ICS 03.060
A 11

JR

中华人民共和国金融行业标准

XX/T XXXXX—XXXX
代替

证券期货业云技术应用安全规范

Specification for information security based on cloud technology of securities and futures industry

点击此处添加与国际标准一致性程度的标识

（送审稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国证券监督管理委员会　　发布

目　　次

前　言

本文件依据GB/T　1.1—2020给出的规则起草。

本文件由全国金融标准化技术委员会证券分技术委员会（SAC/TC　180/SC4）提出。

本文件由全国金融标准化技术委员会（SAC/TC　180）归口。

本文件起草单位：中国证券监督管理委员会科技监管局、中国证券监督管理委员会信息中心、中国证券监督管理委员会证券基金机构监管部、中国证券监督管理委员会期货监管部、深圳证券交易所、中证信息技术服务有限责任公司、中国期货市场监控中心有限责任公司、上海期货交易所、大连商品交易所、郑州商品交易所、中国金融期货交易所、中国证券金融股份有限公司、上交所技术有限责任公司、深圳证券通信有限公司、国泰君安证券股份有限公司、兴业证券股份有限公司、华泰证券股份有限公司、中信证券股份有限公司、国信证券股份有限公司、招商证券股份有限公司、景顺长城基金管理有限公司、华泰期货有限公司。

本文件主要起草人：姚前、张野、刘铁斌、王东明、陈炜、王恺、张靓、林林、孙宏伟、李向东、杨镇、崔慧阳、杨景涛、高心远、王立鹏、冯小根、刘铮、孙增、陈军、江家仁、黄敏强、蔡洪、陈凯辉、王玥、张嵩、李琛、金文佳、林岳、周小琛、孙伟业、甘张生、谢朝海。

引　言

为适应及推进云技术在证券期货业中的应用，特制定本文件，在《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》和《JR/T 0133—2015 证券期货业信息系统托管基本要求》的基础上，基于云计算技术的特点，考虑证券期货机构在云计算技术应用过程中面临的风险，根据各类云服务商、各种服务模式的实际情况，提出了证券期货机构应用云计算技术的安全标准。

在本文件中，**黑体字部分**表示较高等级中增加或增强的要求。

证券期货业云技术应用安全规范

1 范围

本文件提出了证券期货机构在使用云计算技术方面的总体安全原则，规定了证券期货机构在应用云技术过程中规划准备、服务获取、运行监督和服务退出各阶段的安全管理要求。

本文件适用于证券期货机构在公共云、行业云和私有云应用的建立、实施、运行、监视、评审、保持、改进和退出等过程中进行风险识别和风险处置。

国家网络安全监管职能部门及证券期货监管部门依法进行的云安全监督检查可参考使用。

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。

ISO/IEC 20000-1:2018 Information technology – Service management – Part 1: Service management system requirements

ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems - Requirements

GB/T 24405.1-2009 信息技术 服务管理 第1部分 规范

GB/T 22080-2016 信息技术 安全技术 信息安全管理体系要求

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 25069-2010 信息安全技术 术语

GB/T 31167-2014 云计算服务安全指南

JR/T 0060 证券期货业信息系统安全等级保护基本要求（试行）

JR/T 0099-2012 证券期货业信息系统运维管理规范

JR/T 0133-2015 证券期货业信息系统托管基本要求

JR/T 0158-2018 证券期货业数据分类分级指引

3 术语和定义

GB/T 25069-2010、GB/T 31167-2014确定的以及下列术语和定义适用于本文件。

3.1

云计算 cloud computing

通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并按需自助获取和管理资源的模式。

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 31167-2014，定义3.1]

3.2

云服务 cloud service

由云服务商利用云计算平台提供的服务。

3.3

云服务商 cloud service provider

受托方 assignee

云计算服务的供应方。

注：云服务商管理、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。

[GB/T 31167-2014，定义3.3]

3.4

云计算平台 cloud computing platform

由云服务商提供的云计算基础设施及其上服务层软件的集合。

[GB/T 31167-2014，定义3.7]

3.5

云服务客户 cloud service customer

为使用云计算服务同云服务商建立业务关系的参与方。

[GB/T 31167-2014，定义3.4]

3.6

委托方 client

使用云服务的证券期货机构。

3.7

证券期货机构 securities and futures institutions

包括承担证券期货市场公共职能的机构、承担证券期货行业信息技术公共基础设施运营的机构等证券期货市场核心机构及其下属机构，以及证券公司、基金管理公司、期货公司等证券期货经营机构。

3.8

公共云 public cloud

对于云服务商或云服务客户的范围没有限制的云部署模式。

3.9

证券期货行业云 securities and futures community cloud

由中国证券期货行业监管部门认可，云服务商和云服务客户均为证券期货机构的云部署模式。

注：本文件中证券期货行业云简称行业云

3.10

私有云 private cloud

云服务商和云服务客户为同一证券期货机构的云部署模式。

4 总体安全原则

4.1 安全原则

在证券期货业的云计算技术应用中，相关各方应在以下方面确立原则，指导应用过程：

——安全管理责任；

——资源的所有权；

——司法管辖关系；

——安全管理水平；

——审慎采用服务。

4.1.1 安全管理责任

委托方的信息安全管理责任不随服务外包而转移。无论委托方数据和业务是位于内部信息系统还是受托方的云计算平台上，委托方都是信息安全的最终责任人。

4.1.2 资源的所有权

委托方提供给受托方的数据、设备等资源，以及云计算平台上委托方业务系统运行过程中收集、产生、存储的数据和文档等都应属委托方所有，委托方对这些资源的访问、利用、支配等权限不受限制。

4.1.3 司法管辖关系

委托方数据和业务的司法管辖权不因采用云服务而改变。受托方不得将委托方数据及相关信息提供或泄露给未经委托方许可的其他第三方，也不得私自访问、修改、使用委托方数据，明确符合中国法律和司法要求的情形除外。

4.1.4 安全管理水平

承载委托方数据和业务的云计算平台应符合JR/T 0060中相应安全等级的要求，为委托方提供云服务的受托方应符合JR/T 0133-2015。

4.1.5 审慎采用服务

受托方应具备保障委托方数据和业务系统安全的能力，其安全能力应满足受托方要求，并通过委托方及第三方评估机构的安全评估。委托方应选择通过评估的受托方，并监督受托方切实履行安全责任，落实安全管理和防护措施。

4.2 安全过程

证券期货机构应用云计算技术的过程可分为四个阶段：

——规划准备；

——服务获取；

——运行监督；

——服务退出。

4.2.1 规划准备

委托方应基于其系统规划原则，识别云技术应用的安全需求，分析采用云技术产生的风险，制订相应的应对措施，并在系统规划中确保这些风险应对措施被采用，形成安全方案。

4.2.2 服务获取

委托方应根据安全需求和云服务的安全能力选择受托方，与受托方协商合同（或内部协议）、服务水平协议、保密要求等，明确各方享有的权利和应履行的网络安全义务，完成数据和业务向云计算平台的部署或迁移。

4.2.3 运行监督

委托方应定期监督受托方履行合同（或内部协议）约定的责任义务，应督促其业务系统管理者、使用者遵守JR/T 0060、JR/T 0099-2012和JR/T 0133-2015，共同维护数据、业务及云计算环境的安全。

4.2.4 服务退出

委托方应要求受托方履行合同（或内部协议）约定的责任义务，确保退出云服务阶段数据和业务安全，包括提供安全迁移返还委托方数据的能力、彻底清除云计算平台上的委托方数据。

需变更受托方时，委托方应按规划准备阶段和服务获取阶段的要求实施受托方选择，并关注云服务迁移过程的数据和业务安全，委托方应要求原受托方履行合同约定的责任义务。

4.3 主要角色

云服务安全管理的主要角色包括：

——受托方；

——委托方。

4.3.1 受托方责任

受托方承担如下责任：

——通过安全评估；

——持续满足委托方安全要求；

——配合委托方的运行监督工作，对所提供的云服务进行监视；

——合同（或内部协议）关系结束时应满足委托方数据和业务的迁移需求，确保数据安全，数据和业务迁移后，彻底清除委托方各类数据。

4.3.2 委托方责任

委托方承担如下责任：

——部署或迁移到云计算平台上的数据和业务的最终安全责任；

——从已通过安全评估的受托方中选择适合的受托方；

——明确委托方与受托方需要满足的技术与安全要求；

——开展云服务的运行监督活动，根据相关规定开展信息安全检查，确定或认可受托方实施的安全控制措施。

5 规划准备

5.1 识别安全需求

5.1.1 确定安全策略

委托方应确定云计算技术应用的风险接受策略及具体安全要求。

委托方确定安全策略时，应考虑数据、信息系统与云计算平台的安全。

5.1.2 拟定安全级别

委托方应按照GB/T 22240-2020，初步确定拟应用云计算技术的信息系统的网络安全保护等级。

委托方应全面识别应用云计算技术所产生、采集、加工、使用或管理的数据，按照JR/T 0158-2018进行分类分级，并实施相应保护。

5.1.3 制定安全需求

在规划准备阶段，委托方应制定明确的应用云计算技术的信息安全需求：

——信息安全需求应包括数据安全需求、信息系统安全需求与对云计算平台的安全需求；

——信息安全需求应覆盖云计算技术的基础设施、网络通信、安全保卫、基础资源、应用系统、运

维保障、审计、安全组织与人员、风险管理、供应链等方面内容。

5.2 明确安全目标

5.2.1 确定应用范围

委托方应确定与其机构目标相关并影响云计算技术应用的外部和内部信息。

委托方应理解云计算技术相关方的需求和期望，确定与云计算技术有关的相关方以及这些相关方与信息安全有关的要求。

注：相关方的要求可能包括法律法规要求和合同义务。

委托方应确定云计算技术的应用范围边界和适用性，以明确其应用范围。

委托方应确定其所在机构执行的业务活动之间及与其他机构的业务活动之间的接口与依赖性。

5.2.2 提出安全目标

委托方应确定其所在机构云计算技术应用的信息安全目标。云计算技术应用的信息安全目标应满足以下几项基本要求：

——符合本机构的业务目标；

——符合本机构的信息安全目标；

——包含满足适用的安全要求的承诺；

——包含云计算技术应用的持续改进的承诺；

——满足证券期货行业信息技术相关监管规定。

委托方应基于系统的信息安全保护等级和数据的分类分级，综合平衡应用云计算技术后的效益和风险，确定拟部署或迁移到云计算平台上的数据和系统。

5.3 建立安全方案

5.3.1 制定过程

委托方应根据云计算技术应用的信息安全目标，制定云计算安全方案。云计算安全方案应遵循机构建立的业务策略和安全策略。

委托方应组织各相关方对云计算安全方案及相关配套文件的合理性和正确性进行论证和审定，委托方应保存云计算安全方案评审记录，详细记录相关人员的评审意见。云计算安全方案应经过委托方的信息技术管理者与信息安全管理者批准后实施。

5.3.2 内容要求

云计算安全方案应提供符合策略的、覆盖整个机构的云计算安全构建和维护机制。

云计算安全方案应明确一个详细的云计算安全过程和规程，应要求机构内不同业务职能角色进行合作，包括但不限于信息技术、审计、风险管理、负责法律法规符合性的各相关方。

云计算安全方案的内容应包括但不限于以下几个方面内容：

——描述拟采用云服务的信息和业务；

——基于拟部署或迁移到云计算平台上的数据和系统的安全保护等级，确定其云服务安全需求；

——对云部署模式、云服务模式和数据存储位置的要求；

——对业务连续性的要求，对灾备恢复能力、应急响应时间的要求；

——对云平台故障的处置方案；

——对受托方需要提供的资源配置的要求；

——根据云服务安全需求及采用的云服务模式，明确系统自身应采取的安全措施；

——分析系统在服务模式、扩展性、可用性及可移植性等方面的要求，结合云计算平台在这些方面能够提供的服务，确认适合系统的架构及设计；
——系统运维、监控、审计对于云计算平台的要求；
——退出云服务或变更受托方的初步方案；
——对相关方人员进行安全意识、技术和管理培训的方案；
——本单位负责采用云服务的领导、工作机构及其责任。

6 服务获取

6.1 服务获取通用要求

委托方在获取云服务时，应当明确要使用的部署模式。

委托方选择云计算平台时，应要求云计算平台及其所有组成部分的网络安全保护等级不低于拟放置在云计算平台上的系统的网络安全保护等级。

委托方选择受托方时，应确保受托方满足云计算安全方案的要求。

委托方选择受托方时，应考虑但不限于以下服务能力：
——受托方提供的部署模式应满足要求；
——受托方提供的数据存储位置应满足要求；
——受托方应向委托方提供云服务相关技术接口和文档；
——云计算平台系统的连续性、灾备恢复能力和应急响应时间应满足要求；
——云计算平台的可扩展性、可用性、可移植性、互操作性，且其功能、容量、性能应满足要求；
——资源的占用、带宽的租用、监管、迁移或退出服务、培训等费用的计费方式和标准应满足要求；
——受托方提供多种可选的网络、安全、监控、审计等产品，并开放相关接口；
——出现安全事件并造成损失时，依据合同的规定，受托方应能承担相关责任并进行赔偿。

6.2 私有云服务获取

委托方的私有云服务获取过程，应根据私有云承载的业务系统的网络安全保护等级（已确定或初步确定的），按照JR/T 0060进行安全方案设计、产品采购和使用、软件开发、工程实施、测试验收等。

委托方应全面识别在私有云上产生、采集、加工、使用或管理的数据，按照JR/T 0158-2018进行分类分级，并实施数据加密、备份等保护措施。

使用私有云时，委托方应确保其符合对应的网络安全等级保护要求。

6.3 行业云服务获取

委托方在行业云服务获取过程中应考虑以下方面安全要求：
——托管安全；
——服务合同；
——服务水平协议；
——保密协议。

6.3.1 托管安全要求

委托方应选择设立在中国人民共和国境内的受托方。

委托方应根据云计算应用的信息安全目标，每年评估受托方提供的云服务，并督促受托方进行相应整改，当受托方提供的云服务严重违反云服务安全要求时，应及时更换受托方。

委托方应对部署在云计算平台上的数据和系统进行确认。

委托方应对受托方开展信息安全评估，受托方应提供其云服务平台通过相应级别的测评的证据，受托方云计算平台及其所有组成部分应符合JR/T 0060中的第三级或以上安全要求。

受托方应设立信息安全管理职能部门，在开展托管业务两年内宜通过信息安全管理体系认证（如GB/T 22080或ISO/IEC 27001的最新版本）和IT服务管理体系认证（如GB/T 24405.1或ISO/IEC 20000-1的最新版本）。

6.3.2 服务合同

委托方应与受托方签订合同，合同应确认委托方使用云服务的业务用途，合同应明确提出信息安全相关条款。

委托方应确定受托方的职责。在合同中应明确受托方承担以下责任和义务：

——承载委托方的数据和业务的云计算平台须满足委托方的信息安全管理要求；

——委托方提供给受托方的数据、设备、系统等资源，以及云计算平台上委托方业务系统运行过程中收集、产生、存储的数据和文档等属于委托方所有，受托方应保证委托方对这些资源的访问、利用、支配等权利；

——受托方应保证前述资源、系统、数据等项的安全；

——受托方不得将委托方数据及相关信息提供或泄漏给未经许可的其他第三方，明确符合中国法律和司法要求的情形除外；

——受托方应接受委托方相关监管部门对其的信息安全监管，应接受委托方相关监管部门的信息安全延伸检查。

合同应对特殊情况进行约定，包括：

——受托方需配合做好委托方数据和业务的迁移和退出；

——约定合同终止的条件及合同终止后受托方应履行的责任和义务；

——当发生安全事件并造成损失时的责任划分和赔偿措施；

——发生纠纷时，受托方应保持服务的安全水平不低于合同和服务水平协议中的约定。

6.3.3 服务水平协议

委托方应与受托方协商服务水平，并签订服务水平协议。服务水平协议应全面考虑云服务的整个生命周期中可能面临的安全风险，并进行约定。

委托方与受托方签订的服务水平协议，应作为合同附件。

服务水平协议应包括但不限于如下内容：

——明确服务的范围、术语定义、服务类型、服务内容和服务形式，服务的可用性、连续性技术指标等；

——明确受托方云计算系统宜遵从的技术和管理标准、相关制度和规定，并通过独立第三方的信息安全管理体系认证（如GB/T 22080或ISO/IEC 27001的最新版本）和IT服务管理体系认证（如GB/T 24405.1或ISO/IEC 20000-1的最新版本），以及通过不低于等级保护三级的测评认证；

——根据云计算平台拟承载的系统及业务，确定云服务的业务连续性要求；

——若云服务发生信息安全事件或重大威胁时，应及时通知委托方，并积极配合委托方共同开展应急处置工作；

——受托方应配合委托方参与证券期货业应急演练；

——服务水平协议应考虑到服务变更或终止的情况：变更或终止服务时，变更或终止服务的发起方应提前通知对方，对方应做好相应准备。受托方应协助委托方收回所有数据，并保证系统中全

部相关数据被安全删除，并不可恢复。

6.3.4 保密协议

委托方应与受托方签订保密协议。

保密协议应有明确的有效周期。

6.4 公共云服务获取

委托方在公共云服务获取过程中应考虑以下方面安全要求：

——托管安全；

——服务合同；

——服务水平协议；

——保密协议。

6.4.1 托管安全要求

委托方应选择设立在中国人民共和国境内的受托方。

委托方应每年按照已确定的云服务安全要求评估受托方提供的云服务，并督促受托方进行相应整改，当受托方提供的云服务严重违反云服务安全要求时，应及时更换受托方。

委托方应对部署在云计算平台上的数据和系统进行确认。

委托方应对受托方开展信息安全评估，受托方应提供其云服务平台通过相应级别的测评的证据，受托方云计算平台及其所有组成部分应符合JR/T 0060中的第三级或以上安全要求。

受托方应设立信息安全管理职能部门，在开展托管业务两年内宜通过信息安全管理体系认证（如GB/T 22080或ISO/IEC 27001的最新版本）和IT服务管理体系认证（如GB/T 24405或ISO/IEC 20000的最新版本）。

6.4.2 服务合同

委托方应与受托方签订合同，合同应确认委托方使用云服务的业务用途，合同应明确提出信息安全相关条款。

委托方应确定受托方的职责。在合同中应明确受托方承担以下责任和义务：

——承载委托方的数据和业务的云计算平台须满足委托方的信息安全管理要求；

——委托方提供给受托方的数据、设备、系统等资源，以及云计算平台上委托方业务系统运行过程中收集、产生、存储的数据和文档等属于委托方所有，受托方应保证委托方对这些资源的访问、利用、支配等权利；

——受托方应保证前述资源、系统、数据等项的安全；

——受托方不得将委托方数据及相关信息提供或泄漏给未经许可的其他第三方，明确符合中国法律和司法要求的情形除外；

——受托方应接受委托方相关监管部门对其的信息安全监管，应接受委托方相关监管部门的信息安全延伸检查。

合同应对特殊情况进行约定，包括：

——受托方需配合做好委托方数据和业务的迁移和退出；

——约定合同终止的条件及合同终止后受托方应履行的责任和义务；

——当发生安全事件并造成损失时的责任划分和赔偿措施；

——发生纠纷时，受托方应保持服务的安全水平不低于合同和服务水平协议中的约定。

6.4.3 服务水平协议

委托方应与受托方协商服务水平，并签订服务水平协议。服务水平协议应全面考虑云服务的整个生命周期中可能面临的安全风险，并进行约定。

委托方与受托方签订的服务水平协议，应作为合同附件。

服务水平协议应包括但不限于如下内容：

——明确服务的范围、术语定义、服务类型、服务内容和服务形式，服务的可用性、连续性技术指标等；

——明确受托方云计算系统宜遵从的技术和管理标准、相关制度和规定，并通过独立第三方的信息安全管理体系认证（如 GB/T 22080 或 ISO/IEC 27001 的最新版本）和 IT 服务管理体系认证（如 GB/T 24405.1 或 ISO/IEC 20000 的最新版本），以及通过不低于等级保护三级的测评认证；

——应云计算平台拟承载的系统及业务，确定云服务的业务连续性要求；

——若云服务发生信息安全事件或重大威胁时，应及时通知委托方，并积极配合委托方共同开展应急处置工作；

——受托方应配合委托方参与证券期货业应急演练。

服务水平协议应考虑到服务变更或终止的情况：变更或终止服务时，变更或终止服务的发起方应提前通知对方，对方应做好相应准备。受托方应协助委托方收回所有数据，并保证系统中全部相关数据被安全删除，并不可恢复。

6.4.4 保密协议

委托方应与受托方签订保密协议。

保密协议应有明确的有效周期。

7 运行监督

7.1 运行监督通用要求

委托方应实施对受托方和自身的运行管理。受托方应保证安全能力持续符合要求，并积极配合委托方的监督管理。

在采用云服务时，委托方将部分控制和管理任务转移给受托方，但最终安全责任由委托方自身承担。委托方应加强对受托方的运行管理，同时应对自身的云服务使用、管理和技术措施进行有效管理。

7.2 私有云运行监督

私有云应符合JR/T 0060中的第二级或以上安全要求。

私有云不应承载高于其安全保护等级的业务应用系统。

私有云的运行应符合JR/T 0099-2012要求。

7.3 行业云运行监督

委托方应对行业云实施运行监督。

行业云应符合JR/T 0060中的第三级或以上安全要求。

行业云的运行应符合JR/T 0099-2012要求。受托方应依照委托方要求，向委托方提供其符合JR/T 0060及JR/T 0099-2012的必要证据。

受托方应开展周期性的风险评估和监测，保证安全能力持续符合委托方的要求。

受托方未经委托方许可，不得将云服务再进行外包、转包、分包。
受托方应及时响应证券期货行业监管部门或委托方的安全预警通知，按照其要求进行有效的处置。
受托方应及时向委托方通知其发现的委托方安全风险。
行业云应参与证券期货业信息安全联合应急演练。

7.4 公共云运行监督

委托方应对公共云实施运行监督。
公共云应符合JR/T 0060中的第三级或以上安全要求。

7.4.1 运行监督内容

公共云的运行监督，应包含如下内容：
——确保委托方在合同中规定的责任义务和相关政策规定能得到落实，技术标准能得到有效实施；
——确保委托方的服务水平、资源保障能达到合同要求；
——确保委托方的数据安全和服务连续性能达到合同要求；
——确保委托方能及时有效地响应处置突发事件；
——确保委托方能根据业务发展需要或者信息安全事件进行信息安全保障工作的持续改进。

7.4.2 委托方应实施的行为

——委托方在公共云运行管理活动中，应实施如下行为：监督受托方履行合同规定的各项责任和义务；
——对云服务运行风险进行识别、评估和风险提示；
——监督、评价云服务运行管理工作，定期对受托方进行安全检查，督促持续改善；
——对受托方的变更服务内容进行评估并控制；
——制定、实施云服务使用策略、制度与流程；
——制定云服务应急管理方案，定期组织演练；
——在云外保存其业务数据的备份；
——将云服务相关内容纳入信息安全教育培训体系；
——对云服务使用过程进行监控和分析；
——如受托方不能满足委托方的信息安全目标，委托方应选择退出服务或变更受托方。

7.4.3 受托方应实施的行为

受托方在公共云运行管理活动中，应实施如下行为：
——履行合同规定的各项责任和义务；
——通过网络安全等级保护测评；
——按合同要求配合委托方开展的各项安全检查，并按要求整改完善；
——开展周期性的风险评估和监测，保证安全能力持续符合委托方的要求；
——按照合同要求或双方的约定，向委托方提供支持，配合委托方的监督管理；
——受托方未经委托方许可，不得将云服务再进行外包、转包、分包；
——应及时响应证券期货行业监管部门或委托方的安全预警通知，按照其要求进行有效的处置；
——及时向委托方通知其发现的委托方安全风险；
——保持受托信息系统的信息安全保护等级和其他安全保护策略不变；
——保持不同委托方之间的有效隔离；
——确保满足云服务的业务连续性要求；

——对重大变更进行信息安全风险评估，并及时告知委托方；
——出现突发事件及时向委托方报告事件及处置情况；
——对雇员进行背景审查；
——建立完善的内部控制机制，确保雇员和供应商遵守管理要求及流程，有效管理操作风险。

8 服务退出

8.1 服务退出通用要求

服务退出的过程中，委托方对业务的以下要求应得到满足：
——可用性；
——可持续性；
——可移植性；
——可迁移性。

8.1.1 退出过程

委托方退出云服务，或将数据和业务系统迁移至其他云计算平台时，应实施以下行为：
——依据约定的退出条件以及退出时委托方、受托方的责任和义务，与受托方确定数据和业务系统迁移出云计算平台的接口与方案；
——要求受托方完整返还委托方数据及相关文档；
——完成退出后，及时取消受托方对委托方资源的物理及电子访问权限；
——提醒受托方在委托方退出云服务后仍应承担的责任和义务；
——确保受托方按要求彻底清除数据。
委托方如需变更受托方，应在完成新受托方规划、选择、迁移后，再退出原有服务。

8.1.2 数据范围

委托方应识别并明确从云计算平台迁移出的数据范围，包括但不限于：
——委托方移交给受托方的数据和资料；
——委托方业务系统在云计算平台上运行期间产生、收集的数据及相关文档资料，如数据文件、程序代码、说明书、技术资料、运行日志；
——其他委托方应迁移出的数据。

8.1.3 建立数据清单

委托方应明确需迁移的数据的标识、描述、格式和介质，制定详细的移交数据清单，并评审及批准该数据清单的适用性和充分性。
委托方应评审及批准数据清单的适用性和充分性。
数据清单的内容应包括但不限于：
——数据文件。数据文件应标明：文件名称、数据文件内容的描述、存储格式、文件大小、类型（敏感或公开）等。应要求受托方提供解密方法和密钥，实现加密文件的移交；提供技术资料或转换工具，实现非通用格式文件的提交；
——程序代码。针对委托方定制的功能或业务系统，在合同或其他协议中明确是否移交可执行程序、源代码及技术资料，可能涉及的内容包括：可执行程序、源代码、功能描述、设计文档、开发及运行环境描述、维护手册、用户使用手册等（受托方云计算平台、服务等基础设施资源等自

身使用代码除外）；

——其他数据。根据事先的约定和双方协商，确定应移交的其他数据，包括委托方业务运行期间收集、统计的相关数据，如云服务的委托方行为习惯统计、网络流量统计等；

——文档资料。委托方使用云服务过程中提供给受托方的各种文档资料，及双方共同完成的涉及委托方的相关资料。

8.2 私有云服务退出

8.2.1 安全删除数据

退出私有云服务时，应根据数据等级制定信息资产的转移、暂存、清除的方法和过程。

应记录信息转移、暂存和清除的过程，包括参与的人员、转移、暂存和清除的方式以及目前信息所处的位置等。

8.2.2 设备迁移和废弃

应根据要终止的云计算平台，识别要被迁移或废弃的硬件设备、所处的位置以及当前状态等，列出需迁移、废弃的设备的清单。

应根据规定和实际情况制定设备处理方案，包括重用设备、废弃设备、敏感信息的清除方法等。

应根据设备处理方案对设备进行处理，记录设备处理过程，包括参与的人员、处理的方式、是否有残余信息的检查结果等。

8.3 行业云服务退出

8.3.1 验证数据

委托方应监督迁移数据的过程，并采取以下措施对迁移数据实施验证：

——对加密数据进行解密并验证；

——利用工具恢复专有格式数据并验证；

——通过业务系统验证数据的有效性和完整性。

8.3.2 安全删除数据

委托方退出云服务后，应要求受托方安全处理委托方数据，承担相关责任和义务。委托方应要求受托方至少采取以下措施安全处置存放委托方数据的存储介质：

——进行介质清理，确保原信息不可被恢复，介质清理应在重用前完成；

——不可清理的介质应物理销毁；

——存放敏感信息的介质清理后不能用于存放公开信息；

——记录介质清理过程，并对过程进行监督。

8.4 公共云服务退出

8.4.1 验证数据

委托方应监督迁移数据的过程，并采取以下措施对迁移数据实施验证：

——对加密数据进行解密并验证；

——利用工具恢复专有格式数据并验证；

——通过业务系统验证数据的有效性和完整性。

8.4.2 安全删除数据

委托方退出云服务后，应要求受托方安全处理委托方数据，承担相关责任和义务。委托方应要求受托方至少采取以下措施安全处置存放委托方数据的存储介质：

——进行介质清理，确保原信息不可被恢复，介质清理应在重用前完成；

——不可清理的介质应物理销毁；

——存放敏感信息的介质清理后不能用于存放公开信息；

——记录介质清理过程，并对过程进行监督。

参 考 文 献

[1] GB/T 31167-2014 信息安全技术 云计算安全服务指南

[2] JR/T 0133-2015 证券期货业信息系统托管基本要求

[3] ISO/IEC 27001-2013 信息安全管理体系要求（Information technology–Security techniques–Information security management systems–Requirements）

[4] ISO/IEC 27002-2013 信息技术 安全性技术 信息安全控制实施规程（Information technology –Security techniques–Code of practice for information security controls）

[5] ISO/IEC 27017-2015 Information technology -Security techniques-Code of practice for information security controls（Information technology–Security techniques–Code of practice for information security controls based on ISO/IEC 27002 for cloud services）

[6] ISO/IEC 27018-2014 信息技术 安全技术 代码的做法在公共云保护个人可识别信息（PII）的作为PII处理器（Information technology–Security techniques–Code of practice for protection of personally identifiable information(PII) in public clouds acting as PII processors）

[7] CSA 0001-2016 云计算安全技术要求（Cloud Computing Security Technology Requirements (CSTR)）