ICS 35.020
CCS L 70

T/CS

团 体 标 准

T/CS 509—2026

互联网信息系统集成建设技术规范

Technical specification for information system integration construction of internet

2026-07-02 发布 2026-07-02 实施

中国商品学会 发 布

目　　次

前言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 总则 1
4.1 建设范围 1
4.2 建设流程 2
5 总体架构 2
5.1 架构设计要求 2
5.2 架构模型设计 2
6 基础设施层建设要求 3
6.1 机房物理环境 3
6.2 计算资源 3
6.3 存储资源 3
6.4 网络资源 3
6.5 云计算平台 4
7 数据层建设要求 4
7.1 数据标准体系 4
7.2 数据资源目录 4
7.3 数据采集与汇聚 4
7.4 数据治理 5
7.5 数据交换与共享 5
7.6 数据库系统 5
8 应用支撑层建设要求 6
8.1 中间件平台 6
8.2 服务集成与治理 6
8.3 统一认证与权限管理 6
8.4 公共服务组件 7
8.5 技术平台要求 7
9 应用层建设要求 7
9.1 总体要求 7
9.2 业务应用系统 8
9.3 统一门户 qqq8
9.4 第三方系统对接 8
10 安全体系建设要求 8
10.1 等级保护 8

10.2 网络安全 8
10.3 主机与应用安全 8
10.4 数据安全 9
10.5 个人信息保护 9
10.6 密码应用 9
10.7 安全运营 10
11 运维体系建设要求 10
11.1 运维管理体系 10
11.2 监控与告警 10
11.3 变更与发布管理 10
11.4 故障与应急管理 11
11.5 灾备与连续性 11
12 验收与评价 11
12.1 验收条件 11
12.2 测试要求 12
12.3 验收流程 12
12.4 评价指标 12
12.5 交付物清单 12

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。

本文件由中国商品学会提出并归口。

本文件起草单位：河南城建学院、浙江大华技术股份有限公司、河南科技大学、西安速应网络科技有限公司、泉州市浩睿信息科技有限公司、兴能电力建设有限公司、深圳精美科技健康管理有限公司、河南览众工程管理有限公司、浙江时代京云标准科技有限公司。

本文件主要起草人：张洛花、任春龙、买若毅、赵志铎、黄志强、阳隆、舒彦宁、张娜娜、吴彤。

互联网信息系统集成建设技术规范

1 范围

本文件规定了互联网信息系统集成建设的总体架构、基础设施层建设要求、数据层建设要求、应用支撑层建设要求、应用层建设要求、安全体系建设要求、运维体系建设要求和验收与评价等内容。

本文件适用于互联网信息系统的集成建设。

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 50174 数据中心设计规范

GB 50311 综合布线系统工程设计规范

GB 50462 数据中心基础设施施工及验收标准

GB/T 20269 信息安全技术 信息系统安全管理要求

GB/T 20984 信息安全技术 信息安全风险评估方法

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25000.1 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第1部分：SQuaRE指南

GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 28827.1 信息技术服务 运行维护 第1部分：通用要求

GB/T 28827.3 信息技术服务 运行维护 第3部分：应急响应规范

GB/T 31168 信息安全技术 云计算服务安全能力要求

GB/T 32400 信息技术 云计算 概览与词汇

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 35295 信息技术 大数据 术语

GB/T 36344 信息技术数据质量评价指标

GB/T 37988 信息安全技术 数据安全能力成熟度模型

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GB/T 39788 系统与软件工程 性能测试方法

GB/T 42568 工业互联网平台微服务参考框架

SJ/T 11674.1 信息技术服务 集成实施 第1部分：通用要求

3 术语和定义

SJ/T 11674.1、GB/T 35295、GB/T 42568界定的术语和定义适用于本文件。

4 总则

4.1 建设范围

互联网信息系统集成建设范围应包括：

a) 基础设施层：网络、计算、存储、机房环境等；
b) 数据层：数据库、数据仓库、数据治理等；
c) 应用支撑层：中间件、开发平台、集成平台等；
d) 应用层：业务应用系统、门户网站、移动应用等；
e) 安全体系：网络安全、数据安全、应用安全等；
f) 运维体系：监控、告警、故障处理、变更管理等。

4.2 建设流程

系统集成建设应遵循下列流程：
a) 需求分析：明确业务需求、功能需求、非功能需求；
b) 方案设计：编制总体技术方案、详细设计方案；
c) 采购与开发：设备采购、软件开发、系统集成；
d) 部署测试：系统部署、集成测试、性能测试、安全测试；
e) 试运行：系统试运行、问题整改；
f) 验收交付：竣工验收、文档移交、培训交付。

5 总体架构

5.1 架构设计要求

系统总体架构设计应符合下列要求：
a) 分层解耦要求：各层之间通过标准化接口进行交互，层内各组件应满足高内聚、低耦合的要求；
b) 集约化要求：同类资源和能力应统一建设和管理；
c) 可扩展性要求：各层应支持独立扩展、独立升级和独立替换，单层变更不应影响其他层次的正常运行；
d) 高可用性要求：架构应消除单点故障，关键组件应采用多节点冗余部署，系统应具备自动故障检测与切换能力，局部故障不应导致整体服务中断；
e) 开放性要求：技术选型应优先采用开放标准和开源技术。

5.2 架构模型设计

互联网信息系统集成建设采用分层架构模型，分为四个层次和两个体系，框架模型表如表1。

表 1 框架模型表

<table>
<tr><td colspan="2">互联网信息系统集成建设架构模型</td></tr>
<tr><td colspan="2">应用层</td></tr>
<tr><td colspan="2">业务应用系统/门户网站/移动应用/小程序</td></tr>
<tr><td colspan="2">应用支撑层</td></tr>
<tr><td colspan="2">中间件/开发平台/集成平台/API网关</td></tr>
<tr><td colspan="2">数据层</td></tr>
<tr><td colspan="2">数据库/数据仓库/数据湖/数据治理平台</td></tr>
<tr><td colspan="2">基础设施层</td></tr>
<tr><td colspan="2">网络/计算/存储/云平台/机房环境</td></tr>
<tr><td>安全体系</td><td>运维体系</td></tr>
</table>

6 基础设施层建设要求

6.1 机房物理环境

6.1.1 机房应符合下列要求：

a) 供电系统配置不间断电源（UPS），关键设备采用双路供电；
b) 温度控制在18 ℃～28 ℃，相对湿度控制在35 %～75 %；
c) 部署环境监控系统，对温湿度、漏水、烟雾等进行实时监测；
d) 配置门禁系统和视频监控系统。

6.1.2 机房设计应符合GB 50174的规定，根据业务等级确定机房建设等级。

6.1.3 综合布线系统应支持语音、数据、图像及多媒体业务的信息传输，并适应网络架构的扩展与变更，应符合GB 50311的规定。

6.1.4 机房基础设施施工及验收应符合GB 50462的规定。

6.2 计算资源

6.2.1 服务器应根据业务负载特征选择物理服务器或虚拟化部署方式。

6.2.2 物理服务器应符合下列要求：

a) 选用机架式或刀片式服务器；
b) 数据库服务器配置高性能SSD存储；
c) 应用服务器支持集群部署，具备水平扩展能力；
d) 配备冗余电源、冗余风扇，支持热插拔。

6.2.3 虚拟化平台应支持资源池化管理，按需分配和动态调度CPU、内存、存储资源。

6.2.4 容器化部署应具备容器编排能力，支持容器的自动部署、扩缩容和故障自愈。

6.2.5 计算资源应符合下列冗余要求：

a) 应用服务器集群不少于2个节点；
b) 数据库服务器采用主备或集群模式部署；
c) 关键业务系统具备跨可用区部署能力。

6.3 存储资源

6.3.1 存储资源架构应根据数据访问特征选择存储方式，包括块存储、文件存储或对象存储等方式。

6.3.2 存储系统应符合下列要求：

a) 存储容量按照当前需求进行规划，预留扩展空间；
b) 支持在线扩容，扩容过程不影响业务正常运行；
c) 部署存储监控系统，当存储使用率超过80 %时自动告警。

6.3.3 存储资源的关键数据应采用RAID保护或分布式多副本机制。

6.3.4 存储资源应配置独立的备份存储空间，备份存储应与生产存储物理隔离。

6.4 网络资源

6.4.1 网络架构应采用分层设计，分为核心层、汇聚层和接入层。

6.4.2 网络应划分安全域，不同安全域之间应通过防火墙或访问控制策略进行隔离。

6.4.3 网络出口应部署负载均衡设备，支持四层和七层负载均衡。

6.4.4　互联网接入宜部署CDN服务，静态资源应就近分发。

6.5　云计算平台

6.5.1　云计算平台部署应符合GB/T 32400的规定。

6.5.2　云平台安全能力应符合GB/T 31168的规定。

6.5.3　采用公有云服务时，应评估云服务商的安全资质和服务能力。

6.5.4　采用混合云部署时，公有云和私有云之间应进行安全互联，数据应保持一致。

6.5.5　云平台应支持资源弹性伸缩，具备根据负载自动调整计算和存储资源的能力。

7　数据层建设要求

7.1　数据标准体系

7.1.1　建立统一的数据分类编码体系，对数据按主题域进行分类管理。

7.1.2　制定数据元标准，明确数据元的命名规则、类型定义、值域范围和业务含义。

7.1.3　编制并维护数据字典，对系统内所有数据实体和属性进行标准化定义。

7.1.4　数据标准制定应参照GB/T 35295、GB/T 36344的相关要求。

7.2　数据资源目录

7.2.1　建立数据资源目录体系，对数据资源进行统一编目、注册和发布。

7.2.2　数据资源目录应包含资源名称、资源摘要、数据格式、更新频率、共享属性、责任部门等核心元数据。

7.2.3　数据资源目录应支持动态更新，资源信息变更时应在5个工作日内完成目录更新。

7.3　数据采集与汇聚

7.3.1　数据采集宜包括下列方式：

a)　通过API接口实时采集；
b)　通过数据库同步定时采集；
c)　通过文件批量导入采集；
d)　通过日志采集工具采集；
e)　通过物联网网关采集。

7.3.2　数据采集过程中应进行数据校验，对不符合标准的数据进行清洗和转换处理。

7.3.3　数据清洗应包括下列规则：

a)　空值和缺省值处理；
b)　重复数据去重；
c)　格式标准化转换；
d)　异常值识别与处理；
e)　编码一致性校验。

7.3.4　采集的数据应按统一格式入库，入库前应经过质量检测并记录检测结果。

7.3.5　采集的数据应按照统一的汇聚策略汇入数据层，汇聚方式应包括实时汇聚和批量汇聚，实时类数据宜采用消息队列进行流式汇聚，批量类数据宜采用ETL工具进行定时汇聚。

7.3.6 汇聚过程应支持断点续传和失败重试，重试策略应包括重试次数、重试间隔和异常告警。

7.3.7 数据汇聚完成后应进行一致性校验，校验内容包括数据条数比对和关键字段校验，校验不通过的应触发告警并记录异常日志。

7.4 数据治理

7.4.1 数据质量管理符合下列要求：

a) 数据质量管理应覆盖准确性、完整性、一致性、时效性、唯一性和有效性六个维度，符合GB/T 36344的规定；
b) 建立监控指标体系，对数据质量进行评估和报告；
c) 建立问题处理机制，发现问题应确定原因并制定整改措施。

7.4.2 主数据管理符合下列要求：

a) 主数据应实行“一数一源”管理原则，同一主数据实体在系统内应具有唯一权威来源；
b) 主数据的新增、变更和停用应通过统一的管理流程进行审批和执行。

7.4.3 建立元数据管理平台，统一管理技术元数据和业务元数据。元数据应支持数据血缘分析和影响分析。

7.4.4 数据生命周期管理符合下列要求：

a) 明确数据从产生到销毁各阶段的管理要求和处置策略；
b) 根据业务需要和法规要求确定数据保留期限；
c) 过期数据应按策略进行归档或安全销毁，并保留操作记录。

7.5 数据交换与共享

7.5.1 数据交换应通过标准化接口实现，接口规范应包括协议类型、数据格式、认证方式和调用频率限制。

7.5.2 数据交换接口宜采用下列协议：

a) RESTfulAPI：实时数据查询和操作类接口；
b) 消息队列：异步数据传输和事件驱动类场景；
c) WebService：与遗留系统对接。

7.5.3 数据交换应采用JSON或XML格式，字段命名应遵循数据标准体系的规定。

7.5.4 接口应具备版本管理能力，版本升级时应进行向后兼容或提供过渡期。

7.5.5 数据共享应建立共享目录和授权管理机制，数据提供方和使用方应签订数据共享协议。

7.5.6 开放数据接口应通过API网关统一管理，实现认证鉴权、流量控制和访问日志记录。

7.6 数据库系统

7.6.1 数据库应根据业务场景选择关系型数据库或非关系型数据库，选型应考虑数据结构、访问模式、一致性要求和性能需求。

7.6.2 数据库部署应符合下列要求：

a) 生产数据库采用主从复制或集群部署模式；
b) 配置读写分离，将查询类请求分流至只读节点；
c) 设置连接池管理。

7.6.3 数据库备份应符合下列要求：

a) 按数据重要程度设定备份周期，具体见表2；
b) 备份数据保留不少于30天；
c) 每季度进行一次备份恢复演练。

表 2 数据库备份要求

数据重要程度	全量备份	增量备份	差异备份
核心业务数据	每天1次	每天不少于1次	/
重要业务数据	每周1次	每天1次	每月1次
一般业务数据	每月1次	每周1次	/

7.6.4 数据库应进行定期性能分析和优化，包括慢查询分析、索引优化和SQL调优。

8 应用支撑层建设要求

8.1 中间件平台

8.1.1 根据业务需求部署下列中间件：

a) 消息中间件：系统间异步消息传递和事件通知，应支持消息持久化、重试和死信队列；
b) 缓存中间件：热点数据缓存和会话管理，应支持集群模式和数据淘汰策略配置；
c) 应用服务器中间件：托管Web应用，应支持热部署和会话管理；
d) 搜索引擎中间件：全文检索和日志分析，应支持分布式索引和近实时搜索。

8.1.2 中间件应纳入统一监控管理，配置告警阈值和自动恢复策略。

8.2 服务集成与治理

8.2.1 部署API网关或服务总线作为服务集成的统一入口，实现下列功能：

a) 请求路由和协议转换；
b) 认证鉴权和访问控制；
c) 流量控制和限流熔断；
d) 请求日志记录和链路追踪；
e) API文档管理和开发者门户。

8.2.2 微服务架构下应部署服务注册中心，实现服务的自动注册和发现。

8.2.3 服务调用应设置超时时间，超时阈值应根据服务特性独立配置。

8.2.4 具备服务熔断机制，当下游服务错误率超过阈值时自动熔断，不应造成级联故障。

8.2.5 服务应支持多版本并行部署，版本切换应支持灰度发布策略。

8.3 统一认证与权限管理

8.3.1 建设统一身份认证平台，支持下列认证方式：

a) 用户名/密码认证；
b) 短信验证码认证；
c) OAuth 2.0/OIDC协议认证；
d) LDAP/AD域认证；
e) 数字证书认证。

8.3.2 权限管理应支持单点登录（SSO），用户一次登录后可访问授权范围内的所有应用系统。

8.3.3 权限管理应采用基于角色的访问控制（RBAC）模型，复杂场景可扩展为基于属性的访问控制（ABAC）模型。

8.3.4 建立统一的权限分配和审批流程，权限变更应记录操作日志。

8.3.5 统一认证系统安全应符合GB/T 22239中身份鉴别和访问控制的相关规定。

8.4 公共服务组件

8.4.1 建设下列公共服务组件：

a) 统一消息通知服务：短信、邮件、站内信、推送等多种通知渠道；
b) 工作流引擎：业务流程的可视化配置、审批流转和流程监控；
c) 文件管理服务：文件上传、下载、预览和版本管理，大文件应支持分片上传和断点续传；
d) 日志服务：分布式日志的统一采集、存储、检索和分析；
e) 任务调度服务：定时任务和计划任务的统一配置和执行管理。

8.4.2 公共服务组件应以标准化接口方式对外提供服务，各业务应用通过接口调用公共服务能力。

8.5 技术平台要求

8.5.1 微服务架构应遵循下列规范：

a) 每个微服务应有独立的代码仓库、构建流程和部署单元；
b) 服务间通信宜采用轻量级协议；
c) 服务应实现无状态设计，会话数据应存储于共享缓存；
d) 每个服务应提供健康检查接口。

8.5.2 容器编排平台应具备下列能力：

a) 容器的自动部署和滚动更新；
b) 基于资源使用率的自动扩缩容；
c) 容器健康检查和自动重启；
d) 服务发现和负载均衡；
e) 配置管理和密钥管理。

8.5.3 建设DevOps工具链，实现下列能力：

a) 代码版本管理；
b) 持续集成（CI）：代码提交后自动触发编译、测试和构建；
c) 持续交付/部署（CD）：构建产物自动部署至测试环境或生产环境；
d) 自动化测试：单元测试、集成测试和接口测试的自动执行。

9 应用层建设要求

9.1 总体要求

9.1.1 应用系统应符合业务需求规格说明书中定义的功能要求，功能覆盖率应达到100 %。

9.1.2 应用系统应符合下列性能指标：

a) 响应时间：符合GB/T 39788的规定；
b) 并发用户数：设计并发用户数的指标要求；
c) 系统吞吐量：业务高峰期的处理需求。

9.1.3 软件质量应符合GB/T 25000.1中关于功能适合性、性能效率、兼容性、可靠性、安全性、可维护性和可移植性的要求。

9.2 业务应用系统

9.2.1 业务功能设计应基于业务流程分析，功能模块划分应与业务领域保持一致。

9.2.2 业务流程设计应支持流程可配置、可调整，流程变更不应涉及代码修改。

9.2.3 应用系统应支持多终端适配，包括PC端浏览器、移动端App和微信小程序等终端。响应式设计应适配主流屏幕分辨率。

9.2.4 应用系统应支持主流浏览器的应用，包括Chrome、Firefox、Safari和Edge等浏览器。

9.3 统一门户

9.3.1 建设统一门户系统，作为用户访问各业务应用的统一入口。

9.3.2 集成单点登录功能，用户无需重复认证即可访问授权应用。

9.3.3 支持个性化配置，允许用户根据角色和偏好自定义工作台布局。

9.3.4 提供统一的消息中心、待办中心和应用导航。

9.4 第三方系统对接

9.4.1 与第三方系统对接应通过标准化接口实现，接口协议和数据格式应在接口规范文档中明确定义。

9.4.2 接口对接前应进行接口联调测试，联调通过后方可进入集成测试阶段。

9.4.3 建立第三方接口的版本管理和变更通知机制，接口变更应提前通知相关方并评估影响范围。

9.4.4 对接过程中涉及的数据传输应采用加密通道（HTTPS/TLS），敏感数据应进行脱敏处理。

10 安全体系建设要求

10.1 等级保护

10.1.1 信息系统应按照GB/T 22239的规定进行安全等级定级，定级后应向公安机关备案。

10.1.2 安全建设整改应符合GB/T 25070的安全设计技术要求。

10.1.3 系统上线前应完成等级保护测评，测评不合格的不应上线运行。

10.1.4 已上线系统应定期开展等级保护测评，第三级及以上系统每年至少进行一次测评。

10.2 网络安全

10.2.1 在网络边界部署防火墙，配置访问控制策略，默认策略应为拒绝。

10.2.2 部署入侵检测/防御系统（IDS/IPS），对网络流量进行实时监测和分析。

10.2.3 互联网出口应部署DDoS防护能力，防护带宽应符合业务峰值流量需求。

10.2.4 划分网络安全域，不同安全域之间的访问应遵循最小权限原则。

10.2.5 远程运维管理应通过堡垒机进行，不应直接从互联网访问后台管理系统。

10.2.6 网络设备应关闭不必要的服务和端口，管理口应限制访问源地址。

10.3 主机与应用安全

10.3.1 操作系统应进行安全加固，包括下列方式：

a) 安装安全补丁；
b) 关闭不必要的服务和端口；
c) 配置强密码策略和登录失败锁定策略；
d) 启用操作审计日志；
e) 限制特权账户使用。

10.3.2 应用开发应遵循安全编码规范，防范下列常见安全漏洞：

a) SQL注入；
b) 跨站脚本攻击（XSS）；
c) 跨站请求伪造（CSRF）；
d) 文件上传漏洞；
e) 越权访问；
f) 敏感信息泄露。

10.3.3 应用系统上线前应进行安全测试，包括代码安全审计和渗透测试。发现的高危和严重漏洞应在上线前完成修复。

10.3.4 容器和云环境应进行安全基线配置，镜像应从可信源获取并进行安全扫描。

10.4 数据安全

10.4.1 对系统数据进行分类分级管理，数据安全能力应符合GB/T 37988的规定。

10.4.2 数据传输应采用加密通道，重要数据和敏感数据的存储应进行加密处理。

10.4.3 敏感数据应进行脱敏处理，脱敏规则应根据数据使用场景确定。

10.4.4 数据备份策略应符合下列要求：

a) 关键业务数据备份频率为每天一次；
b) 备份数据存储于异地或独立存储介质；
c) 定期验证备份数据的完整性和可恢复性。

10.4.5 部署数据防泄漏（DLP）措施，对敏感数据的访问、传输和复制进行监控和控制。

10.5 个人信息保护

10.5.1 个人信息的收集、存储、使用、共享和删除应符合GB/T 35273的规定。

10.5.2 个人信息收集应遵循最小必要原则，不应收集与业务功能无关的个人信息。

10.5.3 收集个人信息前应向用户告知收集目的、方式和范围，并取得用户明示同意。

10.5.4 个人信息存储应采取加密等安全措施，存储期限不应超过实现处理目的所必要的最短时间。

10.5.5 个人信息共享和对外提供应取得用户单独同意，并进行安全影响评估。

10.5.6 提供用户查询、更正和删除个人信息的途径。

10.6 密码应用

10.6.1 信息系统密码应用应符合GB/T 39786的规定。

10.6.2 采用经国家密码管理局认可的密码产品和密码服务。

10.6.3 密钥管理应符合下列要求：

a) 通过安全的方式生成和分发；
b) 对有效期进行限制并定期更换密钥；

c) 存储采取安全保护措施；
d) 销毁应彻底，不可恢复。

10.7 安全运营

10.7.1 建设安全运营中心（SOC），集中监测、分析和处置安全事件。

10.7.2 部署安全信息和事件管理系统（SIEM），集中采集安全日志后对安全日志进行关联分析。日志保存期限不少于6个月。

10.7.3 建立安全事件应急响应机制，明确应急响应流程和处置措施，符合GB/T 20269的规定。

10.7.4 开展安全风险评估，评估方法应符合GB/T 20984的规定。

10.7.5 建立漏洞管理流程，定期进行漏洞扫描，发现漏洞应进行修复。

11 运维体系建设要求

11.1 运维管理体系

11.1.1 运维管理体系应符合GB/T 28827.1的规定。

11.1.2 制定运维管理制度，宜包括以下制度：

a) 值班管理制度；
b) 变更管理制度；
c) 事件管理制度；
d) 配置管理制度；
e) 安全管理制度。

11.1.3 签订运维服务级别协议（SLA），明确服务内容、响应时限和质量指标。

11.2 监控与告警

11.2.1 建立统一监控平台，监控范围应覆盖基础设施、中间件、数据库、应用系统和业务指标。

11.2.2 基础设施监控应包括：

a) 服务器：CPU使用率、内存使用率、磁盘使用率、网络流量；
b) 网络设备：端口状态、流量、丢包率、时延；
c) 存储设备：容量使用率、IOPS、读写延迟。

11.2.3 应用性能监控（APM）应包括：

a) 接口响应时间和成功率；
b) 服务调用链路追踪；
c) 错误日志和异常统计；
d) JVM/容器资源使用情况。

11.2.4 告警程度分类和应急处理应符合GB/T 28827.3的规定。

11.3 变更与发布管理

11.3.1 所有生产环境的变更应经过审批，紧急变更可事后补录审批记录。

11.3.2 变更应分类管理：

a) 重大变更：涉及架构调整、核心业务逻辑修改，经过技术评审；

b) 一般变更：功能优化、缺陷修复，经过测试验证；
c) 标准变更：配置调整、参数修改，可执行简化审批流程。

11.3.3 版本发布应采用灰度发布策略，先在小范围验证通过后再全量发布。

11.3.4 每次发布应具备回滚方案。

11.4 故障与应急管理

11.4.1 故障应按影响范围和严重程度分级：

a) 一级故障：核心业务系统全面中断，立即启动应急响应；
b) 二级故障：部分业务功能不可用或性能严重下降，在30分钟内响应；
c) 三级故障：非核心功能异常或性能轻微下降，在工作时间内响应。

11.4.2 应急预案应包括下列内容：

a) 故障场景描述；
b) 应急组织和职责分工；
c) 处置流程和操作步骤；
d) 资源保障和联系方式；
e) 事后复盘和改进要求。

11.4.3 应急预案应每年至少演练一次，演练后应进行总结和改进。

11.4.4 故障处置完成后应进行复盘分析，输出故障报告，明确根因和改进措施。故障报告应在故障恢复后3 个工作日内完成。应急响应流程应符合GB/T 28827.3的规定。

11.5 灾备与连续性

11.5.1 根据业务重要性确定灾备等级和策略。

11.5.2 业务的灾难恢复指标应符合GB/T 22239的规定。

11.5.3 灾备数据应进行定期一致性校验。

11.5.4 每年至少进行一次灾难恢复演练。

12 验收与评价

12.1 验收条件

12.1.1 初验应符合下列条件：

a) 系统功能开发完成并通过系统测试；
b) 性能测试、安全测试通过；
c) 等级保护测评通过；
d) 相关文档编制完成；
e) 数据迁移完成并验证通过。

12.1.2 终验应符合下列条件：

a) 试运行期满且试运行期间无重大故障；
b) 初验遗留问题全部整改完成；
c) 运维体系建立并正常运行；
d) 培训工作完成；
e) 全部文档交付完成。

12.1.3 试运行期应不少于30天，关键业务系统试运行期宜不少于90天。

12.2 测试要求

12.2.1 功能测试应覆盖全部业务功能，测试用例应包含正常流程和异常流程。

12.2.2 性能测试应包含下列类型：

a) 负载测试：验证系统在设计并发用户数下的性能表现；
b) 压力测试：验证系统在超出设计负载时的表现和极限承载能力；
c) 稳定性测试：验证系统在正常负载下连续运行不少于72小时的稳定性。

12.2.3 安全测试应包含：

a) 漏洞扫描：对网络、主机、应用进行全面漏洞扫描；
b) 渗透测试：模拟攻击者对系统进行渗透测试；
c) 代码安全审计：对源代码进行安全审计。

12.2.4 兼容性测试应覆盖目标用户使用的主流浏览器和移动终端。

12.2.5 等级保护测评应委托具有资质的测评机构实施，符合GB/T 22239的规定。

12.3 验收流程

验收应按下列流程执行：

a) 验收申请：承建方向建设方提交验收申请及验收材料；
b) 验收方案编制：建设方组织编制验收方案，明确验收内容、方法和标准；
c) 验收实施：按照验收方案逐项进行验证和测试；
d) 验收评审：组织专家评审，形成验收评审意见；
e) 问题整改：对验收中发现的问题进行整改，整改完成后进行复验；
f) 验收确认：验收通过后，各方签署验收报告。

12.4 评价指标

12.4.1 验收评价应符合表2的规定。

表 2 验收评价表

评价指标	要求
功能覆盖率	100 %
功能测试通过率	≥98 %
性能指标达标率	100 %
高危安全漏洞	0个
中危安全漏洞	限期整改
等保测评结果	符合相应等级要求
文档完整性	100 %
用户满意度	≥85分

12.4.2 用户满意度评价应通过问卷调查或访谈方式进行，评价内容包括系统功能、性能、易用性、稳定性和服务质量等方面。

12.5 交付物清单

12.5.1 软件交付物应包括：

a) 应用系统（含源代码）；
b) 数据库脚本和初始数据；
c) 配置文件和部署脚本；
d) 第三方软件及授权。

12.5.2 文档交付物应包括：

a) 需求规格说明书；
b) 总体设计方案；
c) 详细设计方案；
d) 数据库设计文档；
e) 接口规范文档；
f) 测试计划和测试报告；
g) 用户操作手册；
h) 系统运维手册；
i) 部署实施方案；
j) 培训材料；
k) 验收报告。

12.5.3 交付物应进行清点确认，双方签署交付物清单。