ICS 03.060

A11

JR

中华人民共和国金融行业标准

JR/T 0179—2019

保险信息系统上线运行基本要求

Basic requirements of information system running online in insurance industry

2019-12-24 发布　　2019-12-24 实施

中国银行保险监督管理委员会　发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由全国金融标准化技术委员会保险分技术委员会提出并归口。

本标准起草单位：中国太平洋保险（集团）股份有限公司、中国平安保险(集团)股份有限公司、中国阳光保险集团公司。

本标准主要起草人： 胡罡、韩梅、李波、陈华、张洪文、方强、符祥冲、符磊、叶郁、陈轶龙、杨敏华

本标准为首次制定。

引　言

信息系统是保险业销售产品服务客户的重要载体。随着移动互联技术的飞速发展，越来越多的新技术被运用到保险业的信息系统中来，快速发展的市场和人民对保险产品以及承载产品的信息系统的需求，决定了产品开发和信息系统的建设周期被不断压缩，能否快速支持信息系统上线，以及确保上线后系统的运行稳定，决定着保险业是否能快速抓住客户并占有市场，是保险从业机构核心竞争力的重要组成部分。

随着保险业信息系统集中程度的不断提高，新产品创新和投放节奏的不断加快，如何能够通过规范，快速实现信息系统上线，并确保运行稳定，是实现保险业安全生产的重要基础，也是业务拓展的重要保障。

《保险业信息系统上线运行基本要求》的制订，旨在完善保险机构的IT服务管理体系，规范保险机构信息系统上线实施作业，加强保险业信息系统的运行稳定性，提高内外部用户的满意度，提升保险机构的核心竞争力。

保险信息系统上线运行基本要求

1 范围

本标准规定了保险业信息系统上线运行的基本要求，是信息技术服务管理的组成部分，与信息系统运行维护紧密相关，并形成闭环管理，如图1所示：

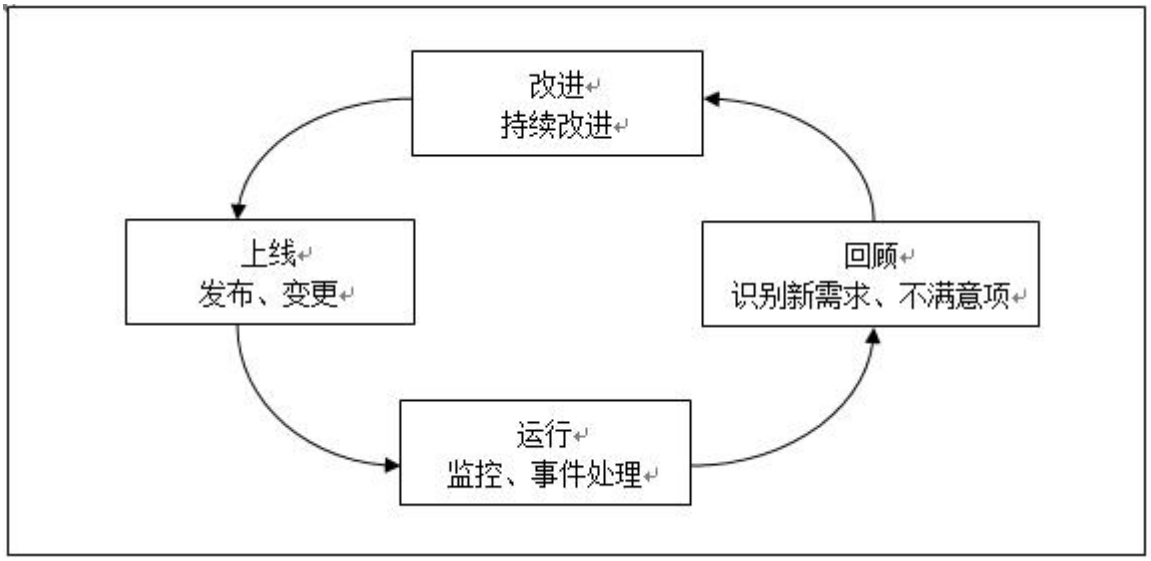

图1 上线运行闭环管理

本标准适用于在境内从事保险业务的保险机构。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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。

ISO/IEC 20000-1:2011 信息技术服务管理第1部分:服务管理体系要求（Information technology – Service management – Part 1: Service management system requirements）

ISO/IEC 20000-2:2011 信息技术服务管理第2部分：服务管理体系应用指南（Information technology – Service management – Part 2: Guidance on the application of service management systems）

JR/T 0079—2013 保险业信息系统运行维护工作规范（Information system operation and maintenance work specification for insurance industry）

GB/Z 20985-2007 信息技术 安全技术 信息安全事件管理指南(Information technology—Security techniques—Information security incident management guide)

GB/T 29264-2012 信息技术服务 分类与代码（Information Technology — Classification and codes for service）

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息技术服务Information Technology Service

指供方为需方提供如何开发、应用信息技术的服务，以及供方以信息技术为手段提供支持需方业务活动的服务。

[GB/T29264-2012，定义 2.1]

3.2

信息技术服务管理 Information Technology Service Management，ITSM

信息技术服务提供方通过协调一致的整合实施人员、流程和信息技术的管理活动，有效交付信息技术服务，满足客户和业务需求的管理活动。

[JR/T 0079—2013，定义 3.1]

3.3

运行维护 Operation and maintenance

采用相关的技术和方法，依据需方提出的服务级别要求，对其所使用的信息系统运行环境(如基础环境、软硬件环境等)、业务系统等提供的综合服务。

[JR/T 0079—2013，定义 3.2]

3.4

流程 Process

用于实现特定目标的一系列有组织的活动。流程获得一个或多个定义的输入，然后将它们变成定义的输出。流程可以包括角色、责任、工具和提供输出所需的管理控制。流程定义可包括政策、标准、指南、活动和工作指令。一个流程的输出常常成为另一个流程的输入。

[JR/T 0079—2013，定义3.3]

3.5

缺陷 Bug，Defect

软件或程序中存在的某种破坏正常运行能力的问题、错误，会导致软件产品在某种程度上不能满足用户的需要。

3.6

安全漏洞 Security Vulnerablitie

在硬件、软件、协议的具体实现或系统安全策略上存在的弱点或者缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。是受限制的计算机、组件、应用程序或其他联机资源无意中留下的不受保护的入口点。

3.7

软件测试 Software Testing

软件测试是一个评估软件产品的过程，通过发现软件产品中的缺陷以提高和改善产品质量。软件测试包括执行软件，以及通过分析和审核软件来达到预防缺陷的目的。

3.8

配置管理数据库 Configuration Management Database（CMDB）

用于记录配置项全生命周期属性及配置项之间关系的存储数据。

[ISO/IEC 20000-1:2011，定义3.4]

3.9

服务级别协议（SLA：Service Level Agreement）

服务提供者和用户之间签署的书面协议，用以记录既定的服务和服务目标。

[ISO/IEC 20000-1:2011，定义3.29]

3.10

服务提供者 Service Provider

一个组织或组织的一部分，其负责管理或交付一项或多项提供给用户的服务。

[ISO/IEC 20000-1:2011，定义3.32]

4 上线流程要求

4.1 总体要求

系统上线的总体要求应涵盖如下内容：

a) 上线管理过程应该协调服务提供者、业务方和其他相关方，对保险信息系统的上线运行进行规划；
b) 良好的规划应该与业务要求相结合，覆盖资源获得、关联影响及部署架构评估和审核、上线及推广计划、部署作业分解、备份、实施、验证及回退等内容；
c) 服务提供者应该确保已经考虑上线版本部署的技术和非技术两个方面；
d) 只有满足测试通过条件的信息系统版本才可被部署上线，版本内容可追溯，并防止被篡改。

4.2 上线策略

系统的上线策略应该包括：

a) 上线管理的角色和职责；
b) 上线版本部署到生产环境的审批流程；
c) 上线系统软件版本的唯一标识和描述；
d) 将变更组合到版本的方法；
e) 为提高效率、可重复性以及安全性，建立、安装、版本部署分发过程的自动化方法；
f) 知识产权转移相关流程；
g) 系统上线的准入、验证和接受的标准；
h) 版本上线的基本周期计划、变更时间窗口，及相关资源环境就绪安排等。

4.3 上线计划

上线计划应该确保受影响信息系统、基础设施、服务和文件的变更得到认可、授权、计划安排、协调和跟踪。

上线计划一般应包括：

a) 版本上线部署计划和可交付物的描述；
b) 所部署版本的相关需求内容、问题、变更范围、在测试期间已发现的缺陷及缺陷状态（开放、已解决、遗留等）；
c) 对于大型系统，上线过程的分阶段回滚决策点和决策标准；
d) 上线完成后，运营验证点和用户验收标准；
e) 上线实施的动作分解表；
f) 上线验证失败后的回退方案，以及各种可能异常情况下的应急处理方案；
g) 对于具有灾备环境的系统，应同时保证灾备环境的版本保持一致；
h) 与客户和服务支持人员的沟通，以及相关准备、文件的提供和培训；
i) 采购、存储、分发、联系、接受物品的工作和流程；
j) 确保维护服务级别所需的支持资源；
k) 对将上线版本部署到运行环境造成影响的相关变更和风险的识别；
l) 上线结束的签署。

4.4 上线评审事项

评审应该包括识别：

a) 软件版本，包含数据库、中间件、操作系统版本等；
b) 部署架构评审；
c) 权限管控是否符合安全的要求，确保不违背标准、方针和法规；
d) 上线软件版本中的已挂起缺陷和系统关联性；
e) 上线和推广的计划是否与监管或者业务要求相匹配；
f) 满足系统上线所必须的资源，包含软件、硬件、人员、供应商、合作伙伴等资源是否就位；
g) 上线版本内容和执行过程是否完整、准确，异常处理及回退方案是否逻辑完备。

4.5 文档

应该依据系统上线的配置项，建立和保存合适的文档，并按照配置管理过程进行管理。文档应包括：

a) 服务级别协议；
b) 支持性文件，包括安装部署、监控、辅助诊断、运行、管理和维护手册；
c) 功能性和非功能性的测试报告；
d) 上线推广和回退计划及测试报告；
e) 服务管理人员、运维支持人员和客户的培训计划；
f) 安全扫描报告、风险评估报告；
g) 版本的配置基准线，包括操作系统和中间件版本、数据库版本、系统文件、等相关配置项；
h) 相关变更、问题和已知挂起缺陷；

i） 关于上线授权、验证的证据。

4.6 上线实施

上线实施过程一般有如下要求：

a） 部署版本的检查，确保部署的版本是测试通过且符合业务要求的；

b） 部署作业应该按照既定的作业分解表实施；

c） 验证通过前应只对特定验证用户开放访问，验证通过后才能开放全部用户访问；

d） 所有验证测试数据应在开放所有用户使用前得到有效处理。

4.7 上线后的验证

上线后的验证一般有如下要求：

a） 上线后的版本号应进行检查，确保部署的版本是正确的版本；

b） 所有的监控、备份已经处于启用状态；

c） 事先设定的验证案例必须全部得到执行；

d） 验证的结果与预期一致；

e） 所有的数据存储和流转都是符合预期的；

f） 各阶段的验证应由获得适当授权的人员进行签署确认。

4.8 试运行（可选）

为检测系统系统长期运行的整体稳定性、可靠性和准确性，可考虑采用全量环境试运行、部分环境灰度发布、部分用户访问流量控制等方法，进行检测和考核：

a） 系统功能和性能；

b） 软件的稳定和可靠；

c） 硬件的稳定和可靠；

d） 数据交互的稳定、可靠、准确和完整；

e） 系统的安全性；

f） 网络连接的可靠性；

g） 用户的体验。

4.9 投产

符合上线投产的预期后，对系统进行投产，并更新配置管理系统中的系统状态。

4.10 回退

回退流程应确保：

a） 回退作业是获得审批通过并授权的；

b） 各关系方都已经正确获知了回退作业的时间和影响；

c） 回退作业应按照既定的回退步骤实施；

d） 所有已经生成并传递到关联系统的数据，都得到了妥善处理；

e） 检查确保上线系统按照回退决策被完整回退或者部分回退，相关回退不再对外提供服务。

5 架构要求

5.1 设计遵循

架构设计应遵循如下要求：

a） 架构设计需遵循相关国家和行业标准、规范、法规；

b） 架构设计需满足SLA要求，应经济高效地保证所交付服务的可用性和业务连续性要求；

c） 技术选型符合相关规范。

5.2 评审要求

生产环境实际部署架构与详细设计文档一致性检查：

a） 部署服务或组件版本是否与设计一致；

b） 部署服务或组件高可用是否与设计一致；

c） 部署容量是否与设计一致。

6 容量要求

6.1 容量指标定义

6.1.1 定义关键容量指标

在应用系统设计时，需要按照应用类型，定义体现系统服务能力的关键业务容量指标，示例：营运类的每秒承保量、每秒核保量、每秒理赔量、互联网类的用户并发访问量等。

6.1.2 确定用户容量需求

按照业务产能计划，在系统上线前需定义关键容量指标在上线时、日常闲时、日常峰时、各类业务活动时的容量需求，并定义在系统交付文档中。

6.1.3 评估容量最大配额

上线前系统应在性能测试环境中进行极限测试，检验该系统关键容量指标极限最大值，并定义在系统交付文档中。

6.2 容量配置

6.2.1 上线容量配置

系统上线前需依据上线业务容量指标要求，进行资源配置设计，转换为技术容量指标要求，如网络带宽、主机计算资源、中间件连接数、数据库存储量等需求，以满足系统上线运行安全运行要求。

6.2.2 容量扩展计划

根据业务产能计划，系统上线前需制定系统闲时、峰时、各类业务活动时的网络带宽、主机计算资源、中间件连接数、数据库存储量等技术容量指标扩展计划。

6.3 容量优化

6.3.1 容量数据采集

系统上线前需设计容量指标数据采集方案，包括指标类型（业务类、技术类）、采集频率、格式、存储、监控告警和数据展现方式等，容量指标采集应和系统上线同步进行，采集的数据应长期保留，以便进行趋势分析。

6.3.2 容量监控告警

系统上线前需定义的容量指标（业务类、技术类）的上限值、下限值以及合理运行期间，对偏移合理运行期间的指标应具备告警功能。

6.3.3 容量分析优化

系统上线后需持续分析运行数据，生产容量报告，并具备一定的预测功能，以支持容量性能持续优化，在日常系统运行以及各类活动时提供决策依据。

7 测试管理要求

7.1 测试机制

7.1.1 测试准入

测试准入应具备如下条件：

a) 开发单元测试报告评审通过，测试环境、测试数据准备就绪，完成测试案例评审；

b) 应用发布文档完整，应用部署文件齐全。

7.1.2 测试准出

测试准出应具备如下条件：

a) 所有测试案例全部执行完毕，不存在未经业务需求方许可的挂起缺陷，缺陷曲线图达到收敛的状态；

b) 输出《集成测试案例》和《集成测试报告》；

c) 对于系统的首次全量版本上线，需特别关注系统非功能类测试结果，与系统设计目标的一致性。其中，性能测试、容量测试通过为测试整体通过的必要条件。

7.1.3 测试环境

测试环境应具备如下条件：

a) 具备独立的测试验证环境；

b) 满足独立配置的资源管理。

7.1.4 测试方案/计划

测试方案/计划一般有如下要求：

a) 根据测试需求分析结果，编写《集成测试方案》，应包含：定义测试方法，确定测试目标。

b) 具备具体的测试计划方案，明确的测试启动、结束条件。

7.1.5 测试案例

测试案例一般有如下要求：

a) 测试案例已归档测试管理工具，已完成回归测试案例的修订；

b) 测试案例需满足测试度量要求。

7.1.6 测试报告

测试报告应具备如下条件：

a) 具有明确测试意见的报告；

b) 需体现缺陷检查数量和缺陷分布及已检出缺陷的关闭情况；

c) 包含发布版本的质量度量。

7.1.7 交付工作检查表

交付工作检查表宜具备如下条件：

a) 检查测试过程各阶段的输入和输出的合规性；

b) 测试过程管理的遗留风险提示。

7.1.8 非功能测试（可选）

非功能测试应具备如下条件，且具有与之匹配测试方法的结论：

a) 配置和安装、卸载测试。

b) 兼容性和互操作性测试；

c) 文档和帮助测试；

d) 错误恢复测试；

e) 性能测试；

f) 可靠性测试；

g) 保密性测试；

h) 压力测试；

i) 可用性测试；

j) 容量测试。

7.1.9 批处理专项测试

针对批量资金类、保单模板类、承保契约类、打印类、短信类等高风险批处理业务交易，有专项测试结果评审。

7.2 评审机制

7.2.1 测试评审

测试评审一般有如下要求：

a) 在整个项目管理生命周期内，测试过程中的所有文档均需评审；

b) 需建立规范的评审制度指引，测试交付文档均需有评审记录。

7.2.2 发布评审

评审检查计划发布的项目数量、需求数量、关联系统数、接口调整检查结果、代码比对结果、源代码是否归档管理、程序包中是否调整配置信息、数据库脚本检查结果和批处理改动检查结果。

7.3 缺陷管理

缺陷管理一般有如下要求：

a) 需对已知的检出缺陷进行登记管理,符合缺陷管理规范；

b) 不存在未经业务需求方许可的挂起缺陷。

7.4 缺陷管理工具

缺陷管理工具一般有如下要求：

a) 缺陷管理宜使用工具进行管理；

b) 建立缺陷管理规范（规范需包括：缺陷严重度定义，优先级定义，缺陷管理闭环流程）；

c) 缺陷管理工具需能够完整记录缺陷、跟踪缺陷解决过程。

8 安全管理要求

8.1 身份鉴别

应对系统中的用户进行身份标识和鉴别。在对每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性。保险信息系统应采用口令、解锁图案以及其他具有相应安全强度的机制进行用户身份鉴别:

a) 身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

b) 应采取必要措施，确保鉴别数据的保密性和完整性；

c) 可采取结束会话、限制非法登录次数和自动退出等措施，实现登录失败处理功能；

d) 身份鉴别成功后，当机器空闲操作时间超过规定值时，应由操作系统或应用系统对用户重新进行身份鉴别。

8.2 访问控制

应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限:

a) 访问控制主体的粒度为用户级或进程级，客体的粒度为文件、数据库表、记录和字段级，访问操作包括对客体的创建、读、写、修改和删除等；

b) 应能够为重要应用提供应用级隔离的运行环境，保证应用的输入、输出、存储信息不被非法获取。

8.3 系统安全审计

应提供安全审计机制，记录系统的相关安全事件，并支持审计信息的汇总：

a） 审计范围应覆盖到访问终端的注册、激活、使用及淘汰各个环节；
b） 审计记录应包括事件的时间、类型、设备标识、用户标识和结果等；
c） 应提供审计记录查询、分类和存储保护；
d） 应保护审计记录的完整性；
e） 根据《网络安全法》要求，相关的日志保存时间不得少于6个月。

8.4 数据完整性保护

应对关键配置文件、核心业务数据等重要数据进行完整性校验。

8.5 数据保密性保护

应确保用户数据在存储、传输和处理过程中的保密性：

a） 应采用防护机制，对存储的鉴别信息、核心业务、用户敏感信息等数据进行保护；
b） 对面向互联网提供服务的涉及敏感信息的应用系统的应用系统，在通信双方建立连接之前，应用系统应采取传输加密技术（包括HTTPS等加密技术）进行会话初始化验证；
c） 应对通信过程中的敏感信息字段进行加密。至少包括用户名、密码，个人信息，涉及资金等重要业务信息。

8.6 安全测试

应确保应用系统上线前，进行安全测试及配置项检查，通过安全测试后，才可上线：

a） 应通过白盒安全测试；
b） 应通过黑盒安全测试；
c） 应通过安全配置项检查；
d） 对于互联网应用，应通过越权渗透测试。

8.7 安全防护

应确保应用系统上线前，纳入安全防护体系，包括但不限于以下安全防护措施：

a） 应采用抗DDoS（分布式拒绝服务）攻击、入侵检测等防护技术；
b） 应采用应用层安全防护技术；
c） 应部署防病毒系统、采用威胁检测技术；
d） 应纳入日志管理系统；
e） 应遵循安全隔离原则，仅开放必要的网络策略。

8.8 安全等级保护要求

信息系统需求确定后，应该完成等保系统的定级工作，对二级及以上系统需完成备案、测评等工作。在系统安全设计时，需依据基本要求中对应等级的具体要求进行安全规划。

9 运行要求

9.1 监控要求

良好、全面、完善的业务健康监控体系，能够帮助IT服务提供者准确、及时、完善地了解业务各个层面的运行状况，通过及时处置监控预警，从而保证系统运行稳定、性能高效和用户体验良好。监控体系可做如下要求：

a) 应根据组织的实际情况和需要构建符合组织系统运行要求的监控体系和工具；
b) 监控应涵盖基础设施、组件、应用和数据层面；
c) 监控内容应覆盖可用性、容量、性能，面向用户的互联网应用还应覆盖用户体验；
d) 监控数据的样本采集频率须满足及时发现和趋势分析的需要；
e) 监控数据样本应妥善保存，以便持续分析；
f) 监控策略和指标应持续优化和调整；
g) 可考虑实现监控的可视化，以便直观的发现运行中的问题；
h) 应建立有效的应急处置机制，以便及时处置监控预警。

9.2 运行保障要求

为确保系统上线后的稳定运行，应建立相应的保障体系，以应对和处置运行过程中可能出现的各种问题，更好的服务业务需要。具体可做如下要求：

a) 应配备一定的资源来满足运行维护的需要；
b) 应遵循相应的流程和规范来进行运行保障，以保证系统安全稳定运行的需要；
c) 应建立相应的应急预案并定期进行演练，以确保从容、有序、快速地应对信息系统突发事件；
d) 应根据系统容灾需要，建立同城、异地等容灾环境，并制定演练计划，确保容灾能力的有效性。

9.3 持续改进的要求

在运行过程中不断优化、完善系统，提高服务质量，是提高核心竞争力的重要保证。具体可做如下要求：

a) 应定期评审和分析服务级别实现的结果；
b) 识别运行过程中的不满意项，并形成定期回顾机制加以督促改进；
c) 应根据组织的目标变动持续改进服务能力；
d) 应使用恰当的质量管理方法以支持续改进活动的开展。

参 考 文 献

[1] GB/T 5271.8-2001 信息技术词汇 第8部分：安全

[2] GB/T 11457-2006 信息技术 软件工程术语

[3] ISO/IEC 20000-1:2011 信息技术服务管理第1部分:服务管理体系要求（Information technology – Service management – Part 1: Service management system requirements）

[4] ISO/IEC 20000-2:2011 信息技术服务管理第2部分：服务管理体系应用指南（Information technology – Service management – Part 2: Guidance on the application of service management systems）

[5] GB/T 29264-2012 信息技术服务 分类与代码（Information Technology — Classification and codes for service）