数据安全管理平台功能要求

Functional Requirements for Data Security Management Platform

目　次

1 范 围

本文件规定了数据安全管理平台在数据安全功能、自身安全功能、性能及安全保障等方面的要求。

本文件适用于数据安全管理平台的设计、开发与测试。

2　规范性引用文件

下列文件中的内容通过文中的规范化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 42250-2022 《信息安全技术 网络安全专用产品安全技术要求》

GB/T 18336.3-2015 《信息技术 安全技术 信息技术安全评估准则 第 3 部分：安全保障组件》

GB/T 25069-2022 《信息安全技术 术语》

GB/T 30279-2020《信息安全技术 网络安全漏洞分类分级指南》

GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》

GB/T 39786 《信息安全技术 信息系统密码应用基本要求》

GB/T 37092 《信息安全技术 密码模块安全要求》

GB/T 25000.51-2016 《系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第 51 部分：就绪可用软件产品（RUSP）的质量要求和测试细则》

GB/T 38634.2《系统与软件工程 软件测试 第 2 部分：测试过程》

GB/T 38634.4-2020《系统与软件工程 软件测试 第 4 部分：测试技术》

GB/T 38667 《信息技术 大数据 数据分类指南》

GB/T 42775 《证券期货业数据安全风险防控 数据分类分级指引》

GB/T 42128 《智能制造 工业数据 分类原则》

GB/T 38674-2020 《信息安全技术 应用软件安全编程指南》

YD/T 3813 《基础电信企业数据分类分级方法》

YD/T 4244 《电信网和互联网数据分类分级技术要求与测试方法》

YD/T 4251 《电信运营商大数据安全管控分类分级技术要求》

YD/T 4243 《电信网和互联网数据资产识别与梳理技术实施指南》

YD/T 4241 《电信网和互联网数据安全评估技术实施指南》

YD/T 4221 《电信大数据平台敏感数据识别实施指南》

YD/T 3956 《电信网和互联网数据安全评估规范》

YD/T 3801 《电信网和互联网数据安全风险评估实施方法》

YD/T 3867 《基础电信企业重要数据识别指南》

NIST SP 800-63-3 《Digital Identity Guidelines（数字身份准则）》

TC260-PG-20212A 《网络安全标准实践指南-网络数据分类分级指引》

TC260-PG-20231A 《网络安全标准实践指南-网络数据安全风险评估实施指引》

3 术语和定义

GB 42250-2022、GB/T 18336.3-2015、GB/T 25069-2022、GB/T 30279-2020、GB/T 22239-2019、GB/T 28448-2019 界定的以及下列术语和定义适用于本文件。

3.1 数据安全管理平台 data security management platform

具有数据分类分级、敏感数据发现、数据资产安全管理、数据安全风险评估、数据安全态势感知等功能的平台，不包括数据防泄露等用于数据自身安全防护的工具或平台。

3.2 数据安全管理平台提供者 data security management platform provider

数据安全管理平台（3.1）产品的研发者、生产者或维护服务提供者。

3.3 数据安全态势感知 data security situation awareness

在数据分类分级的基础上，通过监测发现敏感数据，管理数据资产，并综合其他网络安全态势等信息，分析和处理数据安全事件、相关网络行为及用户行为等因素，掌握数据安全状态，预测数据安全趋势，并进行展示和监测预警的活动。

3.4 敏感数据 sensitive data

一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成严重危害，或者对公共利益造成一般危害，但不会危害国家安全的数据。

3.5 产品供应链 products supply chain

是指为满足数据安全管理平台产品的设计、研发、交付与运维等过程中的供应关系，通过资源和过程将需方、供方相互链接的网链结构，可用于将相关产品和服务提供给数据安全管理平台提供者（3.2）。

3.6 用户信息 user information

个人、法人或者其他组织在安装、使用数据安全管理平台过程中产生、收集、存储、传输、处理的电子方式记录的信息，包括网络流量信息、用户数据信息、安全状态信息、安全配置数据、运行过程日志等信息，也包括个人信息。

3.7 安全漏洞 security vulnerability

数据安全管理平台在需求分析、设计、实现、配置、测试、生产、运行、维护等过程中，无意或有意产生的、有可能被利用的缺陷或薄弱点。

3.8 系统 system

数据安全管理平台作为一个完整的整体，执行 3.1 中所描述的功能，由相关作用或相互依赖关系联合起来的子系统组成，作为一个整体而发挥其作用。

3.9 子系统 subsystem

数据安全管理平台中的二级或下级系统，具有相对独立的功能。

4 缩略语

API	Application Programming Interface	应用编程接口
FTP	File Transfer Protocol	文件传输协议
FTPS	FTP-over-SSL	在安全套接层使用的文件传输协议
HTTP	Hyper Text Transfer Protocol	超文本传输协议
HTTPS	Hyper Text Transfer Protocol Secure	安全超文本传输协议
SFTP	Secure File Transfer Protocol	安全文件传输协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SSH	Secure Shell	安全外壳
SSL	Secure Sockets Layer	安全套接层
Syslog	System log	系统日志

5 功能要求

5.1 总体功能框架

数据安全管理平台包括图 5.1 中的数据分类分级、敏感数据发现、数据资产安全管理、数据安全风险评估、数据安全态势感知等功能，可根据需求实现一种或几种功能。

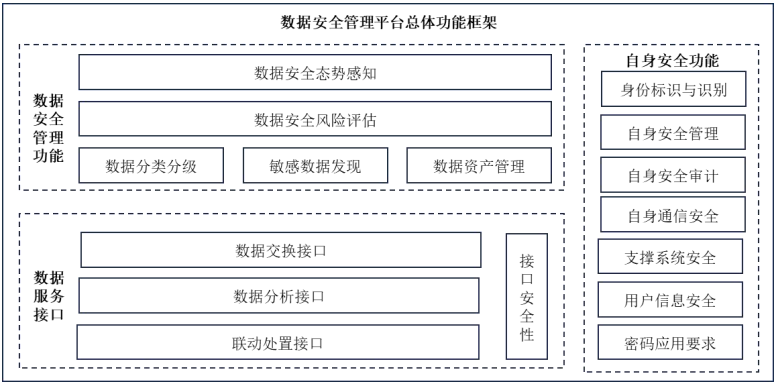

图 5.1 数据安全管理平台总体功能框架

5.2 数据安全管理功能要求

5.2.1 数据分类分级

平台的数据分类分级功能包括但不限于：

1.应遵循合法合规、界限明确、就高从严、注重时效和自主性原则，根据用户和行业需求、业务场景，满足国家和行业标准中给出的数据分类分级方法。

2.应支持对数据分类分级规则进行配置，准确标识数据类别和级别。

3.宜内置数据分类分级模板库，快速匹配不同的用户需求和业务场景。

5. 2. 2　敏感数据发现

平台的敏感数据发现功能包括但不限于：

1. 应根据用户和行业需求、业务场景，满足国家和行业标准给出的敏感数据识别要求。

2.应支持被动接收前端数据源发送的敏感数据，支持手动导入前端数据源的敏感数据。

3.应支持主动发起获取前端数据源的敏感数据，对数据库、文件系统等数据源进行字段级别、内容级别的深度扫描，支持结构化、半结构化和非结构化数据源，支持对扫描频率进行设置。

4.应根据应用场景支持两种或两种以上的采集协议进行敏感数据发现和采集，采集协议包括但不限于 Syslog、FTP/FTPS、SFTP、HTTP/HTTPS、SSH、SNMP 等。

5.应支持基于预置的敏感数据字典库对扫描到的数据进行匹配，识别敏感数据并梳理敏感数据在数据库、文件系统中的分布情况，支持根据应用场景自定义敏感数据字典库。

6.应支持展示平台管理的涉敏数据库及其数据库表、涉敏文件系统及其文件列表、敏感数据分布和类别等信息。

7.宜支持对网络流量的异常监测，通过内置的异常行为

告警规则和用户自定义规则，对异常流量数据进行告警、展示。

8.宜支持数据流转行为监测，对敏感指令、疑似暴力破解、特权账号使用、账号多 IP 使用等风险行为实时识别并告警。

5.2.3 数据资产管理

平台的数据资产管理功能包括但不限于：

1.应根据用户和行业需求、业务场景，满足国家和行业标准给出的数据资产识别和管理要求。

2.应支持通过人工添加、主动探测发现、被动识别等技术手段对目标数据库、文件系统、业务系统等数据源授权添加到平台中进行统一管理。

3.应支持建立数据资产画像。

4.应支持数据资产列表功能，全量统计当前系统中已探测到的数据库及其库表、字段信息，包括该字段的分类分级结果、敏感等级、归属的业务系统等信息。

5.宜实现数据资产地图，展示当前已经授权的数据库、文件系统、业务系统等数据源的分布以及数据分类分级、敏感数据发现等任务的进展情况。

6.宜支持结合内外部的分析能力预测潜在的数据资产风险。

5.2.4 数据安全风险评估

平台的数据安全风险评估功能包括但不限于：

1. 应根据用户和行业需求、业务场景，满足国家和行业标准给出的数据安全风险评估实施要求。

2.应提供数据安全风险核查功能，支持将 API 接口风险、弱口令、不合规配置、资产漏洞等核查结果以*.et、*.xls、*.xlsx等文件格式导入平台。

3.应支持结合数据类型、数据位置、数据重要程度、数据资产脆弱性、威胁信息等分析数据资产风险，评估数据资产风险等级。

4.应支持重要数据处理者对其数据处理活动开展风险评估。

5.可内置数据安全风险评估工具，支持评估准备、信息调研、风险识别、综合分析、评估总结等数据安全风险评估实施各阶段工作：

1）评估准备阶段工作包括确定评估目标、确定评估范围、组建评估团队、开展前期准备、制定评估方案等。

2）信息调研阶段工作包括数据处理者调研、业务和信息系统调研、数据资产调研、数据处理活动调研、安全措施调研等。

3）风险识别阶段工作包括数据安全管理、数据处理活动、数据安全技术、个人信息处理等的风险识别。

4）综合分析阶段工作包括梳理问题清单、数据安全风险分析与评价、提出整改建议。

5）评估总结阶段工作包括风险评估报告、安全风险处置

等。

5. 2. 5 数据安全态势感知

平台的数据安全态势感知功能包括但不限于：

1.应支持对数据的整体安全状况用分值或等级等方式进行评估和展示，例如以数据安全生命周期管理为主线，通过多维度量化指标，精准描述数据安全的实时风险和整体状况。

2.应支持对不同行业、不同区域、不同业务单元或不同数据资产等的局部数据安全状况采用分值或等级等方式进行评估和展示。

3.应支持对不同时间段的整体数据安全状况进行评估和展示。

4.应支持采用多种视图展示整体数据安全态势，展示视图至少包括以下中的两种：雷达图、地理信息图、关联关系图、威胁路径图、趋势图、同/环比图等。

5.应支持分角色展示，针对不同角色用户展示不同内容。

6.应支持展示整体数据安全状况的变化趋势，如分值或等级的变化等。

7.应支持根据应用场景和数据安全业务场景进行不同类型专题数据安全态势的评估和展示，如数据分类分级态势、敏感数据态势、数据资产态势、脆弱性态势、流量态势、攻击态势、异常行为态势、安全事件态势等。

8.应支持利用海量数据分析引擎及模型实现对数据风险的主动发现、精准定位、智能研判、快速处置、严格审计，

完成对数据安全保护工作的闭环处置流程。

9.应支持基于时间或其他数据字段对态势相关数据进行组合查询，支持对查询结果根据字段进行排序。

10.应支持根据数据分析、数据安全态势评估的结果生成统计报表并导出，支持基于指定时间段生成统计报表或生成周期性报表，支持自定义设置统计视图和报表模板，采用多种视图生成统计报表。

11.应支持根据数据分析结果生成整体数据安全状况分析报告并导出，支持根据数据分析结果生成不同区域、不同业务单元等的局部数据安全状况分析报告并导出，支持根据数据分析结果提供对策或修复建议，支持基于指定时间段产生分析报告或生成周期性分析报告，支持自定义设置分析报告的模板。

5.3 自身安全要求

5.3.1 身份标识和鉴别

平台的身份标识与鉴别安全要求包括但不限于：

1.应对用户身份进行标识和鉴别，身份标识具有唯一性。

2.应对用户身份鉴别信息进行安全保护，保障用户鉴别信息存储和传输过程中的保密性。

3.应具有登录失败处理功能，配置并启动结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

4.应具有登录超时处理功能，当登录连接超时自动退出。

5.鉴别机制应具有抗重放攻击的能力。

6.应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

7.当平台中存在默认口令时，应提示用户对默认口令进行修改，以减少用户身份被冒用的风险。

5.3.2　自身安全管理

平台的自身管理要求包括但不限于：

1.应区分管理员角色，划分为系统管理员、安全管理员和审计管理员，三类管理员角色权限能相互制约。系统管理员主要负责平台的日常运行维护工作，包括平台的安装、配置、升级、维护、运行管理，平台用户增加或删除，平台数据备份、运行日志审查和运行情况监控，应急条件下的安全恢复。安全管理员负责平台的安全管理工作，包括平台用户权限的授予与撤销，用户操作行为的安全设计，平台安全事件的审计、分析和处理，应急条件下的安全恢复。审计管理员主要负责对系统管理员和安全管理员的操作行为进行审计跟踪、分析和监督检查，及时发现违规行为。

2.应为授权系统管理员提供策略管理的功能，支持策略的集中管理和自定义设置，包括数据分类分级策略、敏感数据发现策略、监测策略和预警规则等。

3.应为授权系统管理员提供管理数据处理规则的功能，包括新增、删除、修改、查询、启用、停用数据处理规则等。

4.应为授权系统管理员提供数据分类分级模板库、数据分类分级规则库、敏感数据字典库、数据分析模型的管理，包括新增、删除、修改数据分析模型等。

5.应为授权系统管理员提供资产管理的功能，支持对采用人工添加、主动探测发现、被动识别等技术手段获取的资产信息进行管理。

6.应为授权安全管理员提供数据安全事件管理的功能，包括建立并动态维护数据安全事件库，对数据安全事件进行分类和分级等。

7.应建立威胁信息库，为授权安全管理员提供威胁信息管理的功能，支持对不同来源的威胁信息进行汇聚并及时更新。

8.应向授权安全管理员提供设置、查询和修改各种安全策略的功能。

9.应向授权审计管理员提供管理审计日志的功能。

10.应支持更新自身系统的能力，包括对软件系统的升级以及各种特征库、策略库的升级，保障升级安全，避免得到错误的、伪造的升级包和补丁程序。

11.应支持通过 Syslog 协议向日志服务器同步日志等信息。

12.应支持与外部时间服务器进行时间同步。

13.应提供安全策略有效性检查功能，如安全策略匹配情况检测等。

5.3.3 自身安全审计

平台的安全审计要求包括但不限于：

1.应对用户账户的登录和注销、系统启动、配置变更、增加/删除/修改管理员、保存/删除审计日志等操作行为进行监测、记录。

2.应对平台及其组件的运行状态进行监测，对异常状态进行告警，并记录日志。

3.日志记录应包括如下内容：事件发生的日期和时间，事件的类型，事件主体，事件操作结果。

4.应将日志存储于非易失性存储介质中，日志保存时间不少于六个月。

5.应仅允许授权审计管理员访问日志，对日志进行保护，防止受到未预期的删除、修改、覆盖和丢失。

5.3.4 自身通信安全

1.应采用校验技术或密码技术保证远程管理时的所有网络通信数据在传输过程中的完整性。

2.应采用密码技术保证远程管理时的所有网络通信数据在传输过程中的保密性。

3.应限定进行远程管理的 IP、MAC 地址。

4.应分离管理接口与业务接口。

5.3.5 支撑系统安全

平台的支撑系统安全要求包括但不限于：

1.不应提供多余的组件或网络服务。

2.重启不应导致安全策略和日志信息丢失。

3.不应包含已公开的中风险及以上漏洞。

注：漏洞风险等级参照 GB/T 30279 《信息安全技术 网络安全漏洞分类分级指南》中给出的网络安全漏洞分级方法。

5. 3. 6 用户信息安全

1.应仅收集实现功能所必需的用户信息。

2.应明示收集用户信息的目的、方式、范围、种类、存储位置和处理方式。

3.应建立和执行用户信息管理制度和流程，在设计、生产、升级等各阶段保障用户信息的安全，不超范围使用用户信息。

4.应在涉及个人信息处理时提供相关授权功能，在获得授权后方能处理个人信息。个人信息处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。授权功能包括但不限于个人信息收集前的授权同意、个人信息收集的授权撤回等。

5.应对收集到个人信息进行去标识化处理，并采取技术和管理方面的措施，将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理。

6.应在未获得或撤回个人信息收集授权的情况下提供与个人信息无关的安全功能。

7.应在涉及个人信息传输和存储过程中，采用校验技术或密码技术保障个人信息的保密性和完整性。

8.应在涉及个人信息存储时提供对超出保存期限个人信息的处理功能，处理方式应与用户授权的处理方式一致，如采取删除或匿名化处理措施。

5.3.7　密码应用要求

1.应采用密码技术对登录用户进行身份鉴别，保证平台用户身份的真实性。

2.应采用密码技术保证平台重要数据在传输和存储过程中的机密性。

3.宜采用密码技术保证平台的访问控制信息的完整性。

4.宜采用密码技术保证平台重要信息资源安全标记的完整性。

5.宜采用密码技术保证平台重要数据在传输和存储过程中的完整性。

6.以上（5.3.7-1 至 5.3.7-5）如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。

7.以上（5.3.7-1 至 5.3.7-5）采用的密码产品或模块，应达到 GB/T 37092《信息安全技术 密码模块安全要求》中的二级及以上安全要求。

5.3.8　部署与运行环境安全

平台部署运行环境中的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运

维管理应满足 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中第 8.1 节规定的网络安全等级保护三级要求。

5.4 数据服务接口

5.4.1 数据交换接口

1.应支持与不同前端数据源、内部不同模块及其他外部系统通过接口进行数据交换，数据交换包括但不限于数据采集、共享、级联交换。

2.应支持不同类型、字段和格式的数据交换内容，其中类型包括日志、告警信息、威胁信息、数据资产信息、用户信息、脆弱性信息、数据安全事件等，字段和格式应基于类型进行定义。

5.4.2 数据分析接口

1.宜支持为内部不同模块及其他外部系统通过接口进行数据分析。

2.宜支持基于数据分析接口实现算术计算、逻辑关系计算、关联计算等分析能力。

5.4.3 联动处置接口

1.宜支持为内部不同模块及其他外部系统通过接口进行联动处置。

2.宜支持通过接口进行防护策略的更新、扫描策略的下发等操作。