ICS 35.240
CCS L70

团 体 标 准

T/FJAS 031—2026

数据资产——数据合规审核规范

Data assets——specifications for data compliance review

2026 - 03 - 30 发布　　2026 - 04 - 10 实施

福建省标准化协会　　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。

本文件由福建大数据交易所有限公司提出。

本文件由福建省标准化协会归口。

本文件起草单位：福建大数据交易所有限公司、福州交通新能源科技有限公司、福州数据集团有限公司、北京大成(福州)律师事务所、莆田学院、天津大学、福建新世通律师事务所、泉州市中科育成科技发展有限公司、泉州市知识产权保护中心、福建省数据流通控股有限公司、北京智慧财富资本管理集团有限公司、宁德市物资再生利用有限公司。

本文件主要起草人：陈雯珊、胡九龙、张群洪、卢健、陈学军、张兮、陈承正、蔡群、邱江鸿、巫利荣、马新明、钟建文、卞羽、翁磊、杨堃、陈妍意、张趁华、石焱文、陈清、余丽銮、秦源丰、季晓芬、戴旺、翁婷、梁迎莹、沈壮壮、陈铭杰、张绮晖、陈姜锐。

数据资产—数据合规审核规范

1 范围

本文件规定了数据合规审核活动的合规审核准则、数据处理者主体资格审查、数据安全管理制度审核、数据资产分类分级、数据资产全生命周期合规审核、数据资产管理制度与技术措施审核。

本文件适用于各类组织开展数据资产入表及管理的合规审核活动，也可为监管部门、第三方审核机构提供参考。

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 25069-2022 信息安全技术 术语

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 43697-2024 数据安全技术 数据分类分级规则

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据处理者 an organization or individual that processes data

是指在数据处理活动中自主决定处理目的和处理方式的个人或者组织。

[来源：国家数据局《数据领域常用名词解释》（第一批）]

3.2

数据处理 data processing

数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

[来源：国家数据局《数据领域常用名词解释》（第一批）]

3.3

数据资产 data assets

特定主体合法拥有或者控制的，能进行货币计量的，且能带来经济利益或社会效益的数据资源。

[来源：国家数据局《数据领域常用名词解释（第一批）》]

3.4

数据合规 data compliance

数据处理者采取必要措施，在数据处理、数据安全管理过程中应遵守的要求。

注：数据合规包括但不限于数据管理主体合规；数据管理制度合规；数据管理活动合规等。

3.5

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

3.6

个人信息主体 personal information subject

个人信息所标识或者关联的自然人。

3.7

敏感个人信息 sensitive personal information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

[来源：GB/T 43697-2024]

3.8

组织 organization data

具有自身的职责、权威和关系以实现其目标的个人或集体。

注：组织的概念包括但不限于个体经营者、公司、法人、商行、企业、机关、合伙关系、慈善机构或院校，或者其部分或组合，无论注册成立与否、是公共的还是私营的。

[来源：GB/T 25069-2022]

4 合规审核准则

4.1 合法性准则

数据合规审核活动应符合适用的法律法规要求，审核依据、程序、结论及整改建议均需符合法律法规规定。如审核活动中发现潜在风险的，审核机构应向数据处理者予以提示。

4.2 独立性准则

审核机构和审核人员应独立于被审核对象的数据资产处理活动，避免利益关系和外部压力干扰，确保审核结论客观公正。

4.3 客观性准则

收集和记录的审核证据应保证其可信性，应采取科学、透明的方式获得审核证据，应保证审核证据的真实、准确、完整、有效，审核过程应基于客观事实，采用科学合理的审核方式开展审核活动。

4.4 保密性准则

审核机构和人员应对审核过程中获取的数据资产信息、商业秘密、保密商务信息、个人信息等予以保密，不得泄露或非法提供给第三方。

4.5 专业性准则

审核机构和审核人员应具备开展数据合规审核的能力，拥有执行合规审核所需的专业知识、技能及对相关法规的深刻理解，委托第三方机构开展合规审核的，应当对其独立性进行审查。若审核机构和审核人员与被审核方存在可能影响审核公正性的利益关系或其他应当回避情形的，应当予以回避。

4.6 风险导向准则

数据资产合规审核应重点关注高风险环节，如敏感个人信息处理、数据出境、大规模数据共享等，优先审核可能对国家安全、公共利益及个人权益造成重大影响的活动。

5 数据处理者主体资格审查

5.1 审查目标

审查数据处理者是否具备合法、有效且稳定的主体资格，以及其近期是否存在可能影响数据安全责任履行的重大不利情形，以评估其开展数据处理活动的法律基础与合规风险。

5.2 独立民事责任能力审查

应审查数据处理者是否具有独立承担民事责任的法定能力，核实其能否以自身名义对外开展民事活动、享有权利并承担责任。审查应通过查验其在市场监管部门等登记机关依法登记或备案的证明文件等方式进行。

5.3 重大不利情形审查

应通过国家企业信用信息公示系统、信用中国、相关行业监管公开平台等官方或权威公开信息渠道进行查询与核实。审查数据处理者在近一年内或审核方认定的合理期限内，是否存在以下可能对其数据处理活动构成实质性重大不利影响的情形：

a) 因违反数据安全、网络安全、个人信息保护等相关法律法规而受到重大行政处罚或刑事处罚；
b) 发生重大数据安全事件；
c) 被列入严重失信主体名单；
d) 因数据产权、数据使用、收集等数据处理活动违法而受到相关数据处理者起诉及人民法院不利裁决；
e) 其他可能实质影响其持续、稳定、合法履行数据安全保护责任的情形。

6 数据安全管理制度审核

6.1 审核目标

审查数据处理者是否依据数据安全、个人信息保护及网络安全相关法律法规及规范性文件的要求，建立、实施并维护有效的数据安全管理制度体系，以履行其数据安全保护义务。

6.2 数据安全管理办法审核

6.2.1 制度制定

应审查数据处理者是否制定并落实了全面的数据安全管理办法，应包括：

a) 数据分类分级管理办法
   1) 针对数据处理者数据库从对国家安全、公共利益或个人、组织合法权益的危害程度对数据进行分类分级；
   2) 对不同分级的数据分别实施不同的合理的管理和技术保护措施；

b) 数据处理者内部数据安全负责人及数据安全管理组织架构：包括机构的岗位设置、职责内容；
c) 数据安全教育培训机制；
d) 数据处理活动的处理流程管理措施及风险监测机制；
e) 处理敏感个人信息，向境外提供个人信息等对个人权益有重大影响的个人信息处理活动应有前置个人信息保护影响评估流程；
f) 数据共享、委托处理、向境外提供数据等重大数据处理活动应有前置风险评估机制及合作方安全管理要求；
g) 利用互联网等信息网络开展数据处理活动的数据处理者，应当在已制定内部网络安全管理制度和操作流程的基础上制定有数据安全管理办法；

6.2.2 制度落实

应审查数据处理者是否通过流程控制、技术手段、监督检查等方式，确保管理办法中的各项规定在实际数据处理活动中得到有效执行，并保留相关记录。

6.3 数据安全事件应急预案审核

应审查数据处理者是否制定并具备有效实施数据安全事件应急预案的能力，包括：

6.3.1 预案制定：是否依据数据安全相关法律法规及工业和信息化部相关要求，制定专门的数据安全事件应急预案，明确应急组织架构、事件分级、监测预警、处置流程、报告机制和恢复措施；

6.3.2 应急响应机制：是否建立数据安全事件应急响应，以及能否根据数据安全计划的变化及时调整，确保数据安全事件得到及时有效处置，包括：
a) 数据安全事件分级及数据安全事件通报流程；
b) 应急响应启动条件；
c) 响应流程、人员安排和操作守则；

6.3.3 预案落实：是否定期组织应急演练、培训，确保相关人员熟悉预案流程；是否在真实事件中能按预案有效响应，并按要求进行报告和记录。

6.4 数据安全培训机制审核

应审查数据处理者是否建立并运行持续的数据安全培训机制：
a) 机制建立：是否建立了制度化的数据安全培训机制，明确了培训对象、内容、周期和考核要求；
b) 机制落实：是否按计划对全体员工，特别是关键岗位人员定期开展培训，内容涵盖法律法规、内部制度、安全意识和操作技能，并保留培训、考核记录以验证效果。

6.5 重要数据处理者责任落实审核

对于重要数据处理者，应额外审查以下内容：
a) 重要数据处理者是否依法建立专门的管理架构：
   1) 责任机构与人员：是否按照法律要求，明确数据安全负责人和管理机构，并落实数据安全保护责任；
   2) 履职保障：是否为数据安全负责人和管理机构履行职责提供了必要的资源与授权，确保其能够有效参与决策并监督制度执行。
b) 重要数据处理者是否依照网络安全相关法律法规对重要数据采取了备份和加密等措施；

c) 重要数据处理者是否依照网络安全相关法律法规对数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告，风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等；

d) 重要数据处理者是否依法遵守了重要数据的出境安全管理规定：如因业务需要，确需向境外提供重要数据的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

7 数据资产分类分级

7.1 分类分级依据

数据处理者对其数据资产进行分类分级时，应按 GB/T 43697-2024 执行，并适用所属行业主管部门及地区数据安全管理机关的规章制度及规范性文件。

7.2 数据级别划分

应根据数据遭到安全事件后对国家安全、公共利益、组织与个人权益造成的危害程度，将数据从高到低划分为以下级别：

a) 核心数据：指关系国家安全、国民经济命脉、重要民生、重大公共利益等的数据。审核其识别是否审慎，并报请相关主管部门认定；
b) 重要数据：指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、经济运行、社会稳定、公共健康和安全的数据。审核其识别范围是否准确；
c) 一般数据：指核心数据、重要数据之外的数据。可进一步细分，审核其分级是否合理。

7.3 数据资产目录标注

在数据资产目录等清单中，应对以下数据予以明确标注：

a) 级别标注：是否为识别出的重要数据和核心数据设置了明确的级别标识；
b) 个人信息标注：是否依据个人信息保护相关法律法规及 GB/T 35273-2020，对个人信息与敏感个人信息进行了标识。

7.4 无明确标准时的处理

对于尚无明确分类分级标准的数据，应根据其重要程度和潜在危害，按照就高从严的原则确定其级别。

7.5 分级管理措施审核

应审核数据处理者是否根据数据级别，采取与其重要程度相适应的安全保护措施，包括但不限于匿名化、备份、加密、访问控制及对相关数据处理环境的安全防护。

7.6 最小授权原则审核

应审核组织是否依据最小授权原则设定数据访问与操作权限，并采取技术措施防止越权行为。

7.7 重要及核心数据管控审核

针对重要数据和核心数据，应审核是否实施了严格的权限管控、安全审计与操作留痕机制，以实现权限的最小化控制。

8 数据资产全生命周期合规审核

8.1 数据资产梳理与识别

数据资产梳理是数据资产入表的前提基础，旨在全面掌握组织内部数据资产的总体状况、分布、来源与价值，为后续的数据资产确认、合规审核、计量与报告提供依据。

8.2 数据收集环节审核

8.2.1 数据来源合法性

针对数据来源合法性，应重点审核内容如下：

a) 应审核数据收集方式是否符合法定情形，包括：收集个人信息是否已获得个人同意或属于履行法定职责、法定义务范畴；收集个人信息是否为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；是否为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；外部授权使用数据时，数据使用范围与权限是否符合授权协议约定；通过公开渠道收集数据时，数据获取手段是否合法合规，未违反 Robots 协议等公认规范，且该公开数据未附有禁止商业化利用等限制性声明；

b) 禁止通过欺诈、诱骗、胁迫等方式收集数据，或从非法渠道购买数据；

c) 除非有法律规定的合法性根据，收集敏感个人信息需取得个人信息主体的单独同意；收集不满十四周岁未成年人信息需取得未成年人的父母或其他监护人同意；

d) 不应基于任何违反法律法规规定的目的收集数据，不应利用所收集的数据从事任何违反法律法规的行为。

8.2.2 数据收集必要性

收集的数据应与处理目的直接相关，且采取最小必要原则。未经明确授权，不得收集与所提供产品或服务无关的数据。

8.2.3 收集个人信息的告知义务

针对收集个人信息的告知义务，应重点审核内容如下：

a) 收集个人信息前，应向个人信息主体告知数据处理者的名称/姓名和联系方式、处理目的、处理方式、个人信息种类、保存期限以及个人行使权利的方式和程序；

b) 在收集敏感个人信息前，采用单独弹窗、短信、填写框、动画、转至单独提示界面和语言播报等方式向个人进行告知，不得仅采取概括授权方式获得个人同意；告知内容除涵盖 a)项规定事项外，还应包括处理敏感个人信息的必要性以及对个人权益的影响；

c) 个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则；

d) 如数据处理者就本条 a）、b）及 c）款规定事项发生变更的，应当将变更部分告知个人；

e) 个人信息处理者通过制定个人信息处理规则的方式告知本条 a）、b）及 c）款事项的，处理规则应当公开，并且便于查阅和保存。

f） 数据处理者的告知方式需显著、清晰、易懂。
g） 有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知本条 a）、b）及 c）款事项。

8.3 数据存储环节审核

8.3.1 存储期限

针对存储期限，应重点审核内容如下：
a） 应审核数据存储期限是否为实现处理目的所必需的最短时间。对于个人信息，存储期限应符合告知内容及相关法律规定；对于通过授权获得的数据，存储期限应符合协议约定；
b） 存储期限届满、数据提供者撤回授权或提出删除等情形下是否及时对数据做删除或停止除存储和采取必要安全措施之外的其他处理。

8.3.2 数据存储适当性

针对数据存储适当性，应重点审核内容如下：
a） 数据存储安全策略和操作规程的建设落实情况；
b） 存储位置、期限、方式的适当性。

8.3.3 逻辑存储安全

针对逻辑存储安全情况，应重点审核内容如下：
a） 数据库的账号权限管理、访问控制、日志管理、加密管理、版本升级等方面要求的落实情况；
b） 检测逻辑存储系统安全漏洞，查看安全漏洞修复、处置情况；
c） 实施限制数据库管理、运维等人员操作行为的安全管理措施情况；
d） 脱敏后的数据与可用于恢复数据的信息分开存储的情况；
e） 对敏感个人信息、重要数据进行加密存储情况及加密措施有效性；
f） 数据存储在第三方云平台、数据中心等外部区域的安全管理、访问控制情况；
g） 根据安全级别、重要性、量级、使用频率等因素，对数据分域分级差异化存储安全管控情况；
h） 重要数据和核心数据存储的防勒索应对机制情况。

8.3.4 存储介质安全

针对存储介质安全情况，应重点审核内容如下：
a） 存储介质（含移动存储介质）的使用、管理及资产标识情况；
b） 存储介质安全管理规范建设情况，是否明确对存储介质存储数据的安全要求；
c） 对存储介质进行定期或随机性安全检查情况；
d） 存储介质访问和使用行为的记录和审计情况。

8.3.5 备份与恢复

针对数据备份恢复情况，应重点审核内容如下：
a） 数据备份恢复策略和操作规程的建设落实情况；
b） 数据备份的方式、频次、保存期限、存储介质等情况；
c） 提供本地或异地数据灾备功能情况；
d） 定期开展数据备份恢复工作情况；

e) 备份和归档数据访问控制措施的有效性；
f) 定期采取必要的技术措施查验备份和归档数据完整性和可用性情况；
g) 定期开展灾难恢复演练情况。

8.4 数据传输环节审核

8.4.1 传输链路安全性

针对数据传输链路安全性，应重点审核内容如下：
a) 数据传输安全策略和操作规程的建设落实情况；
b) 敏感个人信息和重要数据传输加密情况及加密措施有效性，是否选用安全的密码算法；
c) 个人信息和重要数据传输进行完整性保护情况；
d) 数据传输通道部署身份鉴别、安全配置、密码算法配置，密钥管理等防护措施情况；
e) 数据传输、接收记录和安全审计情况；
f) 采取安全传输协议等安全措施情况；
g) 数据异常传输检测发现及处置情况；
h) 制定数据跨主体传输管理规则，以及跨主体数据传输安全技术措施建立情况。

8.5 数据使用和加工环节审核

8.5.1 数据使用和加工合法性

针对数据使用和加工合法性情况，应重点审核内容如下：
a) 使用和加工数据时，遵守法律、行政法规，尊重社会公德和伦理，遵守商业道德和职业道德等情况；
b) 是否存在危害国家安全、公共利益的数据使用和加工行为，损害个人、数据处理者合法权益的数据使用和加工行为；
c) 是否制作、发布、复制、传播违法信息；
d) 应用算法推荐技术、深度合成技术提供互联网信息服务、生成式 AI 技术提供服务的，是否按照互联网信息服务相关法律法规及监管规定开展相关工作。

8.5.2 数据正当使用

针对数据正当使用情况，应重点审核内容如下：
a) 数据使用加工安全策略和操作规程的建设落实情况；
b) 数据使用是否获得数据提供方、数据主体等相关方授权；
c) 数据使用行为与承诺或用户协议的一致性；
d) 开展数据处理活动以及研究开发数据新技术，是否有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理；
e) 使用数据开展用户画像、信息推送、内容呈现等业务，造成用户受不公平的价格待遇、平台公共竞争秩序受到影响、平台内劳动者正当权益受到损害等风险情况；
f) 数据使用加工目的、方式、范围，与行政许可、合同授权等的一致性；
g) 是否存在个人信息和重要数据滥用情况。

8.5.3 数据导入导出

针对数据导入导出情况，应重点审核内容如下：

a) 数据导出安全评估和授权审批流程建设情况；
b) 导入导出审计策略和日志管理机制建设情况；
c) 导出权限管理、导出操作记录情况；
d) 导出数据的存储介质的标识、加密、使用、销毁管理情况；
e) 定期对个人信息和重要数据导出行为进行安全审计情况；
f) 对导入数据的格式、安全性和完整性校验情况。

8.5.4 数据处理环境

针对数据处理环境安全情况，应重点审核内容如下：

a) 数据处理环境设置身份鉴别、访问控制、隔离存储、加密、脱敏等安全措施情况；
b) 大数据平台等处理组件按照基线要求进行安全配置、配置核查情况；
c) 处理环境中的安全漏洞情况，已发现漏洞的处置情况。

8.5.5 数据使用和加工安全措施

针对数据使用和加工安全措施情况，应重点审核内容如下：

a) 在数据清洗、转换、建模、分析、挖掘等加工过程中，对数据特别是个人信息和重要数据的保护情况；
b) 数据防泄露措施建设情况；
c) 数据使用加工过程中采取的数据脱敏、水印溯源、加密存储等安全保护措施情况；
d) 数据访问与操作行为的最小化授权、访问控制、审批等管理情况；
e) 数据使用权限管理情况，如是否存在未授权访问，超范围授权，权限未及时收回，特权账号设置不合理等情况；
f) 数据加工过程中对个人信息、重要数据等敏感数据的操作行为记录、定期审计情况；
g) 高风险行为审计及回溯工作开展情况；
h) 委托加工数据的，是否明确约定受托方的安全保护义务，并采取技术措施或其他约束手段防止受托方非法留存、扩散数据。

8.6 数据提供环节审核

8.6.1 数据提供合法正当必要性

针对数据提供合法正当必要性，应重点审核内容如下：

a) 提供、委托处理、共同处理数据，以及数据接收方处理数据的目的、方式，范围等是否合法、正当、必要；
b) 数据接收方的诚信、守法等情况；
c) 数据提供是否遵守法律法规和监管政策要求，是否存在非法买卖、提供他人个人信息或重要数据行为；
d) 对外提供的个人信息和重要数据范围，应遵循最小必要原则。对外提供个人信息的，数据接收方、数据种类等应与向个人信息主体告知的隐私政策、用户协议一致；重要数据的对外提供，应符合数据安全相关法律法规的规定。

8.6.2 数据提供管理

针对数据提供管理情况，应重点审核内容如下：

a) 数据提供安全策略和操作规程的建设落实情况；
b) 数据对外提供的，组织是否有落实内部审批机制及审批情况；
c) 对外提供数据前，数据安全风险评估情况和个人信息保护影响评估情况；
d) 签订合同协议情况，是否在合同协议中明确了处理数据的目的、方式、范围、数据安全保护措施、安全责任义务及罚则；以及协议中是否有限制数据的再次对外提供；与数据接收方订立或者拟订立的相关合同中关于数据安全的要求能否有效约束数据接收方履行数据安全保护义务；
e) 开展共享、交易、委托处理、向境外提供数据等高风险数据处理活动前的安全评估情况；
f) 监督数据接收方到期返还、删除数据的情况；
g) 向境外执法机构提供境内数据的情况；
h) 核心数据跨主体流动前是否经过国家有关部门评估。

8.6.3 数据提供技术措施

针对数据提供技术措施情况，应重点审核内容如下：

a) 对外提供的敏感数据是否进行加密及加密有效性；
b) 对所提供数据及数据提供过程的监控审计情况；
c) 对外提供数据时采取签名、添加水印、脱敏等安全措施情况；
d) 跟踪记录数据流量、接收者信息及处理操作信息情况，记录日志是否完备、是否能够支撑数据安全事件溯源；
e) 数据提供、委托处理、共同处理的安全保障措施及有效性，采取或者拟采取的技术和管理措施等能否有效防范数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险；
f) 多方安全计算、联邦学习等技术应用安全情况。

8.6.4 数据接收方

针对数据接收方，应重点审核内容如下：

a) 数据接收方的诚信状况、违法违规等情况；
b) 数据接收方处理数据的目的、方式、范围等的合法性、正当性、必要性；
c) 接收方是否承诺具备保障数据安全的管理、技术措施和能力并履行责任义务；
d) 是否考核接收方的数据保护能力，掌握其发生的历史网络安全、数据安全事件处置情况；
e) 对接收方数据使用、再转移、对外提供和安全保护的监督情况。

8.6.5 数据转移安全

针对因合并、分立、解散、被宣告破产等原因向外转移数据，或承接其他数据处理者转移数据等场景，应重点审核内容如下：

a) 是否向有关主管部门报告；
b) 是否制定数据转移方案；
c) 接收方数据安全保障能力，是否满足数据转移后数据接收方不降低现有数据安全保护水平风险；
d) 没有接收方的，对相关数据删除或停止除存储和采取必要安全措施外的处理的情况。

8.6.6 数据出境安全

针对数据出境安全，应重点审核内容如下：

a) 数据出境场景梳理是否合理、完整，是否覆盖全部业务场景和产品类别；
b) 出境线路梳理是否合理、完整，是否覆盖公网出境、专线出境等情形；
c) 涉及个人信息或重要数据出境的，按照有关规定开展数据出境安全评估、个人信息保护认证、个人信息出境标准合同签订的情况；
d) 针对公网出境场景，监测核查实际出境数据是否与申报内容一致。

8.7 数据公开环节审核

8.7.1 数据公开适当性

针对数据公开适当性，应重点审核内容如下：

a) 数据公开目的、方式、范围的适当性；
b) 数据公开目的、方式、方位与行政许可、合同授权的一致性；
c) 公开的数据内容与法律法规要求的符合程度；
d) 对公开的数据进行必要的脱敏处理、数据水印、防爬取、授权控制情况；
e) 应评估数据公开可能引发的衍生风险，包括基于已公开数据结合其他信息推断出未公开的敏感信息、关联信息，以及对国家安全、公共利益或组织合法权益造成损害的风险。

8.7.2 数据公开管理

针对数据公开管理情况，应重点审核内容如下：

a) 数据公开的安全制度、策略、操作规程和审核流程的建设落实情况；
b) 数据公开的条件、审批程序，涉及重大基础设施的信息公开是否经过主管部门批准，涉及个人信息公开是否取得个人单独同意；
c) 因法律法规、监管政策的更新，对不宜公开的已公开数据的处置情况；
d) 对公开数据是否采取脱敏处理、防爬取、数字水印等控制措施。

8.8 数据删除环节审核

8.8.1 数据删除管理

针对数据删除管理，应重点审核内容如下：

a) 数据删除流程和审批机制的建设落实情况；
b) 数据删除安全策略和操作规程，是否明确数据销毁对象、原因、销毁方式和销毁要求及对应操作规程；
c) 是否按照法律法规、合同约定、隐私政策等及时删除数据；
d) 委托第三方进行数据处理的，是否在委托结束后监督第三方删除或返还数据；
e) 数据删除有效性、彻底性验证情况，以及可能存在的多副本同步删除情况；
f) 是否明确数据存储期限，并于存储期限到期后按期删除数据或停止除存储和采取必要安全措施之外的处理，明确不可删除数据的类型及原因；
g) 缓存数据、到期备份数据的处理情况。

9 数据资产管理制度与技术措施审核

9.1 制度建设

应审查是否建立数据资产管理制度，包括：

a) 是否建立覆盖数据全生命周期的数据资产管理制度，包括数据分级分类、安全保护、风险评估、应急处置等；
b) 数据资产管理制度是否明确责任部门及岗位职责。

9.2 技术措施

针对技术措施，应重点审核内容如下：

a) 网络安全防护：主要包括网络资源管理、网络隔离、边界防护等；
b) 身份鉴别与访问控制：主要包括身份鉴别、访问控制、授权管理等；
c) 监测预警：主要包括安全监测预警和信息报告机制的建设落实、异常行为监测指标建设等；
d) 数据脱敏：主要包括数据脱敏规则、脱敏方法和脱敏数据的使用限制等；
e) 数据防泄露：主要包括数据防泄露技术手段部署、数据防泄露技术措施有效性等；
f) 数据接口安全：主要包括对外接口安全、接口安全控制等；
g) 数据备份恢复：主要包括数据备份恢复策略和操作规程的建设落实情况、数据灾备、数据备份、恢复等。

参 考 文 献

[1] 中华人民共和国数据安全法[Z]. 2021-06-10.

[2] 中华人民共和国网络安全法[Z]. 2016-11-07.

[3] 中华人民共和国个人信息保护法[Z]. 2021-08-20.

[4] 工业和信息化部. 工业和信息化领域数据安全管理办法（试行）[EB/OL]. (2022-12-08)[2025-12-11].

[5] 工业和信息化部. 工业和信息化领域数据安全事件应急预案（试行）[EB/OL]. (2023-11-23)[2025-12-11].