ICS 35.100.05，35.240.40
L79，A11

T /IA C

中 国 保 险 行 业 协 会 团 体 标 准

T/IAC XXXXX—2018

云计算保险风险评估指引

Guidance on cloud computing insurance risk assessment

（征求意见稿）

201X-XX-XX 发布　　XXXX - XX - XX 实施

中国保险行业协会　　发　布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草

本标准由中国保险行业协会提出并归口

本标准起草单位：中国信息通信研究院，中国人民财产保险股份有限公司

本标准起草人

引　言

本标准规定了云计算风险管理框架，针对云计算运行过程中面临的服务不可用、数据丢失、数据泄露等风险，提出风险管理方法。云计算风险管理流程包括风险评估、风险处置、风险接受、风险沟通以及风险监视和评审等内容。

云计算保险风险评估指引

1 范围

本标准规定了云计算风险评估方法，针对云计算运行过程中面临出现的服务不可用、数据丢失、数据泄露等风险后果提出管理方法。

本标准适用于保险公司在云服务商为云平台投保时，由保险公司或第三方评估机构进行云服务商风险管理水平的评估，以作为投保的有效依据。

注：本标准不适用于技术路线风险和政治风险的风险评估。

2 规范性引用文件

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

GB/T 22081-2008 信息技术 安全技术 信息安全管理实用规则

GB/T 32400-2015 信息技术 云计算 概览与词汇

JR/T 0166-2018 云计算技术金融应用规范技术架构

YDB 144－2014 云计算协议参考框架

3 术语和定义

下列术语和定义适用于本文件。

3.1

云计算 cloud computing

一种通过网络将可伸缩、弹性的共享物理和虚拟资源池按需自服务的方式供应和管理的模式。

注：资源包括服务器、操作系统、网络、软件、应用和存储设备等。

[GB/T 32400-2015，定义3.2.5]

3.2

云计算服务 cloud computing service

使用定义的接口，借助云计算提供一种或多种资源的能力。

注：资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。

[GB/T 32400-2015，定义3.2.5]

3.3

云计算厂商 cloud service provider

云计算的供应方。

注：云计算厂商管理、运营、支撑云计算的基础设施及软件，通过网络交付云计算的资源。

3.4

云计算平台 cloud computing platform

云服务提供者和云服务合作者提供的云计算基础设施及其上服务软件的集合。
[JR/T 0166-2018，定义3.8]

3.5

风险 risk

事态的概率及其结果的组合。
[GB/T 22081-2008，定义2.9]

3.6

风险评估 risk assessment

风险分析和风险评价的整个过程。

[GB/T 22081-2008，定义2.11]

3.7

风险管理 risk management

指导和控制一个组织相关风险的协调活动。

注：风险管理一般包括风险评估、风险处置、风险接受和风险沟通。

[GB/T 22081-2008，定义2.13]

3.8

风险处置 risk treatment

选择并且执行措施来更改风险的过程。
[GB/T 22081-2008，定义2.14]

3.9

威胁 treat

可能导致对系统或组织的损害的不期望事件发生的潜在原因。
[GB/T 22081-2008，定义2.16]

3.10

脆弱性 vulnerability

可能会被一个或多个威胁所利用的资产或一组资产的弱点。
[GB/T 22081-2008，定义2.17]

4 概述

本标准规定了云计算风险评估方法。风险评估需要对云计算关键点包括基础设施、网络、计算资源、存储资源、应用、业务、数据、管理规范、运维运营、风险整合划分等进行识别，并对风险管控措施进行识别，根据风险识别结果估算出风险概率。云计算风险管理流程见图1。

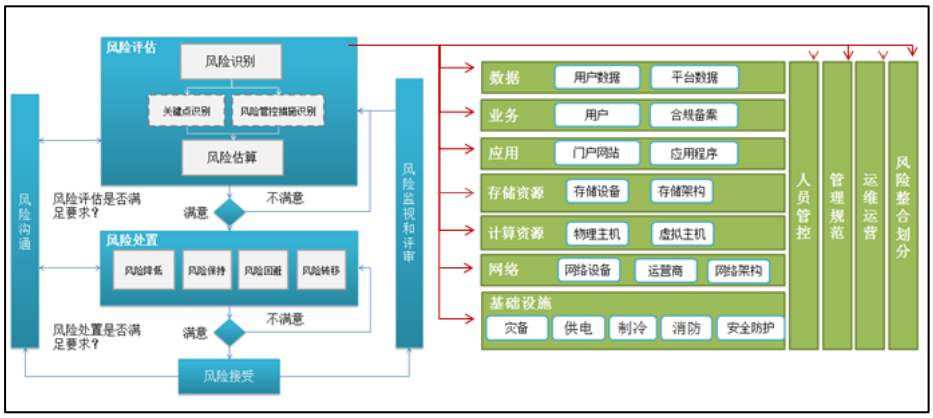

图1 云计算风险管理流程

5 风险评估

5.1 风险识别

风险识别的目的是确定可能发生什么将导致潜在的损失，包括云计算关键点识别、威胁识别、脆弱点识别、风险管控措施识别。

5.1.1 云计算关键点识别

云计算涉及基础设施、网络、计算资源、存储、应用、业务、数据、人员、管理规范、运维运营等多个关键环节，有些属于云计算厂商自身资产，有些涉及第三方合作单位。云计算关键点分类见表1。

表1 云计算关键点

类别	描述
基础设施	数据中心
网络	网络设备、网络运营商、网络架构
计算资源	物理服务器、虚拟主机
存储资源	存储设备、存储架构
应用	云计算门户网站等
业务	云计算
数据	用户数据、系统数据
人员	运维人员
管理规范	运维管理规范、应急事件响应管理规范
运维运营	云计算平台运维
风险整合划分	云计算面临风险的责任划分

云计算关键点应依据在业务价值和可用性上的影响程度进行赋值。云计算关键点的权重见表2。

表2　云计算关键点权重

权重	标识	定义
3	高	非常重要，被破坏后可能对云计算造成非常严重的损失
2	中	比较重要，被破坏后可能对云计算造成中等程度的损失
1	低	不太重要，被破坏后可能对云计算造成较低的损失

5.1.2　云计算威胁识别

威胁是一种对云计算构成潜在破坏的可能性因素，是客观存在的。造成威胁的因素包括环境因素、技术故障和人为因素等。威胁分类见表3。

表3 威胁分类

威胁类型		描述
环境因素		断电、静电、灰尘、潮湿、温度、洪灾、火灾、地震等环境条件和自然灾害
技术故障		硬件故障、云平台软件漏洞
人为因素	外部人员威胁	黑客攻击、系统入侵、未经授权的系统访问、系统篡改、窃取信息
	内部人员威胁	误操作、恶意行为

判断威胁出现的频率是威胁识别的重要工作。威胁频率等级划分为三级，分别代表威胁出现的频率的高低，等级数值越大，威胁出现的频率越高，对云计算关键点的影响越大。威胁发生可能性的权重见表4。

表4 威胁发生可能性

权重	标识	定义
3	高	威胁出现的频率很高，在大多数情况下几乎不可避免或者可以证实经常发生过
2	中	威胁出现的频率中等，在某种情况下可能会发生或被证实曾经发生过
1	低	威胁出现的频率较低，一般不太可能发生，也没有被证实发生过

5.1.3　云计算脆弱性识别

脆弱性是对云计算所依托的一个或多个系统、管理流程的弱点总称。威胁利用云计算的脆弱性才能造成危害，如果没有相应的威胁发生，单纯的脆弱性本身不会对云计算造成损害，如果云计算足够健壮，再严重的威胁也不对云计算造成损失。

脆弱性的识别方法包括问卷调查、工具检测、人工核查、文档查阅、渗透性测试等。

脆弱性的识别按照云计算的关键点进行对应识别，脆弱性与云计算商的风险管控措施相对应，对于风险管理措施强的环节，往往脆弱性较低或者不存在。

5.1.4　风险管理能力识别

云计算商已采取的风险管控措施，包括基础设施风险管控、网络风险管控、计算资源风险管控、存储资源风险管控、应用风险管控、业务风险管控、数据风险管控、人员风险管控、管理流程规范、运维运营、风险整合划分，与云计算关键点一一对应。

控制能力的强弱划分为三级，分别代表抵御威胁的能力高低，等级数值越大，控制能力越强，反之越弱。风险控制能力系数的权重见图5。

表5 风险控制能力系数

权重	标识	定义
3	高	控制能力强，在大多数情况下抵御风险事故
2	中	控制能力中等，在某种情况下可能会发生无法抵御风险的情况
1	低	控制能力弱，一般无法抵御相应风险

5.1.4.1 云计算外部环境风险管理能力

5.1.4.1.1 基础设施风险管理

基础设施风险管理指对云计算所依托数据中心的管理能力,包括是否具备灾备数据中心以及在建筑结构、电力、空调、消防、物理安全等方面的风险管控能力，具体分类如下：

a）灾备数据中心

本指标定义为数据中心机房应具备灾备数据中心；

b）建筑结构

数据中心在建筑设计方面抗击突发事件的能力，包括数据中心抗震设防情况、数据中心耐火等级、数据中心主机房吊挂负载情况、数据中心屋面防水等级、数据中心防静电等级；

c）电力冗余

本指标定义为数据中心抵御电力事故的能力，包括市电供电条件、数据中心电源供电情况、变压器冗余、后备柴油发电机冗余、后备柴油发电机基本容量、柴油发电机燃料存储量、不间断电源系统配置冗余、不间断电源系统电池备用长度等。；

d）空调冗余

本指标定义为数据中心抵御空调风险事故能力，包括机房空调冗余情况，冷水机组、冷冻和冷却水泵冗余情况；

e）消防

本指标定义为数据中心抵御火灾风险事故能力，包括自动灭火系统和火灾报警系统设置情况，灭火设备或系统应使用独立的电源；

f）物理安全

本指标定义为数据中心对人员进出的管理能力，包括出入控制，制定和维护具有机房访问权限的人员名单，及时从授权访问名单中删除不再需要访问机房的人员。

5.1.4.1.2 网络风险管理能力

网络风险管控指对云计算所使用的外部网络以及内部网络的风险管理能力，具体分类如下：

a）外部网络质量控制

本指标定义为云计算厂商应选择网络连通稳定的电信运营商，支持多线BGP；

b）网络冗余

本指标定义为云计算网络层应具备网络设备级冗余、网路链路级冗余和网关级冗余；

c）网络架构

本指标定义为云计算厂商网络支持安全域划分，包括云平台生产域、运维管理域、办公域、DMZ域、Internet域；云平台支持多租户网络隔离。将允许外部公开直接访问的组件，划分在一个与内部网络逻辑隔离的子网络上。并确保允许外部人员访问的组件与允许客户访问的组件在逻辑层面实现严格的网络隔离；

d）访问控制

本指标定义为在不同网络区域边界部署访问控制机制，设置访问控制规则；

e）远程访问控制

本指标定义为云计算厂商能实时监视云计算平台的远程访问，并对远程执行特权命令进行限制；

f）攻击防御

本指标定义为云计算厂商应监测到云平台的网络攻击行为，能记录攻击类型、攻击时间、攻击流量等，并采取相应的防御措施，包括防DDos攻击、防ARP攻击、防CC攻击等；

g）入侵防御

本指标定义为云计算厂商应监测到网络入侵行为，并记录入侵行为的源IP、时间、类型等，并采取相应的防御措施，入侵行为包括端口扫描、木马后门攻击、缓冲区溢出攻击、IP碎片攻击、SQL注入、命令执行、代码注入、XSS跨站攻击、异常文件上传、Webshell和网络蠕虫攻击等；

h）通信线路保护

云计算厂商使用一定的安全防护手段对云计算平台通信线路进行保护。

5.1.4.2 云计算平台风险管理能力

5.1.4.2.1 云计算平台建设风险管理

本指标定义为云计算平台研发或优化过程中，应采取一定措施控制风险，具体分类如下：

a）需求评审

云计算厂商在开发前，应对需求进行评审，控制潜在风险；

b）开发测试

云计算厂商应采取一定措施控制开发过程中的风险。

5.1.4.2.2 计算资源风险管理能力

计算资源风险管理包括宿主机、云主机、中间件的风险管理，具体分类如下：

a）计算资源冗余

本指标定义为计算资源应具备冗余，包括计算资源高可用设计、双机热备等手段；

b）漏洞管理

本指标定义为云计算厂商应具备高危漏洞扫描和修复能力，包括CVE等公共漏洞库公示漏洞、系统软件漏洞以及其它高危漏洞；

c）基线检查

本指标定义为云计算厂商对宿主机、云计算管理平台等，应具备账号安全检查、弱口令检查、配置风险检查、端口状态检查、进程状态检查；

d）病毒管理

本指标定义为云计算厂商应具备病毒检查和查杀能力，包括网站后门、木马等。

5.1.4.2.3 存储资源风险管理能力

本指标定义为云计算厂商应对云计算存储资源具备管理手段措施，具体分类如下：

a）存储设备冗余

本指标定义为云计算厂商存储设备应具备冗余，使用磁盘阵列，并具备分布式存储；

b）数据备份策略

本指标定义为云计算厂商应具备对数据备份和恢复的能力。一方面，云服务商应周期性对云计算平台的备份系统和备份数据进行测试；另一方面，应支持云服务使用者自行备份和恢复数据。

5.1.4.2.4 应用风险管理

本指标定义为云计算厂商应对门户网站以及对外提供的软件服务具备风险管理措施，具体分类如下：

a）web漏洞管理

本指标定义为云计算厂商应具备web漏洞扫描及修复能力，包括注入漏洞、跨站脚本漏洞、失效身份认证和会话管理、不安全的直接对象引用、安全配置错误、敏感信息泄露、缺少功能性的访问控制、跨站请求伪造、含有已知漏洞的组件、未验证的重定向和转发；

b）web防护

本指标定义为云计算厂商应具备web应用防御系统；

c）账号安全

本指标定义为云计算厂商应对用户账号具备安全检查能力，包括弱口令检查、防暴力破解、防恶意注册等。

5.1.4.2.5 数据风险管理能力

本指标定义为云计算厂商对用户数据的风险管控，具体分类如下：

a）数据持久性管理

指标定义为云计算厂商应具备控制手段确保数据不丢失，包括数据备份、数据防篡改；

b）数据可用性管理

本指标定义为云计算厂商应具备控制手段确保数据正常使用；

c）数据私密性管理

本指标定义为云计算厂商对数据的隐私保护能力，包括数据隔离、数据加密。

5.1.4.2.6 运维风险管理能力

本指标定义为云计算厂商运维风险管理措施，具体分类如下：

a）监控能力

本指标定义为云计算厂商应对云平台涉及的各硬件、系统具备监控能力，包括动力环境监控、物理设备监控、网络流量监控、数据库监控、应用层监控；具备可视化的监控平台；

b）告警管理

本指标定义为云计算厂商各管理平台应具备告警管理，包括告警内容管理、故障检测和处理等；

c）权限管理

本指标定义为云计算厂商对运维人员权限的管理，包括账号管理、认证管理、权限管理、审计管理；

d）日志管理

本指标定义为云计算厂商应具备日志记录、日志查看以及日志审计功能，包括用户访问日志、运维人员操作日志、系统日志；

e）资产管理

本指标定义为云计算厂商能够实现对云平台相关的软硬件信息资产进行管理，包括信息收集、资产变更管理以及统计报表；

f）计费管理

本指标定义为云计算厂商应具备准确的计费能力，具体包括计费规则设置、计费项配置等；

g）运维工具管理

云计算厂商应审批、控制并监视信息系统维护工具的使用。

5.1.4.3 云计算管理流程风险管理能力

本指标定义为云计算厂商内部管理流程风险管理能力，具体分类如下：

a）管理制度体系

云计算厂商应针对研发、测试、运维等多个环节制定相关管理制度；

b）事件管理

本指标定义为云计算厂商需要具备事件管理规范，包括事件记录和分类、事件处理、事件关闭、事件总结、突然事件处理机制；

c）问题管理

本指标定义为云计算厂商需要具备问题管理规范，针对云平台薄弱环节具备查明原因，制定解决方案的能力，包括问题确定、问题分析、问题监控、问题处理、问题录入；

d）变更管理

本指标定义为云计算厂商需要具备变更过程管理流程,包括变更分类与记录、变更控制、变更分析、改进措施等；

e）配置管理

本指标定义为云计算厂商应具备云平台各系统配置项管理规范，包括配置项管理和工作程序管理；

f）发布管理

本指标定义为云计算厂商具备规范的流程确保测试的软硬件进入正式运行环境，包括版本测试、版本控制、版本部署及发布等。

5.1.4.4 云计算人员风险管理能力

本指标定义为云计算厂商对内部员工的风险管理措施，具体分类如下：

a）人员背景调查

本指标定义为云计算厂商应对内部员工进行审查；

b）岗位风险管理

云计算厂商应标识出相关岗位的风险；建立上岗人员的筛选准则；按照一定的频率，评审和更新各岗位的风险标识；根据岗位风险，明确并分配所有岗位的信息安全职责，并与客户共同确定涉及云服务的风险责任；

c)人员离职

云计算厂商一旦决定终止某人员的雇佣，应在一定的期限内，禁止该人员对信息系统的访问；终止或撤销与该人员相关的任何身份鉴别物或凭证；与该人员进行离职面谈；收回该人员所有涉及安全的本组织信息系统相关资产；确保之前由该人员控制的信息和信息系统仍然可用；

d）安全培训

本指标定义为云计算厂商应对内部员工定期开展安全培训，包括环境风险、软件漏洞、员工责任意识等；保存人员的培训记录；

e）保密管理

本指标定义为云计算厂商应要求员工签署保密条款。

5.1.4.5 云计算合规风险管理能力

本指标定义为云计算厂商对合规风险的管理能力，具体分类如下：

a）审计

云计算厂商应制定并维护审计记录，如账号登录、账号管理、客体访问、策略变更、特权功能、系统事件等；建立协调机制，与本组织内外需要审计信息的其他组织就安全审计功能进行协调，以增强相互间的支持，协调确定可审计事件清单；制定信息系统内需连续审计的事件清单，并确定各事件的审计频率，该清单为上述可审计事件清单的子集；

b）审计分析

云计算厂商应对审计记录进行审查和分析，以发现不当或异常活动，并向相关人员报告；当法律法规、客户的需求或信息系统面临的威胁环境发生变化时，调整对审计记录进行审查、分析、报告的策略；

c）合规备案审计

本指标定义为云计算厂商应对使用云资源从事经营性的互联网信息服务的用户具备合规备案排查能力。

5.2 风险估算

在完成了云计算关键技术识别、威胁识别、脆弱点、风险管控措施识别后，结合云计算应用价值，将采用适当的方法确定风险事件发生的可能性，综合云服务关键技术权重及威胁发生可能性判风险一旦发生造成的损失，最终得到风险值。

云计算风险值 = 云计算关键点权重×威胁出现概率×风险管控能力系数

注：实际估算过程中，威胁点对于不同云计算差异不大，因此风险估算过程可简化为：

云计算风险值 = 云计算关键点权重×风险管控能力系数。

附 录 A
（资料性附录）
云计算风险管理能力评估指标及权重

表 A.1 风险管理能力评估指标及权重

评估项	权重	评估子项
一、风险管理组织架构		
组织架构合理	1	组织架构合理
制定风险管理策略	1	制定风险管理策略
执行风险管理要求	1	执行风险管理要求
二、云计算外部环境风险管理能力		
灾备数据中心	1	灾备数据中心
建筑结构	1	抗震能力
		耐火能力
		主机房负载
		防水能力
		防静电能力
电力冗余	3	市电供电条件
		电源供电情况
		变压器冗余
		柴油发电机冗余
		后备柴油发电机基本容量
		柴油发电机燃料存储量
		不间断电源系统配置冗余
		不间断电源系统电池备用时长
空调冗余	2	机房空调冗余
		冷水机组、冷冻和冷却水泵冗余
消防	1	自动灭火系统
		火灾报警系统
		独立电源
物理安全	1	出入控制
		视频监控系统
		机械锁安装
		设备访问控制
外部网络质量控制	2	电信运营商网路质量
		支持多线 BGP
网络冗余	1	网络设备冗余
		网络链路级冗余
		网关级冗余
网络架构	1	安全域划分

		租户隔离
		网络拓扑图
访问控制	1	访问控制
远程访问	1	远程访问控制
攻击防范	2	防 DDos 攻击、防 ARP 攻击、防 CC 攻击
入侵防范	1	入侵防御
通信线路保护	1	通信线路保护
三、云计算平台风险管理能力		
3.1 云计算平台建设风险管理		
需求评审	1	需求评审
开发测试	1	开发测试
3.2 计算资源风险管理		
计算资源冗余	2	计算资源冗余
漏洞管理	3	漏洞扫描
		漏洞修复
基线检查	2	基线检查
病毒管理	2	病毒检查
		病毒查杀
3.3 存储资源风险管理		
存储设备冗余	3	存储设备冗余
		异地存储
数据备份策略	2	数据备份方式
3.4 应用风险管理		
Web 型漏洞检测及修复	2	web 漏洞扫描
		web 漏洞修复
Web 防护	2	Web 防护
账号安全	3	弱口令检查
		防暴力破解
		防恶意注册
3.5 数据风险管理		
数据存储持久性	3	数据备份
		数据完整性
数据可用性	3	数据可用性
数据私密性	3	数据加密
3.6 运维风险管理		
监控管理	3	动力环境监控
		物理设备层
		系统层监控
		网络监控
		数据库监控
		云平台监控

		应用层监控
告警管理	1	告警内容管理
		故障检测和处理
权限管理	1	统一账号管理
		身份认证
		权限管理
		审计管理
日志管理	1	用户访问日志
		运维人员操作日志
		系统运行日志
		日志审计
资产管理	1	信息收集
		资产变更管理
		统计报表
计费管理	1	计费规则
		计费配置
运维工具管理	1	运维工具管理
四、云计算人员风险管理能力		
人员背景调查	2	人员背景调查
岗位风险管理	2	岗位风险管理
人员离职	1	人员离职
安全培训	2	安全教育培训
保密管理	1	保密管理
五、云计算管理流程风险管理能力		
管理制度体系	2	管理制度体系
事件管理流程	2	事件记录和分类
		事件处理
		事件关闭
		事故总结
		应急响应
问题管理流程	2	问题确定和记录
		问题分析和转交
		监控问题
		问题处理
		问题录入
变更管理流程	2	变更分类和记录
		变更控制
		变更分析
		改进措施
配置管理流程	1	配置项管理
		工作程序管理

发布管理流程	2	版本测试
		版本控制
		版本部署及发布
六、云计算合规风险管理能力		
审计	2	审计能力
审计分析	2	审计分析
合规备案	2	合规备案
七、风险沟通与监测		
风险告知	2	风险告知
安全责任划分	1	安全责任划分
威胁情报	3	威胁情报能力
持续监测	2	持续监测能力
八、风险处置		
风险处置	2	风险处置

附 录 B
（资料性附录）
风险评估结果

表 B.1 风险管理能力评估指标及权重

风险管理能力等级	分数	风险系数
先进级	95 分以上	0.7
增强级	(90,95]	0.8
增强级	(85,90]	0.9
增强级	(80,85]	1.0
基础级	(75,80]	1.1
基础级	(70,75]	1.2
基础级	(60,70]	1.3
——	60 分以下	--

注：以上风险系数可理解为企业的投保系数，分数越高，风险系数越低，投保保费越低；分数越低，风险系数越高，投保保费越高。

参 考 文 献

[1] GB/T 31167-2014 信息安全技术 云计算服务安全指南
[2] GB/T 31168-2014 信息安全技术 云计算服务安全能力要求
[3] GA/T 1390.2-2017 信息安全技术 网络安全等级保护基本要求 第 2 部分：云计算安全扩展要求
[4] GB/T 22080-2008 信息技术 安全技术 信息安全管理体系要求
[5] GB/T 22081-2008 信息技术 安全技术 信息安全管理实用规则
[6] GB/T 31496-2015 信息技术 安全技术 信息安全管理体系实施指南
[7] JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引
[8] JR/T 0072-2012 金融行业信息系统信息安全等级保护测评指南
[9] JR/T 0073-2012 金融行业信息安全等级保护测评服务安全指引
[10] JR/T 0167-2018 云计算技术金融应用规范 安全技术要求
[11] JR/T 0166-2018 云计算技术金融应用规范 技术架构
[12] JR/T 0168-2018 云计算技术金融应用规范 容灾
[13] ISO/IEC TR 27015:2012 信息技术 安全技术 金融服务信息安全管理指南