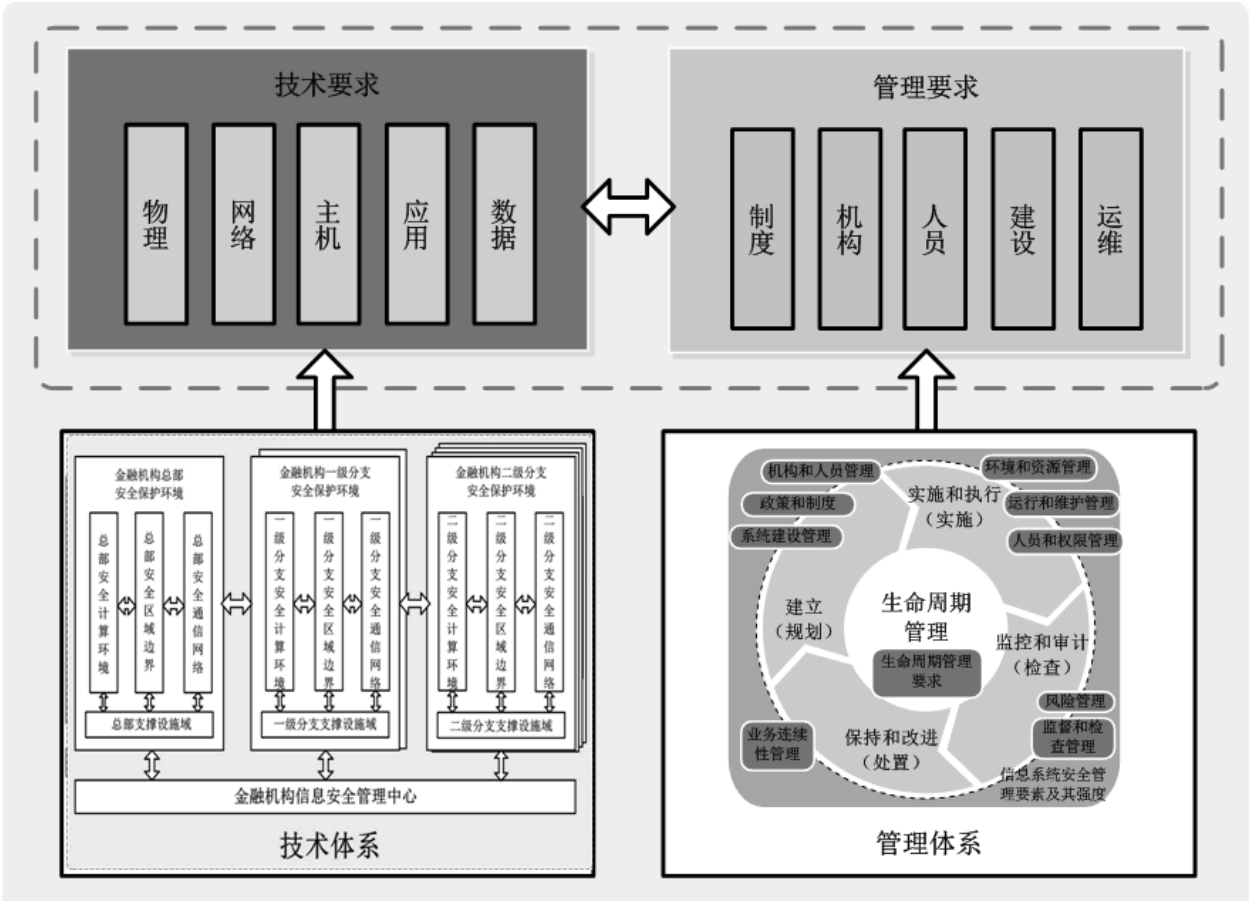

图 5 信息安全保障总体框架图

两项要求指由技术要求和管理要求综合形成的保障要求，技术要求涉及物理安全、网络安全、主机安全、应用安全、数据安全五方面要求；管理要求涉及安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理五方面要求。

两个体系指由技术体系和管理体系综合形成的保障体系。技术体系以“一个中心，三重防护”为核心理念，划分计算环境、区域边界、通信网络与管理中心，并且结合金融行业的系统与业务现状，进行分区分域保护；管理体系遵从生命周期法则，从建立、实施和执行、监控和审计、保持和改进四个过程进行科学化的管理，通过循环改进的思路形成“生命环”的管理方法。

技管交互指技术要求与管理要求的交融以及技术体系与管理体系的互补，从安全保障要求和安全保障方法两方面体现技术与管理并重的基本思想。

综合保障指该框架通过对保障要求和保障方法的综合考虑，通过技术与管理的有效结合，在遵循国家等级保护要求的前提下，满足金融行业的业务特殊性要求。

5.2 技术体系

参考《设计要求》的安全域模型，将 “安全域纵深防护”、“多层次立体防御” 和“信息安全等级保护”等安全防护思想相结合，建立金融行业信息安全保障技术体系模型。依据金融行业的组织结构、网络架构将每个机构作为一个整体保护对象，设计金融机构信息安全保障框架，如图6所示，总部和各个分支机构都是独立的安全域，每个安全域又细分计算环境域、区域边界、通信网络和支撑设施域，各金融机构根据本机构结构情况参考执行。

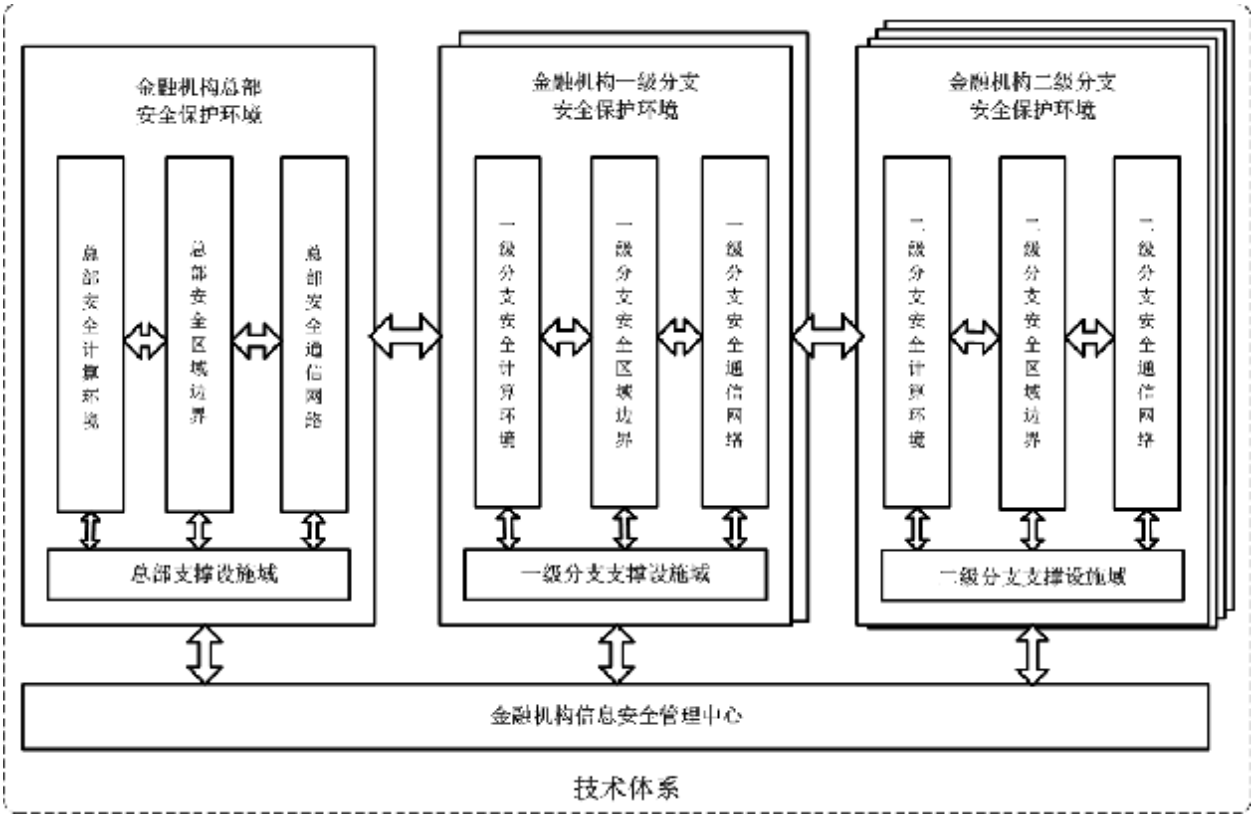

图 6 金融机构总体技术架构图

通过划分安全域的方法，将金融行业信息系统按照业务流程及特点、重要程度和等级的不同层面划分为不同的安全域，各个安全域内部又可以根据信息系统的元素对象划分为不同的安全子域，并针对每个安全域或安全子域来标识其中的关键资产，分析所存在的安全隐患和面临的安全风险，然后给出相应的保护措施，从而建立纵深防御体系，实现深度防护的目标。

5.2.1 计算环境

计算环境是对定级系统的信息进行存储、处理及实施安全策略的相关部件，计算环境安全是信息系统安全保护的核心与基础。计算环境安全指保障终端、服务器操作系统、数据库、上层应用系统以及应用业务处理全过程的安全。通过在操作系统核心层设置以访问控制为主体的系统安全机制，形成严密的安全保护环境，从而有效防止非授权用户访问和授权用户越权访问，确保信息和信息系统的保密性和完整性，为业务应用系统的正常运行、免遭恶意破坏提供支撑和保障。计算环境防护主要针对信息系统的主机安全、应用安全及数据安全。计算环境包含接入域，交换域和服务域。

5.2.1.1 接入域

根据金融行业的业务特点和接入关系而细分出的安全域，是应用系统防范的第一道屏障。根据接入的不同可分为对内系统接入子域、对外系统接入子域和用户接入子域三个部分。

a) 对内系统接入子域——部署与金融行业内部机构互联的网络设施以及相关的应用服务设施且不对外部机构提供服务。该子域物理上分布在总部、一级分支机构、二级分支机构。
b) 对外系统接入子域——部署与外部机构互联的网络设施以及相关应用服务设施。该子域物理上分布在总部、一级分支机构、二级分支机构。
c) 用户接入子域——部署金融机构内部各类桌面终端，该子域物理上分布在总部、一级分支机构、二级分支机构。

5.2.1.2 交换域

是由通信设施构成，主要负责各个安全域数据的交换。

5.2.1.3 服务域

服务域将应用系统的层次架构与服务设施类别相结合，服务域划分为以下两个子域：

a) 对外服务子域——部署为外部机构提供服务的信息系统业务服务设施，外部服务子域只与基础服务平台、对外资源产生逻辑访问关系。其中基础服务平台包括操作系统平台、基础架构平台和业务基础平台；对外资源部署为外部机构提供服务的信息系统资源服务设施（主要包括数据库服务器、存储系统）。对外资源设施为外部业务服务设施提供数据资源服务，是纵深防御体系重点防护的 IT 核心资产。

b) 对内服务子域——部署为金融机构内部提供服务的信息系统业务服务设施。内部服务子域只与基础服务平台、对内资源产生逻辑访问关系。其中对内资源部署为金融机构内部提供服务的信息系统资源服务设施（主要包括数据库服务器、存储系统）。对内资源服务设施只为对内业务服务设施提供数据资源服务，是纵深防御体系重点防护的 IT 核心资产。

5.2.2 区域边界

区域边界是定级系统的安全计算环境边界，及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。区域边界包括互联网区域边界、外部区域边界和内部区域边界，分别与互联网、外部机构和内部机构相连，并包含一系列针对互联网、内外机构不同威胁、风险而采用的安全策略。

区域边界安全指通过对进入和流出应用环境的信息流进行安全检查和访问控制，确保不会有违背系统安全策略的信息流经过边界。区域边界是物理网络分区与边界整合的分析依据，同时还是用户或外联应用接入计算环境域前重要的应用接入点，区域边界暴露在安全体系框架的最外面，是风险点集中的环节，是安全防护的重点。区域边界防护主要针对信息系统的网络安全。

由于不同系统之间存在业务互联和数据互联，因此不同系统间会存在安全级别、安全风险不同的情况。区域边界作为定级系统的安全计算环境边界，必须确保具有不同级别系统之间的可信互连机制。互连机制的建立必须基于较高级别系统或安全域的安全防护要求设置访问控制策略以及其他安全策略，可采用网络安全隔离技术或部署信息交换系统(比如前置系统等)实现，通过对不同级别的系统之间的可信互联进行严格约束来保证不会出现因高级别系统与低级别系统之间防护差异而导致的安全漏洞。

5.2.3 通信网络

通信网络是定级系统安全计算环境之间进行信息传输及实施安全策略的相关部件，通信网络安全指通信网络设备通过对通信双方进行可信鉴别验证，建立安全通道，并实施数据传输保护，确保数据在传输过程中不会被窃听、篡改和破坏。通信网络防护主要针对信息系统的网络安全。

5.2.4 支撑设施

支撑设施对计算环境、区域边界和通信网络实施统一的安全策略管理，确保系统配置完整可信，用户操作权限严格划分和审计全程追踪。从功能上可细分为系统管理、安全管理、综合审计管理以及物理支撑实施管理，各管理员职责和权利明确，三权分立，相互制约。

5.3 管理体系

要建成完善的安全管理体系，首先根据金融机构信息化建设进程的实际需求，逐步建立起安全管理机构、各项安全管理制度及人员配置；其次通过专职安全机构、人员对制度的执行，提高信息安全保障能力；后续根据执行结果检查各项制度存在的问题和缺陷；最后依据检查结果对制度进行改进。从而形成建立、实施和执行、监控和审计、保持和改进的循环过程，形成完善的管理体系。如图7所示：

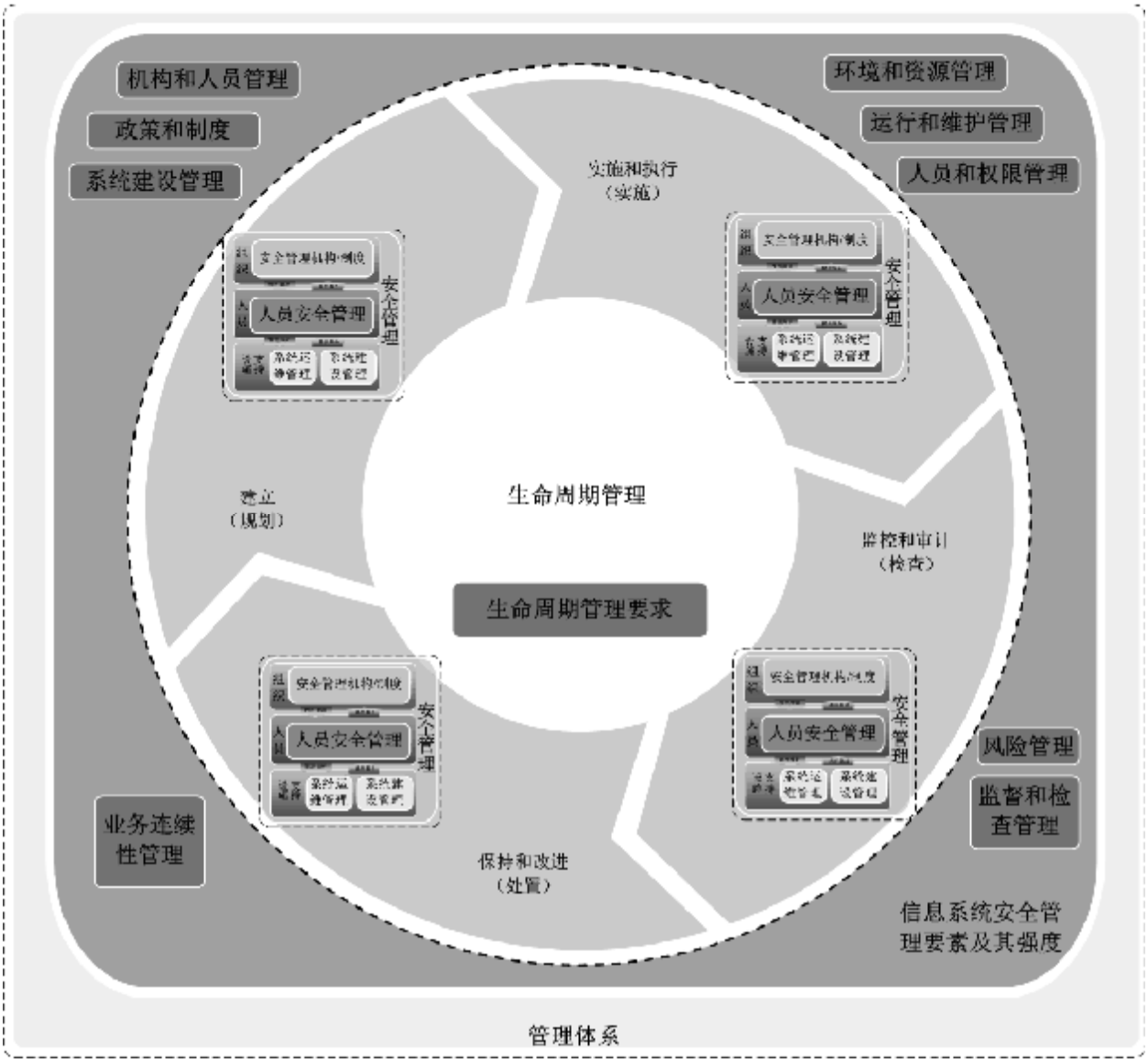

图 7 信息安全管理体系框架图

安全管理内容涵盖组织、人员、支持设施三大类。其中，组织涉及机构与制度管理；人员涉及人员管理；支撑设施涉及系统建设和系统运维管理。如图8所示：

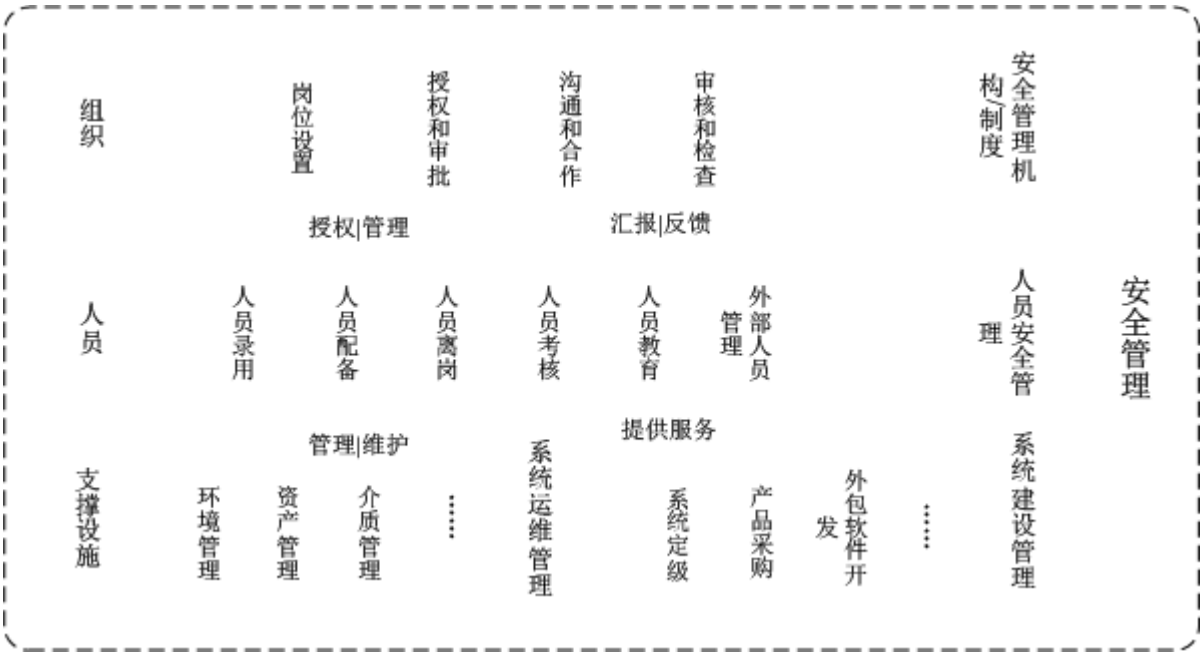

图 8 安全管理内容

6 保护要求

6.1 二级要求

6.1.1 技术要求

6.1.1.1 物理安全

1) 物理位置的选择（G2）
   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**以及交通、通信便捷地区。**
2) 物理访问控制（G2）
   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）**
3) 防盗窃和防破坏（G2）
   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）、门禁系统等重要设施实行全面监控。（F2）**
4) 防雷击（G2）
   a) 机房建筑应设置避雷装置；
   b) 机房应设置交流电源地线。
5) 防火（G2）

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）**

6) 防水和防潮（G2）
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。

7) 防静电（G2）
a) 关键设备应采用必要的接地防静电措施。

8) 温湿度控制（G2）
a) 机房应设置温、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。

9) 电力供应（A2）
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）**

10) 电磁防护（S2）
a) 电源线和通信线缆应隔离铺设，避免互相干扰。

6.1.1.2 **网络安全**

1) 结构安全（G2）
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。**

2) 访问控制（G2）
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。

3) 安全审计（G2）
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。**

4) 边界完整性检查（S2）
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。

5) 入侵防范（G2）
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。

6) 网络设备防护（G2）
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）**

6.1.1.3 主机安全

1) 身份鉴别（S2）
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。

2) 访问控制（S2）
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。

3) 安全审计（G2）
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**。

4) 入侵防范（G2）
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。

5) 恶意代码防范（G2）
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。

6) 资源控制（A2）
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。

6.1.1.4 应用安全

1) 身份鉴别（S2）

a) 应提供专用的登录控制功能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。

2) 访问控制（S2）
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）**

3) 安全审计（G2）
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**。

4) 通信完整性（S2）
a) 应采用校验码技术保证通信过程中数据的完整性。

5) 通信保密性（S2）
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。

6) 软件容错（A2）
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）**

7) 资源控制（A2）
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。

6.1.1.5 **数据安全及备份恢复**

1) 数据完整性（S2）
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。

2) 数据保密性（S2）
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。

3) 备份和恢复（A2）
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。

6.1.2 **管理要求**

6.1.2.1 **安全管理制度**

1) 管理制度（G2）

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。

2) 制定和发布（G2）
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**；**
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。

3) 评审和修订（G2）
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。

6.1.2.2 **安全管理机构**

1) 岗位设置（G2）
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。

2) 人员配备（G2）
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。

3) 授权和审批（G2）
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。

4) 沟通和合作（G2）
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。

5) 审核和检查（G2）
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。

6.1.2.3 **人员安全管理**

1) 人员录用（G2）
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）**

2) 人员离岗（G2）

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。**

3) 人员考核（G2）
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。

4) 安全意识教育和培训（G2）
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。

5) 外部人员访问管理（G2）
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）**

6.1.2.4 系统建设管理

1) 系统定级（G2）
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。

2) 安全方案设计（G2）
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。

3) 产品采购和使用（G2）
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）**

4) 自行软件开发（G2）
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。

5) 外包软件开发（G2）

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）**

6) 工程实施（G2）

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。

7) 测试验收（G2）

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）**

8) 系统交付（G2）

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；(F2)**

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。

9) 安全服务商选择（G2）

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；

e) 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。

6.1.2.5 系统运维管理

1) 环境管理（G2）

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。

2) 资产管理（G2）
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。

3) 介质管理（G2）
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）**

4) 设备管理（G2）
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。

5) 网络安全管理（G2）

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。**

6) 系统安全管理（G2）

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。

7) 恶意代码防范管理（G2）

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。

8) 密码管理（G2）

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）**

9) 变更管理（G2）

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）**

10) 备份与恢复管理（G2）

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；**

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）**

11) 安全事件处置（G2）

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）**

12) 应急预案管理（G2）

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）**

6.2 三级要求

6.2.1 技术要求

6.2.1.1 物理安全

1) 物理位置的选择（G3）

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**以及交通、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）**

2) 物理访问控制（G3）

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。

3) 防盗窃和防破坏（G3）

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）**

4) 防雷击（G3）

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。

5) 防火（G3）

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）

6) 防水和防潮（G3）

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。

7) 防静电（G3）

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）

8) 温湿度控制（G3）

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1的规定：

表 1 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）

9) 电力供应（A3）

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1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）**

10) 电磁防护（S3）

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)**

6.2.1.2 网络安全

1) 结构安全（G3）

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；

2) 访问控制（G3）

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）**

3) 安全审计（G3）

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。**

4) 边界完整性检查（S3）

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。

5) 入侵防范（G3）

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。

6) 恶意代码防范（G3）

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。

7) 网络设备防护（G3）

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）**

6.2.1.3 主机安全

1) 身份鉴别（S3）

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；（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。**

2) 访问控制（S3）

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) 宜对重要信息资源设置敏感标记；
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。

3) 安全审计（G3）
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。

4) 剩余信息保护（S3）
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。

5) 入侵防范（G3）
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。

6) 恶意代码防范（G3）
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）**

7) 资源控制（A3）
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）**

6.2.1.4 应用安全

1) 身份鉴别（S3）
   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）**
2) 访问控制（S3）
   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。
3) 安全审计（G3）
   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）**
4) 剩余信息保护（S3）
   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。
5) 通信完整性（S3）
   a) 应采用密码技术保证通信过程中**关键**数据的完整性。
6) 通信保密性（S3）
   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**；
7) 抗抵赖（G3）
   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。**

8) 软件容错（A3）

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）**

9) 资源控制（A3）

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。

6.2.1.5 数据安全及备份恢复

1) 数据完整性（S3）

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。

2) 数据保密性（S3）

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。

3) 备份和恢复（A3）

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）**

6.2.2 管理要求

6.2.2.1 安全管理制度

1) 管理制度（G3）
   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。
2) 制定和发布（G3）
   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。
3) 评审和修订（G3）
   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。

6.2.2.2 安全管理机构

1) 岗位设置（G3）
   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）**
2) 人员配备（G3）
   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。
3) 授权和审批（G3）
   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）**

4) 沟通和合作（G3）
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。

5) 审核和检查（G3）
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）**

6.2.2.3 人员安全管理

1) 人员录用（G3）
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）**

2) 人员离岗（G3）
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**。

3) 人员考核（G3）

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。

4) 安全意识教育和培训（G3）
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。

5) 外部人员访问管理（G3）
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）**

6.2.2.4 系统建设管理

1) 系统定级（G3）
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。

2) 安全方案设计（G3）
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。

3) 产品采购和使用（G3）
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）**

4) 自行软件开发（G3）

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）。**

5) 外包软件开发（G3）

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）**

6) 工程实施（G3）

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）**

7) 测试验收（G3）

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）**

8) 系统交付（G3）

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）**

9) 系统备案（G3）

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。

10) 等级测评（G3）

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。

11) 安全服务商选择（G3）

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。

6.2.2.5 **系统运维管理**

1) 环境管理（G3）

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。

2) 资产管理（G3）

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。

3) 介质管理（G3）

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）**

4) 设备管理（G3）

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。

5) 监控管理和安全管理中心（G3）
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。

6) 网络安全管理（G3）
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）**

7) 系统安全管理（G3）

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）**

8) 恶意代码防范管理（G3）

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。

9) 密码管理（G3）

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）**

10) 变更管理（G3）

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，确保生产系统的安全；（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）**

11) 备份与恢复管理（G3）

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）**

12) 安全事件处置（G3）

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）**

13) 应急预案管理（G3）

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）**

6.3 四级要求

6.3.1 技术要求

6.3.1.1 物理安全

1) 物理位置的选择（G4）

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**以及交通、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。

2) 物理访问控制（G4）

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。

3) 防盗窃和防破坏（G4）

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）**

4) 防雷击（G4）

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。

5) 防火（G4）

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）**

6) 防水和防潮（G4）

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。

7) 防静电（G4）

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）**

8) 温湿度控制（G4）

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2的规定：

表2 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）**

9) 电力供应（A4）

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）**

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）**

10) 电磁防护（S4）

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)**

6.3.1.2 网络安全

1) 结构安全（G4）

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）**

2) 访问控制（G4）

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）**

3) 安全审计（G4）

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。

4) 边界完整性检查（S4）
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。

5) 入侵防范（G4）
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）**

6) 恶意代码防范（G4）
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。

7) 网络设备防护（G4）
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）**

6.3.1.3 主机安全

1) 身份鉴别（S4）
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。**

2) 安全标记（S4）
a) 应对所有主体和客体设置敏感标记。

3) 访问控制（S4）
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。

4) 可信路径（S4）
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。

5) 安全审计（G4）
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。

6) 剩余信息保护（S4）
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。

7) 入侵防范（G4）
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。

8) 恶意代码防范（G4）
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）**

9) 资源控制（A4）

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）**

6.3.1.4 应用安全

1) 身份鉴别（S4）

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）**

2) 安全标记（S4）

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。

3) 访问控制（S4）

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**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；

4) 可信路径（S4）

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。

5) 安全审计（G4）

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）**

6) 剩余信息保护（S4）
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。

7) 通信完整性（S4）
a) 应采用密码技术保证通信过程中数据的完整性。

8) 通信保密性（S4）
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。

9) 抗抵赖（G4）
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**。

10) 软件容错（A4）
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）**

11) 资源控制（A4）
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。

6.3.1.5 数据安全及备份恢复

1) 数据完整性（S4）

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。

2) 数据保密性（S4）

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。

3) 备份和恢复（A4）

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）**

6.3.2 管理要求

6.3.2.1 安全管理制度

1) 管理制度（G4）

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。

2) 制定和发布（G4）

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。

3) 评审和修订（G4）

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。

6.3.2.2 安全管理机构

1) 岗位设置（G4）
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）**

2) 人员配备（G4）
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）**

3) 授权和审批（G4）
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）**

4) 沟通和合作（G4）
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。

5) 审核和检查（G4）
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）**

6.3.2.3 人员安全管理

1) 人员录用（G4）
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）**

2) 人员离岗（G4）
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**。

3) 人员考核（G4）
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。

4) 安全意识教育和培训（G4）
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。

5) 外部人员访问管理（G4）

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）**

6.3.2.4 系统建设管理

1) 系统定级（G4）

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。

2) 安全方案设计（G4）

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。

3) 产品采购和使用（G4）

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。

4) 自行软件开发（G4）

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）**

5) 外包软件开发（G4）
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）**

6) 工程实施（G4）
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）**

7) 测试验收（G4）
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）**

8) 系统交付（G4）

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）

9) 系统备案（G4）

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。

10) 等级测评（G4）

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。

11) 安全服务商选择（G4）

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**。

6.3.2.5 **系统运维管理**

1) 环境管理（G4）

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；**

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。

2) 资产管理（G4）

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。

3) 介质管理（G4）

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）**

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）**

4) 设备管理（G4）

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。

5) 监控管理和安全管理中心（G4）

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。

6) 网络安全管理（G4）

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）**

7) 系统安全管理（G4）

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。

8) 恶意代码防范管理（G4）

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。

9) 密码管理（G4）

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，并**遵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）**

10) 变更管理（G4）

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）**

11) 备份与恢复管理（G4）

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）**

12) 安全事件处置（G4）

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）**

13) 应急预案管理（G4）

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；**

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）**

附录 A
（资料性附录）
等级保护实施措施

A.1 网络安全

A.1.1 二级要求及措施

序号	要求的内容	对应技术措施	实现方式
结构安全			
1	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。	设备高可用性	可以通过以下方式保证处理能力具有冗余性： a) 高可用性设计： 双机热备：双机热备一 般分为主-从模式，在正常情况下由主机进行数据包的处理工作，从机实时监测主机的工作状态，如果从机出现了问题，会将主机的工作接管过来，确保网络不出现单点故障。 HA 集群：多台设备同时工作，同时进行数据包的处理工作（轮询是一种处理方式），无主从的区别，如果一台设备出现故障，另外的设备会将该设备工作接管过来。HA 集群在确保消除单点故障的基础上，还能提高该点的处理能力。 产品软硬件 bypass 功能：产品软硬件 bypass 功能可以保证设备在断电或者死机时，数据包还能通过故障设备，网络不中断。 b) 设备高性能设计：设备的高性能设计，如比较高的吞吐量、并发连接数能保证满足业务高峰期的需要。 在安全产品的部署上尽量采取双机的部署模式，特别是在核心数据区的边界或者流量比较大的区域边界处。并尽可能的选择具有软硬件 bypass 功能的产品。
2	应保证接入网络和核心网络的带宽满足业务高峰期需要。	设备高可靠性	可以通过以下方式保证带宽满足业务高峰期需要： a) 设备高性能设计：设备的高性能设计，如比较高的吞吐量、并发连接数能保证满足业务高峰期的需要。 b) 防火墙要适合金融业网间互联的网络带宽要求，不能成为网络瓶颈，或明显影响网络工作效率。
3	应绘制与当前运行情况相符的网络拓扑结构图。	拓扑规划	可以通过以下方式保证与当前运行情况相符的网络拓扑结构图： a) 拓扑规划设计 b) DNS 服务器配置中对主机的命名应采用不规则的方式，以保护整个网络的拓扑结构
4	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	地址规划与安全域隔离设计	可以通过以下方式保证地址分配要求： a) 地址规划设计 b) 安全域设计：防火墙、UTM 安全网关产品可以进行不同网段的划分，并为个子网、网段分配地址段。另外支持安全域划分，对不同的安全域实施不同的安全策略，提供等级不同的安全保护。防火墙至少有 3 个网络接口，分别用于外联区，内部网络和中立区；内部网络和中立区之间的访问设置访问策略，只允许彼此之间需要访问的地址和端口；内部网络对外联区的访问采用网络地址转换，同时只开放需要访问的端口；外联网络对中立区的访问设置严格的端口和 IP 访问策略，对不

	地址段。生产网、互联网、办公网之间都应实现有效隔离。		提供外部服务的 IP 地址和端口严格禁止；原则上禁止从外联区直接访问内部网络 在不同的情况下使用防火墙或者 UTM 安全网关进行网络隔离，在面临威胁较为**严峻**的情况下，如病毒、入侵，选择 UTM 安全网关进行网络隔离。
访问控制			
1	应在网络边界部署访问控制设备，启用访问控制功能。	网络访问控制	可以通过以下方式保证访问控制： a) 软硬件防火墙：防火墙为标准的网络访问控制设备，可对源接口、目的接口、协议类型、源地址、目的地址、服务和报文通讯时间等对象设置访问控制策略。 b) UTM 安全网关：UTM 安全网关产品包括了防火墙功能。 c) VLAN 间访问控制技术：可在交换机上设置 VLAN 之间的 ACL 列表，实现端口级别的访问控制策略，但列表过多的话会影响交换机的性能。 在网络访问控制设备的选择上尽可能使用防火墙或者 UTM 安全网关产品，如果边界面临的风险比较复杂（如同时面临了恶意代码、病毒等威胁），建议使用 UTM 安全网关产品。
2	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。	网络访问控制	可以通过以下方式保证访问控制的控制粒度： a) 软硬件防火墙：防火墙为标准的网络访问控制设备，可对源接口、目的接口、协议类型、源地址、目的地址、服务和报文通讯时间等对象设置访问控制策略，可实现网段级允许/拒绝控制。 b) UTM 安全网关：UTM 安全网关产品包括了防火墙功能。 c) VLAN 间访问控制技术：可在交换机上设置 VLAN 之间的 ACL 列表，实现端口级、网段级的访问控制策略，但列表过多的话会影响交换机的性能。 d) 入侵防护系统：入侵防护系统产品包括了防火墙功能。 e) 终端/服务器安全保护系统：具有主机防火墙功能，可以对终端/服务器访问的目的地址、源地址、服务以及发起访问的进程进行控制，只有允许的进程才能对指定的源地址、目的地址和服务进行访问。可实现网段级、端口级的控制粒度。 选择专业的安全产品进行网段级粒度的访问控制，终端/服务器安全保护系统可以与防火墙、UTM 安全网关产品形成联动方案，组成从边界到终端/服务器的全网访问控制方案。
3	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。	网络访问控制	可以通过以下方式保证访问控制实现的用户粒度： a) 软硬件防火墙：可使用 web 认证、sslvpn 用户、L2TP 用户认证功能和安全策略结合，根据用户/用户组对系统资源的访问进行控制。 b) UTM 安全网关：UTM 安全网关产品具有防火墙功能。 c) 终端/服务器安全保护系统：具有内网访问控制能力，可以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。 选择专业的安全产品进行用户级粒度的访问控制，终端/服务器安全保护系统可以与防火墙、UTM 安全网关产品形成联动方案，组成从边界到主机的全网访问控制方案。
4	应限制具有拨号访问权限的用户数量。	网络访问控制	可以通过以下方式保证访问控制的拨号访问权限： a) 软硬件防火墙：支持 L2TP、SSL VPN 拨号用户，可以在用户组中限定用户数量。

			b) UTM 安全网关：支持 L2TP、SSL VPN 拨号用户，可以在用户组中限定用户数量。 在拨号访问时选择 L2TP、SSL VPN 等技术确保安全加密访问，并由设备进行拨号用户数的限制。
安全审计			
1	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。	日志审计措施	可以通过以下方式保证日志记录： a) 日志审计系统：能够对网络中的 TCP 流量按协议进行统计分析，并能够对用户行为进行详细的记录和分析，包括 Telnet、FTP、rlogin、X11、nfs、Netbios、oracle、sybase、informix、db2、sqlserver、HTTP、SMTP、POP3 等用户行为。 b) 其他设备的日志审计功能（如防火墙、UTM）：防火墙和 UTM 安全网关具有日志审计功能，可以记录访问的源、目的地址、服务、时间、用户以及攻击报警信息。 c) 网管系统：可以使用专门的网管系统对网络设备的运行状况进行记录。 使用专门的日志审计系统对网络流量、用户行为等进行日志记录；防火墙与 UTM 安全网关的日志功能可配合日志审计系统；使用网管系统对网络设备的运行状况进行记录。
2	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**。	日志审计措施	可以通过以下方式保证日志记录： a) 日志审计系统：可提供包括源 IP、源端口、目的 IP、目的端口、MAC 地址、登录账号、操作内容、时间等信息的查询。 b) 其他设备的日志审计功能（如防火墙、UTM）：防火墙和 UTM 安全网关具有日志审计功能，可以记录访问的源、目的地址、服务、时间、用户以及攻击报警信息。 使用专门的日志审计系统对网络流量、用户行为等进行日志记录；防火墙与 UTM 安全网关的日志功能可配合日志审计系统；
边界完整性检查			
1	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。	准入控制	可以通过以下方式保证准入控制： a) 终端/服务器安全保护系统：具有防非法外联功能，可以对未通过准许私自联到外部网络的行为（例如 modem 拨号、ADSL 拨号、私联网线和私设 IP 等行为）进行检查和控制。 b) 防火墙：具备外联控制功能，可以控制内部用户不能访问外部网络，或者必须经过认证才能访问外部网络；另外能够进一步对 IM、P2P、网络游戏等外联行为进行控制。 c) UTM 安全网关：具备外联控制功能，可以控制内部用户不能访问外部网络，或者必须经过认证才能访问外部网络；另外能够进一步对 IM、P2P、网络游戏等外联行为进行控制。 使用防火墙/UTM 安全网关+终端/服务器安全保护系统的全网外联控制方案，杜绝私联外网行为的出现。
入侵防范			
1	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	入侵检测与防范措施	可以通过以下方式保证入侵防范： a) 入侵检测系统：可在网络的任意位置监视各种攻击行为，包括：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。入侵检测系统将检测的结果逐级汇总，

	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。		形成分布分级管理的管理方式。 b) 入侵防护系统：可监视各种攻击行为，包括：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。 c) UTM安全网关：可监视各种攻击行为，包括：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。 d) DNS服务器：采用设置区域列表存取下限、监督DNS使用的端口，防止远程缓存溢出攻击和拒绝服务攻击；要通过活动目录安全实现DNS的安全；要能够有效地防止DNS欺骗、域名劫持攻击。 **应**按照不同的网络情况，合理的部署入侵检测系统、入侵防护系统与UTM安全网关；如在边界处部署入侵防护系统与UTM安全网关，在交换机上部署入侵检测系统。
网络设备防护			
1	应对登录网络设备的用户进行身份鉴别。	身份认证	可以通过以下方式保证登录网络设备的身份鉴别： a) 设备自身的登录账号与口令：网络设备、安全设备大多都支持登录账户与口令认证。 b) 数字证书认证：数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。可以对网络上传输的信息进行加密和解密、数字签名和签名验证，除了身份认证的功能，还可确保网上传递信息的机密性、完整性。网络设备、安全设备大多都支持数字证书认证。 c) 第三方认证技术，RADIUS、LADP、TACAS+(思科私有)：这些认证技术都有独立的认证服务器，用户先到认证服务器上进行账户与口令的认证，认证通过后才可登录安全设备或网络设备进行管理。大多数网络设备和安全设备都支持RADIUS、LADP认证技术，TACAS+为思科私有协议，一般只有思科设备支持。 **应**在登录网络设备时使用数字证书认证或者第三方认证技术。
2	应对网络设备的管理员登录地址进行限制。	地址绑定、网络访问控制	可以通过以下方式保证登录地址限制： a) 地址绑定技术：IP与MAC地址相绑定，防止地址盗用与欺骗。 b) 地址访问控制技术：使用防火墙、UTM安全网关等设备设置管理员登录地址的限制。
3	网络设备用户的标识应唯一。	标识鉴别	可以通过以下方式保证网络设备的标识唯一： a) 设备命名管理：通过设备命名管理，可以在设备管理上实现标识唯一。 b) 管理账号命名管理：通过管理账号命名管理可以实现用户标识唯一。
4	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。	身份鉴别	可以通过以下方式保证网络设备口令安全： a) 定期口令修改：能提高口令的安全性。 b) 口令强度规定：数字、字母、特殊符号设置能提高口令的安全性。
5	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	登录控制	可以通过以下方式保证网络设备登录失败处理： a) 登录失败次数设置 b) 登录失败限制措施设置 c) 登录超时设置

	和当网络登录连接超时自动退出等措施。		
6	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。	通讯加密、网络访问控制	可以通过以下方式保证网络设备远程管理不被窃听： a) 使用加密的通讯协议，如 SSH、HTTPS：SSH 与 HTTPS 能对传输的鉴别信息进行加密，防止在网络传输过程中被窃听。 b) 网络管理协议采用 SNMPV2，同时应参照口令管理方式设置口令，对于网络设备不支持 SNMPv2 的，允许采用其他方式进行管理，如私有协议。
7	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。	配置文件备份	可以建立 FTP 文件服务器，每月把重要网络设备的配置文件(起始配置和当前配置)上传到服务器上。如果网络设备配置发生变动，可以及时上传配置文件到服务器。
8	应定期对网络设备运行状况进行检查。	运行状况检查	定期进行网络巡检(通常情况下是每天进行巡检)，巡检时 通过网络监控软件如 nagios 等对网络设备的重要监控指标或实际需要进行监控，检查内容包括：cpu 运行状况，网络流量统计，网络用户数统计，设备空间使用状况等。
9	关闭非业务所必需的网络端口，包括停止这些端口上的服务程序，并建立业务服务及端口明细表，并建立相应的端口开放审批制度。	服务最小化	执行如下操作，检查各端口关闭和开启情况 #Show ip interface brief 关闭不必要服务的端口或登陆网路设备 service stop 命令停止不必要服务。同时记录已开启的服务及其对应的端口，形成文档保存，并建立相应的服务和端口开启的审批制度。
10	应定期检验网络设备软件版本信息。	版本检查	每月检查网络设备版本，版本升级时更新版本记录表。同时，根据网络设备运行情况，定期对版本进行评估。
11	应建立网络设备的时钟同步机制。	时钟同步	建立可独立基于 NTP/SNTP 协议工作的时间同步服务器，服务器与标准时钟信号信息一致，并设置网络设备自动与时间服务器的同步。
12	应定期检查并锁定或撤销网络设备中多余的用户账号。	账号最小化	定期检查和梳理网路设备账号并文字记录查询情况，删除或锁定多余账号

A.1.2 三级要求及措施

序号	要求的内容	对应技术措施	实现方式
结构安全			
1	应保证主要网络	设备高可用性	可以通过以下方式保证处理能力具有冗余性：

	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。		a) 高可用性设计： 双机热备：双机热备一般分为主-从模式，在正常情况下由主机进行数据包的处理工作，从机实时监测主机的工作状态，如果从机出现了问题，会将主机的工作接管过来，确保网络不出现单点故障。 HA 集群：多台设备同时工作，同时进行数据包的处理工作（轮询是一种处理方式），无主从的区别，如果一台设备出现故障，另外的设备会将该设备工作接管过来。HA 集群在确保消除单点故障的基础上，还能提高该点的处理能力。 产品软硬件 bypass 功能：产品软硬件 bypass 功能可以保证设备在断电或者死机时，数据包还能通过故障设备，网络不中断。 b) 设备高性能设计：设备的高性能设计，如比较高的吞吐量、并发连接数能保证满足业务高峰期的需要。 应在安全产品的部署上尽量采取双机的部署模式，特别是在核心数据区的边界或者流量比较大的区域边界处。并尽可能的选择具有软硬件 bypass 功能的产品。
2	应保证网络各个部分的带宽满足业务高峰期需要。	设备高可靠性	可以通过以下方式保证带宽满足业务高峰期需要： a) 设备高性能设计：设备的高性能设计，如比较高的吞吐量、并发连接数能保证满足业务高峰期的需要。 b) 防火墙要适合金融业网间互联的网络带宽要求，不能成为网络瓶颈，或明显影响网络工作效率。
3	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。	路由控制	可以通过以下方式保证路由控制： a) 在路由器上设置：路由器上可以设置业务终端与服务器之间的路由，选用的路由器产品应符合 GB/T 18018—1999 路由器安全技术要求。 b) 在软硬件防火墙、UTM 安全网关上进行路由控制：防火墙于 UTM 安全网关支持静态路由、策略路由，可以通过 RIP、OSPF 学习动态路由功能，支持通过等价路由进行流量负载分担。通过合理的路由控制，在业务终端和服务器之间设定安全的访问路径。选用的防火墙产品应符合国家标准 GB/T 18019－1999 和 GB/T 18020－1999。
4	应绘制与当前运行情况相符的网络拓扑结构图。	拓扑规划	可以通过以下方式保证与当前运行情况相符的网络拓扑结构图： a) 拓扑规划设计 b) DNS 服务器配置中对主机的命名应采用不规则的方式，以保护整个网络的拓扑结构
5	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	地址规划与安全域隔离设计	可以通过以下方式保证地址分配要求： a) 地址规划设计 b) 安全域设计：防火墙、UTM 安全网关产品可以进行不同网段的划分，并为个子网、网段分配地址段。另外支持安全域划分，对不同的安全域实施不同的安全策略，提供等级不同的安全保护。 c) 防火墙至少有 3 个网络接口，分别用于互联网，办公网和生产网；办公网和生产网之间的访问设置访问策略，只允许彼此之间需要访问的地址和端口；办公网对互联网的访问采用网络地址转换，同时只开放需要访问的端口；互联网对生产网的访问设置严格的端口和 IP 访问策略，对不提供外部服务的 IP 地址和端口严格禁止；原则上禁止从互联网直接访问办公网络。

	效隔离。		
6	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。	拓扑规划设计与网络访问控制	可以通过以下方式保证拓扑设计与网络访问控制： a) 合理的拓扑规划设计 b) 软硬件防火墙隔离：防火墙可以将内部与外部信息系统、重要网段与其他网段进行隔离，防火墙至少有 3 个网络接口，分别用于互联网，办公网和生产网；办公网和生产网之间的访问设置访问策略，只允许彼此之间需要访问的地址和端口；办公网对互联网的访问采用网络地址转换，同时只开放需要访问的端口；互联网对生产网的访问设置严格的端口和 IP 访问策略，对不提供外部服务的 IP 地址和端口严格禁止；禁止从互联网直接访问办公网络。 c) UTM 安全网关隔离：UTM 安全网关产品可以将内部与外部信息系统、重要网段与其他网段进行隔离。 应在不同的情况下使用防火墙或者 UTM 安全网关进行网络隔离，在面临威胁较为的情况下，如病毒、入侵，选择 UTM 安全网关进行网络隔离。
7	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。	流量/带宽管理	可以通过以下方式保证流量/带宽管理： a) 网络设备 QOS 设置：可以按照不同的路径设置带宽。 b) 软硬件防火墙带宽管理：可以设置最大大带宽、最小带宽、保证带宽，带宽粒度一般为 KB 级。 c) UTM 安全网关带宽管理：可以设置最大大带宽、最小带宽、保证带宽，带宽粒度一般为 KB 级。
访问控制			
1	应在网络边界部署访问控制设备，启用访问控制功能。	网络访问控制	可以通过以下方式保证访问控制： a) 软硬件防火墙：防火墙为标准的网络访问控制设备，可对源接口、目的接口、协议类型、源地址、目的地址、服务和报文通讯时间等对象设置访问控制策略。 b) UTM 安全网关：UTM 安全网关产品包括了防火墙功能。 c) VLAN 间访问控制技术：可在交换机上设置 VLAN 之间的 ACL 列表，实现端口级别的访问控制策略，但列表过多的话会影响交换机的性能。 应在网络访问控制设备的选择上尽可能使用防火墙或者 UTM 安全网关产品，如果边界面临的风险比较复杂（如同时面临了恶意代码、病毒等威胁），建议使用 UTM 安全网关产品。
2	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。	网络访问控制	可以通过以下方式保证访问控制的控制粒度： a) 软硬件防火墙：防火墙为标准的网络访问控制设备，可对源接口、目的接口、协议类型、源地址、目的地址、服务和报文通讯时间等对象设置访问控制策略，可实现网段级允许/拒绝控制。 b) UTM 安全网关：UTM 安全网关产品包括了防火墙功能。 c) VLAN 间访问控制技术：可在交换机上设置 VLAN 之间的 ACL 列表，实现端口级、网段级的访问控制策略，但列表过多的话会影响交换机的性能。 d) 入侵防护系统：入侵防护系统产品包括了防火墙功能。 e) 终端/服务器安全保护系统：具有主机防火墙功能，可以对终端/服务器访问的目的地址、源地址、服务以及发起访问的进程进行管理，只

			有允许的进程才能对指定的源地址、目的地址和服务进行访问。可实现网段级、端口级的控制粒度。 应选择专业的安全产品进行网段级粒度的访问控制，终端/服务器安全保护系统可以与防火墙、UTM 安全网关产品形成联动方案，组成从边界到主机的全网访问控制方案。
3	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。	网络访问控制	可以通过以下方式保证访问控制命令级的实现： a) 软硬件防火墙：防火墙可以实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制； b) UTM 安全网关：UTM 安全网关可以实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制； c) 入侵防护系统：入侵防护系统可以实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；
4	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。	网络访问控制	可以通过以下方式保证该要求的实现： a) 软硬件防火墙：可以基于不同协议的会话超时机制，超时后网络接连终止。超时时间可以采用默认配置，也可以由用户更改。 b) UTM 安全网关：可以基于不同协议的会话超时机制，超时后网络接连终止。超时时间可以采用默认配置，也可以由用户更改。 应使用防火墙与 UTM 安全网关实现该要求目标。
5	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。	网络访问控制	可以通过以下方式保证该要求的实现： a) 软硬件防火墙：支持带宽限制和并发连接数限制。可以根据安全策略限定最大网络带宽，可以设定系统的、具体 IP 的最大并发连接数。 b) UTM 安全网关：支持带宽限制和并发连接数限制。可以根据安全策略限定最大网络带宽，可以设定系统的、具体 IP 的最大并发连接数。 c) 终端/服务器安全保护系统：具有流量控制功能，可以实现基于端口、协议和进程的流量控制，网络并发连接数控制。 应使用防火墙、UTM 安全网关和终端/服务器安全保护系统实现该要求目标。
6	重要网段应采取技术手段防止地址欺骗。	网络访问控制	可以通过以下方式保证该要求的实现： a) 软硬件防火墙：IP-MAC 绑定措施来防止 ARP 欺骗。 b) UTM 安全网关：IP-MAC 绑定措施来防止 ARP 欺骗。 c) 终端/服务器安全保护系统：具备 ARP 欺骗防护和ＩＰ仿冒控制能力，可以有效防止重要网段的地址欺骗。 应采用防火墙、UTM 安全网关与终端/服务器安全保护系统相结合的方案来防止地址欺骗。
7	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。	网络访问控制	可以通过以下方式保证访问控制实现的用户粒度： a) 软硬件防火墙：可使用 web 认证、sslvpn 用户、L2TP 用户认证功能和安全策略结合，根据用户/用户组对系统资源的访问进行控制。 b) UTM 安全网关：UTM 安全网关产品具有防火墙功能。 c) 终端/服务器安全保护系统：具有内网访问控制能力，可以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。 应选择专业的安全产品进行用户级粒度的访问控制，终端/服务器安全保护系统可以与防火墙、UTM 安全网关产品形成联动方案，组成从边界到主机的全网访问控制方案。

8	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。	网络访问控制	可以通过以下方式保证访问控制的拨号访问权限： a) 软硬件防火墙：支持 L2TP、SSL VPN 拨号用户，可以在用户组中限定用户数量。 b) UTM 安全网关：支持 L2TP、SSL VPN 拨号用户，可以在用户组中限定用户数量。 应在拨号访问时选择 L2TP、SSL VPN 等技术确保安全加密访问，并由设备进行拨号用户数的限制。
9	网络设备应按最小安全访问原则设置访问控制权限。	网络访问控制	可以通过以下方式保证访问控制实现的用户粒度： a) 软硬件防火墙：可使用 web 认证、sslvpn 用户、L2TP 用户认证功能和安全策略结合，根据用户/用户组对系统资源的访问进行控制。 b) UTM 安全网关：UTM 安全网关产品具有防火墙功能。 c) 终端/服务器安全保护系统：具有内网访问控制能力，可以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。 应选择专业的安全产品进行用户级粒度的访问控制，终端/服务器安全保护系统可以与防火墙、UTM 安全网关产品形成联动方案，组成从边界到主机的全网访问控制方案。
安全审计			
1	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。	日志审计措施	可以通过以下方式保证日志记录： a) 日志审计系统：能够对网络中的 TCP 流量按协议进行统计分析，并能够对用户行为进行详细的记录和分析，包括 Telnet、FTP、rlogin、X11、nfs、Netbios、oracle、sybase、informix、db2、sqlserver、HTTP、SMTP、POP3 等用户行为。 b) 其他设备的日志审计功能（如防火墙、UTM）：防火墙和 UTM 安全网关具有日志审计功能，可以记录访问的源、目的地址、服务、时间、用户以及攻击报警信息。 c) 网管系统：可以使用专门的网管系统对网络设备的运行状况进行记录。 应使用专门的日志审计系统对网络流量、用户行为等进行日志记录；防火墙与 UTM 安全网关的日志功能可配合日志审计系统；使用网管系统对网络设备的运行状况进行记录。
2	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。	日志审计措施	可以通过以下方式保证日志记录： a) 日志审计系统：可提供包括源 IP、源端口、目的 IP、目的端口、MAC 地址、登录账号、操作内容、时间等信息的查询。 b) 其他设备的日志审计功能（如防火墙、UTM）：防火墙和 UTM 安全网关具有日志审计功能，可以记录访问的源、目的地址、服务、时间、用户以及攻击报警信息。 应使用专门的日志审计系统对网络流量、用户行为等进行日志记录；防火墙与 UTM 安全网关的日志功能可配合日志审计系统；
3	应能够根据记录数据进行分析，并生成审计报表。	日志审计措施	可以通过以下方式保证生成审计报表： a) 日志审计系统：可提供网络审计数据分析功能。 b) 其他设备的日志审计功能（如防火墙、UTM）：可提供网络审计数据分析功能。 应使用日志审计系统和设备上的日志审计功能来实现该要求目标。

4	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。	日志审计措施	可以通过以下方式对审计记录进行保护： a) 日志审计系统：具有审计记录保护功能，可以避免受到未预期的删除、修改或覆盖等。 b) 其他设备的日志审计功能（如防火墙、UTM）：具有审计记录保护功能，可以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。 建议人行用户选择具有审计记录保护功能的审计产品。
		边界完整性检查	
1	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。	准入控制	可以通过以下方式保证准入控制： a) 终端管理：终端管理产品具有防非法外联功能，可以对未通过准许私自联到外部网络的行为（例如 modem 拨号、ADSL 拨号、私联网线和私设 IP 等行为）进行检查，并阻断其行为。 b) 防火墙：具备外联控制功能，可以控制内部用户不能访问外部网络，或者必须经过认证才能访问外部网络；另外能够进一步对 IM、P2P、网络游戏等外联行为进行控制。 c) UTM 安全网关：具备外联控制功能，可以控制内部用户不能访问外部网络，或者必须经过认证才能访问外部网络；另外能够进一步对 IM、P2P、网络游戏等外联行为进行控制。 应使用防火墙/UTM 安全网关+终端管理的全网外联控制方案，杜绝私联外网行为的出现。
2	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。	准入控制	可以通过以下方式保证准入控制： a) 终端/服务器安全保护系统：具有防非法外联功能，可以对未通过准许私自联到外部网络的行为（例如 modem 拨号、ADSL 拨号、私联网线和私设 IP 等行为）进行检查，并阻断其行为。 b) 防火墙：具备外联控制功能，可以控制内部用户不能访问外部网络，或者必须经过认证才能访问外部网络；另外能够进一步对 IM、P2P、网络游戏等外联行为进行控制。 c) UTM 安全网关：具备外联控制功能，可以控制内部用户不能访问外部网络，或者必须经过认证才能访问外部网络；另外能够进一步对 IM、P2P、网络游戏等外联行为进行控制。 应使用防火墙/UTM 安全网关+终端/服务器安全保护系统的全网外联控制方案，杜绝私联外网行为的出现。
入侵防范			
1	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。	入侵检测与防范措施	可以通过以下方式保证入侵防范： a) 入侵检测系统：可在网络的任意位置监视各种攻击行为，包括：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。入侵检测系统将检测的结果逐级汇总，形成分布分级管理的管理方式。 b) 入侵防护系统：可监视各种攻击行为，包括：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。 c) UTM 安全网关：可监视各种攻击行为，包括：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。 d) DNS 服务器：采用设置区域列表存取下限、监督 DNS 使用的端口，防止

			远程缓存溢出攻击和拒绝服务攻击；要通过活动目录安全实现 DNS 的安全；要能够有效地防止 DNS 欺骗、域名劫持攻击。 应按照不同的网络情况，合理的部署入侵检测系统、入侵防护系统与 UTM 安全网关；如在边界处部署入侵防护系统与 UTM 安全网关，在交换机上部署入侵检测系统。
2	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。	入侵检测与防范措施	可以通过以下方式保证入侵防范： a) 入侵检测系统：当检测到攻击行为时，可记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时可提供报警及自动采取相应动作。 b) 入侵防护系统：当检测到攻击行为时，可记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时可提供报警及自动采取相应动作。 c) UTM 安全网关：当检测到攻击行为时，可记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时可提供报警及自动采取相应动作。 应按照不同的网络情况，合理的部署入侵检测系统、入侵防护系统与 UTM 安全网关；如在边界处部署入侵防护系统与 UTM 安全网关，在交换机上部署入侵检测系统。
恶意代码防范			
1	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。	内容安全措施	可以通过以下方式保证内容安全措施的实现： a) 入侵防护系统：防病毒和入侵防护功能，可对恶意代码进行检测和清除。 b) UTM 安全网关：防病毒和入侵防护功能，可对恶意代码进行检测和清除。 应使用入侵防护系统与 UTM 安全网关进行恶意代码的检测和清除。
2	应定期对恶意代码防护设备进行代码库升级和系统更新。	内容安全措施	可以通过以下方式保证内容安全措施的实现： c) 入侵防护系统：具有病毒库与入侵库，可以定期升级。 d) 入侵检测系统：具有入侵库，可以定期升级。 e) UTM 安全网关：具有病毒库与入侵库，可以定期升级。 应定期更新入侵防护系统、入侵检测系统与 UTM 安全网关的恶意代码库和检测系统本身。
网络设备防护			
1	应对登录网络设备的用户进行身份鉴别。	身份认证	可以通过以下方式保证登录网络设备的身份鉴别： a) 设备自身的登录账号与口令：网络设备、安全设备大多都支持登录账户与口令认证。 b) 数字证书认证：数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。可以对网络上传输的信息进行加密和解密、数字签名和签名验证，除了身份认证的功能，还可确保网上传递信息的机密性、完整性。网络设备、安全设备大多都支持数字证书认证。 c) 第三方认证技术，RADIUS、LADP、TACAS+(思科私有)：这些认证技术都有独立的认证服务器，用户先到认证服务器上进行账户与口令的认证，认证通过后才可登录安全设备或网络设备进行管理。大多数网络设备和安全设备都支持 RADIUS、LADP 认证技术，TACAS+为思科私有协

			议，一般只有思科设备支持。 应在登录网络设备时使用数字证书认证或者第三方认证技术。
2	应对网络设备的管理员登录地址进行限制。	地址绑定、网络访问控制	可以通过以下方式保证登录地址限制： a) 地址绑定技术：IP 与 MAC 地址相绑定，防止地址盗用与欺骗。 b) 地址访问控制技术：使用防火墙、UTM 安全网关等设备设置管理员登录地址的限制。
3	网络设备用户的标识应唯一。	标识鉴别	可以通过以下方式保证网络设备的标识唯一： a) 设备命名管理：通过设备命名管理，可以在设备管理上实现标识唯一。 b) 管理账号命名管理：通过管理账号命名管理可以实现用户标识唯一。
4	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。	身份鉴别	可以通过以下方式保证登录网络设备的身份鉴别： a) 设备自身的登录账号与口令 b) 数字证书认证 c) 第三方认证技术，RADIUS、LADP、TACAS+(思科私有)
5	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。	身份鉴别	可以通过以下方式保证网络设备口令安全： a) 定期口令修改：能提高口令的安全性。 b) 口令强度规定：数字、字母、特殊符号设置能提高口令的安全性。
6	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。	登录控制	可以通过以下方式保证网络设备登录失败处理： a) 登录失败次数设置 b) 登录失败限制措施设置 c) 登录超时设置
7	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。	通讯加密、网络访问控制	可以通过以下方式保证网络设备远程管理不被窃听： a) 使用加密的通讯协议，如 SSH、HTTPS：SSH 与 HTTPS 能对传输的鉴别信息进行加密，防止在网络传输过程中被窃听。 b) 网络管理协议采用 SNMPV2，同时应参照口令管理方式设置口令，对于网络设备不支持 SNMPv2 的，允许采用其他方式进行管理，如私有协议。
8	应实现设备特权用户的权限分离。	管理权限分离	可以通过以下方式保证管理用户的权限分离： 管理员、审计员、超级用户的权限设置与分离：其中管理员只具有管理配置设备的权限；审计员只具有审计分析的权限；超级用户具有管理员与审计员的权限。
9	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。	文件备份	可以建立 FTP 文件服务器，每月把重要网络设备的配置文件(起始配置和当前配置)上传到服务器上。如果网络设备配置发生变动，可以及时上传配置文件到服务器。
10	应定期对网络设	运行检查	定期进行网络巡检(通常情况下是每天进行巡检)，巡检时

	备运行状况进行检查。		通过网络监控软件如 nagios 等对网络设备的重要监控指标或实际需要进行监控，监控内容包括：cpu 运行状况，网络流量统计，网络用户数统计，设备空间使用状况等。
11	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。	服务最小化	执行如下操作，检查各端口关闭和开启情况 #Show ip interface brief 关闭不必要服务的端口或登陆网路设备 service stop 命令停止不必要服务。同时记录已开启的服务及其对应的端口，形成文档保存，并建立相应的服务和端口开启的审批制度。
12	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。	版本检查	每月检查网络设备版本，版本升级时更新版本记录表。同时，根据网络设备运行情况，定期对版本进行评估。
13	应建立网络设备的时钟同步机制。	时钟同步	建立可独立基于 NTP/SNTP 协议工作的时间同步服务器，服务器与标准时钟信号信息一致，并设置网络设备自动与时间服务器的同步
14	应定期检查并锁定或撤销网络设备中多余的用户账号。	账号最小化	定期检查和梳理网路设备账号并文字记录查询情况，删除或锁定多余账号。

A.1.3 四级要求及措施

序号	要求的内容	对应技术措施	实现方式
结构安全			
1	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。	设备高可用性	可以通过以下方式保证处理能力具有冗余性： a) 高可用性设计： 双机热备：双机热备一般分为主-从模式，在正常情况下由主机进行数据包的处理工作，从机实时监测主机的工作状态，如果从机出现了问题，会将主机的工作接管过来，确保网络不出现单点故障。 HA 集群：多台设备同时工作，同时进行数据包的处理工作（轮询是一种处理方式），无主从的区别，如果一台设备出现故障，另外的设备会将该设备工作接管过来。HA 集群在确保消除单点故障的基础上，还能提高该点的处理能力。 产品软硬件 bypass 功能：产品软硬件 bypass 功能可以保证设备在断电或者死机时，数据包还能通过故障设备，网络不中断。 b) 设备高性能设计：设备的高性能设计，如比较高的吞吐量、并发连接数能保证满足业务高峰期的需要。 应在安全产品的部署上尽量采取双机的部署模式，特别是在核心数据区的边界或者流量比较大的区域边界处。并尽可能的选择具有软硬件 bypass 功能的产品。
2	应保证网络各个	设备高可靠性	可以通过以下方式保证带宽满足业务高峰期需要：

	部分的带宽满足业务高峰期需要。		a) 设备高性能设计：设备的高性能设计，如比较高的吞吐量、并发连接数能保证满足业务高峰期的需要。 b) 防火墙要适合金融业网间互联的网络带宽要求，不能成为网络瓶颈，或明显影响网络工作效率。
3	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。	路由控制	可以通过以下方式保证路由控制： a) 在路由器上设置：路由器上可以设置业务终端与服务器之间的路由，选用的路由器产品应符合 GB/T 18018—1999 路由器安全技术要求。 b) 在软硬件防火墙、UTM 安全网关上进行路由控制：防火墙于 UTM 安全网关支持静态路由、策略路由，可以通过 RIP、OSPF 学习动态路由功能，支持通过等价路由进行流量负载分担。通过合理的路由控制，在业务终端和服务器之间设定安全的访问路径，选用的防火墙产品应符合国家标准 GB/T 18019－1999 和 GB/T 18020－1999。
4	应绘制与当前运行情况相符的网络拓扑结构图。	拓扑规划	可以通过以下方式保证与当前运行情况相符的网络拓扑结构图： a) 拓扑规划设计 b) DNS 服务器配置中对主机的命名应采用不规则的方式，以保护整个网络的拓扑结构
5	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。	地址规划与安全域隔离设计	可以通过以下方式保证地址分配要求： a) 地址规划设计 b) 安全域设计：防火墙、UTM 安全网关产品可以进行不同网段的划分，并为个子网、网段分配地址段。另外支持安全域划分，对不同的安全域实施不同的安全策略，提供等级不同的安全保护。防火墙至少有 3 个网络接口，分别用于互联网，办公网和生产网；办公网和生产网之间的访问设置访问策略，只允许彼此之间需要访问的地址和端口；办公网对互联网的访问采用网络地址转换，同时只开放需要访问的端口；互联网对生产网的访问设置严格的端口和 IP 访问策略，对不提供外部服务的 IP 地址和端口严格禁止；原则上禁止从外联区直接访问内部网络，在不同的情况下使用防火墙或者 UTM 安全网关进行网络隔离，在面临威胁较为严峻的情况下，如病毒、入侵，选择 UTM 安全网关进行网络隔离。
6	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。	拓扑规划设计与网络访问控制	可以通过以下方式保证拓扑设计与网络访问控制： a) 合理的拓扑规划设计。 b) 软硬件防火墙隔离：防火墙可以将内部与外部信息系统、重要网段与其他网段进行隔离。 c) UTM 安全网关隔离：UTM 安全网关产品可以将内部与外部信息系统、重要网段与其他网段进行隔离。 应在不同的情况下使用防火墙或者 UTM 安全网关进行网络隔离，在面临威胁较为的情况下，如病毒、入侵，选择 UTM 安全网关进行网络隔离。
7	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	流量/带宽管理	可以通过以下方式保证流量/带宽管理： a) 网络设备 QOS 设置：可以按照不同的路径设置带宽。 b) 软硬件防火墙带宽管理：可以设置最大大带宽、最小带宽、保证带宽，带宽粒度一般为 KB 级。 c) UTM 安全网关带宽管理：可以设置最大大带宽、最小带宽、保证带宽，带宽粒度一般为 KB 级。

	要主机。		
8	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。	地址规划与安全域隔离设计	a) 前置设备功能设置：接收第三方机构上传的交易请求，经格式转换或其他处理后发送到业务主机；从主机接收响应回复，经分析处理后发送到相应的第三方机构；从而有效的防止联网系统与入网金融机构业务主机系统的隔离。 b) 合理的拓扑规划设计。 软硬件防火墙隔离：防火墙可以将内部与外部信息系统、重要网段与其他网段进行隔离。 UTM 安全网关隔离：UTM 安全网关产品可以将内部与外部信息系统、重要网段与其他网段进行隔离。 应在不同的情况下使用防火墙或者 UTM 安全网关进行网络隔离，在面临威胁较为的情况下，如病毒、入侵，选择 UTM 安全网关进行网络隔离。
9	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。	网络隔离	可以通过以下方式保证拓扑设计与网络访问控制： 合理的拓扑规划设计。 软硬件防火墙隔离：防火墙可以将内部与外部信息系统、重要网段与其他网段进行隔离。 UTM 安全网关隔离：UTM 安全网关产品可以将内部与外部信息系统、重要网段与其他网段进行隔离。 应在不同的情况下使用防火墙或者 UTM 安全网关进行专业网络与公用网路隔离，在面临威胁较为的情况下，如病毒、入侵，选择 UTM 安全网关进行网络隔离。
10	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。	链路备份	可以通过以下方式保证： 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 或其他方式的通信链路。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。
访问控制			
1	应在网络边界部署访问控制设备，启用访问控制功能。	网络访问控制	可以通过以下方式保证访问控制： a) 软硬件防火墙：防火墙为标准的网络访问控制设备，可对源接口、目的接口、协议类型、源地址、目的地址、服务和报文通讯时间等对象设置访问控制策略。 b) UTM 安全网关：UTM 安全网关产品包括了防火墙功能。 c) VLAN 间访问控制技术：可在交换机上设置 VLAN 之间的 ACL 列表，实现端口级别的访问控制策略，但列表过多的话会影响交换机的性能。

			应在网络访问控制设备的选择上尽可能使用防火墙或者UTM安全网关产品，如果边界面临的风险比较复杂（如同时面临了恶意代码、病毒等威胁），建议使用UTM安全网关产品。
2	应不允许数据带通用协议通过。	网络访问控制	常用通用协议包括：ICMP、POP3、HTTP、TELNET、FTP等。此项需要研究业务系统的非通用协议。如原计划使用HTTP协议，可以通过将HTTP协议格式私有化后使用或者构造全新的协议。
3	应根据数据的敏感标记允许或拒绝数据通过。	网络访问控制	需要研究业务系统所定义的敏感标记。
4	应不开放远程拨号访问功能。	网络访问控制	可以通过以下方式保证不开放远程拨号访问功能： a) 软硬件防火墙：可以在每个业务口控制是否允许远程拨号，可以设定不开放远程拨号。 b) UTM 安全网关：可以在每个业务口控制是否允许远程拨号，可以设定不开放远程拨号。
5	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。	网络访问控制	可以通过以下方式保证访问控制实现的用户粒度： a) 软硬件防火墙：可使用web认证、sslvpn用户、L2TP用户认证功能和安全策略结合，根据用户/用户组对系统资源的访问进行控制。 b) UTM安全网关：UTM安全网关产品具有防火墙功能。 c) 终端/服务器安全保护系统：具有内网访问控制能力，可以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。 应选择专业的安全产品进行用户级粒度的访问控制，终端/服务器安全保护系统可以与防火墙、UTM安全网关产品形成联动方案，组成从边界到主机的全网访问控制方案。
6	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。	网络访问控制	可以通过以下方式保证该要求的实现： i) 软硬件防火墙：支持带宽限制和并发连接数限制。可以根据安全策略限定最大网络带宽，可以设定系统的、具体IP的最大并发连接数。 j) UTM 安全网关：支持带宽限制和连接数限制。可以根据安全策略限定最大网络带宽，可以设定系统的、具体IP的最大并发连接数。 k) 终端/服务器安全保护系统：具有流量控制功能，可以实现基于端口、协议和进程的流量控制，网络连接数控制。 应使用防火墙、UTM安全网关和终端/服务器安全保护系统实现该要求目标。
7	网络设备应按最小安全访问原则设置访问控制权限。	端口最小化	可以通过以下方式保证访问控制实现的用户粒度： a) 软硬件防火墙：可使用web认证、sslvpn用户、L2TP用户认证功能和安全策略结合，根据用户/用户组对系统资源的访问进行控制。 b) UTM安全网关：UTM安全网关产品具有防火墙功能。 c) 终端/服务器安全保护系统：具有内网访问控制能力，可以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。 应选择专业的安全产品进行用户级粒度的访问控制，终端/服务器安全保护系统可以与防火墙、UTM安全网关产品形成联动方案，组成从边界到主机的全网访问控制方案。
安全审计			
1	应对网络系统中	日志审计措施	可以通过以下方式保证日志记录：

	的网络设备运行状况、网络流量、用户行为等进行日志记录。		a) 日志审计系统：能够对网络中的 TCP 流量按协议进行统计分析，并能够对用户行为进行详细的记录和分析，包括 Telnet、FTP、rlogin、X11、nfs、Netbios、oracle、sybase、informix、db2、sqlserver、HTTP、SMTP、POP3 等用户行为。 b) 其他设备的日志审计功能（如防火墙、UTM）：防火墙和 UTM 安全网关具有日志审计功能，可以记录访问的源、目的地址、服务、时间、用户以及攻击报警信息。 c) 网管系统：可以使用专门的网管系统对网络设备的运行状况进行记录。 应使用专门的日志审计系统对网络流量、用户行为等进行日志记录；防火墙与 UTM 安全网关的日志功能可配合日志审计系统；使用网管系统对网络设备的运行状况进行记录。
2	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。	日志审计措施	可以通过以下方式保证日志记录： a) 日志审计系统：可提供包括源 IP、源端口、目的 IP、目的端口、MAC 地址、登录账号、操作内容、时间等信息的查询。 b) 其他设备的日志审计功能（如防火墙、UTM）：防火墙和 UTM 安全网关具有日志审计功能，可以记录访问的源、目的地址、服务、时间、用户以及攻击报警信息。 应使用专门的日志审计系统对网络流量、用户行为等进行日志记录；防火墙与 UTM 安全网关的日志功能可配合日志审计系统；
3	应能够根据记录数据进行分析，并生成审计报表。	日志审计措施	可以通过以下方式保证生成审计报表： a) 日志审计系统：可提供网络审计数据分析功能。 b) 其他设备的日志审计功能（如防火墙、UTM）：可提供网络审计数据分析功能。 应使用日志审计系统和设备上的日志审计功能来实现该要求目标。
4	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。	日志审计措施	可以通过以下方式对审计记录进行保护： a) 日志审计系统：具有审计记录保护功能，可以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。 b) 其他设备的日志审计功能（如防火墙、UTM）：具有审计记录保护功能，可以避免受到未预期的删除、修改或覆盖等。 应选择具有审计记录保护功能的审计产品。
5	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。	日志审计措施	可以通过以下方式对审计记录进行保护： a) 日志审计系统：可以定义存储空间阀值，当存储空间接近极限时，将不记录设计事件。 b) 其他设备的日志审计功能（如防火墙、UTM）：可以定义存储空间阀值，当存储空间接近极限时，将不记录设计事件。
6	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。	日志审计措施	可以通过以下方式对审计记录进行保护： a) 日志审计系统：支持集中审计设计，支持钟保持与时钟服务器同步。 b) 其他设备的日志审计功能（如防火墙、UTM）：支持集中审计设计，支持钟保持与时钟服务器同步。
边界完整性检查			

1	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。	准入控制	可以通过以下方式保证准入控制： a) 终端/服务器安全保护系统：具有防非法外联功能，可以对未通过准许私自联到外部网络的行为（例如 modem 拨号、ADSL 拨号、私联网线和私设 IP 等行为）进行检查，并阻断其行为。 b) 防火墙：具备外联控制功能，可以控制内部用户不能访问外部网络，或者必须经过认证才能访问外部网络；另外能够进一步对 IM、P2P、网络游戏等外联行为进行控制。 c) UTM 安全网关：具备外联控制功能，可以控制内部用户不能访问外部网络，或者必须经过认证才能访问外部网络；另外能够进一步对 IM、P2P、网络游戏等外联行为进行控制。 **应**使用防火墙/UTM 安全网关+终端/服务器安全保护系统的全网外联控制方案，杜绝私联外网行为的出现。
2	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。	准入控制	可以通过以下方式保证准入控制： a) 终端/服务器安全保护系统：具有防非法外联功能，可以对未通过准许私自联到外部网络的行为（例如 modem 拨号、ADSL 拨号、私联网线和私设 IP 等行为）进行检查，并阻断其行为。 b) 防火墙：具备外联控制功能，可以控制内部用户不能访问外部网络，或者必须经过认证才能访问外部网络；另外能够进一步对 IM、P2P、网络游戏等外联行为进行控制。 c) UTM 安全网关：具备外联控制功能，可以控制内部用户不能访问外部网络，或者必须经过认证才能访问外部网络；另外能够进一步对 IM、P2P、网络游戏等外联行为进行控制。 **应**使用防火墙/UTM 安全网关+终端/服务器安全保护系统的全网外联控制方案，杜绝私联外网行为的出现。
入侵防范			
1	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。	入侵检测与防范措施	可以通过以下方式保证入侵防范： a) 入侵检测系统：可在网络的任意位置监视各种攻击行为，包括：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。入侵检测系统将检测的结果逐级汇总，形成分布分级管理的管理方式。 b) 入侵防护系统：可监视各种攻击行为，包括：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。 c) UTM 安全网关：可监视各种攻击行为，包括：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。 d) DNS 服务器：采用设置区域列表存取下限、监督 DNS 使用的端口，防止远程缓存溢出攻击和拒绝服务攻击；要通过活动目录安全实现 DNS 的安全；要能够有效地防止 DNS 欺骗、域名劫持攻击。 **应**按照不同的网络情况，合理的部署入侵检测系统、入侵防护系统与 UTM 安全网关；如在边界处部署入侵防护系统与 UTM 安全网关，在交换机上部署入侵检测系统。
2	当检测到攻击行为时，应记录攻	入侵检测与防范措施	可以通过以下方式保证入侵防范： a) 入侵检测系统：当检测到攻击行为时，可记录攻击源 IP、攻击类型、

	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。		攻击目的、攻击时间，在发生严重入侵事件时可提供报警及自动采取相应动作。 b) 入侵防护系统：当检测到攻击行为时，可记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时可提供报警及自动采取相应动作。 c) UTM 安全网关：当检测到攻击行为时，可记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时可提供报警及自动采取相应动作。 **应**按照不同的网络情况，合理的部署入侵检测系统、入侵防护系统与 UTM 安全网关；如在边界处部署入侵防护系统与 UTM 安全网关，在交换机上部署入侵检测系统。
3	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。	入侵检测与防范措施	a) 网络型入侵检测系统具有本地或异地分布式部署、远程管理的能力。 b) 系统设置集中管理中心，对分布式、多级部署的入侵检测系统进行统一集中管理，形成多级管理结构。
恶意代码防范			
1	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。	内容安全措施	可以通过以下方式保证内容安全措施的实现： a) 入侵防护系统：防病毒和入侵防护功能，可对恶意代码进行检测和清除。 b) UTM 安全网关：防病毒和入侵防护功能，可对恶意代码进行检测和清除。 **应**使用入侵防护系统与 UTM 安全网关进行恶意代码的检测和清除。
2	应定期对恶意代码防护设备进行代码库升级和系统更新。	内容安全措施	可以通过以下方式保证内容安全措施的实现： a) 入侵防护系统：具有病毒库与入侵库，可以定期升级。 b) 入侵检测系统：具有入侵库，可以定期升级。 c) UTM 安全网关：具有病毒库与入侵库，可以定期升级。 **应**定期更新入侵防护系统、入侵检测系统与 UTM 安全网关的恶意代码库和检测系统本身。
网络设备防护			
1	应对登录网络设备的用户进行身份鉴别。	身份认证	可以通过以下方式保证登录网络设备的身份鉴别： a) 设备自身的登录账号与口令：网络设备、安全设备大多都支持登录账户与口令认证。 b) 数字证书认证：数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。可以对网络上传输的信息进行加密和解密、数字签名和签名验证，除了身份认证的功能，还可确保网上传递信息的机密性、完整性。网络设备、安全设备大多都支持数字证书认证。 c) 第三方认证技术，RADIUS、LADP、TACAS+(思科私有)：这些认证技术都有独立的认证服务器，用户先到认证服务器上进行账户与口令的认证，认证通过后才可登录安全设备或网络设备进行管理。大多数网络设备和安全设备都支持 RADIUS、LADP 认证技术，TACAS+为思科私有协议，一般只有思科设备支持。

			应在登录网络设备时使用数字证书认证或者第三方认证技术。
2	应对网络设备的管理员登录地址进行限制。	地址绑定、网络访问控制	可以通过以下方式保证登录地址限制： a) 地址绑定技术：IP 与 MAC 地址相绑定，防止地址盗用与欺骗。 b) 地址访问控制技术：使用防火墙、UTM 安全网关等设备设置管理员登录地址的限制。
3	网络设备用户的标识应唯一。	标识鉴别	可以通过以下方式保证网络设备的标识唯一： a) 设备命名管理：通过设备命名管理，可以在设备管理上实现标识唯一。 b) 管理账号命名管理：通过管理账号命名管理可以实现用户标识唯一。
4	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。	身份鉴别	可以通过以下方式保证登录网络设备的身份鉴别： a) 设备自身的登录账号与口令 b) 数字证书认证 c) 第三方认证技术，RADIUS、LADP、TACAS+(思科私有)
5	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。	身份鉴别	可以通过以下方式保证网络设备口令安全： a) 定期口令修改：能提高口令的安全性。 b) 口令强度规定：数字、字母、特殊符号设置能提高口令的安全性。
6	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。	身份鉴别	可以通过以下方式保证网络设备的身份鉴别信息至少有一种是不可伪造的： c) 数字证书 d) 动态口令牌
7	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。	登录控制	可以通过以下方式保证网络设备登录失败处理： a) 登录失败次数设置 b) 登录失败限制措施设置 c) 登录超时设置
8	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。	通讯加密、网络访问控制	可以通过以下方式保证网络设备远程管理不被窃听： a) 使用加密的通讯协议，如 SSH、HTTPS：SSH 与 HTTPS 能对传输的鉴别信息进行加密，防止在网络传输过程中被窃听。 b) 网络管理协议采用 SNMPV2，同时应参照口令管理方式设置口令，对于网络设备不支持 SNMPv2 的，允许采用其他方式进行管理，如私有协议。
9	应实现设备特权用户的权限分离。	管理权限分离	可以通过以下方式保证管理用户的权限分离： a) 管理员、审计员、超级用户的权限设置与分离：其中管理员只具有管理配置设备的权限；审计员只具有审计分析的权限；超级用户具有管理员与审计员的权限。
10	对网络设备系统自带的的服务端口进行梳理，关	服务最小化	执行如下操作，检查各端口关闭和开启情况 #Show ip interface brief 关闭不必要服务的端口或登陆网路设备 service stop 命令停止不必要服

	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。		务。同时记录已开启的服务及其对应的端口，形成文档保存，并建立相应的服务和端口开启的审批制度。
11	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。	版本检查	每季度检查网络设备版本，版本升级时更新版本记录表。同时，根据网络设备运行情况，定期对版本进行评估。
12	应建立网络设备的时钟同步机制。	时钟同步	建立可独立基于 NTP/SNTP 协议工作的时间同步服务器，服务器与标准时钟信号信息一致，并设置网络设备自动与时间服务器的同步。
13	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。	文件备份	可以建立 FTP 文件服务器，每月把重要网络设备的配置文件(起始配置和当前配置)上传到服务器上。如果网络设备配置发生变动，可以及时上传配置文件到服务器。
14	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。	账号最小化	每季度检查和梳理网路设备账号并文字记录查询情况，删除或锁定多余账号。

A.2 主机安全

A.2.1 二级要求及措施

序号	要求的内容	对应技术措施	实现方式
身份鉴别			
1	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。	身份认证	可以通过以下方式保证身份认证的实现： a) 身份认证：具有身份认证与标识、鉴别功能，如账号与口令认证、数字证书认证等，可以实现登录用户的身份标识和鉴别。
2	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。	身份认证	可以通过以下方式保证身份认证的实现： a) 身份认证：具有身份认证与标识、鉴别功能，如账号与口令认证、数字证书认证等，用户标识不易被冒用，关键系统的静态口令可以在 6 位以上并由字母、数字、符号等混合组成并定期更换。 l WIN2000 系统 1. 运行 secpol.msc 命令 2. 打开“本地安全设置”对话框，依次展开“帐户策略－密码策略” 3. 查看是否具有设置 4. 密码策略，密码长度大于 8 位、必须启用密码复

			杂性要求； l Hp-unix 系统 检查系统口令的配置策略: more /tcb/files/auth/system/default l oracle 系统 在Oracle中,可以通过修改用户概要文件来设置密码的安全策略。 与密码安全有关系的设置如下： FAILED_LOGIN_ATTEMPTS:最大错误登录次数 PASSWORD_GRACE_TIME:口令失效后锁定时间 PASSWORD_LIFE_TIME:口令有效时间 PASSWORD_LOCK_TIME:登录超过有效次数锁定时间 PASSWORD_REUSE_MAX:口令历史记录保留次数 PASSWORD_RESUSE_TIME:口令历史记录保留时间 PASSWORD_VERIFY_FUNCTION:口令复杂度审计函数 检查方法： 开始菜单->程序->Oracle - OraHome92->Enterprise Manager Console
3	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。	身份认证	可以通过以下方式保证身份认证的实现： 身份认证：身份认证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自动退出等措施。 l WIN2000 系统 1、运行中输入 secpol.msc 命令 2、打开“本地安全设置”对话框，依次展开“帐户策略－账户锁定策略” 3、修改帐户锁定阀值。 l Hp-unix 系统 检查系统允许的单次会话中的登录尝试次数: more /tcb/files/auth/system/default。 l oracle 系统

			在Oracle中,可以通过修改用户概要文件来设置密码的安全策略。 与密码安全有关系的设置如下： FAILED_LOGIN_ATTEMPTS:最大错误登录次数 PASSWORD_GRACE_TIME:口令失效后锁定时间 PASSWORD_LIFE_TIME:口令有效时间 PASSWORD_LOCK_TIME:登录超过有效次数锁定时间 PASSWORD_REUSE_MAX:口令历史记录保留次数 PASSWORD_RESUSE_TIME:口令历史记录保留时间 PASSWORD_VERIFY_FUNCTION:口令复杂度审计函数 检查方法： 开始菜单->程序->Oracle - OraHome92->Enterprise Manager Console
4	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。	通信加密	可以通过以下方式保证通信加密的实现： 通信加密：可以使用SSL加密或者VPN系统进行加密，防止防止鉴别信息在网络传输过程中被窃听。
5	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。	身份认证	可以通过以下方式保证身份认证的实现： 身份认证：具有身份认证与标识、鉴别功能，如账号与口令认证、数字证书认证等。可以为不通用户分配不同的用户名，确保用户名具有唯一性。
访问控制			
1	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。	访问控制	可以通过以下方式保证访问控制的实现： 访问控制：为终端和服务器提供基于安全策略的访问控制，可以控制用户对资源的访问。
2	应实现操作系统和数据库系统特权用户的权限分离。	权限分离	可以通过以下方式保证访问控制的实现： 权限分离：对服务器进行安全加固设置，实现操作系统和数据库系统特权用户的权限分离。
3	应限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令。	漏洞扫描系统	可以通过以下方式保证访问控制的实现： a) 漏洞扫描系统必须具备以下功能：具有安全策略配置功能；Web脆弱性扫描；FTP脆弱性扫描；RPC脆弱性扫描；NIS脆弱性扫描；PROXY扫描；NT用户、组、口令、注册表等脆弱性扫描；SNMP脆弱性扫描；木马扫描；浏览器漏洞扫描；Dos服务扫描；操作系统范围,可以对多种操作系统进行漏洞扫描；网络设备扫描；邮件服务器脆弱性扫描；口令脆弱性扫描；端口扫描；生成报告；更

			新方式。 b) 漏洞扫描系统：漏扫系统可以有效的发现 Windows 操作系统的默认账户，以及默认口令，并可进行密码强度测试。
4	应及时删除多余的、过期的账户，避免共享账户的存在。	账户控制	可以通过以下方式保证访问控制的实现： 账户控制：有效及时删除多余的、过期的账户，避免共享账户的存在。
安全审计			
1	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。	安全审计	可以通过以下方式保证安全审计的实现： a) 安全审计系统：安全审计系统可以覆盖到服务器上的每个操作系统用户和数据库用户，具有技术手段收集操作系统与数据库系统的日志。 b) 终端/服务器安全保护系统:审计范围能够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。
2	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。	安全审计	可以通过以下方式保证安全审计的实现： a) 安全审计系统：够提供对网络方式操作主机的行为进行审计备案，包括 telnet/FTP 运维操作、数据库等操作等均能够提供全面记录和备案，通过策略制定可以对重要操作进行重点分析。 b) 终端/服务器安全保护系统：能够对服务器和重要的 PC 客户端进行行为审计，包括重要的用户行为、系统资源的异常使用、重要系统命令等系统内重要的安全事件。
3	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。	安全审计	可以通过以下方式保证安全审计的实现： a) 安全审计系统：提供网络行为的原始记录供事后追查取证，包括系统记录源 IP、源端口、目的 IP、目的端口、MAC 地址、登录账号、操作内容、时间等信息。 b) 终端/服务器安全保护系统：记录能够包括事件的日期、时间、类型、主体标识、客体标识和结果等。
4	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。	安全审计	可以通过以下方式保证安全审计的实现： a) 安全审计系统：通过身份鉴别方式后才可进行读取访问，对审计记录的删除操作必须是专门的管理员进行操作，所有操作行为均有完善的自身审计。 b) 终端/服务器安全保护系统：能够针对审计记录进行保护，避免受到未预期的删除、修改或覆盖,保存时间不少于一个月。
入侵防范			
1	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。	主动防御	可以通过以下方式保证入侵防范的实现： 终端/服务器安全保护系统：能够保证服务器、PC 终端的操作系统仅安装需要的组件和应用程序，进行实时补丁更新。尽量关闭 telnet、ftp、smtp、pop3、snmp、rpc、windows terminal 等服务。内部的远程管理可以使用 ssh 这类安全的工具。尽量关闭外部的远程管理端口。
恶意代码防范			

1	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。	病毒查杀、主动防御	可以通过以下方式保证恶意代码防范的实现： a) 防病毒系统：可以及时更新防恶意代码软件版本和恶意代码库。 b) 终端/服务器安全保护系统：采用主动防御技术，引入白名单，对系统所有可执行程序进行保护，从根本上阻断恶意代码攻击。
2	应支持防恶意代码软件的统一管理。	统一管理	可以通过以下方式保证恶意代码防范的实现： a) 防病毒系统：支持防恶意代码软件的统一管理。 b) 终端/服务器安全保护系统：具备统一管理功能。
资源控制			
1	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。	资源控制	可以通过以下方式保证资源控制的实现： 终端安全保护系统：具备终端多层网络准入控制能力，可以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。
2	应根据安全策略设置登录终端的操作超时锁定。	资源控制	可以通过以下方式保证资源控制的实现： 操作超时设置：通过对操作系统本身的安全策略设置，实现登录终端的操作超时锁定。
3	应限制单个用户对系统资源的最大或最小使用限度。	资源控制	可以通过以下方式保证资源控制的实现： 系统资源使用限制：设置资源控制模块，限制单个用户对系统资源的最大或最小使用限度。

A.2.2 三级要求及措施

序号	要求的内容	对应技术措施	实现方式
身份鉴别			
1	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	身份认证	可以通过以下方式保证身份认证的实现： 身份认证：具有身份认证与标识、鉴别功能，如账号与口令认证、数字证书认证等，可以实现登录用户的身份标识和鉴别。
2	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。	身份认证	可以通过以下方式保证身份认证的实现： 身份认证：具有身份认证与标识、鉴别功能，如账号与口令认证、数字证书认证等，可以实现登录用户的身份标识和鉴别。
2	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 以上并由字母、数字、符号等混合组成并每三个月更换口令。	身份认证	可以通过以下方式保证身份认证的实现： 身份认证：具有身份认证与标识、鉴别功能，如账号与口令认证、数字证书认证等，用户标识不易被冒用，口令可以在 7 位以上并由字母、数字、符号等混合组成并每三个月更换。 l WIN2000 系统 1. 运行 secpol.msc 命令 2. 打开“本地安全设置”对话框，依次展开“帐户策略－密码策略” 3. 查看是否具有设置 4. 密码策略，密码长度大于 8 位、必须启用密码

			复杂性要求； l Hp-unix 系统 检查系统口令的配置策略: more /tcb/files/auth/system/default l oracle 系统 在 Oracle 中，可以通过修改用户概要文件来设置密码的安全策略。与密码安全有关系的设置如下： FAILED_LOGIN_ATTEMPTS:最大错误登录次数 PASSWORD_GRACE_TIME:口令失效后锁定时间 PASSWORD_LIFE_TIME:口令有效时间 PASSWORD_LOCK_TIME:登录超过有效次数锁定时间 PASSWORD_REUSE_MAX:口令历史记录保留次数 PASSWORD_RESUSE_TIME:口令历史记录保留时间 PASSWORD_VERIFY_FUNCTION:口令复杂度审计函数 检查方法： 开始菜单->程序->Oracle - OraHome92->Enterprise Manager Console
3	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。	身份认证	可以通过以下方式保证身份认证的实现： 身份认证：身份认证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自动退出等措施。 l WIN2000 系统 1、运行中输入 secpol.msc 命令 2、打开“本地安全设置”对话框，依次展开“帐户策略—账户锁定策略” 3、修改帐户锁定阀值。 l Hp-unix 系统 检查系统允许的单次会话中的登录尝试次数: more /tcb/files/auth/system/default。 l oracle 系统 在 Oracle 中，可以通过修改用户概要文件来设置密码的安全策

			略。与密码安全有关系的设置如下： FAILED_LOGIN_ATTEMPTS:最大错误登录次数 PASSWORD_GRACE_TIME:口令失效后锁定时间 PASSWORD_LIFE_TIME:口令有效时间 PASSWORD_LOCK_TIME:登录超过有效次数锁定时间 PASSWORD_REUSE_MAX:口令历史记录保留次数 PASSWORD_RESUSE_TIME:口令历史记录保留时间 PASSWORD_VERIFY_FUNCTION:口令复杂度审计函数 检查方法： 开始菜单->程序->Oracle - OraHome92->Enterprise Manager Console
4	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。	通信加密	可以通过以下方式保证通信加密的实现： 通信加密：可以使用 SSL 加密或者 VPN 系统进行加密，防止防止鉴别信息在网络传输过程中被窃听。
6	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。	身份认证	可以通过以下方式保证身份认证的实现： 身份认证：具有身份认证与标识、鉴别功能，如账号与口令认证、数字证书认证、生物特征等。具有两种以上组合的鉴别技术对管理用户进行身份鉴别。
访问控制			
1	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。	访问控制	可以通过以下方式保证访问控制的实现： 访问控制：为终端和服务器提供基于安全策略的访问控制，可以控制用户对资源的访问。
2	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。	安全管理平台	可以通过以下方式保证访问控制的实现： 安全管理平台：安全管理平台可以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。
3	应实现操作系统和数据库系统特权用户的	权限分离	可以通过以下方式保证访问控制的实现： 权限分离：对服务器进行安全加固设置，实现操作系统和数据库系统

	权限分离。		特权用户的权限分离。
4	应禁用和严格限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令。	漏洞扫描系统	可以通过以下方式保证访问控制的实现： a) 漏洞扫描系统必须具备以下功能：具有安全策略配置功能；Web 脆弱性扫描；FTP 脆弱性扫描；RPC 脆弱性扫描；NIS 脆弱性扫描；PROXY 扫描；NT 用户、组、口令、注册表等脆弱性扫描；SNMP 脆弱性扫描；木马扫描；浏览器漏洞扫描；Dos 服务扫描；操作系统范围,可以对多种操作系统进行漏洞扫描；网络设备扫描；邮件服务器脆弱性扫描；口令脆弱性扫描；端口扫描；生成报告；更新方式。 b) 漏洞扫描系统：漏扫系统可以有效的发现 Windows 操作系统的默认账户，以及默认口令，并可进行密码强度测试。
5	应及时删除多余的、过期的账户，避免共享账户的存在。	账户控制	可以通过以下方式保证访问控制的实现： 账户控制：有效及时删除多余的、过期的账户，避免共享账户的存在。
6	应对重要信息资源设置敏感标记。	标记	可以通过以下方式保证访问控制的实现： 标记：在操作系统层设置信息标记功能，对信息资源进行标记。
7	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。	访问控制	可以通过以下方式保证访问控制的实现： 访问控制：在操作系统层，设置访问控制功能，对有敏感标记的信息进行控制。
安全审计			
1	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。	安全审计	可以通过以下方式保证安全审计的实现： a) 安全审计系统：安全审计系统可以覆盖到服务器上的每个操作系统用户和数据库用户，具有技术手段收集操作系统与数据库系统的日志。 b) 终端/服务器安全保护系统：审计范围能够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。
2	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。	安全审计	可以通过以下方式保证安全审计的实现： a) 安全审计系统：够提供对网络方式操作主机的行为进行审计备案，包括 telnet/FTP 运维操作、数据库等操作等均能够提供全面记录和备案，通过策略制定可以对重要操作进行重点分析。 b) 终端/服务器安全保护系统：能够对服务器和重要的 PC 客户端进行行为审计，包括重要的用户行为、系统资源的异常使用、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、网络进出数据等系统内重要的安全相关事件。
3	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。	安全审计	可以通过以下方式保证安全审计的实现： a) 安全审计系统：提供网络行为的原始记录供事后追查取证，包括系统记录源 IP、源端口、目的 IP、目的端口、MAC 地址、登录账号、操作内容、时间等信息。 b) 终端/服务器安全保护系统：记录能够包括事件的日期、时间、类型、主体标识、客体标识和结果等。 c) 并定期备份审计记录，保存时间不少于半年。

4	应能够根据记录数据进行分析，并生成审计报表。	安全审计	可以通过以下方式保证安全审计的实现： a) 安全审计系统：可提供专业的网络审计数据分析功能，系统提供了数十种统计报表和灵活的条件供管理员定期分析，支持报表模板、条件模板，提供多维分析功能，支持 XLS/CSV/PDF 等格式的报表导出。 b) 终端/服务器安全保护系统：能够对审计数据进行分析，并形成审计报表。
5	应保护审计进程，避免受到未预期的中断。	安全审计	可以通过以下方式保证安全审计的实现： a) 安全审计系统：通过身份鉴别方式后才可进行读取访问，对审计记录的删除操作必须是专门的管理员进行操作，所有操作行为均有完善的自身审计。 b) 终端/服务器安全保护系统：保护审计进程避免受到未预期的中断。
6	应保护审计记录，避免受到未预期的删除、修改或覆盖等。	安全审计	可以通过以下方式保证安全审计的实现： a) 安全审计系统：通过身份鉴别方式后才可进行读取访问，对审计记录的删除操作必须是专门的管理员进行操作，所有操作行为均有完善的自身审计。 b) 终端/服务器安全保护系统：能够针对审计记录进行保护，避免受到未预期的删除、修改或覆盖。
剩余信息保护			
1	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。	剩余信息保护	可以通过以下方式保证剩余信息保护的实现： a)专用设备：针对操作系统和数据库系统剩余信息保护的专用设备。
2	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。	剩余信息保护	可以通过以下方式保证剩余信息保护的实现： 专用设备：针对操作系统和数据库系统剩余信息保护的专用设备。
入侵防范			
1	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。	主动防御	可以通过以下方式保证入侵防范的实现： a) 终端/服务器安全保护系统：采用主动防御技术，对系统所有可执行程序进行保护，检测针对服务器的入侵行为，记录入侵者的源 IP、攻击的类型、攻击的目的、攻击的时间、并提供报警。 b) 对于下载客户端程序的 Web 服务器，注意关闭其目录浏览功能，关闭 put 功能。 c) 对于提供下载客户端程序功能的 web 服务器，不要将下载地址直接作为该页面 URL 的参数，以避免网页的欺骗。

			d) 对于网站服务器，对外尽量使用静态页面。必要时可以考虑关闭 ping 功能，防止 ping 攻击（但采用此措施将丧失一定的监控能力）。
2	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。	主动防御	可以通过以下方式保证入侵防范的实现： 终端/服务器安全保护系统：采用主动防御技术，对系统所有可执行程序进行保护，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根本性的阻断破坏行为的发生。
3	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。	主动防御	可以通过以下方式保证入侵防范的实现： 终端/服务器安全保护系统：能够保证服务器、PC 终端的操作系统仅安装需要的组件和应用程序，进行实时补丁更新。尽量关闭 telnet、ftp、smtp、pop3、snmp、rpc、windows terminal 等服务。内部的远程管理可以使用 ssh 这类安全的工具。尽量关闭外部的远程管理端口。
恶意代码防范			
1	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。	病毒查杀、主动防御	可以通过以下方式保证恶意代码防范的实现： a) 防病毒系统：可以及时更新防恶意代码软件版本和恶意代码库。 b) 终端/服务器安全保护系统：采用主动防御技术，引入白名单，对系统所有可执行程序进行保护，从根本上阻断恶意代码攻击。
2	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。	病毒查杀、主动防御	可以通过以下方式保证恶意代码防范的实现： a) 恶意代码库：防病毒软件的恶意代码库与入侵防御系统、UTM 安全网关的恶意代码库不同。 b) 终端/服务器安全保护系统：采用主动防御技术，引入白名单，拜托对恶意代码库的依赖，对系统所有可执行程序进行保护，从根本上阻断恶意代码攻击。
3	应支持防恶意代码的统一管理。	统一管理	可以通过以下方式保证恶意代码防范的实现： a) 防病毒系统：支持防恶意代码软件的统一管理。 b) 终端/服务器安全保护系统：具备统一管理功能。
4	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	病毒监控	可以通过以下方式保证恶意代码防范的实现： 防病毒系统：支持防恶意代码软件的统一管理。终端/服务器安全保护系统：具备收集网内计算机发过来的病毒感染信息并能

	监控。		对信息进行分析和处理的能力。
资源控制			
1	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。	资源控制	可以通过以下方式保证资源控制的实现： 终端安全保护系统：具备终端多层网络准入控制能力，可以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。
2	应根据安全策略设置登录终端的操作超时锁定。	资源控制	可以通过以下方式保证资源控制的实现： 操作超时设置：通过对操作系统本身的安全策略设置，实现登录终端的操作超时锁定。
3	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。	资源控制	可以通过以下方式保证资源控制的实现： 服务器安全保护系统：可以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。
4	应限制单个用户对系统资源的最大或最小使用限度。	资源控制	可以通过以下方式保证资源控制的实现： 系统资源使用限制：设置资源控制模块，限制单个用户对系统资源的最大或最小使用限度。
5	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。	资源控制	可以通过以下方式保证资源控制的实现： 服务器安全保护系统：可以监控系统的状态，并设定报警阀值，如果系统服务水平降低到最小值，将进行报警。
6	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。	资源控制	对服务器的业务用途进行明确的定义，不允许利用服务器进行收发邮件，浏览互联网等一些操作。

A.2.3 四级要求及措施

序号	要求的内容	对应技术措施	实现方式
身份鉴别			
1	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。	身份认证	可以通过以下方式保证身份认证的实现： 身份认证：具有身份认证与标识、鉴别功能，如账号与口令认证、数字证书认证等，可以实现登录用户的身份标识和鉴别。
2	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。	身份认证	可以通过以下方式保证身份认证的实现： 身份认证：具有身份认证与标识、鉴别功能，如账号与口令认证、数字证书认证等，用户标识不易被冒用，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。 l WIN2000 系统 1. 运行 secpol.msc 命令 2. 打开“本地安全设置”对话框，依次展开“帐户策略－密

			码策略” 3. 查看是否具有设置 4. 密码策略，密码长度大于8位、必须启用密码复杂性要求； l Hp-unix系统 检查系统口令的配置策略: more /tcb/files/auth/system/default l oracle系统 在 Oracle 中，可以通过修改用户概要文件来设置密码的安全策略。与密码安全有关系的设置如下： FAILED_LOGIN_ATTEMPTS:最大错误登录次数 PASSWORD_GRACE_TIME:口令失效后锁定时间 PASSWORD_LIFE_TIME:口令有效时间 PASSWORD_LOCK_TIME:登录超过有效次数锁定时间 PASSWORD_REUSE_MAX:口令历史记录保留次数 PASSWORD_RESUSE_TIME:口令历史记录保留时间 PASSWORD_VERIFY_FUNCTION:口令复杂度审计函数 检查方法： 开始菜单->程序->Oracle - OraHome92->Enterprise Manager Console
3	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。	身份认证	可以通过以下方式保证身份认证的实现： 身份认证：身份认证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自动退出等措施。 l WIN2000系统 1、运行中输入secpol.msc命令 2、打开“本地安全设置”对话框，依次展开“帐户策略—账户锁定策略” 3、修改帐户锁定阀值。 l Hp-unix系统 检查系统允许的单次会话中的登录尝试次数:

			more /tcb/files/auth/system/default。 l oracle 系统 在 Oracle 中，可以通过修改用户概要文件来设置密码的安全策略。与密码安全有关系的设置如下： FAILED_LOGIN_ATTEMPTS:最大错误登录次数 PASSWORD_GRACE_TIME:口令失效后锁定时间 PASSWORD_LIFE_TIME:口令有效时间 PASSWORD_LOCK_TIME:登录超过有效次数锁定时间 PASSWORD_REUSE_MAX:口令历史记录保留次数 PASSWORD_RESUSE_TIME:口令历史记录保留时间 PASSWORD_VERIFY_FUNCTION:口令复杂度审计函数 检查方法： 开始菜单->程序->Oracle - OraHome92->Enterprise Manager Console
4	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。	身份认证	可以通过以下方式保证身份认证的实现： 身份认证：可以设置鉴别警示信息，描述未授权访问可能导致的后果。
5	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。	身份认证	可以通过以下方式保证通信加密的实现： 通信加密：可以使用 SSL 加密或者 VPN 系统进行加密，防止防止鉴别信息在网络传输过程中被窃听。
6	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。	身份认证	可以通过以下方式保证身份认证的实现： 身份认证：具有身份认证与标识、鉴别功能，如账号与口令认证、数字证书认证等。可以为不通用户分配不同的用户名，确保用户名具有唯一性。
7	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	身份认证	可以通过以下方式保证身份认证的实现： 身份认证：具有身份认证与标识、鉴别功能，如账号与口令认证、数字证书认证，指纹识别等。具有两种以上组合的鉴别技术对管理用户进行身份鉴别。双因素身份认证伪造的可能性低。

	特征等作为身份鉴别信息。		
安全标记			
1	应对所有主体和客体设置敏感标记。	安全标记	可以通过以下方式保证身份认证的实现： 终端/服务器安全保护系统：在操作系统层实现对所有主体和客体设置敏感标记。
访问控制			
1	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。	访问控制	可以通过以下方式保证访问控制的实现： 访问控制：实现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。
2	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。	访问控制	可以通过以下方式保证访问控制的实现： a) 访问控制：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。 b) 在服务端安装篡改侦测系统，定期检查对于内容发布起主要作用的文件和数据库内容，当发生修改时予以报警、停止或者内容退回。此种检查可以通过对上述文件和数据库内容使用摘要算法予以处理，然后与内部存储的摘要值进行核对。
3	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。	安全管理平台	可以通过以下方式保证访问控制的实现： 安全管理平台：安全管理平台可以根据管理用户的角色(系统管理员、安全管理员、安全审计员等)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。
4	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。	权限分离	可以通过以下方式保证访问控制的实现： 权限分离：对服务器进行安全加固设置，实现操作系统和数据库系统特权用户的权限分离。
5	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。	权限控制	可以通过以下方式保证访问控制的实现： 账户控制：禁用或严格限制默认帐户的访问权限或重命名这些账户名称并修改其口令。
6	应及时删除多余的、过期的账户，避免共享账户的存在。	账户控制	可以通过以下方式保证访问控制的实现： 账户控制：有效及时删除多余的、过期的账户，避免共享账户的存在。
可信路径			
1	对通过互联网远程访问操作系统、数据库系	可信路径	可以通过以下方式保证可信路径的实现： 终端/服务器安全保护系统：能够在操作系统与用户之间建立一条安

	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。		全的信息传输路径，保证鉴别信息不被窃取和篡改。
2	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。	可信路径	可以通过以下方式保证可信路径的实现： 终端/服务器安全保护系统：能够在操作系统与用户之间建立一条安全的信息传输路径，保证访问信息不被窃取和篡改。
安全审计			
1	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。	安全审计	可以通过以下方式保证安全审计的实现： a) 安全审计系统：安全审计系统可以覆盖到服务器上的每个操作系统用户和数据库用户，具有技术手段收集操作系统与数据库系统的日志。 b) 终端/服务器安全保护系统：审计范围能够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。
2	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。	安全审计	可以通过以下方式保证安全审计的实现： a) 安全审计系统：够提供对网络方式操作主机的行为进行审计备案，包括 telnet/FTP 运维操作、数据库等操作等均能够提供全面记录和备案，通过策略制定可以对重要操作进行重点分析。 b) 终端/服务器安全保护系统：能够对服务器和重要的 PC 客户端进行行为审计，包括重要的用户行为、系统资源的异常使用、重要系统命令等系统内重要的安全事件。
3	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。	安全审计	可以通过以下方式保证安全审计的实现： a) 安全审计系统：提供网络行为的原始记录供事后追查取证，包括系统记录源 IP、源端口、目的 IP、目的端口、MAC 地址、登录账号、操作内容、时间等信息。 b) 终端/服务器安全安全系统：记录能够包括事件的日期、时间、类型、主体标识、客体标识和结果等。
4	应能够根据记录数据进行分析，并生成审计报表。	安全审计	可以通过以下方式保证安全审计的实现： a) 安全审计系统：可提供专业的网络审计数据分析功能，系统提供了数十种统计报表和灵活的条件供管理员定期分析，支持报表模板、条件模板，提供多维分析功能，支持 XLS/CSV/PDF 等格式的报表导出。 b) 终端/服务器安全保护系统：能够对审计数据进行分析，并形成审计报表。
5	应保护审计进程，避免受到未预期的中断。	安全审计	可以通过以下方式保证安全审计的实现： a) 安全审计系统：通过身份鉴别方式后才可进行读取访问，对审计记录的删除操作必须是专门的管理员进行操作，所有操作行为均有完善的自身审计。 b) 终端/服务器安全管理系统：保护审计进程避免受到未预期的中

			断。
6	应保护审计记录，避免受到未预期的删除、修改或覆盖等。	安全审计	可以通过以下方式保证安全审计的实现： a) 安全审计系统：通过身份鉴别方式后才可进行读取访问，对审计记录的删除操作必须是专门的管理员进行操作，所有操作行为均有完善的自身审计。 b) 终端/服务器安全保护系统：安装防篡改系统，能够针对审计记录进行保护，避免受到未预期的删除、修改或覆盖。
7	应能够根据信息系统的统一安全策略，实现集中审计。	安全审计	可以通过以下方式保证安全审计的实现： a) 安全审计系统：支持统一安全策略，可以实现集中审计。 b) 终端/服务器安全保护系统：支持统一安全策略，可以实现集中审计。
剩余信息保护			
1	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。	剩余信息保护	可以通过以下方式保证剩余信息保护的实现： 专用设备：针对操作系统和数据库系统剩余信息保护的专用设备。
2	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。	剩余信息保护	可以通过以下方式保证剩余信息保护的实现： 专用设备：针对操作系统和数据库系统剩余信息保护的专用设备。
入侵防范			
1	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。	主动防御	可以通过以下方式保证入侵防范的实现： a) 终端/服务器安全保护系统：采用主动防御技术，对系统所有可执行程序进行保护，检测针对服务器的入侵行为，记录入侵者的源IP、攻击的类型、攻击的目的、攻击的时间、并提供报警。 b) 对于下载客户端程序的Web服务器，注意关闭其目录浏览功能，关闭put功能。 c) 对于提供下载客户端程序功能的web服务器，不要将下载地址直接作为该页面URL的参数，以避免网页的欺骗。 d) 对于网站服务器，对外尽量使用静态页面。必要时可以考虑关闭ping功能，防止ping攻击（但采用此措施将丧失一定的监控能力）。
2	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	主动防御	可以通过以下方式保证入侵防范的实现： 终端/服务器安全保护系统：采用主动防御技术，对系统所有可执行程序进行保护，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根本性的阻断破坏行为的发生。

	将受到破坏时进行事前阻断。		
3	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。	主动防御	可以通过以下方式保证入侵防范的实现： 终端/服务器安全保护系统：能够保证服务器、PC 终端的操作系统仅安装需要的组件和应用程序，进行实时补丁更新。尽量关闭 telnet、ftp、smtp、pop3、snmp、rpc、windows terminal 等服务。内部的远程管理可以使用 ssh 这类安全的工具。尽量关闭外部的远程管理端口。
恶意代码防范			
1	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。	病毒查杀、主动防御	可以通过以下方式保证恶意代码防范的实现： a) 防病毒系统：可以及时更新防恶意代码软件版本和恶意代码库。 b) 终端/服务器安全保护系统：采用主动防御技术，引入白名单，对系统所有可执行程序进行保护，从根本上阻断恶意代码攻击。
2	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。	病毒查杀、主动防御	可以通过以下方式保证恶意代码防范的实现： a) 恶意代码库：防病毒软件的恶意代码库与入侵防御系统、UTM 安全网关的恶意代码库不同。 b) 终端/服务器安全保护系统：采用主动防御技术，引入白名单，拜托对恶意代码库的依赖，对系统所有可执行程序进行保护，从根本上阻断恶意代码攻击。
3	应支持防恶意代码的统一管理。	统一管理	可以通过以下方式保证恶意代码防范的实现： a) 防病毒系统：支持防恶意代码软件的统一管理。 b) 终端/服务器安全保护系统：具备统一管理功能。
4	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。	病毒监控	可以通过以下方式保证恶意代码防范的实现： 防病毒系统：支持防恶意代码软件的统一管理。 终端/服务器安全保护系统：具备收集网内计算机发过来的病毒感染信息并能对信息进行分析和处理的能力。
资源控制			
1	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。	资源控制	可以通过以下方式保证资源控制的实现： 终端安全保护系统：具备终端多层网络准入控制能力，可以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。
2	应根据安全策略设置登录终端的操作超时锁定。	资源控制	可以通过以下方式保证资源控制的实现： 操作超时设置：通过对操作系统本身的安全策略设置，实现登录终端的操作超时锁定。

3	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。	资源控制	可以通过以下方式保证资源控制的实现： 服务器安全保护系统：可以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。
4	应限制单个用户对系统资源的最大或最小使用限度。	资源控制	可以通过以下方式保证资源控制的实现： 系统资源使用限制：设置资源控制模块，限制单个用户对系统资源的最大或最小使用限度。
5	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。	资源控制	可以通过以下方式保证资源控制的实现： a) 定期对系统的性能和容量进行规划。 b) 服务器安全保护系统：可以监控系统的状态，并设定报警阀值，如果系统服务水平降低到最小值，将进行报警。
6	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。	资源控制	对服务器的业务用途进行明确的定义，不允许利用服务器进行收发邮件，浏览互联网等一些操作。

A.3 应用安全

A.3.1 二级要求及措施

序号	要求的内容	对应技术措施	实现方式
身份鉴别			
1	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。	身份认证与访问控制	可以通过以下方式保证身份认证措施的实现： 身份认证与访问控制系统：具有身份认证功能，如账号与口令认证、数字证书认证、双因素身份认证（如令牌卡）等，可以实现登录用户的身份标识和鉴别。
2	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。	身份认证与访问控制	可以通过以下方式保证用户身份标识唯一和鉴别信息复杂度检查的实现： 身份认证与访问控制系统：具有身份认证功能，如账号与口令认证、数字证书认证、双因素身份认证（如令牌卡）等，可以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；
3	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。	身份认证与访问控制	可以通过以下方式保证登录失败处理功能的实现： 身份认证与访问控制系统：具有登录失败处理功能，当登录失败时可以采取结束会话、限制非法登录次数和自动退出等措施；
4	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。	身份认证与访问控制	可以通过以下方式保证身份鉴别功能的实现： 身份认证与访问控制系统：系统具有账号与口令、数字证书认证、双因素身份认证（如令牌卡）等功能，可以保证身份鉴别、用户身份标识唯一性检查。可以设置用户身份鉴别信息复杂度（如口令长度与强度、是否启用数字证书）；具有登录失败处理能力，如中止连接，可以根据安全策略配置相关参数。

访问控制			
1	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。	应用访问控制	可以通过以下方式保证应用的访问控制功能的实现： a) 应用访问控制：应用软件在开发时可以开发专门的访问控制模块，依据安全策略控制用户对文件、数据库表等客体的访问。 b) 制定资源访问控制列表，根据实际的应用，把资源和用户角色关联起来，标识用户角色对资源的访问权限；提供角色的制定、编辑、更新。根据具体应用实际，制定出恰当的角色信息，以便和用户的实际身份相映射等服务。
2	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。	应用访问控制	可以通过以下方式保证应用的访问控制功能的实现： a) 应用访问控制：应用软件在开发时可以设置专门的访问控制模块，规定主体与客体及它们之间的操作。 b) 制定资源访问控制列表，根据实际的应用，把资源和用户角色关联起来，标识用户角色对资源的访问权限；提供角色的制定、编辑、更新。根据具体应用实际，制定出恰当的角色信息，以便和用户的实际身份相映射等服务。
3	应由授权主体配置访问控制策略，并严格限制默认账户的访问权限。	应用访问控制	可以通过以下方式保证应用的访问控制功能的实现： a) 应用访问控制：应用软件在开发时可以设置专门的访问控制模块，限制默认账户的访问权限。 b) 制定资源访问控制列表，根据实际的应用，把资源和用户角色关联起来，标识用户角色对资源的访问权限；提供角色的制定、编辑、更新。根据具体应用实际，制定出恰当的角色信息，以便和用户的实际身份相映射等服务。
4	应授予不同账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。	应用访问控制	可以通过以下方式保证应用的访问控制功能的实现： a) 应用访问控制：应用软件在开发时可以设置专门的访问控制模块，设置不同账号的最小权限，并在它们之间形成相互制约的关系。 b) 制定资源访问控制列表，根据实际的应用，把资源和用户角色关联起来，标识用户角色对资源的访问权限；提供角色的制定、编辑、更新。根据具体应用实际，制定出恰当的角色信息，以便和用户的实际身份相映射等服务。
5	生产系统应建立关键账户与权限的关系表。	应用访问控制	梳理生产系统中的关键账号(比如生产系统的系统管理员账号，重要业务人员的账号等)并建立与该账号对应的权限明细表，形成文档保存，权限发生变更时，明细表也应及时变更。
安全审计			
1	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。	日志审计	可以通过以下方式保证安全审计功能的实现： 日志审计系统：日志审计系统可以审计每个用户，包括主机、服务器、网络设备、安全设备的安全事件，其中安全设备可以检测与记录应用系统的重要安全事件。
2	应保证不提供删除、修改或覆盖审计记录的功能。	日志审计	可以通过以下方式保证安全审计功能的实现： 日志审计系统：日志审计系统可以设置用户权限，不具备权限的用户无法删除、修改或覆盖审计记录。

3	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。	日志审计	可以通过以下方式保证安全审计功能的实现： 日志审计系统：日志审计系统可以记录事件日期、时间、发起者信息、被访问者/被攻击者信息、事件类型、安全级别、事件内容描述和结果等内容，保存时间不少于一个月。
通信完整性			
1	应采用校验码技术保证通信过程中数据的完整性。	通信加密	可以通过以下方式保证通信完整性功能的实现： 加密网关：加密网关中会使用到校验码技术保证通信过程中数据的完整性。
通信保密性			
1	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。	通信加密	可以通过以下方式保证通信保密性功能的实现： a) VPN 网关：支持 ipsec vpn 和 ssl vpn，对于应用系统的通信可使用 VPN 技术进行加密。 b) 加密网关：链路加密机可以对数据进行加密。 建议使用防火墙或者 UTM 安全网关中的 VPN 模块来实现此功能，保护安全投资。
2	应对通信过程中的敏感信息字段进行加密。	通信加密	可以通过以下方式保证通信保密性功能的实现： a) VPN 网关：对于敏感数据，可通过 VPN 技术进行加密。 b) 加密网关：链路加密机可以对数据进行加密。 建议使用防火墙或者 UTM 安全网关中的 VPN 模块来实现此功能，保护安全投资
软件容错			
1	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。	软件容错机制、风险评估	可以通过以下方式保证数据有效性检验功能： a) 软件容错机制：在应用系统开发时，就考虑软件检查机制，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) 风险评估服务:风险评估服务可以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；
2	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。	软件容错机制	可以通过以下方式保证在故障发生时，应用系统应能够继续提供一部分功能： 软件容错机制：在应用系统开发时，就考虑软件容错机制，使故障发生时，应用系统还能继续提供一部分功能。
3	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。	软件容错	在应用系统开发时，应考虑系统错误信息屏蔽机制(比如采用 catch 方式处理产生系统错误的异常状况或其他设计方法进行有效处理)，当发生故障时，不得将系统错误信息反馈给客户。
资源控制			
1	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	资源控制	可以通过以下方式保证应用系统在一段时间内未作任何响应，另一方应能够自动结束会话； 应用系统控制：在应用系统开发时，就设置通信双方的超时机制，使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；

	够自动结束会话。		
2	应能够对应用系统的最大并发会话连接数进行限制。	连接数控制	可以通过以下方式保证对应用系统的最大并发会话连接数进行限制； a) 软硬件防火墙：可以限制网络的最大并发会话连接数；通过针对特定 IP 的连接限制，能够限制特定应用系统最大并发会话连接数。 b) UTM 安全网关：可以限制网络的最大并发会话连接数；通过针对特定 IP 的连接限制，能够限制特定应用系统最大并发会话连接数。 应根据信息系统不同的情况选择防火墙和UTM安全网关产品：在面临威胁较为的情况下，如病毒、入侵，选择 UTM 安全网关进行网络隔离。
3	对于有会话的应用系统，应能够对单个账户的多重并发会话进行限制。	会话限制	可以通过以下方式保证对单个账户的多重并发会话进行限制： 账号多重并发会话限制：在应用系统开发时，就设置账户多重并发会话限制功能，实现对单个账户的多重并发会话进行限制。

A.3.2 三级要求及措施

序号	要求的内容	对应技术措施	实现方式
身份鉴别			
1	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。	身份认证与访问控制	可以通过以下方式保证身份认证措施的实现： 身份认证与访问控制系统：具有身份认证功能，如账号与口令认证、数字证书认证、双因素身份认证（如令牌卡）等，可以实现登录用户的身份标识和鉴别。
2	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。	身份认证与访问控制	可以通过以下方式保证身份认证措施的实现： 身份认证与访问控制系统：具有身份认证功能，如账号与口令认证、数字证书认证、双因素身份认证（如令牌卡，指纹识别）等，可以实现登录用户的身份标识和鉴别。
3	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。	身份认证与访问控制	可以通过以下方式保证用户身份标识唯一和鉴别信息复杂度检查的实现： 身份认证与访问控制系统：具有身份认证功能，如账号与口令认证、数字证书认证、双因素身份认证（如令牌卡）等，可以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；
4	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	身份认证与访问控制	可以通过以下方式保证登录失败处理功能的实现： 身份认证与访问控制系统：具有登录失败处理功能，当登录失败时可以采取结束会话、限制非法登录次数和自动退出等措施；

	和自动退出等措施。		
5	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。	身份认证与访问控制	可以通过以下方式保证身份鉴别功能的实现： 身份认证与访问控制系统：系统具有账号与口令、数字证书认证、双因素身份认证（如令牌卡）等功能，可以保证身份鉴别、用户身份标识唯一性检查。可以设置用户身份鉴别信息复杂度（如口令长度与强度、是否启用数字证书）；具有登录失败处理能力，如中止连接，可以根据安全策略配置相关参数。
6	应用软件客户端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。	身份认证	服务器对客户端德连接提供 session-timeout 设置功能，客户端登录成功后长时间会话闲置，服务器将对其锁定。
7	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。	身份认证	服务器检测到客户端的密码是初始密码时，提供强制修改客户端密码的功能。
8	修改密码时，不允许新设定的密码与旧密码相同。	身份认证	客户端每次修改密码服务器记录新密码和旧密码，每个客户端都对应唯一的密码表。客户端每次提交新密码，服务器检索密码表，查看是否有重复的密码，如果有，则禁止客户端提交新密码。
访问控制			
1	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。	应用访问控制	可以通过以下方式保证应用的访问控制功能的实现： a) 应用访问控制：应用软件在开发时可以开发专门的访问控制模块，依据安全策略控制用户对文件、数据库表等客体的访问。 b) 制定资源访问控制列表，根据实际的应用，把资源和用户角色关联起来，标识用户角色对资源的访问权限；提供角色的制定、编辑、更新。根据具体应用实际，制定出恰当的角色信息，以便和用户的实际身份相映射等服务。
2	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。	应用访问控制	可以通过以下方式保证应用的访问控制功能的实现： a) 应用访问控制：应用软件在开发时可以设置专门的访问控制模块，规定主体与客体及它们之间的操作。 b) 制定资源访问控制列表，根据实际的应用，把资源和用户角色关联起来，标识用户角色对资源的访问权限；提供角色的制定、编辑、更新。根据具体应用实际，制定出恰当的角色信息，以便和用户的实际身份相映射等服务。
3	应由授权主体配置访问控制策略，并严格限制默认账户的访问。	应用访问控制	可以通过以下方式保证应用的访问控制功能的实现： a) 应用访问控制：应用软件在开发时可以设置专门的访问控制模块，限制默认账户的访问权限。 b) 制定资源访问控制列表，根据实际的应用，把资源和用户角色关联起来，标识用户角色对资源的访问权限；提供角色的制定、编辑、更新。根据具体应用实际，制定出恰当的角色信息，以便和用户的实际身份相映射等服务。
4	应授予不同账户为完成各自承担任务所需的最小权限，并在它们	应用访问控制	可以通过以下方式保证应用的访问控制功能的实现： a) 应用访问控制：应用软件在开发时可以设置专门的访问控制模块，设置不同账号的最小权限，并在它们之间形成相互制约的

	之间形成相互制约的关系。		关系。 b) 制定资源访问控制列表，根据实际的应用，把资源和用户角色关联起来，标识用户角色对资源的访问权限；提供角色的制定、编辑、更新。根据具体应用实际，制定出恰当的角色信息，以便和用户的实际身份相映射等服务。
5	应有生产系统关键账户与权限的关系表。	应用访问控制	梳理生产系统中的关键账号(比如生产系统的系统管理员账号，重要业务人员的账号等)并建立与该账号对应的权限明细表，形成文档保存，权限发生变更时，明细表也应及时变更。
6	**宜**具有对重要信息资源设置敏感标记的功能。	应用信息标记	可以通过以下方式保证应用信息标记功能的实现： 应用信息标记：应用软件在开发时可以设置信息标记功能，使应用系统能对重要信息资源设置敏感标记。
7	**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。	应用访问控制	可以通过以下方式保证应用访问控制功能的实现： a) 应用访问控制::：应用软件在开发时可以设置专门的访问控制模块，可以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。 b) 制定资源访问控制列表，根据实际的应用，把资源和用户角色关联起来，标识用户角色对资源的访问权限；提供角色的制定、编辑、更新。根据具体应用实际，制定出恰当的角色信息，以便和用户的实际身份相映射等服务。
安全审计			
1	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。	日志审计	可以通过以下方式保证安全审计功能的实现： 日志审计系统：日志审计系统可以审计每个用户，包括主机、服务器、网络设备、安全设备的安全事件，其中安全设备可以检测与记录应用系统的重要安全事件。
2	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。	日志审计	可以通过以下方式保证安全审计功能的实现： 日志审计系统：日志审计系统可以设置用户权限，不具备权限的用户无法删除、修改或覆盖审计记录；通过服务器的安全加固配置，使非授权人员无法单独中断审计进程。
3	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，并定期备份审计记录，保存时间不少于半年。	日志审计	可以通过以下方式保证安全审计功能的实现： 日志审计系统：日志审计系统可以记录事件日期、时间、发起者信息、被访问者/被攻击者信息、事件类型、安全级别、事件内容描述和结果等内容。
4	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。	日志审计	可以通过以下方式保证安全审计功能的实现： 日志审计系统：日志审计系统可以提供对审计记录数据进行统计、查询、分析及生成审计报表等功能。
5	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	日志审计	日志审计系统：日志审计系统可以提供用户上一次成功登录的日期、时间、方法、位置、错误登录等信息。

	的日期、时间、方法、位置、错误登录等信息，以便用户及时发现可能的问题。		
剩余信息保护			
1	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。	剩余信息保护	可以通过以下方式保证剩余信息保护功能的实现： 剩余信息保护：在软件开放时，开发剩余信息保护功能，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；
2	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。	剩余信息保护	可以通过以下方式保证剩余信息保护功能的实现： 剩余信息保护：在软件开放时，开发剩余信息保护功能。可以保证系统内的文件、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。
通信完整性			
1	应采用密码技术保证通信过程中关键数据的完整性。	通信加密	可以通过以下方式保证通信完整性功能的实现： 加密网关：加密网关中会使用到密码技术保证通信过程中数据的完整性。
通信保密性			
1	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。	通信加密	可以通过以下方式保证通信保密性功能的实现： a) VPN 网关：对于敏感数据，可通过 VPN 技术进行加密。 b) 加密网关：链路加密机可以对数据进行加密。 建议使用防火墙或者 UTM 安全网关中的 VPN 模块来实现此功能，保护安全投资。
2	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。	通信加密	可以通过以下方式保证通信保密性功能的实现： a) VPN 网关：对于敏感数据，可通过 VPN 技术进行加密，包括整个报文或会话过程。 b) 加密网关：链路加密机可以对数据进行加密，包括整个报文或会话过程。 建议使用防火墙或者 UTM 安全网关中的 VPN 模块来实现此功能，保护安全投资。
抗抵赖			
1	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。	认证签名系统	可以通过以下方式保证应用系统抗抵赖功能的实现： 认证签名系统：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；
2	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。	认证签名系统	可以通过以下方式保证应用系统抗抵赖功能的实现： 认证签名系统：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；

软件容错			
1	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。	风险评估	可以通过以下方式保证数据有效性检验功能： a) 软件容错机制：在应用系统开发时，就考虑软件检查机制，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) 风险评估服务：风险评估服务可以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；
2	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。	软件容错机制	可以通过以下方式保证在故障发生时，自动保护当前所有状态，保证系统能够进行恢复： 软件容错机制：在应用系统开发时，就考虑软件容错机制，使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。
3	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。	软件容错机制	在应用系统开发时，应考虑系统错误信息屏蔽机制(比如采用 catch 方式处理产生系统错误的异常状况或其他设计方法进行有效处理)，当发生故障时，不得将系统错误信息反馈给客户。
资源控制			
1	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。	资源控制	可以通过以下方式保证应用系统在一段时间内未作任何响应，另一方应能够自动结束会话； 应用系统控制：在应用系统开发时，就设置通信双方的超时机制，使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；
2	应能够对应用系统的最大并发会话连接数进行限制。	连接数控制	可以通过以下方式保证对应用系统的最大并发会话连接数进行限制； a) 软硬件防火墙：可以限制网络的最大并发会话连接数；通过针对特定 IP 的连接限制，能够限制特定应用系统最大并发会话连接数。 b) UTM 安全网关：可以限制网络的最大并发会话连接数；通过针对特定 IP 的连接限制，能够限制特定应用系统最大并发会话连接数。 **应**根据信息系统不同的情况选择防火墙和 UTM 安全网关产品：在面临威胁 较为的情况下，如病毒、入侵，选择 UTM 安全网关进行网络隔离。
3	对于有会话的应用系统，应能够对单个账户的多重并发会话进行限制。	会话限制	可以通过以下方式保证对单个账户的多重并发会话进行限制： 账号多重并发会话限制：在应用系统开发时，就设置账户多重并发会话限制功能，实现对单个账户的多重并发会话进行限制。
4	应能够对一个时间段内可能的并发会话连接数进行限制。	会话限制	可以通过以下方式保证能够对一个时间段内可能的并发会话连接数进行限制； 会话限制：在应用系统开发时就设置并发会话连接数限制功能，保证对一个时间段内可能的并发会话连接数进行限制。

5	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。	资源分配	可以通过以下方式保证资源分配功能的实现： 资源分配：在应用系统开发时就设置资源分配功能，保证对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额。
6	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。	安全管理与监控	可以通过以下方式保证安全管理与监控功能的实现： 安全管理与监控系统：可以对主机、服务器的 CPU、内存、磁盘利用率等信息进行监控，并设定报警阀值，可以进行检测和报警。
7	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账户或请求进程的优先级，根据优先级分配系统资源。	安全管理与监控	可以通过以下方式保证安全管理与监控功能的实现： 安全管理与监控系统：可以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账户或请求进程的优先级，根据优先级分配系统资源。

A.3.3 四级要求及措施

序号	要求的内容	对应技术措施	实现方式
身份鉴别			
1	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。	身份认证与访问控制	可以通过以下方式保证身份认证措施的实现： 身份认证与访问控制系统：具有身份认证功能，如账号与口令认证、数字证书认证、双因素身份认证（如令牌卡）等，可以实现登录用户的身份标识和鉴别。
2	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。	身份认证与访问控制	可以通过以下方式保证身份认证措施的实现： 身份认证与访问控制系统：具有身份认证功能，如账号与口令认证、数字证书认证、双因素身份认证（如令牌卡，指纹识别）等，可以实现登录用户的身份标识和鉴别。
3	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。	身份认证与访问控制	可以通过以下方式保证用户身份标识唯一和鉴别信息复杂度检查的实现： 身份认证与访问控制系统：具有身份认证功能，如账号与口令认证、数字证书认证、双因素身份认证（如令牌卡）等，可以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；
4	应提供登录失败处理功能，可采	身份认证与访问控制	可以通过以下方式保证登录失败处理功能的实现： 身份认证与访问控制系统：具有登录失败处理功能，当登录失败时可以

	取结束会话、限制非法登录次数和自动退出等措施。		采取结束会话、限制非法登录次数和自动退出等措施；
5	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。	身份认证与访问控制	可以通过以下方式保证身份鉴别功能的实现： 身份认证与访问控制系统：系统具有账号与口令、数字证书认证、双因素身份认证（如令牌卡）等功能，可以保证身份鉴别、用户身份标识唯一性检查。可以设置用户身份鉴别信息复杂度（如口令长度与强度、是否启用数字证书）；具有登录失败处理能力，如中止连接，可以根据安全策略配置相关参数。
7	应用软件客户端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。	身份认证	服务器对客户端德连接提供 session-timeout 设置功能，客户端登录成功后长时间会话闲置，服务器将对其锁定。
8	系统应强制客户首次登录时修改初始密码。	身份认证	服务器检测到客户端的密码是初始密码时，提供强制修改客户端密码的功能。
9	修改密码时，不允许新设定的密码与旧密码相同。	身份认证	客户端每次修改密码服务器记录新密码和旧密码，每个客户端都对应唯一的密码表。客户端每次提交新密码，服务器检索密码表，查看是否有重复的密码，如果有，则禁止客户端提交新密码。
安全标记			
1	宜提供为主体和客体设置安全标记的功能并在安装后启用。	安全标记	可以通过以下方式保证安全标记功能的实现： 安全标记功能：应用软件在开发时，可以设置安全标识模块，为主体和客体设置安全标记的功能。
访问控制			
1	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。	应用访问控制	可以通过以下方式保证应用的访问控制功能的实现： a) 应用访问控制：应用软件在开发时可以开发专门的访问控制模块，提供自主访问的控制功能（管理员或用户可以设置），依据安全策略控制用户对文件、数据库表等客体的访问。 b) 制定资源访问控制列表，根据实际的应用，把资源和用户角色关联起来，标识用户角色对资源的访问权限；提供角色的制定、编辑、更新。根据具体应用实际，制定出恰当的角色信息，以便和用户的实际身份相映射等服务。
2	自主访问控制的覆盖范围应包括与信息安全直接	应用访问控制	可以通过以下方式保证应用的访问控制功能的实现： a) 应用访问控制：应用软件在开发时可以设置专门的访问控制模块，规定与信息安全直接相关的主体与客体及它们之间的操作。

	相关的主体、客体及它们之间的操作。		b) 制定资源访问控制列表，根据实际的应用，把资源和用户角色关联起来，标识用户角色对资源的访问权限；提供角色的制定、编辑、更新。根据具体应用实际，制定出恰当的角色信息，以便和用户的实际身份相映射等服务。
3	应由授权主体配置访问控制策略，并禁止默认账户的访问。	应用访问控制	可以通过以下方式保证应用的访问控制功能的实现： a) 应用访问控制：应用软件在开发时可以设置专门的访问控制模块，禁止默认账户的访问权限。 b) 制定资源访问控制列表，根据实际的应用，把资源和用户角色关联起来，标识用户角色对资源的访问权限；提供角色的制定、编辑、更新。根据具体应用实际，制定出恰当的角色信息，以便和用户的实际身份相映射等服务。
4	应授予不同账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。	应用访问控制	可以通过以下方式保证应用的访问控制功能的实现： a) 应用访问控制：应用软件在开发时可以设置专门的访问控制模块，设置不同账号的最小权限，并在它们之间形成相互制约的关系。 b) 制定资源访问控制列表，根据实际的应用，把资源和用户角色关联起来，标识用户角色对资源的访问权限；提供角色的制定、编辑、更新。根据具体应用实际，制定出恰当的角色信息，以便和用户的实际身份相映射等服务。
5	应有生产系统内关键账户与权限的关系表。	应用访问控制	梳理生产系统中的关键账号(比如生产系统的系统管理员账号，重要业务人员的账号等)并建立与该账号对应的权限明细表，形成文档保存，权限发生变更时，明细表也应及时变更。
6	宜具有对重要信息资源设置敏感标记的功能。	应用信息标记	可以通过以下方式保证应用信息标记功能的实现： 应用信息标记：应用软件在开发时可以设置信息标记功能，使应用系统能对重要信息资源设置敏感标记。
7	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。	应用访问控制	可以通过以下方式保证应用的访问控制功能的实现： a) 应用访问控制：应用软件在开发时可以设置专门的访问控制模块，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。 b) 制定资源访问控制列表，根据实际的应用，把资源和用户角色关联起来，标识用户角色对资源的访问权限；提供角色的制定、编辑、更新。根据具体应用实际，制定出恰当的角色信息，以便和用户的实际身份相映射等服务。
可信路径			
1	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。	通信加密	可以通过以下方式保证安全的信息传输路径功能的实现： VPN 网关：支持 ipsec vpn 和 ssl vpn，对于应用系统的通信可使用 VPN 技术进行加密和身份鉴别，确保建立一条安全的信息传输路径。 建议使用防火墙或者 UTM 安全网关中的 VPN 模块来实现此功能，保护安全投资。
2	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	通信加密	可以通过以下方式保证安全的信息传输路径功能的实现： VPN 网关：支持 ipsec vpn 和 ssl vpn，对于应用系统的通信可使用 VPN 技术进行加密和身份鉴别，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。 建议使用防火墙或者 UTM 安全网关中的 VPN 模块来实现此功能，保护安全投资。

	一条安全的信息传输路径。		
安全审计			
1	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。	日志审计	可以通过以下方式保证安全审计功能的实现： 日志审计系统：日志审计系统可以审计每个用户，包括主机、服务器、网络设备、安全设备的安全事件，其中安全设备可以检测与记录应用系统的重要安全事件。
2	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。	日志审计	可以通过以下方式保证安全审计功能的实现： 日志审计系统：日志审计系统可以设置用户权限，不具备权限的用户无法删除、修改或覆盖审计记录；通过服务器的安全加固配置，使非授权人员无法单独中断审计进程。
3	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，并定期备份审计记录，保存时间不少于一年。	日志审计	可以通过以下方式保证安全审计功能的实现： 日志审计系统：日志审计系统可以记录事件日期、时间、发起者信息、被访问者/被攻击者信息、事件类型、安全级别、事件内容描述和结果等内容，并定期备份审计记录，保存时间不少于一年。
4	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。	日志审计	可以通过以下方式保证安全审计功能的实现： 日志审计系统：日志审计系统可以提供对审计记录数据进行统计、查询、分析及生成审计报表等功能。
5	应根据系统统一安全策略，提供集中审计接口。	日志审计	可以通过以下方式保证安全审计功能的实现： 日志审计系统：日志审计系统可以提供集中审计接口。
6	对于从互联网客户端登陆的应用系统，对于重要的业务系统，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、错误登录等信息，以便用户及时发现可能的问题。	日志审计	日志审计系统：日志审计系统可以提供用户上一次成功登录的日期、时间、方法、位置、错误登录等信息。
剩余信息保护			
1	应保证用户鉴别	剩余信息保护	可以通过以下方式保证剩余信息保护功能的实现：

	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。		剩余信息保护：在软件开放时，开发剩余信息保护功能，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；
2	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。	剩余信息保护	可以通过以下方式保证剩余信息保护功能的实现： 剩余信息保护：在软件开放时，开发剩余信息保护功能。可以保证系统内的文件、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。
通信完整性			
1	应采用密码技术保证通信过程中数据的完整性。	通信加密	可以通过以下方式保证通信完整性功能的实现： 加密网关：加密网关中会使用到密码技术保证通信过程中数据的完整性。
通信保密性			
1	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。	通信加密	可以通过以下方式保证通信保密性功能的实现： a) VPN 网关：对于敏感数据，可通过 VPN 技术进行加密。 b) 加密网关：链路加密机可以对数据进行加密。 建议使用防火墙或者 UTM 安全网关中的 VPN 模块来实现此功能，保护安全投资。
2	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。	通信加密	可以通过以下方式保证通信保密性功能的实现： a) VPN 网关：对于敏感数据，可通过 VPN 技术进行加密，包括整个报文或会话过程。 b) 加密网关：链路加密机可以对数据进行加密，包括整个报文或会话过程，如采用 SSL 协议，最低需达到 128 位的加密强度。 建议使用防火墙或者 UTM 安全网关中的 VPN 模块来实现此功能，保护安全投资。
3	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。	通信加密	可以通过以下方式保证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的实现： a) VPN 网关：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。 b) 加密网关：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。 建议使用防火墙或者 UTM 安全网关中的 VPN 模块来实现此功能，保护安全投资。
抗抵赖			
1	应具有在请求的情况下为数据原	认证签名系统	可以通过以下方式保证应用系统抗抵赖功能的实现： 认证签名系统：具有在请求的情况下为数据原发者或接收者提供数据原

	发者或接收者提供数据原发证据的功能。		发证据的功能；
2	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。	认证签名系统	可以通过以下方式保证应用系统抗抵赖功能的实现： 认证签名系统：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；
软件容错			
1	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。	风险评估	可以通过以下方式保证数据有效性检验功能： a) 软件容错机制：在应用系统开发时，就考虑软件检查机制，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) 风险评估服务：风险评估服务可以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；
2	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。	软件容错机制	可以通过以下方式保证在故障发生时，自动保护当前所有状态，保证系统能够进行恢复： 软件容错机制：在应用系统开发时，就考虑软件容错机制，使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。
3	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。	软件容错机制	可以通过以下方式保证在故障发生时立即自动启动新的进程，恢复原来的工作状态。 软件容错机制：在应用系统开发时，就考虑软件容错机制，使故故障发生时立即自动启动新的进程，恢复原来的工作状态。
4	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。	软件容错机制	在应用系统开发时，应考虑系统错误信息屏蔽机制(比如采用 catch 方式处理产生系统错误的异常状况或其他设计方法进行有效处理)，当发生故障时，不得将系统错误信息反馈给客户。
资源控制			
1	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	资源控制	可以通过以下方式保证应用系统在一段时间内未作任何响应，另一方应能够自动结束会话； 应用系统控制：在应用系统开发时，就设置通信双方的超时机制，使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；

	话。		
2	应能够对应用系统的最大并发会话连接数进行限制。	连接数控制	可以通过以下方式保证对应用系统的最大并发会话连接数进行限制； a) 软硬件防火墙：可以限制网络的最大并发会话连接数；通过针对特定 IP 的连接限制，能够限制特定应用系统最大并发会话连接数。 b) UTM 安全网关：可以限制网络的最大并发会话连接数；通过针对特定 IP 的连接限制，能够限制特定应用系统最大并发会话连接数。 应根据信息系统不同的情况选择防火墙和 UTM 安全网关产品：在面临威胁较为的情况下，如病毒、入侵，选择 UTM 安全网关进行网络隔离。
3	对于有会话的应用系统，应能够对单个账户的多重并发会话进行限制。	会话限制	可以通过以下方式保证对单个账户的多重并发会话进行限制： 账号多重并发会话限制：在应用系统开发时，就设置账户多重并发会话限制功能，实现对单个账户的多重并发会话进行限制。
4	应能够对一个时间段内可能的并发会话连接数进行限制。	会话限制	可以通过以下方式保证能够对一个时间段内可能的并发会话连接数进行限制； 会话限制：在应用系统开发时就设置并发会话连接数限制功能，保证对一个时间段内可能的并发会话连接数进行限制。
5	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。	资源分配	可以通过以下方式保证资源分配功能的实现： 资源分配：在应用系统开发时就设置资源分配功能，保证对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额。
6	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。	安全管理与监控	可以通过以下方式保证安全管理与监控功能的实现： 安全管理与监控系统：可以对主机、服务器的 CPU、内存、磁盘利用率等信息进行监控，并设定报警阀值，可以进行检测和报警。
7	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账户或请求进程的优先级，根据优先级分配系统资源。	安全管理与监控	可以通过以下方式保证安全管理与监控功能的实现： 安全管理与监控系统：可以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账户或请求进程的优先级，根据优先级分配系统资源。

A.4 数据安全

A.4.1 二级要求及措施

序号	要求的内容	对应技术措施	实现方式
数据完整性			
1	应能够检测到鉴别信息和重要业	完整性校验	可以通过以下方式保证完整性校验的实现： a) 完整性校验：设置完整性校验模块，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。		务数据是否在采集、传输、使用和存储过程中完整性受到破坏。
数据保密性			
1	应采用加密或其他保护措施实现鉴别信息的存储保密性。	加密系统	可以通过以下方式保证数据保密性的实现： b) 加密系统：加密系统可以保证鉴别信息的存储保密性。
备份和恢复			
1	应能够对重要信息进行备份和恢复。	存储备份系统	可以通过以下方式保证备份和恢复的实现： 存储备份系统：能够对重要信息进行备份和恢复，并可以设置各种备份策略，如果全局备份、增量备份等。
2	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。	冗余设计	可以通过以下方式保冗余设计的实现： 冗余设计：可以实现关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性。

A.4.2 三级要求及措施

序号	要求的内容	对应技术措施	实现方式
数据完整性			
1	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。	完整性校验	可以通过以下方式保证完整性校验的实现： 完整性校验：设置完整性校验模块，检测到系统管理数据、鉴别信息和重要业务数据是否在采集、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；
数据保密性			
1	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。	通信保密	可以通过以下方式保证通信保密的实现： VPN 系统：VPN 系统可以保证系统管理数据、鉴别信息和重要业务数据传输保密性。
备份和恢复			
1	应提供本地数据备份与恢复功能，采取实时备份与异步	存储备份系统	可以通过以下方式保证备份与恢复的实现： 存储备份系统：可以供本地数据备份与恢复功能，完全数据备份至少每周一次，备份介质场外存放，数据保存期限依照国家相关规定；

	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。		
2	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。	存储备份系统	可以通过以下方式保证备份与恢复的实现： 存储备份系统：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；
3	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。	灾难备份	建立灾备机房， 保证与生产中心直线距离至少达到 100 公里且位于不同城市的灾难备份中心，可以接管所有核心业务的运行。
4	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。	灾难备份	对灾备方案的关键技术环节(如数据备份，数据恢复等重要技术)进行详细测试，并形成测试报告。
5	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。	存储备份系统	可以通过以下方式保证备份与恢复的实现： 存储备份系统：可采用磁带、磁盘镜像技术进行数据的冗余备份，备份的冗余数据至少要保留一周；
6	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。	存储备份系统	异地备份中心配备恢复所需的全部运行环境(硬件环境，软件环境，维护人员配备等)，系统运行状态保持在就绪状态或运行状态。

A.4.3 四级要求及措施

序号	要求的内容	对应技术措施	实现方式
数据完整性			

1	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。	完整性校验	可以通过以下方式保证完整性校验的实现： 完整性校验：设置完整性校验模块，检测到系统管理数据、鉴别信息和重要业务数据是否在采集、传输、使用和存储过程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；
2	应对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。	安全通信	可以通过以下方式保证安全通信的实现： 安全通信：设置专用通信协议或安全通信协议服务，如 HTTPS 或者 VPN 加密，避免来自基于通用通信协议的攻击破坏数据完整性。
数据保密性			
1	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。	通信保密	可以通过以下方式保证通信保密的实现： a) VPN 系统：VPN 系统可以保证系统管理数据、鉴别信息和重要业务数据传输保密性。 b) 硬件加密机应通过国家商用密码委员会的安全认证并被允许在国内金融机构中使用。此外还必须满足以下要求：支持单倍长（B64，在单倍长密钥算法中使用）和双倍长（B128，在双倍长密钥算法中使用）的密钥；支持本文中对 PIN 的规定，验证、转换 PIN 的密文；支持本文中对 MAC 的规定，验证和产生 MAC；能对密钥作验证；受到非法攻击时，加密机内部保护的密钥自动销毁。
2	应对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。	安全通信	可以通过以下方式保证安全通信的实现： 安全通信：设置专用通信协议或安全通信协议服务，如 HTTPS 或者 VPN 加密，避免来自基于通用通信协议的攻击破坏数据保密性。
备份和恢复			
1	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	存储备份系统	可以通过以下方式保证备份与恢复的实现： 存储备份系统：可以供本地数据备份与恢复功能，完全数据备份至少每周一次，备份介质场外存放， 数据保存期限至少 15 年；

	年。		
2	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。	存储备份系统	可以通过以下方式保证备份与恢复的实现： 存储备份系统：可采用磁带、磁盘镜像技术进行数据的冗余备份，备份的冗余数据至少要保留一个月；
3	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。	存储备份系统	可以通过以下方式保证备份与恢复的实现： 存储备份系统：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；
4	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。	存储备份系统	可以通过以下方式保证备份与恢复的实现： 存储备份系统：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；
5	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。	灾难备份	异地备份中心配备恢复所需的全部运行环境(硬件环境，软件环境，维护人员配备等)，系统运行状态保持在就绪状态或运行状态。
6	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。	灾难备份	对灾备方案的关键技术环节(如数据备份，数据恢复等重要技术)进行详细测试，并形成测试报告。
7	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。	冗余设计	可以通过以下方式保证冗余技术设计网络的实现： 冗余设计：采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；
8	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。	存储备份系统	可以通过以下方式保证系统高可用性的实现： 高可用性设计：提供主要网络设备、通信线路和数据处理系统的硬件冗余。

附录 B

（资料性附录）

金融行业安全要求的选择和使用说明

金融行业技术类安全要求按其保护的侧重点不同，将其下的基础控制点分为四类，另外根据金融行业特点加入增强安全要求：

信息安全类（S 类）——关注的是保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改。

如，自主访问控制，该控制点主要关注的是防止未授权的访问系统，进而造成数据的修改或泄漏。至于对保证业务的正常连续运行并没有直接的影响。

服务保证类（A 类）——关注的是保护系统连续正常的运行，避免因对系统的未授权修改、破坏而导致系统不可用。

如，数据的备份和恢复，该控制点很好的体现了对业务正常运行的保护。通过对数据进行备份，在发生安全事件后能够及时的进行恢复，从而保证了业务的正常运行。

通用安全保护类（G 类）——既关注保护业务信息的安全性，同时也关注保护系统的连续可用性。

大多数技术类安全要求都属于此类，保护的重点既是为了保证业务能够正常运行，同时数据要安全。如，物理访问控制，该控制点主要是防止非授权人员物理访问系统主要工作环境，由于进入工作环境可能导致的后果既可能包括系统无法正常运行（如，损坏某台重要服务器），也可能窃取某些重要数据。因此，它保护的重点二者兼而有之。

金融行业增强安全保护类（F 类）——根据金融行业业务特点提出的特殊安全要求。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。

金融行业技术安全要求按其保护的侧重点不同分为 S、A、G、F 四类，如果从另外一个角度考虑，根据信息系统安全的整体结构来看，金融行业信息系统安全可从五个层面：物理、网络、主机、应用和数据对系统进行保护，因此，技术类安全要求也相应的分为五个层面上的安全要求：

——物理层面安全要求：主要是从外界环境、基础设施、运行硬件、介质等方面为信息系统的安全运行提供基本的后台支持和保证；

——网络层面安全要求：为信息系统能够在安全的网络环境中运行提供支持，确保网络系统安全运行，提供有效的网络服务；

——主机层面安全要求：在物理、网络层面安全的情况下，提供安全的操作系统和安全的数据库管理系统，以实现操作系统和数据库管理系统的安全运行；

——应用层面安全要求：在物理、网络、主机等层面安全的支持下，实现用户安全需求所确定的安全目标；

——数据及备份恢复层面安全要求：全面关注信息系统中存储、传输、处理等过程的数据的安全性。

信息系统由于承载的业务不同，对其的安全关注点会有所不同，有的更关注信息的安全性，即更关注对搭线窃听、假冒用户等可能导致信息泄密、非法篡改等；有的更关注业务的连续性，即更关注保证系统连续正常的运行，免受对系统未授权的修改、破坏而导致系统不可用引起业务中断。

不同安全保护等级的信息系统，其对业务信息的安全性要求和系统服务的连续性要求是有差异的；即使相同安全保护等级的信息系统，其对业务信息的安全性要求和系统服务的连续性要求也有差异。信息系统的安全保护等级由业务信息安全性等级和系统服务保证性等级较高者决定（见 GB/T 22240-2008），因此，对某一个定级后的信息系统的安全保护的侧重点可以有多种组合。

信息系统定级后，不同安全保护等级的信息系统可能形成的定级结果组合见表 B.1。

表B.1 各等级信息系统定级结果组合

安全保护等级	信息系统定级结果的组合
第二级	S1A2G2，S2A2G2，S2A1G2
第三级	S1A3G3，S2A3G3，S3A3G3，S3A2G3，S3A1G3

第四级	S1A4G4，S2A4G4，S3A4G4，S4A4G4，S4A3G4，S4A2G4，S4A1G4

本标准中的每一个安全保护等级的基本安全要求按照业务信息安全性等级和系统服务保证性等级相同的情况组织，也就是每一级的基本安全要求针对 S1A1G1、S2A2G2、S3A3G3 和 S4A4G4 情况给出。

对于确定了安全保护等级的信息系统，选择和使用基本安全要求时，可以按照以下过程进行：

a)、明确信息系统应该具有的安全保护能力，根据信息系统的安全保护等级选择基本安全要求，包括技术要求和管理要求。简单的方法是根据本标准，一级系统选择第一级基本安全要求，二级系统选择第二级基本安全要求，三级系统选择第三级基本安全要求，四级系统选择第四级基本安全要求，以此作为出发点。

b)、根据信息系统的定级结果对基本安全要求进行调整。根据系统服务保证性等级选择相应等级的系统服务保证类（A 类）基本安全要求；根据业务信息安全性等级选择相应等级的业务信息安全类（S 类）基本安全要求。例如，某系统根据 S2、A3 定为三级系统，那么可按照 S2 类基本安全要求和 A3 类基本安全要求进行系统建设。

c)、针对金融行业信息系统的特点，分析可能在某些方面的特殊安全保护能力要求，选择较高级别的基本安全要求或补充基本安全要求。对于本标准中提出的基本安全要求无法实现或有更加有效的安全措施可以替代的，可以对基本安全要求进行调整，调整的原则是保证不降低整体安全保护能力。

总之，保证不同安全保护等级的信息系统具有相应级别的安全保护能力，满足相应级别的基本安全要求，是信息系统等级保护的核心。选用本标准中提供的基本安全要求是保证信息系统具备一定安全保护能力的一种途径和出发点，在此出发点的基础上，可以参考等级保护的其他相关标准和安全方面的其他相关标准，调整和补充基本安全要求，从而实现信息系统在满足等级保护基本要求基础上，又具有自身特点的保护。

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