ICS 03.060
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0233—2021

证券期货业经营机构内部应用系统日志规范

Specification for internal application system log in securities and futures industry operating institutions

2021－11－02 发布　　2021－11－02 实施

中国证券监督管理委员会　发布

目　　次

前　言

本文件按照GB/T　1.1-2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

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/TC180/SC4）提出。

本文件由全国金融标准化技术委员会（SAC/TC180）归口。

本文件起草单位：中国证券监督管理委员会、中证信息技术服务有限责任公司、海通证券股份有限公司、东方证券资产管理有限公司、国泰君安证券股份有限公司、兴业证券股份有限公司、华泰期货有限公司、恒生电子有限公司、汇添富基金管理股份有限公司、嘉实基金管理有限公司、国信证券股份有限公司。

本文件主要起草人：姚前、蒋东兴、周云晖、陆骋、金星、周思宇、王恺、周皓、张喆、李震、李向东、王洪涛、熊友根、周靖、牟大恩、李云亮、陈雄、曾宏祥、陈君、刘斌、洪伟、郑鸿鹏、胡卫宁、钱敏、彭志刚、翁建平、刘浩、骆跃芳、向宁宁、任猛、刘汉西、刘政。

引　言

日志用来记录用户操作、系统运行状态、业务逻辑执行情况等，是一个系统的重要组成部分。目前证券期货行业机构的信息系统在日志管理和使用方面缺少规范性文件，有不少行业机构的信息系统日志存在日志内容无效、日志格式及日志级别随意、日志存在信息安全问题、日志存储方式杂乱等问题，同时缺乏相应的日志监控及报警措施等。鉴于行业机构信息系统的日志存在诸多问题，因此有必要通过本文件来规范行业机构对信息系统日志的管理和使用，督促行业机构解决当前信息系统日志管理和使用存在的问题。

证券期货业经营机构内部应用系统日志规范

1 范围

本文件规定了证券期货业经营机构内部应用系统日志基本要求、日志管理、日志记录、日志存储、日志采集、日志监控、日志审计和日志销毁相关要求。

本文件适用于证券期货业经营机构（以下简称经营机构）应用系统相关日志的管理。

注1：经营机构，如证券公司、期货公司、公募基金管理人（包括公募基金公司和取得公募基金资格的资产管理机构）等；

注2：服务机构，例如软件开发商、信息商、服务商等。

注3：服务机构在开展涉及证券期货业相关应用系统服务和技术服务时适用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 22239—2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 34960.5—2018 信息技术服务 治理 第5部分：数据治理规范

GB/T 36626—2018 信息安全技术 信息系统安全运维管理指南

JR/T 0099—2012 证券期货业信息系统运维管理规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

应用系统 application system

由应用软件、系统软件、网络设备、安全设备以及应用软件所依赖的软件包构成的软、硬件资源的统称。

3.2

日志 log

计算机系统、设备、软件等在某种情况下按时间记录的有序数据集合。

3.3

日志采集 log collection

从信息使用者的需要出发，通过各种渠道和形式获取日志（3.2）相关信息的过程。

3.4

日志转储 log dump

将日志（3.2）内容转换为另外一种更具可读性的方式。

3.5

敏感信息 sensitive information

在金融行业包括用户的个人信息以及交易相关的信息等。

注：这类数据涉及到用户的隐私数据以及如用户手机号、身份证号、银行卡号、密码、交易标的代码、名称、价格、数量等。

3.6

响应码 response code

每类请求处理结果的状态码。

3.7

日志代理 log agent

完成日志采集并向日志管理中心（3.8）发送采集到的日志数据的功能组件。

注：日志代理包括软件代理和硬件代理。

3.8

日志管理中心 log administration center

由软件和硬件构成的对日志数据进行采集、集中存储、分析、查询、监控等处理的统一服务平台的统称。

4 基本要求

4.1 日志记录设计要求

在应用系统规划和设计前期，应根据系统具体的业务场景规划完善的日志记录方案，日志记录设计基本要求如下：

a) 从数据保护的角度出发，根据 IT 系统承载的业务数据设置合理的日志记录要求，包括但不限于以下内容：
   1) 完整：在保障业务系统稳定运行的前提下，日志记录应完整；
   2) 安全：日志记录中对于敏感信息应做脱敏处理或通过适当访问权限控制，避免因日志分析导致业务敏感数据泄密；
   3) 可读：日志中不应记录无意义信息，防止无意义的日志淹没重要的信息；
   4) 可解析：日志记录应易于解析；
   5) 分类：日志应分类分级分别记录；
   6) 时效性：日志应被实时、有序记录，记录应及时；
b) 日志格式要求：
   1) 通用：应满足通用的格式要求，以便与日志管理中心和第三方日志管理平台进行对接；
   2) 统一：日志格式应保持统一，日志信息应准确、完整和可靠；
c) 除了日志记录自身要求之外，经营机构还应符合本文件要求制定合理的日志数据全生命周期管理细则，涵盖日志记录、采集、转储、存储、备份、传输、使用、销毁等过程。

4.2 日志记录内容要求

记录必要的程序执行过程和状态，以便于问题跟踪和排查、系统监控、流程恢复及数据分析参考等。由于业务场景不同，日志记录会有所不同，日志记录基本内容要求如下：

a) 支持系统运维：
   1) 监控告警：应反映系统运行状态；
   2) 问题定位：为快速、准确地定位线上问题提供足够数据支撑；

3) 容量预警：反映系统性能瓶颈，预警系统潜在风险，为优化系统性能、或者根据日志信息调整系统行为等提供数据支撑；

b) 为业务流程回放、恢复等提供数据支撑；

c) 日志应当满足内部和外部各类审计的需要：

1) 反映出安全攻击行为，如登录错误、异常访问、恶意攻击等；

2) 反映关于网络中所发生的事件信息，如软件和硬件性能信息、故障检测和入侵检测信息等；

d) 为提升系统业务价值和运营效果等业务提供数据支撑。

5 日志管理

5.1 日志管理组织

经营机构宜设立日志管理组织，具体包括：

a) 经营机构宜设立日志管理的组织，通常由技术运维团队或系统运行团队承担，负责日志相关的管理和使用工作；

b) 经营机构宜设定日志管理负责人，依据 GB/T 36626—2018 中 6.1.4 的内容由技术运团队负责人或系统运行团队负责人承担，负责组织、协调、管理日志的管理和运维工作，以及在系统建设时日志需求规划制定及日志验收工作；

c) 经营机构宜设置合理的日志管理和运维岗位，规定岗位职责及技能要求；

d) 经营机构宜配备一定数量的日志管理和运维人员。日志管理和运维人员宜具备一定的计算机基础理论知识和专业技术经验；

e) 经营机构宜与日志管理和运维人员签署保密协议，保密协议宜至少包括保密范围、保密期限等内容；

f) 经营机构宜制定年度培训计划，对日志管理和运维人员进行必要的技术、业务、安全等培训，并留存培训记录。

5.2 制度管理

经营机构应制定覆盖日志管理工作各个环节的、体系化的日志管理制度和操作流程，具体内容：

a) 经营机构应制定涵盖日志记录、转储、存储、备份、传输、使用、销毁等各项工作的管理制度和操作流程，并将本文件的要求在研发、运维、项目管理等相关制度和流程中体现，明确：

1) 日志管理的具体要求；

2) 日志管理工作中涉及的角色和职责；

3) 日志管理的相关制度和操作流程的制定、发布、维护、更新的机制；

b) 经营机构应至少每年一次评审、修订日志管理制度和操作流程；

c) 证券期货机构应明确责任人，对日志存储介质的使用、转储、送修、销毁及存储环境进行管理。

5.3 环境管理

除应用系统自身开启日志功能之外，应用系统所依赖的软件和硬件环境也应为应用系统日志的生成提供足够的条件，同时也应开启相关的日志功能，具体要求如下：

a) 应用服务器应有足够的磁盘空间，日志输出路径应对应服务器较大空闲空间的盘符，并且在服务器重启时不会丢失数据；

b) 应用系统所依赖的网络设备、安全设备、操作系统、数据库系统、中间件等应开启日志功能；

c) 应用服务器应设置一定的访问和隔离权限，防止非授权用户修改日志信息；

d) 应在不影响应用系统正常运行的前提下，部署合理的应用系统运行环境统计服务程序，周期性收集系统运行数据，包括CPU、内存和磁盘等使用情况以及核心进程的CPU、内存、磁盘和网络使用情况，并有适当的自动化的阈值监控和告警机制，管理人员应定期查看系统负荷和性能峰值；
e) 应用服务器时钟信息应与证券期货机构的时钟同步服务器同步，运维人员应定期检查时间同步情况并予以记录。

6 日志记录

6.1 对应用系统最小影响要求

日志记录涉及I/O读写操作，会对应用性能有一定的影响，因此日志记录尽可能将对应用系统的影响降至最小：

a) 应不影响应用系统、程序的正常运行；
b) 应设置默认的、合理的日志记录级别；
c) 应简明扼要地记录日志内容；
d) 对于高频重复出现的日志，应控制合理的日志记录频率，例如当同类型的日志出现一定阀值时才记录一次。

6.2 可读性要求

可读性要求如下：

a) 日志记录应易于阅读和解析；
b) 日志记录格式应统一和固定，可使用JSON格式、键值对格式，或以易于与日志内容本身区分的分隔符分隔的字符串组成，不宜使用二进制格式记录，通讯协议报文本身应为二进制格式除外；
c) 日志记录应采用统一的字符集编码，建议使用“UTF-8”格式；
d) 应将应用系统运行日志、业务日志、统计日志、审计日志等分别独立记录，分别存储；
e) 应为不同的日志类型添加业务标签，以便快速查找相同类型日志，宜使用字母与数字的组合字符串表示，字母表示业务属性，数字表示该业务下的日志类型编码；
f) 对于包含客户交易流水等敏感信息的交易日志，应做脱敏处理或与其他业务日志分开存储，并通过一定的访问权限控制以满足数据安全的要求。

6.3 完整性要求

日志完整性要求如下：

a) 每条日志应独立成行，一条完整日志不应使用换行符进行跨行记录；
b) 单行日志长度建议不超过4KB，若单行长度超过4KB及以上，建议仅记录该行日志核心要素，避免记录过多无效内容导致日志质量下降；
c) 在多线程场景，任意一条日志不应被截断、覆盖或丢失；
d) 应完整记录异常情况发生前、中、后关联的日志信息；
e) 对于反映访问链路和用户访问轨迹的日志，日志记录应可追踪；
f) 日志记录应支持多线程记录，且多线程之间的日志记录不应产生冲突；
g) 在分布式存储、数据备份、数据采集等操作时应满足数据完备的要求。

6.4 一致性要求

日志一致性要求如下：

a) 同一应用系统日志文件命名格式和风格应保持一致；
b) 同一应用系统日志字段命名格式和风格应保持一致；
c) 同一应用系统同一业务类型日志级别应保持一致；
d) 在数据备份、数据采集等操作时应验证数据与日志源数据一致。

6.5 安全性要求

证券期货机构应在日志全生命周期满足日志安全记录、安全传输、安全访问、安全存储等要求。日志访问、存储和传输应遵循GB/T 36626—2018、GB/T 22239—2008和JR/T 0099—2012中关于安全规定的相关要求。

6.6 监控要求

日志监控要求如下：

a) 监控程序不应对日志文件的独占访问；
b) 应合理设置日志监控指标，可根据实际需要对日志的内容、格式、日志文件的大小、日志文件的更新时间等方面进行必要监控；
c) 应及时监控日志的记录情况，验证日志记录的时效性、完整性和可靠性。

6.7 记录时机

宜记录日志与不宜记录日志时机如下。

a) 在以下场景宜记录日志：
   1) 应用系统软件启动及退出时，宜在日志中记录软件的启动和退出过程；
   2) 应用系统重要的启动配置；
   3) 应用系统所有的错误信息；
   4) 应用系统所有的警告信息；
   5) 应用系统捕获到异常时，宜记录易于定位异常的有效信息，如异常发生的上下文，异常发生的位置，具体异常信息等；
   6) 接口调用较长时间等待时；
   7) 重要的业务状态变化；
   8) 定时任务启动和执行情况；
   9) 重要的逻辑分支和导向分支的执行条件；
   10) 客户端访问日志；
   11) 记录系统各主要模块之间的请求和响应；
   12) 业务流程与预期不符；
   13) 系统核心角色和组件关键动作；
   14) 耗时程序的执行进度；
   15) 应用程序操作数据库的 SQL 语句；
b) 在以下场景不宜记录日志：
   1) 函数入口。函数入口表示一个重要事件的开始或是日志处于调试级别除外；
   2) 循环体。避免在循环体多次迭代中记录日志。若需要记录日志，则应设置达到合理的迭代次数之后再输出一次日志；
   3) 大消息或是大文件的内容；

4) 对于高频率出现的正常日志，宜采用日志记数方法，设置达到合理的次数之后再输出一次日志。

6.8 日志分类

6.8.1 类别及基本内容

日志类别及基本内容如下。

a) 根据应用系统自身及其依赖的软件和硬件环境，应用系统的日志分类包括：操作系统日志、数据库日志、网络设备日志、信息安全设备日志、第三方库和应用框架日志和应用系统自身日志。

b) 每一类日志记录中都应记录以下基本内容：
   1) 事件发生的日期和时间；
   2) 事件发生的服务器信息，如机器 IP；
   3) 事件定位信息，如事件发生的完整路径信息；
   4) 事件描述；
   5) 操作者信息（如有）；
   6) 操作结果状态（如有）。

6.8.2 操作系统日志

操作系统日志除应记录基本内容外，还宜记录以下信息：

a) 操作系统的启动、关闭信息；
b) 用户登录、退出信息；
c) 权限变更信息；
d) 系统运行状态信息，包括内存使用率、CPU 占用率、磁盘使用情况等；
e) 主机系统服务或配置变更信息。

6.8.3 数据库日志

数据库日志应记录以下信息：

a) 数据库系统的启动、关闭信息；
b) 用户登录、退出信息；
c) 用户的关键操作信息，如添加或删除数据库，修改表结构等；
d) 数据库运行状态信息，包括数据库故障信息，对数据库监控及报警信息等；
e) 慢 SQL 监控日志。

6.8.4 网络设备日志

网络设备日志应记录以下信息：

a) 设备的启动、关闭信息；
b) 用户登录、退出信息；
c) 端口变化信息；
d) IP 地址变更信息；
e) 网络状态信息，包括丢包率、拥堵情况、带宽变化等；
f) 设备运行状态信息，包括网络设备故障信息，对设备监控报警信息等。

6.8.5 信息安全设备日志

信息安全设备日志应记录以下信息：

a) 设备的启动、关闭信息；
b) 用户登录、退出信息；
c) 端口变化信息；
d) IP 地址变化信息；
e) 信息安全事件信息，如病毒爆发、攻击事件等；
f) 设备运行状态信息，包括设备故障信息，对设备监控报警信息等。

6.8.6 应用系统自身日志

应用系统日志，具体细分为以下内容。

a) 运行日志，包括系统运行的过程日志、性能日志、调试日志、调用日志和诊断日志：
   1) 过程日志：记录应用系统运行过程的日志。包括服务启动、关闭、配置加载、外部服务调用和返回、程序异常、后台操作等业务系统运行情况等的日志；
   2) 性能日志：反映系统性能的日志。包括一个请求从开始到结束整个过程所产生的调用链信息，并且记录相关方法、过程、功能的调用耗时信息等；
   3) 调试日志：用于程序运行调试或测试的日志。这类日志一般会记录的十分详细，例如方法的调用关系、各种参数、主要变量等，在业务系统正式上线后应适当调高日志级别，生产环境不建议开启调试日志，特殊场景除外；
   4) 调用日志：用于记录调用方来源信息、请求报文、响应报文以及响应时间，对于敏感信息应做脱敏处理；
b) 业务日志，表示应用系统业务相关的日志，主要包括用户行为日志、业务行为日志、交易日志和诊断日志：
   1) 用户行为日志：记录用户操作行为的日志。用户行为日志信息包括但不限于用户标识、登录时间、登录 IP 以及系统操作日志等；
   2) 业务行为日志：记录应用系统内部业务处理相关的日志，通常为业务处理的逻辑描述、状态和结果的留痕信息。此类日志包括业务标识、业务处理耗时、业务请求参数、处理状态及处理结果等信息；
   3) 交易日志：交易日志应记录经脱敏处理后的业务流水、交易报文等信息，可用于分析系统的业务特征，如交易量、活跃客户数、交易流动性等，以及用户异常交易行为监控及交易异常问题排查等。此类日志包括用户标识、交易业务参数、交易状态及结果等信息，涉及敏感信息应进行脱敏处理；
   4) 诊断日志：记录应用系统的异常信息，用于问题排查和监控。此类日志应记录异常发生的出处信息、详细异常信息以及异常堆栈信息等；
c) 第三方库和应用框架日志，此类日志是由应用系统引入的第三方库和第三方技术框架所输出的日志，此类日志内容和格式通常不能更改，但可以配置其日志级别及日志存放位置。为了不干扰应用系统业务日志，推荐将第三方库和第三方框架日志输出到独立文件进行存储。

6.9 日志分级

6.9.1 日志级别

当前开发语言提供的日志库都提供多个日志级别，在日志记录时不应将所有信息都记录在同一个日志级别中，而应根据具体业务场景选取合理的日志级别。日志级别从高到低至少应分为五档，从高到低各日志各级别说明如下：

a) 致命（FATAL）：严重错误。该类错误可导致整个系统或是一系列功能无法使用，甚至导致系统瘫痪、关闭和退出等，如磁盘空间满、数据库不可用等。在某些情况下，若某个业务场景发生的错误需要特别关注时也可使用该级别，如交易支付两次通知支付结果状态不一致。处于该级别的日志表示应立即进行人工干预处理；
b) 错误（ERROR）：普通错误。在程序可以控制的范围内，通常不会造成连锁影响或者重大影响，不会影响系统本身运行，只对单次业务处理有影响。该级别表示虽然发生错误事件，但系统仍可正常运行，错误需尽快修复，只是影响程度比 FATAL 级别稍低。一般用来记录程序中发生的异常错误信息，或者记录业务逻辑出错。例如调用某个接口不通而改调用备选接口，或因用户余额不足扣款失败等。记录该级别日志时，应包括异常发生的堆栈信息、详细的异常信息、异常发生的出处信息等；
c) 警告（WARN）：警告级别。表明会出现潜在错误的情形，不影响系统正常运行，但需要引起注意的警告信息。比如内存不足、使用过期方法等；
d) 信息（INFO）：普通日志信息。系统运行的关键时点的操作信息以及系统运行的关键步骤等信息，一般用于记录业务日志。这个级别记录了系统日常运转中有意义的事件，但同时也应该有足够的信息以用于业务追踪、业务监控及异常排查等；
e) 调试（DEBUG）：程序调试信息。指出细粒度信息事件，用于程序调试和测试。调式信息主要便于开发人员进行错误分析和定位，一般记录一些运行中的细粒度的事件，比如记录某个操作的具体步骤信息。DEBUG 日志仅允许在开发和测试环境开启，如果在生产环境需要开启 DEBUG 级别的日志，应征得日志管理人员同意。

日志级别用来指定日志信息的重要程度，在测试阶段可以打开所有级别的日志，系统上线后,宜只输出INFO及以上级别的日志。应用系统应支持日志级别作为参数灵活配置。

6.9.2 分级要求

日志分级基本要求如下：

a) 应根据本文件制定内部统一的日志级别，同时应有日志级别清晰明确的描述和适用场景；
b) 日志级别别可动态配置；
c) 在日志输出时高于最低日志级别的日志记录应都输出；
d) 建议将不同日志级别的日志分别输出、分开存储；
e) 对于 FATAL 级别的日志应有相关的预警措施，例如手机短信、邮件等实时通知提醒。

6.10 日志命名

6.10.1 日志文件命名

本项要求包括但不限于以下内容。

a) 日志以文件形式存储时，文件名称中应至少包括应用系统标识、业务类型标识、日志文件产生时间等便于识别日志文件的相关要素内容。不同要素之间需用分隔符连接，要素命名应当简洁、含义明确。日志文件命名要素包括但不仅限于以下内容：
    1) 应用系统标识，建议以应用系统英文名称作为应用系统标识；
    2) 日志类别标识，用于表示日志所记录数据类别，如用户访问日志、应用系统所使用的具体技术框架的日志等；
    3) 日志文件产生的时间标识，通常当前正在使用的日志文件不带时间标识，在日志归档时应加上时间标识；
    4) 日志级别标识；

5) 日志批次标识，如果日志以大小或时间进行切割归档时，应增加日志批次标识；

b) 同一应用系统内日志命名方式和风格保持统一，同一应用系统内日志文件名应具有唯一性；

c) 如果日志文件根据大小分隔时，日志文件名应增加文件编号，如采用四位数字字符串，并以0001作为起始文件编号。日志文件命名规则为：应用系统标识-日志类型标识[日志文件产生的时间标识|日志级别标识]-日志批次标识.log；

d) 如果日志文件以时间分隔时，建议每个日志文件以该日志文件的起始时间作为编号，时间采用24小时制。

示例：某系统项目英文名称为account,采用spring框架开发，日志每日滚动，当前日期为2019年12月27号，则用于记录用户访问的日志文件可命名为account-access.log。在2019年12月28日凌晨日志滚动后，该日志文件会被自动重命名为account-access-20191227.log,同时会创建一个新的文件名为account-access.log的日志文件。用于记录框架的日志命名为account-spring.log，日志滚动后的日志被重命名为account-spring-20191227.log,同时会创建一个名称为account-spring.log的日志文件。

6.10.2 日志字段命名

本项要求包括但不限于以下内容：

a) 同一应用系统日志字段命名应统一，推荐使用小写字母加下划线风格，如客户端IP，命名为client_ip；

b) 同一应用系统日志字段含义应统一和唯一；

c) 同一应用系统日志字段顺序应一致，同一类型的日志，应保持各字段顺序一致。

6.11 记录要素

本项要求每条日志至少应包含以下信息：

a) 时间戳：表示本条日志产生的时间点。宜参照GB/T 7408-2005时间格式，记录的时间应至少精确到秒，建议时间戳字段同时指定时区；

b) 来源标识：表示本次业务请用的来源方。如果来源方是是用户操作，可记录用户账户、机器IP，如果是服务器，建议记录发起调用的系统服务名称（业务名称+实例ID）、机器IP；

c) 跟踪标识：表示本条功能处理的跟踪标志，宜全局唯一,伴随着本次业务处理全程；

d) 日志级别（见6.9.1）；

e) 代码位置，对于日志级别为错误及以上的日志还应记录代码位置，通常为方法的完整路径和在日志记录点在源码中所处的行号；

f) 响应码：不同级别和类型的日志，都应该同时输出响应码，以便于日志收集和监控；

g) 日志内容：用于记录便于业务人员、运维人员和日志审计人员阅读的日志内容。对于异常日志信息，需要同时记录异常堆栈信息。

6.12 字段分隔

为方便对日志进行采集、解析，建议使用JSON格式或是健值对格式记录日志。若采用分隔符分隔日志中记录中的各个字段，具体要求如下：

a) 应用系统开发时，应有规划对日志记录要素进行分隔，可全局统一使用一类分隔符；

b) 在日志记录时应用系统应以固定且无歧义的分隔符对日志要素信息进行分隔标注；

c) 应用系统交付时应用系统开发者应提供日志分隔说明；

d) 日志解析时应验证日志分隔说明的准确性，日志分隔说明应及时准确更新。

6.13 文件分隔

文件分隔具体要求如下。

a) 日志以文件的方式生成时，应进行文件分割和转储。应至少满足以下要求之一：
   1) 以一定的周期生成日志文件，一般以一个自然日为一个周期；
   2) 单个日志文件不超过一定大小，当单个周期内日志量较大时按照文件编号顺序生成新文件，即同时按照时间和日志大小进行文件分割。不建议日志文件只以日志量大小进行分隔；
b) 日志的分割规则应可以配置，配置项可包含：
   1) 文件进行分割转储的周期；
   2) 单个日志文件的最大文件大小，单个日志文件最大不宜超过 200MB。

7 日志存储

7.1 存储要求

日志作为一种重要的数据资源，应遵循数据存储的基本要求：

a) 操作系统、数据库系统、业务应用系统等的系统日志应由相关管理员进行定期转存和清理，以保障系统日志有足够的存储空间，安全管理员及相关管理员保存和管理转存的日志，应满足安全存储要求；
b) 日志宜保留在只读的介质上。除了在本地保存以外，日志还应传输到安全的日志服务器上，不应将日志保存于共享的文件系统中；
c) 应加密存储含有敏感信息的离线日志；
d) 在日志保留期内，任何人不应对所有的原始日志和记录进行更改、删除等操作；
e) 同一应用系统日志应设置为统一的存储路径，可根据业务类型不同设置不同子目录进行存储；
f) 建议建立双备份制度，对重要日志除了在本地服务器存储外，还应拷贝到其他介质上，以防遭病毒、自然灾害等破坏而遗失，以便系统一旦发生故障时能快速恢复；
g) 日志文件应集中管理并加以保护，应设置日志文件访问控制权限，防止未授权的访问篡改。

7.2 备份归档

日志备份归档具体内容如下：

a) 证券期货机构应按照国家主管部门的有关要求，制定日志备份及验证策略，根据不同的业务场景明确日志备份范围、备份方式、备份频度、存放地点、存放时限、有效性验证方式和管理责任人；
b) 证券期货机构在制定日志备份和验证策略时：
   1) 应制定日志归档、备份方面的运维管理制度，对日志进行定期归档和备份，日志管理人员负责日志的安全管理；
   2) 日志归档、备份时应不影响生产系统的正常运行；
   3) 对于重要的日志数据建议要具有本地、同城和异地备份的能力；
   4) 备份日志不得更改，应定期组织日志恢复演练，形成日志恢复演练报告；
   5) 归档及备份日志应存储在可靠存储设备中，并指定专人负责，妥善保管；
   6) 对存放重要日志数据的介质应采取加密存储措施，并根据所承载数据的重要程度对介质进行分类和标识管理；
   7) 备份日志数据需要指定专人负责，不应未授权访问，严格执行数据交接管理规定和登记管理制度；
   8) 安全级别为高的应用系统，日志保存时间建议至少为 36 个月；

9） 安全级别为中或者低的应用系统，日志保存时间建议至少为12个月；
10）IT基础设备和系统的日志保存时间建议至少为12个月。

8 日志采集

日志采集要求如下。

a） 日志采集流程应按照经营机构依据本文件要求制定的日志管理制度中数据转储、传输和使用要求；
b） 日志采集不应影响应用系统的正常运行；
c） 日志采集应对用户网络和业务的影响最小化；
d） 日志实时采集时所使用的数据采集工具应能够满足时效性要求，保障较低的传输延迟；
e） 日志采集时应满足以下安全要求：
   1） 日志在不可信任的环境中进行传输时应加密处理，避免中间过程截取日志；
   2） 日志的使用应做到有留痕，可追溯；
   3） 日志应经过授权才可采集和使用；
   4） 未经允许，证券期货机构外的第三方应用系统和机构不得以任何形式采集、访问和下载业务系统日志；
   5） 日志提供方应明确日志的安全保护要求，并明确告知数据接受方；
   6） 日志接收方对于获取的不同应用系统的日志进行汇聚时，应满足安全保护要求；
   7） 在未验证日志安全备份前，任何人不应以任何理由删除日志；
f） 为了更好的保存日志和后续的处理，应创建专门的日志采集服务器，并将采集的数据输送到统一、集中的日志管理中心；
g） 应实时采集、记录、跟踪网络运行状态，监测、记录网络安全事件的技术措施，并留存网络日志；
h） 日志采集应满足GB/T 36626—2018中8.3中关于访问控制相关的要求。

9 日志监控

应提供业务系统及其服务运行状况监控视图，并配备相关的自动化报警工具，及时发现日志及业务系统的异常，分析和快速修复问题，确保业务系统高效稳定运行。日志监控主要内容如下。

a） 经营机构宜制定日志监控相关的方案和实施细则，并将监控内容和结果借助软件、硬件设备进行可视化展示；
b） 经营机构宜制定日志监控相关反馈机制、应急处理机制及相关责任人；
c） 在制定日志监控时要兼顾本规范对日志自身规定的监控和应用系统业务的监控，二者相辅相成，进而不断优化日志、日志监控、应用系统和应用系统依赖的软件、硬件设施；
d） 经营机构宜设置合理的自动化监控工具的预警阈值，并定期进行检查和评估，并形成评估报告；
e） 经营机构宜针对不同应用系统设置合理的监测频度和监控范围；
f） 监控要素及指标包括但不限于以下内容：
   1） 从访问日志中提取访问量、访问成功率、访问响应时间等高价值信息，并能够监控和展现这些应用性能指标；
   2） 系统负责人应根据本文件要求对异常的日志进行分析处理，发现异常及时上报IT风险管控组；

3) 日志审计系统应支持对信息系统中各类主机、数据库、应用和设备的安全事件进行实时采集、实时分析、异常报警、集中存储和事后分析功能，支持分布式部署，具备对各类网络设备、安全设备、操作系统、中间件服务器、通用服务、数据库和其它应用进行全面的日志安全审计能力；
4) 应支持自动对各种类型的日志进行实时分析，并能将紧急、严重的事件日志通过设备远程主控台、短信、邮件、微信等多媒体方式向管理员及相关人员发送实时告警消息；
5) 应实时对应用系统依赖的网络设备及系统平台的性能状态、安全访问、异常事件产生的日志进行分析统计，按数据源输出监控分析报表；

g) 除了本文件要求之外，还应遵循 GB/T 34960.5—2018 关于数据治理过程制定的要求。

10 日志审计

10.1 日志审计要求

日志审计除经营机构内部审计部门根据审计规范要求进行审计之外，还应建立相关的日志审计系统。

10.2 内部审计

内部审计由经营机构内部审计部门负责对日志进行审计，具体内容如下：

a) 经营机构内部审计部门应每年对应用系统的日志记录的准确性、完整性、安全性进行审计，并出具审计报告；
b) 经营机构内部审计部门应按照本文件对日志的记录、转储、存储、备份、销毁过程按照审计规范进行审计；
c) 建议经营机构内部审计部门每季度组织对各系统的日志配置策略和日志检查记录等进行审计，对各系统管理员和系统操作员的活动记录日志每月进行审计；
d) 经营机构应对主机系统进行审计，妥善管理并及时分析处理审计记录；
e) 经营机构应对重要用户行为、异常操作和重要系统命令的使用等进行重点审计；
f) 经营机构应按照审计报告及时进行整改；
g) 审计报告建议至少保存 3 年。

10.3 系统审计

建议经营机构建立统一的日志管理中心，负责日志采集统一接入、日志存储、日志备份、日志分析及告警、日志审计、日志访问权限控制、日志检索等。建议日志采集模块实时不间断地采集生产环境的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的日志信息，并将这些信息汇集到日志管理中心进行集中化存储、索引、备份，并支持全文检索、实时搜索、审计、告警、响应，支持出具丰富的报表报告，获悉全网的整体安全运行态势，进行基于日志的综合审计和日志全生命周期管理，从而最大化的保障网络、主机和应用系统安全机制的有效性。

11 日志销毁

经营机构在进行日志销毁时应遵循 JR/T 0099—2012 对数据与介质管理中销毁的相关规定，日志销毁应采用安全可靠的方式，如采用复写法、消磁法、剪碎法及焚毁法等。

参考文献

[1] GB/T 7408-2005 数据元和交换格式 信息交换 日期和时间表示法
[2] GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则
[3] GB/T 34960.5—2018 信息技术服务 治理 第5部分：数据治理规范
[4] JR/T 0059—2010 证券期货经营机构信息系统备份能力标准
[5] JR/T 0060—2010 证券期货业信息系统安全等级保护基本要求（试行）
[6] JR/T 0067—2011 证券期货业信息系统安全等级保护测评要求（试行）
[7] JR/T 0099—2012 证券期货行业信息系统运维管理规范
[8] JR/T 0175—2019 证券期货业软件测试规范