《检测实验室数字化管理系统建设规范》

编制说明

《检测实验室数字化管理系统建设规范》编制组

2026 年 2 月

《检测实验室数字化管理系统建设规范》
编制说明

1.任务来源

《检测实验室数字化管理系统建设规范》的任务来源是由中国智慧工程研究会批准立项，由扬州市生态环境监测监控中心、乌鲁木齐市疾病预防控制中心（乌鲁木齐市卫生监督所）、赣州市综合检验检测院、重庆市疾病预防控制中心（重庆市预防医学科学院）、上海机动车检测认证技术研究中心有限公司河南分公司、江苏叁山生态环境发展有限公司、扬州润达交通工程质量检测有限公司、大玮检测科技有限公司、云南华测检测认证有限公司、舒兰市农产品质量安全监督检测中心、襄阳市公共检验检测中心、舜泰检测科技集团有限公司、丽水市质量检验检测研究院等单位起草编制。

2.目的意义

本文件的制定旨在适应检测实验室管理由传统纸质与分散式台账向数字化、集成化和智能化转型的行业发展需求，针对实验室在样品流转、检验检测过程控制、数据记录与追溯、质量体系运行以及资源统筹管理等方面普遍存在的信息孤岛、流程割裂、数据一致性不足和风险预警滞后等问题，提出统一的数字化管理系统建设要求。随着检测任务规模增长、项目类型复杂化以及监管与合规要求持续强化，实验室数字化建设不再局限于信息系统“上线”，而是需要形成覆盖人员、设备、方法、样品、环境、数据与报告的全流程管控能力。本文件通过规范系统总体架构、功能模块、数据标准、接口集成与安全控制要求，推动实验室管理从“事后记录”向“过程受控”、从“人工核对”向“系统校验”转变，从而提升检测数据的真实性、完整性与可追溯性，降低管理成本与差错风险，增强实验室质量管理能力和服务能力。

3.编制思路和原则

3.1.编制思路

本文件在编制思路上坚持以质量管理体系要求与业务流程重构为主线，围绕

检测实验室全生命周期业务链条，构建“需求分析—架构设计—模块建设—数据治理—集成联通—验证验收—运行运维”的系统建设路径。内容组织强调以样品管理为核心主线贯穿委托受理、任务下达、方法选择、检验检测实施、数据采集与审核、报告编制与发放、留样与归档等环节，同时将设备管理、人员资质与培训、耗材与试剂管理、环境监测、质量控制与不符合项管理、能力验证与内审管理等管理要素纳入统一平台，实现业务与质量管理一体化。系统建设方法突出标准化与可配置性并重，在统一数据口径、流程节点与权限控制的基础上，兼顾不同实验室规模、专业领域与管理模式差异，通过可配置流程、参数化规则与灵活报表能力保证系统落地可行，并通过接口与数据交换机制实现与仪器数据采集系统、电子签名、财务与采购、人力资源以及监管平台等外部系统的协同联动。

3.2.编制原则

本文件的编制遵循合规性、可靠性与可追溯性原则，强调数字化管理系统应能够支撑实验室相关法律法规、质量体系要求与监督管理要求的落实，确保数据链路完整、审计轨迹清晰、权限边界明确；遵循真实性与完整性保障原则，强调对原始记录、关键参数与结果数据的防篡改控制、版本管理、留痕审计与备份恢复机制，避免“系统化失真”；遵循安全性与分级防护原则，结合实验室数据的敏感性和业务重要性，提出身份鉴别、访问控制、网络隔离、加密传输、漏洞管理与应急响应等要求，确保系统在网络化运行环境下具备必要的安全韧性；遵循适用性与可实施性原则，强调系统建设应与实验室业务流程相匹配，避免脱离现场实际导致重复录入或“系统外运行”；同时遵循扩展性与可持续运维原则，强调系统架构与数据标准应支持未来业务扩展、仪器接入、算法应用与监管对接，并通过运维机制保障系统长期稳定运行。

4.编制过程

本标准修订讨论会均采用线上征集专家意见的形式，线上会议共计 2 次，会议期间广泛听取专家意见，并形成意见汇总表。

5.内容修订说明

本次修订主要围绕提升系统建设要求的可落地性与数据治理深度进行了完

善。修订中进一步明确了系统总体架构与功能边界，强化了样品全流程闭环管理、关键节点审核机制与质量控制规则的表达，使业务过程受控要求更具可执行性；对数据标准与接口集成要求进行了细化，突出统一编码体系、主数据管理、数据校验规则与跨系统一致性控制，减少信息孤岛与重复录入带来的差错风险；对电子签名、审计追踪与数据防篡改机制的要求进行了强化，确保关键数据可追溯、可复核、可审计；同时，结合实验室数字化应用的发展趋势，修订中完善了系统安全防护、备份容灾与应急恢复要求，并强化了上线验证、验收测试与运行评估相关内容，使系统建设从“功能交付”升级为“能力交付”，进一步支撑实验室高质量、合规化与精益化管理目标的实现。

ICS 35.240.99
CCS A 40

T/WEA

团　　体　　标　　准

T/WEA XXXX—2026

检测实验室数字化管理系统建设规范

Specification for construction of digital management systems for testing laboratories

（征求意见稿）

2026－XX－XX 发布　　2026－XX－XX 实施

中国智慧工程研究会　　发 布

目　　次

前言 III
引言 V
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　总体建设原则 2
5　系统总体架构与部署要求 4
6　功能要求 5
7　数据管理与接口要求 7
8　信息安全与权限控制要求 9
9　实施与验收要求 11
10　运行维护与持续改进要求 13

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。

本文件由中国智慧工程研究会提出并归口。

本文件起草单位：

本文件主要起草人：

引　言

随着信息技术、网络技术和数据技术的快速发展，检测实验室在质量管理、技术运行、资源配置和风险控制等方面正面临由传统管理模式向数字化、信息化、智能化管理模式转型的迫切需求。检测实验室作为保障产品质量、安全生产、生态环境、公共健康和工程建设质量的重要技术支撑机构，其管理活动具有业务流程复杂、数据类型多样、合规要求严格、可追溯性要求高等特点，传统以人工记录、分散系统或局部信息化为主的管理方式，已难以满足现代检测活动对效率、准确性、透明性和持续改进的要求。

在检测活动全生命周期中，样品受理、任务分配、检测实施、数据采集、结果计算、报告编制、质量控制、设备管理、人员管理以及档案留存等环节高度关联，任何环节的信息缺失、传递滞后或数据失真，均可能对检测结果的可靠性、公正性和可追溯性产生不利影响。数字化管理系统通过对检测实验室业务流程、管理要素和数据资源的系统化整合，可实现信息的集中采集、统一存储、自动处理和规范流转，有助于提升检测活动的规范性、一致性和运行效率，是推动检测实验室管理能力现代化的重要技术基础。

近年来，检测实验室在实验室信息管理系统、设备管理系统、质量管理系统等方面开展了不同程度的信息化建设，但在系统架构设计、功能模块划分、数据标准统一、业务流程协同、安全与权限控制以及系统运行维护等方面仍存在建设水平参差不齐、技术路线不统一、系统兼容性不足等问题。一些系统重功能实现、轻整体规划，重业务操作、轻管理支撑，未能充分体现检测实验室在合规管理、质量风险控制和持续改进方面的实际需求，影响了数字化建设成效的充分发挥。

在国家推动数字经济发展、加强质量基础设施建设和提升检验检测服务能力的大背景下，检测实验室数字化管理系统建设亟需形成统一、规范、可操作的技术和管理要求，对系统建设目标、总体架构、功能配置、数据管理、安全保障和运行维护等内容作出明确规定，以引导检测实验室科学开展数字化建设工作，避免重复建设和资源浪费，提升系统建设的整体性和前瞻性。

本文件在系统梳理检测实验室管理特点和数字化建设实践经验的基础上，结合检测实验室在质量管理、技术管理和运行管理等方面的共性需求，对检测实验室数字化管理系统建设提出通用性、规范性要求，旨在为检测实验室开展数字化管理系统规划、建设、实施和持续优化提供统一依据。通过本文件的实施，可促进检测实验室管理模式转型升级，提升检测活动全过程信息化、规范化和可追溯水平，为检测结果的科学性、公正性和权威性提供有力支撑。

检测实验室数字化管理系统建设规范

1 范围

本文件规定了检测实验室数字化管理系统建设的总体建设原则、系统总体架构与部署要求、功能要求、数据管理与接口要求、信息安全与权限控制要求、实施与验收要求及运行维护与持续改进要求等内容。

本文件适用于开展检验检测活动的各类检测实验室（包括但不限于企业内部实验室、第三方检验检测机构实验室、科研与高校实验室中承担检测任务的实验室）在新建、改建或升级检测实验室数字化管理系统时的规划、设计、开发（或选型）、实施、验收及运行维护等工作；亦适用于检测实验室对既有信息化系统进行整合、数据治理和能力提升的建设活动。

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 19001 质量管理体系　要求

GB/T 22239 信息安全技术　网络安全等级保护基本要求

GB/T 27025 检测和校准实验室能力的通用要求

GB/T 35273 信息安全技术　个人信息安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

检测实验室 testing laboratory

依法开展检验、检测或校准活动，具备相应技术能力、管理体系和资源条件，对样品或对象实施检测并出具检测数据、结果或报告的组织或其内部技术单元。

3.2

数字化管理系统 digital management system

基于信息技术对检测实验室管理活动和技术活动进行统一支撑，实现业务流程数字化、管理过程信息化、数据资源集中化和运行状态可视化的软件系统与技术平台的统称。

3.3

实验室信息管理系统 laboratory information management system

用于支撑检测实验室样品管理、检测任务管理、数据采集与处理、报告生成及追溯管理的核心信息系统，通常作为实验室数字化管理系统的重要组成部分。

3.4

检测业务流程 testing workflow

围绕检测任务实施而形成的，从样品受理、检测实施、结果计算到报告出具和归档的全过程活动及其顺序关系。

3.5

检测数据 testing data

在检测活动中产生或使用的，与样品、检测方法、检测过程和检测结果相关的原始记录、过程数据和结果数据的集合。

3.6

数据可追溯性 data traceability

检测数据能够沿着时间顺序和业务流程，追溯其来源、处理过程、责任主体和使用结果的特性。

3.7

权限控制 access control

依据用户角色、岗位职责和授权规则，对系统功能访问、数据查看、数据修改和操作行为进行限制和管理的机制。

3.8

电子记录 electronic record

在检测实验室数字化管理系统中以电子形式形成、存储和管理的，与检测活动或管理活动相关的信息记录。

3.9

电子签名 electronic signature

用于识别签署人身份并表明其对电子记录或电子文件内容认可的电子数据。

4 总体建设原则

4.1 规划先行原则

检测实验室数字化管理系统建设应与实验室发展规划、业务范围、能力建设目标和管理体系要求相一致，应开展现状调研与需求分析，形成总体建设方案与实施路线，明确建设范围、建设边界、阶段目标、资源投入、风险控制措施及验收评价方式。

4.2 过程支撑与体系一致原则

系统建设应覆盖检测业务全流程关键环节，并应与实验室质量管理体系运行要求保持一致，应支持组织架构、岗位职责、授权签字、文件控制、记录控制、内部审核、管理评审、不符合工作控制、纠正措施等管理活动的信息化落地与证据留存。

4.3 数据统一与可追溯原则

系统建设应建立统一的数据模型、数据字典和编码规则，应实现样品、任务、方法、设备、人员、环境、原始记录、计算过程、结果数据、报告与归档信息之间的关联关系，应保证数据在形成、传递、处理、审核、批准、发布和归档全过程可追溯、可核查、可审计。对关键数据应支持版本管理与变更记录，确保任何修改均可追踪到责任主体、修改时间、修改原因及影响范围。

4.4 合规性与风险控制原则

系统建设应满足相关法律法规、监管要求及实验室适用的认可/评审要求，应识别并控制数字化运行风险，至少应覆盖数据完整性风险、权限滥用风险、记录篡改风险、接口数据失真风险、系统中断风险和信息泄露风险。系统应支持质量控制活动的计划、实施、判定与处置记录管理，并应具备对关键过程节点的强制控制能力。

4.5 安全可控与最小授权原则

系统建设应落实信息安全与数据安全要求，应建立基于角色的权限控制机制并执行最小授权原则，应对用户身份、认证方式、访问控制、操作审计、敏感数据保护、备份与恢复等提出明确配置要求。涉及个人信息、商业秘密或受限数据的处理，应采取相应的脱敏、加密、隔离或访问审批等控制措施。

4.6 开放兼容与可扩展原则

系统建设应采用模块化、组件化设计，应支持与仪器设备、办公系统、财务/采购系统、平台系统及外部监管平台的数据交换与接口对接。系统应提供标准化接口能力并支持接口管理、调用鉴权与接口日志审计，确保系统具备可扩展、可演进和可维护能力。

4.7 易用性与可靠性原则

系统建设应满足岗位作业便利性与操作一致性要求，应支持移动端或现场作业终端的适配需求。系统应具备稳定运行能力，应明确性能指标、并发能力、容灾与恢复目标，并应提供运行监控、告警、故障定位与应急处置支撑，保障业务连续性。

5 系统总体架构与部署要求

5.1 架构总体要求

系统应采用分层、模块化架构设计，宜包括表现层、业务服务层、数据层以及支撑保障层；支撑保障层宜包括统一身份认证、权限管理、日志审计、接口管理、消息与任务调度、配置管理、运行监控等通用能力。

系统应支持按业务域解耦部署与按模块独立扩展，关键业务模块应具备故障隔离能力。

系统应支持功能扩展、版本升级与在线维护，升级过程不应破坏既有数据完整性与可追溯性。

5.2 部署模式要求

系统可采用本地部署、私有云部署或混合云部署。涉及受限数据、敏感数据或有专门监管要求的业务场景，应采用满足合规要求的部署模式，并应明确数据存储位置、访问边界与安全控制措施。

系统部署应具备环境隔离能力，至少应区分生产环境、测试环境与开发/验证环境；生产环境与非生产环境之间应进行访问隔离，非生产环境不应使用真实敏感数据，确需使用时应采取脱敏或等效保护措施。

系统应支持多实验室、多场地或多分支机构的统一部署与分级管理，且应满足跨场地访问的安全控制要求。

5.3 网络与基础环境要求

系统应在满足安全策略的前提下支持局域网访问与经授权的广域网/远程访问；远程访问应采用安全通道并进行强身份认证。

系统应明确服务器、存储、网络设备与终端设备的配置要求，容量规划应覆盖业务增长、数据增长与峰值并发需求。

系统应支持与实验室仪器设备、采集终端、打印与扫描设备等基础设施的互联互通，且应保证连接稳定性与数据传输完整性。

5.4 性能与容量要求

系统应确定性能指标，至少应包括响应时间、吞吐能力、并发用户数、任务处理能力与批量数据处理能力等。

系统应根据检测业务量、样品量、原始数据规模与留存年限进行容量规划，应明确数据库容量、文件存储容量与日志容量，并应预留扩展空间。

系统应支持关键操作的性能保障机制，关键业务环节在峰值业务期间不应出现影响正常运行的明显性能退化。

5.5 高可用与业务连续性要求

系统应具备业务连续性保障能力，应明确可用性目标、故障恢复策略与应急处置流程。

系统应配置备份机制，至少应包括数据库备份与文件数据备份；备份应定期校验可用性，并应按规定开展恢复演练。

系统应具备容灾或冗余能力，关键业务模块宜采用主备、集群或等效机制；发生硬件故障、软件故障或误操作时，应能够在规定时间内恢复关键业务与关键数据。

5.6 时间一致性与记录可信要求

系统应采用统一时间源进行时间同步，关键业务记录、审计日志与电子签名相关记录应使用一致的时间基准。

系统应对关键记录形成、修改、审核、批准、发布与归档等操作生成不可抵赖的日志信息，日志内容应包含操作者身份、时间、对象、操作类型、前后变化信息及结果状态等要素。

系统应具备防篡改机制或等效控制措施，用于保障关键记录与关键日志的完整性与可信性。

5.7 配置与版本管理要求

系统应具备配置管理能力，应对基础数据、业务规则、模板、计算公式、接口参数、权限策略等关键配置进行版本控制。

系统应记录配置变更历史，变更应可追溯到变更发起人、审批人、变更时间、变更原因及影响范围；对影响检测结果或报告输出的变更，应执行评估与验证。

系统上线与升级应执行变更控制，升级前应进行验证，升级后应保留升级记录与验证证据。

6 功能要求

6.1 功能设置总体要求

检测实验室数字化管理系统应围绕检测业务全过程和实验室管理活动进行功能配置，应覆盖检测任务执行所必需的核心业务功能，并应对质量管理、资源管理和运行监控提供有效支撑。

系统功能设置应与实验室业务规模、检测领域和管理复杂程度相适应，应避免功能缺失影响业务合规运行，亦应避免过度配置造成系统复杂化和使用负担。

6.2 核心业务功能要求

系统应具备对样品、检测任务和检测过程的全过程管理能力，应支持从委托受理到报告归档的闭环运行。

系统应支持检测数据的采集、处理、审核和结果输出，应能够关联检测方法、设备、人员和环境条件信息。

系统应支持检测报告的生成、审核、批准、发布和归档管理，应确保报告内容与检测数据一致，并满足可追溯要求。

6.3 管理支撑功能要求

系统应支持实验室质量管理活动的信息化实施，应对文件控制、记录控制、不符合工作、纠正措施、内部审核和管理评审等活动提供功能支撑。

系统应支持设备、计量器具、人员能力和耗材等资源的管理，应能够反映资源状态与使用情况，并为检测活动提供约束或提示。

系统应支持对实验室运行状态的统计分析和综合展示，为管理决策提供数据依据。

6.4 功能模块划分

检测实验室数字化管理系统宜按业务域划分功能模块，各功能模块之间应数据关联、逻辑清晰、接口明确。典型功能模块及其主要功能见表1。

表1 检测实验室数字化管理系统主要功能模块

模块类别	模块名称	主要功能说明
检测业务模块	样品与委托管理	委托登记、样品编号、流转状态管理、受理信息记录
检测业务模块	任务与过程管理	任务分配、检测进度控制、过程节点记录
数据管理模块	数据采集与计算	原始数据录入、自动采集、计算与结果生成
输出管理模块	报告管理	报告模板管理、编制、审核、批准与发布
质量管理模块	质量控制	文件控制、不符合工作、纠正措施记录
资源管理模块	设备与人员管理	设备状态、校准信息、人员资质与授权管理
支撑管理模块	档案与追溯	电子记录归档、版本管理与追溯查询
决策支持模块	统计分析与展示	业务统计、质量分析、运行状态可视化

6.5 功能协同与流程一致性要求

各功能模块之间应通过统一的数据模型实现协同运行，避免重复录入和数据孤岛。

系统应确保业务流程与管理流程的一致性，功能跳转、状态变化和权限控制应符合既定流程逻辑，不应允许绕过关键控制节点。

6.6 功能逻辑关系示意

检测实验室数字化管理系统各功能模块之间的逻辑关系宜形成清晰的分层与协同结构，其典型逻辑关系示意如图1所示。

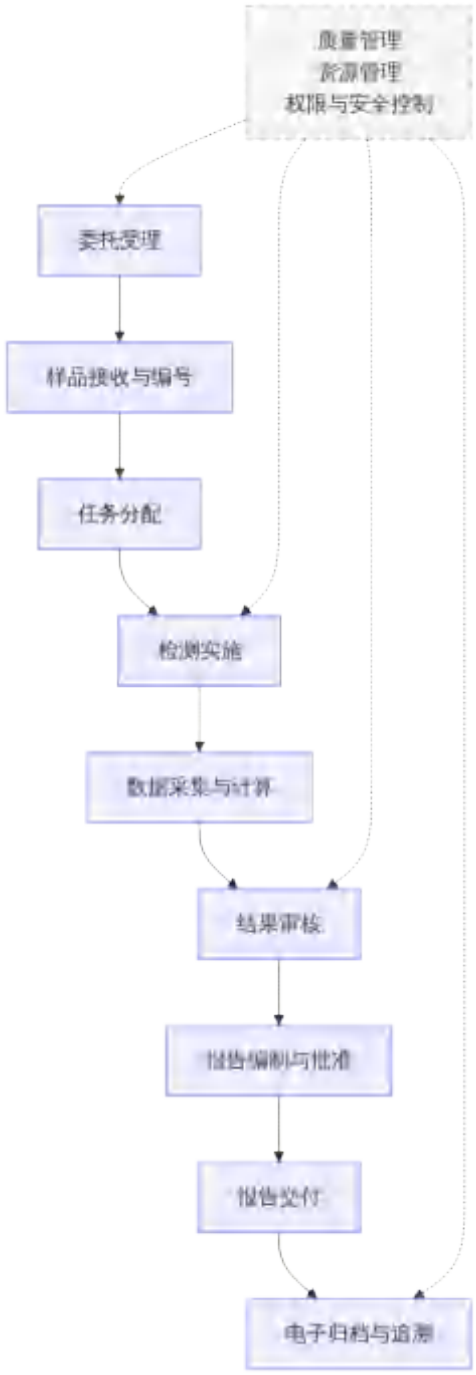

图1　检测实验室数字化管理系统业务流程示意图

7　数据管理与接口要求

7.1　总体要求

系统应建立统一的数据管理机制，应覆盖数据定义、数据采集、数据处理、数据存储、数据使用、数据共享、数据归档与数据销毁等环节。系统应保证检测数据在形成、传递、处理、审核、批准、发布与归档全过程的完整性、准确性、一致性与可追溯性。

系统应对关键数据对象建立唯一标识并形成关联关系，关键数据对象至少应包括委托信息、样品信息、检测任务信息、检测方法信息、设备信息、人员信息、环境条件信息、原始记录、计算过程、结果数据、报告文件、审核批准记录及归档信息。

7.2 数据模型与数据字典

系统应建立数据模型，明确核心业务对象、属性、状态及其关系，数据模型应支持对样品—任务—过程—数据—报告—归档链路的关联表达。

系统应建立数据字典与编码规则，并应对编码的生成规则、位数长度、可读性要求和唯一性要求作出规定。数据字典至少应覆盖样品编号、任务编号、报告编号、设备编号、人员编号、方法编号、部门/岗位编码、状态码、异常/不符合分类码等。

系统的数据字典与编码规则应支持扩展，扩展不应破坏既有数据的一致性与可追溯性；涉及跨系统交换的编码规则应保持稳定，并应具备版本管理能力。

7.3 数据采集与数据质量控制

系统应支持检测数据的电子化采集与管理，原始记录应以电子记录形式存储或以电子化方式实现等效管理。

系统应对数据采集方式进行控制，数据采集方式可包括人工录入、文件导入、接口采集、仪器直连采集等；对可能影响结果准确性的采集方式应设置校验规则与审核要求。

系统应具备数据质量控制能力，至少应包括必填项校验、格式校验、逻辑一致性校验、范围/阈值校验、异常提示、重复数据识别等；对关键计算结果应支持复核与一致性检查。

系统应记录数据处理过程，涉及计算、换算、修约、统计或判定规则的，应保留计算依据、参数来源、计算版本及结果输出记录；自动计算与自动判定规则的变更应执行评估与验证并可追溯。

7.4 数据存储与留存

系统应明确结构化数据与非结构化数据（如附件、图像、谱图、原始文件、扫描件等）的存储方式，应保证数据可长期读取与可检索。

系统应规定数据留存期限与留存策略，应支持按业务类别、数据类型或监管要求进行差异化留存管理；对到期数据的处置应具备审批与记录机制。

系统应支持数据备份与恢复，备份策略应覆盖数据库、文件存储与关键配置；备份数据应采取访问控制措施，防止未授权访问与篡改。

7.5 数据权限、审计与防篡改

系统应对数据访问、数据修改、数据导出与数据删除实施权限控制，应实现按角色授权与最小授权。

系统应记录数据相关操作日志，日志应至少包含操作者身份、时间、对象、操作类型、结果状态及必要的前后变化信息；关键数据与关键记录的日志应具备防篡改能力或等效控制措施。

系统不应允许未授权的数据删除；确需删除或更正的，应执行审批并保留证据链，且应能追溯删除或更正的原因、责任主体与影响范围。

7.6 数据交换与接口管理

系统应具备接口管理能力，应支持与仪器设备、采集终端、报告签章系统、电子档案系统、质量管理系统以及必要的外部平台进行数据交换。

系统应采用标准化接口方式，接口宜支持基于服务的调用机制；接口应具备鉴权控制、访问频率控制、异常处理与调用日志记录能力。

系统应对接口数据交换内容进行约束，应明确字段含义、数据类型、单位、精度、编码规则与校验规则；接口应支持版本管理，接口变更应评估对业务与数据一致性的影响，并应保留变更记录。

7.7 外部数据共享与导出控制

系统应支持对外提供数据共享或数据导出能力，但应进行权限控制与审批控制；涉及敏感数据、受限数据或个人信息的数据共享与导出，应采取脱敏、加密或等效保护措施。

系统应对数据导出形成记录，应能追溯导出人、导出时间、导出范围、导出用途与导出结果；必要时应支持导出文件水印、有效期控制或访问追踪等措施。

8 信息安全与权限控制要求

8.1 总体要求

系统应建立覆盖系统全生命周期的信息安全控制体系，至少应包括身份认证、访问控制、数据安全、日志审计、安全配置、漏洞管理、备份恢复与应急处置等内容。系统的安全措施应与实验室业务风险、数据敏感等级和部署模式相适配，并应满足相关法律法规及管理要求。

系统应对数据进行分级分类管理，应识别敏感数据、受限数据、个人信息及关键业务数据，并据此配置差异化的访问控制、存储保护、传输保护和审计要求。

8.2 身份认证要求

系统应对所有用户实施身份识别与认证，未经认证的用户不应访问系统资源。

系统应支持基于账号口令的认证方式，并宜支持多因素认证；对具备高权限的用户、远程访问用户及涉及敏感数据访问的用户，应采用强认证机制。

系统应具备账户生命周期管理能力，应支持账户创建、启用、停用、注销及权限回收，并应与岗位变动、离职离岗等管理流程联动。

系统应限制认证失败重试次数，超过阈值时应采取锁定、延时或告警等控制措施；账户解锁应具备审批或授权机制并可追溯。

8.3 访问控制与授权模型要求

系统应采用基于角色的访问控制机制，并应支持按岗位、职责、组织层级和业务范围进行授权。

系统应执行最小授权原则，应仅授予用户完成岗位职责所必需的功能权限与数据权限，并应定期开展权限核查与清理。

系统应支持细粒度权限控制，应至少支持功能级、数据对象级与操作级权限控制；对报告批准、电子签名、数据更正、配置变更、接口管理等高风险操作，应实施强制授权与二次确认等控制。

系统应支持“职责分离”控制，对关键业务活动宜实现相互制约，至少应在检测实施、结果审核、报告批准等环节避免由同一用户完成全部关键步骤，确需例外时应保留审批与记录。

8.4 数据安全要求

系统应对数据存储与传输采取保护措施，涉及敏感数据、受限数据或个人信息的数据传输宜采用加密通道，存储宜采用加密或等效保护措施。

系统应对关键数据的更正、删除与覆盖进行限制，关键数据的更正应保留原值与新值、变更原因、变更时间、变更人及审批信息，并应可追溯。

系统应支持防篡改控制或等效机制，至少应对关键记录、关键日志、电子签名关联数据以及报告发布记录提供完整性保护。

系统应支持数据脱敏或掩码展示能力，对非必要岗位用户展示敏感字段时应进行脱敏处理。

8.5 日志审计要求

系统应具备安全审计能力，应记录用户登录、认证失败、权限变更、数据导出、关键数据修改、报告审核批准、电子签名、接口调用、系统配置变更及异常事件等日志。

审计日志应包含操作者身份、时间、来源地址或终端标识、操作对象、操作类型、结果状态等要素；对关键操作宜记录前后变化信息。

审计日志应具备防篡改能力或等效控制措施，日志留存期限应满足业务追溯与合规要求；日志的访问应受权限控制，非授权人员不应查看或导出审计日志。

系统应支持审计查询与审计报表输出，应支持按用户、时间、对象、事件类型等条件检索，并应支持异常行为分析与告警联动。

8.6 安全配置与漏洞管理要求

系统应提供安全基线配置能力，应对口令策略、会话超时、访问白名单/黑名单、密码强度、权限默认策略等进行统一配置。

系统应建立漏洞管理机制，应定期开展漏洞扫描、补丁评估与补丁更新；补丁更新应执行变更控制，更新前应验证兼容性，更新后应保留验证与发布记录。

系统应对第三方组件、开源组件或商业中间件进行版本管理，应识别组件风险并及时处置高危漏洞。

8.7 终端与运维安全要求

系统运维应实施分级授权与操作留痕，运维账号应与普通业务账号隔离，高权限运维操作应具备审批或双人复核等控制措施。

系统应限制管理接口暴露范围，管理接口不应直接暴露于不可信网络；远程运维应采用安全通道并记录完整审计日志。

系统应制定应急处置机制，应至少覆盖账号异常、权限滥用、数据泄露、系统中断与重大故障等场景，并应定期开展演练或验证。

8.8 备份恢复与安全事件处置要求

系统应制定备份策略并实施定期备份，备份数据应采取访问控制与完整性校验措施；备份介质或备份存储应具备安全防护能力。

系统应制定恢复策略并定期开展恢复演练，演练应形成记录并评估恢复效果；恢复过程不应破坏数据可追溯链。

系统应具备安全事件处置能力，应支持事件发现、告警、隔离、处置、取证与复盘；重大安全事件应形成事件报告与整改记录。

9 实施与验收要求

9.1 实施总体要求

系统实施应依据总体建设方案组织开展，应明确实施范围、实施计划、里程碑节点、职责分工、质量控制措施与风险控制措施。实施过程应进行记录管理，形成可追溯的实施证据。

系统实施宜采用分阶段实施策略，至少应包括需求确认、方案设计、系统配置/开发、联调测试、数据准备与迁移、培训与试运行、验收与上线等阶段；对关键业务模块的上线应设置回退方案。

9.2 需求确认与方案设计

实施前应开展需求确认，需求应覆盖业务需求、管理需求、合规需求与安全需求，并应形成需求规格说明或等效文件。需求变更应执行变更控制，应记录变更原因、影响分析、审批过程与实施结果。

方案设计应明确系统架构、功能模块、业务流程、数据模型、接口方案、权限模型、日志审计方案以及备份容灾方案等内容；涉及检测结果计算、判定规则与报告输出逻辑的，应明确规则来源与验证方法。

9.3 系统配置、开发与测试

系统配置或开发应与已确认需求一致，配置项与开发项应纳入版本管理。对影响业务规则、数据处理或报告输出的配置项，应形成配置清单并可追溯。

系统测试应覆盖功能测试、接口测试、权限测试、安全测试、性能测试与可靠性测试等内容；关键业务流程应进行端到端测试，并应覆盖异常场景与边界条件。

测试应形成测试计划、测试用例、测试记录与缺陷处置记录；缺陷修复后应进行回归测试并保留证据。

9.4 数据准备与迁移

涉及历史数据迁移的，应制定数据迁移方案，明确迁移范围、数据来源、数据映射关系、数据清洗规则、迁移校验方法与回退措施。

数据迁移应保证数据完整性与一致性，应对样品、任务、报告、设备、人员、方法等关键数据对象保持唯一标识与关联关系；迁移后的关键数据应进行抽样核查或全量校验，并形成校验记录。

历史电子文件或扫描件迁移时，应确保文件可读、可检索，并保留文件来源信息与迁移过程记录。

9.5 培训与试运行

系统上线前应组织用户培训，培训对象应覆盖系统管理员、质量负责人/授权人员、关键岗位用户及一般用户；培训内容应覆盖业务操作、权限规则、数据录入规范、异常处理与安全要求。培训应形成签到、课件、考核或等效记录。

系统应进行试运行，试运行期间应至少覆盖典型业务流程和关键控制点，试运行中发现的问题应闭环处置并形成记录；试运行通过后方可进入验收与正式上线。

9.6 验收条件与验收内容

系统验收应满足以下条件：需求与方案文件齐备，核心功能实现并通过测试，关键流程试运行验证通过，数据迁移（如适用）完成并校验合格，安全与权限策略配置完成并验证通过，运维与应急资料齐全。

验收内容应至少包括：

a）功能符合性：样品、任务、数据、报告、归档等核心业务功能符合需求且流程闭环；

b）数据与追溯：关键数据对象关联完整，关键记录可追溯，计算过程与审核批准链完整；

c）权限与安全：身份认证、授权模型、最小授权、职责分离、审计日志等配置有效；

d）接口与集成：与仪器设备或外部系统的接口联调通过，接口日志与异常处理符合要求；

e）性能与可靠性：满足规定的响应时间、并发能力与稳定性要求，备份恢复策略可用；

f）文档与交付：交付资料完整且可用于后续运行维护与持续改进。

9.7 验收记录与问题整改

验收应形成验收方案、验收记录与验收结论文件。验收记录应包含验收范围、验收依据、验收项、验证方法、验证结果、问题清单及处置情况。

验收发现问题应进行分级管理并整改闭环，整改应记录责任人、整改措施、完成时间、复验结果；对影响合规运行或数据可靠性的重大问题未整改完成前，不应进入正式上线。

9.8 上线交付与运行移交

系统上线应执行上线审批与发布管理，应明确上线时间窗口、影响范围、回退方案及应急联系人。

系统交付应至少包含用户手册、管理员手册、配置清单、接口说明、数据字典、权限矩阵、备份恢复方案、应急处置预案、培训资料与版本发布说明等资料。

上线后应进行运行移交与支持期管理，支持期内应对问题响应、缺陷修复与优化需求建立闭环机制，并保留全过程记录。

10 运行维护与持续改进要求

10.1 总体要求

系统投入运行后应建立运行维护管理机制，应明确运维组织、运维职责、运维流程、服务响应要求及考核方式，并应形成可追溯的运维记录。

系统运行维护应保障业务连续性与数据可信性，应对运行风险、数据风险与安全风险实施持续监测与控制，并应与实验室质量管理体系的持续改进机制相衔接。

10.2 运行监控与告警

系统应具备运行监控能力，应对关键资源与关键服务进行监测，至少应包括服务器资源、数据库状态、存储容量、接口调用状态、队列/任务调度状态、关键业务服务可用性等。

系统应具备告警能力，应对认证异常、权限异常、接口异常、关键服务中断、存储容量不足、备份失败等事件触发告警；告警应可追溯并应支持分级处置。

系统宜建立运行态势看板或等效展示能力，支持对业务量、任务处理状态、报告出具情况、异常事件统计等运行指标的可视化监控。

10.3 故障管理与问题处置

系统应建立故障管理流程，应覆盖故障受理、定位分析、处置恢复、复盘改进等环节，并应形成故障记录。

系统故障处置应明确响应时间与升级机制；对影响核心业务的重大故障，应启动应急处置程序并保留处置证据。

故障复盘应识别根因并制定纠正与预防措施，涉及配置变更、程序修复或安全加固的，应纳入变更管理并验证效果。

10.4 变更管理与版本管理

系统应建立变更管理机制，变更范围应至少包括功能调整、业务规则调整、计算公式与判定规则调整、报告模板调整、接口调整、权限策略调整、数据库结构调整、运行参数调整及补丁更新等。

变更应执行评估、审批、实施、验证与回退控制，应记录变更原因、影响分析、实施步骤、验证结果与发布信息；对可能影响检测结果、报告输出或追溯链的变更，应进行专项验证并保留证据。

系统应对版本进行管理，版本发布应具备发布说明，至少应说明新增功能、修复内容、风险提示与回退方式；历史版本与配置应可追溯。

10.5 账户与权限例行审查

系统应定期开展账户与权限审查，审查内容应至少包括无效账户、超范围授权、共享账户风险、高权限账户使用情况及职责分离执行情况。

人员岗位变动、离职离岗等情形发生时，应及时调整权限并回收不再需要的授权；权限调整应留存审批与变更记录。

对涉及报告批准、电子签名、系统配置管理、接口管理等高权限角色，应加强使用审计，必要时实施双人复核或分级审批。

10.6 数据治理与质量维护

系统应建立数据治理机制，应对主数据、基础数据与关键业务数据的维护责任、维护频次、变更规则和校验规则进行规定。

系统应支持数据质量检查与异常数据处理，应对重复数据、缺失数据、异常值、编码不一致等情形进行识别与处置；处置过程应可追溯。

系统宜定期开展数据一致性核查，重点核查样品—任务—数据—报告—归档链路的关联完整性与可追溯性，发现问题应形成整改闭环。

10.7 备份恢复与演练

系统应按备份策略开展定期备份，并应定期验证备份可用性；备份失败应触发告警并及时处置。

系统应定期开展恢复演练或等效验证，演练内容至少应包含数据库恢复与文件数据恢复；演练应形成记录并评估恢复目标达成情况。

发生误操作、数据损坏或灾害事件时，应按恢复预案执行恢复，并应保证恢复过程不破坏数据追溯链与审计链。

10.8 安全运行与持续加固

系统应开展安全运行管理，应定期检查安全配置有效性，至少应包括认证策略、口令策略、会话策略、权限策略、接口鉴权与日志审计等。

系统应建立漏洞处置与安全加固机制，应对高危漏洞及时处置并验证修复效果；涉及安全事件的，应按安全事件处置流程进行取证、分析与整改。

系统宜定期开展安全风险评估或等效检查，并将评估结果纳入持续改进计划。

10.9 持续改进与绩效评价

系统应建立持续改进机制，应收集用户反馈、运行指标、故障数据、审计发现与质量管理活动结果，并据此形成优化需求清单。

系统优化应遵循变更管理要求，优化效果应可验证并形成记录；对与检测质量、合规性和效率提升相关的优化项，宜建立量化评价指标。

系统运行维护活动及持续改进活动的记录应纳入实验室记录控制范围，并按规定进行保存与管理。