金融信创运维自查清单

二十项，按五道关编排，一个下午可以盘完一遍

出品：监控易团队

文档编号：MX-ZCX-2026-01　　版本：V1.0　　生效日期：2026 年 11 月 12 日

适用对象：银行、证券、保险、信托、金融租赁、企业集团财务公司等信息科技与运维团队

目　　录

一、怎么用这份清单

二、第一关：异构适配与双栈

三、第二关：工具缺位与开放不足

四、第三关：性能与高可用

五、第四关：告警与数据割裂

六、第五关：并行期与合规

七、二十项填完，怎么读结果

八、如果分数不低，先做这三步

九、清单说明与获取方式

十、版本与修订记录

一、怎么用这份清单

这份清单把金融信创改造之后最容易出问题的环节，归成五道关：异构适配与双栈、工具缺位与开放不足、性能与高可用、告警与数据割裂、并行期与合规。每一关四项，共二十项，编号 01 到 20 连续。

用法很简单：逐项读“自查项”，按“怎么查”给出的动作确认一次，再对照“判定参考”填结果。判定参考对每一项都给了两档，能落到哪一档就填哪一档；两档都不符合的，按“已满足”理解即可，不必再补第三档。我们建议的状态只有三种，先不必纠结细分：

已满足：查得到、看得见、有记录，且能拿出证据（截图、报表、日志、测试报告都算）。

待补充：有部分能力，但缺指标、缺覆盖或缺证明。

未覆盖：目前没有，或只能靠人工台账维持。

整份盘完，一般一个下午到一天。不需要提前准备材料，也不需要厂商到场，运维同事自己就能填完。填完请保留原始记录，它是后面立项、选型、验收的共同底稿。

六类机构的关注点不完全一样，填的时候可以按自身业务调权重：银行重基础设施与核心系统的批处理窗口；证券看重交易时段，开盘前后的采集动作本身不能成为负担，判断时优先看时延与采集开销；保险核心系统涉及双录与保全批处理，夜间窗口长，但要保证次日开门前跑完；信托与金融租赁看资金链路与多租户隔离；企业集团财务公司看集团资金归集与监管报送。清单主体按通用口径写，条目不变，权重自己调。

执行提示：“怎么查”里涉及资产清单、接口清单、网络拓扑与链路拨测，都属于敏感操作。建议在受控环境或经变更审批后执行；导出的清单与截图先脱敏（IP、账号、客户标识替换后再外发），避免自查过程本身产生新的信息暴露。

关于判定线：文中出现的“秒级采集”“覆盖六成”“五套以上”“30 秒粒度”这类表述，都是我们在项目里常用的经验参考值，不是行业标准，也不是监管要求；如果与本单位的既有基线冲突，以本单位基线为准，并在记录里写明理由。

二、第一关：异构适配与双栈

这一关的共性是“看得见吗”。环境里同时存在两种以上国产处理器或操作系统，是最常见的起点。四项都围绕一件事：监控能不能在国产环境里原生把自己跑起来，并且看到该看的深度。

表 1　第一关自查项（4 项）

序号	自查项	怎么查	判定参考
01	资产清单是否标明了 CPU 架构、操作系统版本、虚拟化或云平台类型?	随机抽二十台服务器核对清单字段，除架构与版本外，看有没有 CPU 型号、内核版本、虚拟化/云平台类型、是否容器化；再抽一台国产 CPU 机器登录查看实际信息，与清单比对是否一致。	缺架构或版本任一项，或抽检与实际不符 → 待补充；字段齐全且抽检一致 → 已满足
02	采集端能否在 ARM 架构服务器上原生运行，采集频率是否仍在秒级?	在一台鲲鹏或飞腾机器上部署采集端，记录采集方式（本地 Agent 还是远程无代理）、声明的最细采集间隔（1 秒 / 5 秒 / 10 秒），并与一台同规模 x86 采集点的周期做对比。	装不上（架构不支持）→ 未覆盖；能装但周期从秒级降到分钟级 → 待补充；原生运行且周期与 x86 基线相当 → 已满足

序号	自查项	怎么查	判定参考
03	国产数据库采到的是深度指标，还是只显示“存活”？	选一个国产库实例，按数据库类型核对指标映射表（达梦、人大金仓、OceanBase、GaussDB 的指标名差异较大），看连接数、慢查询、表空间、主备延迟、锁等待是否都有采集。	只有端口与存活状态 → 未覆盖；有部分指标但名称对不上或缺项 → 待补充；主流指标齐全且与官方视图口径一致 → 已满足
04	信创与存量两套环境的资产，能否关联并在一张视图里同时看到?	选一个在两套环境里都有节点的业务系统，看两边资产在系统里是否有可关联的标识（同一业务维度、同一资产 ID），每条告警是否带环境来源标记。	两边资产各自独立、只能人工比对 → 未覆盖；可关联但告警缺来源标识 → 待补充；既同视图聚合又带来源标识 → 已满足

三、第二关：工具缺位与开放不足

这一关的共性是“接得上吗”。性能不够可以加机器，开放性不足是结构问题：数据取不出来，大平台接不上，安全平台也拿不到，最后成了孤岛。四项从入口数量、接口能力、覆盖范围、部署形态四个角度看。

表 2　第二关自查项（4 项）

序号	自查项	怎么查	判定参考
05	监控系统的登录入口有几个？纳管对象重叠多少？告警是否收敛到一处?	数清值班日常登录的入口数量；统计同一对象是否被两套以上系统重复纳管，算重叠比例；再看告警是分散在各系统还是收敛到一个工作台。	入口五个以上、重叠高于三成、告警分散 → 未覆盖；入口二到四个或重叠一到三成 → 待补充；统一入口、重叠低于一成、告警单点收敛 → 已满足

序号	自查项	怎么查	判定参考
06	监控数据能否以标准接口向上输出给大运维平台、数据中台与安全平台?	向厂商索取接口清单与字段说明，分别确认三件事：接口协议（SNMP / API / 消息队列）、数据格式（JSON / XML）、推送方式（主动上报或被动拉取），并要求给一个字段样例。	只能在界面查看、导不出实时数据 → 未覆盖；有接口但缺字段说明或缺推送能力 → 待补充；协议、格式、推送方式齐全并有样例 → 已满足
07	采集覆盖是否包含网络设备、安全设备、存储与机房动环，而不只是服务器?	按类别分别统计已纳管比例：服务器、网络设备、安全设备、存储、动环分开算；安全设备与动环单独列出，不被服务器数量稀释。	安全设备与动环两类都没纳管 → 未覆盖；仅服务器与网络为主 → 待补充；五类均有覆盖且比例均衡 → 已满足
08	是否支持跨网闸、跨区域多级部署，链路中断后数据能否续传?	检查隔离区与生产区是否各有采集点；在测试环境或经变更审批后模拟一次链路中断，记录断链时长、恢复后的补齐时限、有没有断点记录。	只支持单点部署 → 未覆盖；支持多级但断链后数据丢一段 → 待补充；多级部署且能按断点续传补齐 → 已满足

四、第三关：性能与高可用

这一关的共性是“撑得住吗”。国产化之后单机算力有差距，压力会转移到架构与监控上。判断标准不是“能不能跑”，而是单采集点还在不在安全区、粒度能不能到秒、一年之后查得动查不动、平台自己会不会成为单点。

表 3　第三关自查项（4 项）

序号	自查项	怎么查	判定参考
09	单采集点的资源占用与单轮询耗时，是否还在安全区?	先记录单采集点纳管对象数（仅作记录，不作阈值），再观察采集进程的 CPU 与内存占用率，以及单轮询实际耗时占配置周期的比例。	单轮询耗时超过周期的五成，或采集进程资源占用持续超过七成 → 待补充；两项都在安全区 → 已满足

序号	自查项	怎么查	判定参考
10	能否按设备类型或指标分别配置频率？最细粒度到多少？	分两问查：一是能否按设备类型或指标分别配置采集频率（是 / 否）；二是当前支持的最细采集粒度，具体到几秒，并确认采集频率与上报频率是否同频。	不能分设备分指标配置 → 待补充；可配置但最细粒度大于 30 秒 → 待补充；可配置且达 5 秒级、采集与上报同频 → 已满足
11	满一年数据量下的查询响应如何？压缩比有没有实测值？	在满一年数据量下测两个常用查询：近 7 天单指标曲线、近 30 天告警列表，看响应是否在 5 秒内；压缩比看有没有可复现的实测值（自测或第三方均可），并注明测试时的数据规模。	查询超 5 秒，且拿不出压缩比实测数据 → 待补充；两项都有实测记录 → 已满足
12	采集端与管理端是否解耦？管理端故障会不会连带影响采集与告警？	拆两问：一是管理端重启时，采集是否继续、数据是否先缓存再续传；二是管理端是多节点还是单节点、能否切换。	重启导致采集中断或数据丢失 → 未覆盖；仅通知延迟但数据能补齐 → 待补充；采集独立、管理端可切换 → 已满足

五、第四关：告警与数据割裂

这一关的共性是“报得准吗”。告警按设备报、不按影响报，是告警风暴的根源；一条链路抖动派生几十条，值班的人只能凭经验挑。四项分别对应重复率、分级维度、依赖关系与发现时延。

表 4　第四关自查项（4 项）

序号	自查项	怎么查	判定参考
13	告警重复率多少？一次链路故障会派生多少条告警？	先定口径：同一资源同一指标，在收敛窗口内重复上报计为一次重复。再导出上月告警明细算重复率；另外单独记录一次链路故障派生的告警条数，作为辅助指标。	重复率高于三成（经验参考线）→ 待补充；低于三成且单次故障派生条数可控 → 已满足

序号	自查项	怎么查	判定参考
14	告警分级是否包含业务影响面，而不只是设备严重级别?	看分级规则里是否引用业务影响面字段，例如影响客户数、交易链路、监管报送；再看这些字段有没有真正参与定级，而不只是展示。	没有分级规则、只有严重 / 警告 / 提示 → 未覆盖；有业务影响面字段但未与业务依赖关联 → 待补充；已按影响面定级并用于值班派单 → 已满足
15	是否维护了业务与资源的依赖关系，能说清哪台设备影响哪个业务?	指一个业务系统，看能否下钻到底层资源；再确认这份依赖关系是记在工具里，还是记在文档和表格里。	没有任何依赖记录 → 未覆盖；有文档表格但未与监控告警关联 → 待补充；依赖已进工具并用于告警定级或影响分析 → 已满足
16	从故障发生到有人知道，中位数多久？巡检是否还靠手工?	取近三个月故障单，算“从故障发生到首个有效告警”的时间中位数；统计自动巡检覆盖率与单轮耗时，并注明样本量与统计周期。	中位数超 30 分钟、无自动告警、依赖人工巡检 → 未覆盖；中位数 10 到 30 分钟 → 待补充；中位数 10 分钟以内且巡检自动 → 已满足

六、第五关：并行期与合规

这一关的共性是“说得清吗”。并行期最容易出事，因为判断不了是新系统还是老系统的问题；合规这头很实，等保要的不是“有监控”，而是三权分立、操作留痕、日志可审计。

表 5　第五关自查项（4 项）

序号	自查项	怎么查	判定参考
17	并行期同一业务能否按业务维度聚合？告警是否带环境来源标识?	选一个并行期的业务系统，看信创与存量资源能否在同一视图按业务维度聚合；再检查每条告警是否带环境来源标识（信创 / 存量）。	两套界面各看一半、需人工比对 → 待补充；有统一视图但来源标识缺失 → 待补充；两者都具备 → 已满足

序号	自查项	怎么查	判定参考
18	工具与流程是否两套并行？变更记录能否与监控侧对上？	抽 5 条近期变更单，逐条看能否在监控侧找到对应时间的配置变更记录、告警抑制记录或维护窗口记录。	完全没有变更与监控的关联机制 → 未覆盖；5 条中 3 条以上无法关联 → 待补充；5 条中 4 条以上可关联 → 已满足
19	等保要求的三权分立、操作留痕、日志可审计、字段脱敏，实际做到哪一步？	拆三项核查：一是是否按角色分权（管理员、操作员、审计员三权分立）；二是操作日志是否含操作人、时间、对象、结果且不可篡改；三是账号、IP、客户标识等敏感字段是否脱敏展示。	三权未分立，或操作日志缺任一要素 → 未覆盖；有日志但脱敏未覆盖敏感字段 → 待补充；三项齐全 → 已满足
20	立项或招标文件里，四类可核验参数是否都写明？	逐项核对技术需求：纳管规模是否写明对象数与指标项上限；采集速度是否写明最细粒度与单轮询耗时；压缩比是否写明实测值与测试规模；国产软硬件适配范围是否写明具体 CPU、操作系统、数据库清单。	两项以上缺失 → 未覆盖；任一项只写“满足需求”这类无量化的表述 → 待补充；四项均量化 → 已满足

七、二十项填完，怎么读结果

计分口径先说清：每项只填一个状态，“未覆盖”记 1 分，“待补充”记 0.5 分，“已满足”记 0 分，不做严重度加权。二十项满分为 20 分，分数越高说明缺口越多。落进下面四档，覆盖 0 到 20 全区间，不设“以上不再细分”的开口档。

总分区间	建议的下一步
0 至 4 分	体系基本完整，按季度复核一次即可，不用额外投入。
4.5 至 9 分	进入专项评估：先挑分数最集中的一关，做一个最小范围的试点，把指标、告警、流程一起定下来。

总分区间	建议的下一步
9.5 至 14 分	建议随本轮信创改造同步立项，不要等验收之后再补；按第八节的顺序推进，先纳管后收敛。
14.5 至 20 分	先做资产与采集补全，再谈告警治理与智能分析。此时上任何高级功能，都会被基础数据的缺口吃掉效果。

另外建议单独看一项：第 17 项，并行期同一业务能否按业务维度聚合。这一项如果是“待补充”或“未覆盖”，并行期出故障时，定位时间往往不是按分钟算，而是按小时算。它和总分高低无关，但优先级通常最高。

八、如果分数不低，先做这三步

这部分不是完整方案，只是我们做了几十个项目之后，比较稳的一个开工顺序。

第一步，先纳管后收敛。按机房动环、网络、服务器与操作系统、数据库、中间件、应用、安全设备七类盘一遍资产，能装采集端的装采集端，网络设备走 SNMP，数据库走原生接口，装不了的走无侵入探测。完成标准很朴素：服务器、网络、数据库三类对象覆盖率到百分之百，缺的那几台要能说清为什么缺。

第二步，先试点后推广。选点不选最复杂的，选有代表性、有痛点、有人盯着的那一个。试点的交付物不是一套软件，而是四样东西：指标模型、告警规则、值班流程、验收记录。推广时复制这四样、改参数，不重新设计。

第三步，先指标后智能。关联分析要靠依赖关系，趋势预测要靠历史基线，这两样都在指标层。先跑七到三十天的基线，再做阈值动态化，最后才上关联与根因。跳过基线直接上智能，学出来的是错的。

九、清单说明与获取方式

边界声明：本清单是方法性自查工具，仅供内部自查参考，不构成监管合规结论，也不替代等保测评、监管检查或第三方审计。清单不含报价与服务承诺，也不构成对任何产品或厂商的推荐；第 20 项涉及的参数口径，均以第三方测试报告与正式材料为准。各单位请结合自身监管口径使用。

引用的说明：清单为方法工具，不引用具体标准条款作出判定；文中涉及等保要求的部分，仅提示应核查的方向（分权分域、操作留痕、日志可审计、敏感字段脱敏），实际是否符合，应以本单位等保测评结论为准。

获取方式：需要电子版或后续更新版，在监控易公众号回复“运维自查”四个字，系统会自动发送，不用留联系方式，也不用等人工回复。后续按行业整理的版本，会分别用“银行自查”“证券自查”“保险自查”发布，回复对应词即可。

更多运维资料，可在监控易官网的“资料下载”栏目自取，不需要注册。如果在使用中遇到清单没覆盖的场景，可以在公众号文章下留言写清环境与现象，我们整理后会做公开答疑。

更新与索取：本版为 V1.0，文档编号 MX-ZCX-2026-01，生效日期 2026 年 11 月 12 日。若后续修订，会沿用同一编号、递增版本号，并在下表登记；官网与公众号发出的均为最新版，旧版不再分发。需要引用本清单的段落，请注明版本号，避免不同版本混用。

十、版本与修订记录

版本	日期	修订内容	编制
V1.0	2026-11-12	首次发布。按外部审稿意见补充边界声明、版本控制、数据保密提示与判定口径，二十项判定统一为两档。	监控易团队

如对本清单有修订建议，可在公众号留言，我们会在下一版一并处理。