

服务中断时，如何维护信任

银行、金融与保险 / 8页 / 2026年10月3日

建议决策：将客户信息视为服务连续性的一部分。

什么会削弱信任

服务中断后，客户立即需要决定等待、重试、致电还是寻找替代方案。如果信息无法帮助他们作出选择，技术故障还会成为被忽视的体验。因此，传播应从业务韧性方案准备阶段就与运营和客户关系团队连接。

建议的管理选择

管理层确认单一事实基准、发布职责和适合事件进展的更新频率。专业团队判断监管义务，传播部门保证对公众解释的一致性。重点不是制造令人安心的措辞，而是提供准确、实用并能随事实变化而修订的信息。

需要确定的责任

指定事件情况负责人、客户信息负责人和发言人，确定备用渠道、脆弱客户支持方式及错误信息更正程序。事件复盘应分别检查服务恢复、个人后果处理和预防行动，不能以技术恢复替代全部问题的解决。

决策要点

客户在读完我们的第一条信息后，能否知道现在该做什么、去哪里获得帮助？

韧性也是公众体验

系统可用性、业务连续性和客户理解，需要放在一起审视。

挑战不只来自网络攻击

欧洲监管机构于2026年发布的DORA重大ICT事件首份报告，强调系统故障、外部事件和供应商依赖的作用[1]。准备工作不能只围绕入侵情景；系统迁移、第三方故障或配置错误，同样可能需要协调回应。

同一故障带来不同后果

不可用可能让个人无法付款、企业无法完成交易，或员工无法答复请求。总体消息应辅以适合这些情形的操作指引。银行或保险机构还需要区分真正受到影响的人，与担心自己受影响但实际未受影响的人。

安抚不能代替事实确定性

“一切都是安全的”可能超出调查所能证明的范围。更有用的做法是说明受影响功能、已检查事项和行动路径。承认不确定性，并不妨碍展示有序应对：谁在处理、何时更新、如何求助。

决策要点

可信回应可以承认未知，但必须清楚说明已知影响和可执行的下一步。

一份情况报告，多种有用回答

一致性并不意味着向所有对象发送完全相同的文字。

建设共同事实基础

情况报告应记录发现时间、受影响服务、已确认范围、已采取措施和未知事项，并保留版本及审批责任。面对客户的员工，应能及时获取最新版，而不是依赖非正式邮件转发。

调整解释而不改变事实

客户需要行动指引，员工需要答复及转介路径，媒体需要公开解释和跟进渠道，主管机构接收适用程序要求的信息。不同审核和时限应互相协调，但公开传播不能被当作监管通知的替代品。

为常用渠道失效做好准备

网站、应用或邮件工具本身可能不可用。必须测试备用渠道和消息真实性验证方式。诈骗者可能利用故障传播，指引应导向已知联系方式，不得引导客户提交密码、验证码或其他机密信息。

对象	需要的信息	共同基础
客户	影响、行动与帮助	已确认事实
员工	答复和转介路径	更新后的情况报告
媒体与主管机构	解释或规定的信息	一致事实与适用程序

决策要点

统一事实、区分对象，并在平时验证备用信息渠道是否真正可用。

用三种情景检验回应能力

以下情景用于组织演练，不描述真实金融机构的事故。

支付不可用，原因尚未查明

首次回应说明已观察到的影响、确实可用的替代方式和下次更新时间，不能承诺尚未确认的恢复期限。管理层决定支持资源投入、需要直接联系的客户群，以及技术结论形成前可以公开的信息。

故障同时引发数据泄露传言

仅有服务不可用，并不能证明数据被窃取。获授权团队评估情况，传播既避免无证据确认，也避免过早否认。“尚未发现”不等于“没有风险”。每项声明都应说明其范围，并依据事实向受影响人员提供适当指引。

不受欢迎的商业决定引发批评

事故后宣布调价，可能被认为与客户体验脱节。管理层应检查时间安排、经济理由及申诉或支持方式。传播不能单独解决服务质量与业务决定之间的矛盾，但应在发布前将矛盾明确呈现。

决策要点

演练重点是如何在信息不完整时作出合理决策，而不是背诵预设声明。

恢复服务后继续维护关系

技术事故结束，并不意味着受影响客户的问题已经结束。

区分三个阶段

恢复指功能重新可用；补救涉及个人后果、待核查交易或投诉；学习涉及原因和预防措施。混淆这三个阶段，容易在客户仍等待答复时，就宣布问题已经完全解决。

解释敏感经营决定

关闭网点、调整保障范围或改变服务，应说明理由、时间和实际后果。决定合法或符合合同，并不自动使其易于理解。一线团队必须能够回答具体情况，或引导客户进入清晰的处理程序。

让公共事务连接真实体验

机构关系有助于理解地方期待、服务可及性和公共决策者的关切，但必须同客户实际体验及本地传播结合。管理层应区分必须履行的义务、自愿承诺，以及仍有对话空间的选择。

决策要点

结束事故沟通之前，先确认个人后果的处理责任和后续联系渠道。

组织可验证的信任信息

良好声誉需要公众能够找到、理解并核实的信息。

准备媒体关系

发言人与专家应共享事件时间线、范围和词汇。回答记者时，要区分已证实事实与假设。事后说明改进措施可能有价值，但不能泄露有利于攻击者的细节，也不能作出绝对安全保证。

避免数字渠道互相矛盾

帮助页面、应用通知、机构网站和社交媒体应指向权威参考信息。旧事故指引要标注日期和结束状态，否则搜索或AI可能把过去情形呈现为当前问题。GEO工作从内容准确、可获取和一致开始[2]。

观察信息是否真正有用

测试公众实际会问的问题：服务是否可用、如何求助、品牌是否相同、应该联系谁。记录错误回答和引用来源，测试中不使用个人数据。品牌被引用的次数，不能说明客户是否得到了安全可用的指引。

决策要点

恢复状态、帮助路径和联系方式，应比声誉口号更容易被找到。

90天让回应机制可执行

计划应与既有业务连续性和事故管理程序协调。

第1至30天：识别差距

把正式程序与客户在服务中断时的真实路径比较，找出同时失效的渠道、没有替补的负责人和矛盾消息。结合近期投诉原因及一线重复问题，形成有明确责任人的整改清单。

第31至60天：模拟压力

让运营、安全、合规、客户关系、人力资源和传播共同演练，并在过程中逐步改变信息。检查首次发布、更正和多渠道协调能力。评价重点是部分信息条件下的决策，而不是对熟悉脚本的背诵。

第61至90天：建立跟踪

更新指引，培训替补人员，测试备用手段。准备复盘模板，分别记录客户后果、信息质量和运营改进。管理层追踪尚未修复的差距并提供资源，后续演练应变化情景，避免产生虚假的准备感。

决策要点

机制有效的证据，是演练中能发现并纠正错误，而不是文件已经齐全。

衡量什么能保护客户关系

指标既要反映发布速度，也要反映公众实际体验。

建议跟踪的指标

观察确认影响到发布有用信息的时间、不同渠道一致性、因解释不足产生的重复请求，以及个人后果的处理情况。保留计算基础，按事故范围区分，避免总体平均值掩盖小范围客户的严重问题。

谨慎解释变化

联系量增加可能反映担忧，也可能说明帮助渠道更容易找到。公开讨论减少，不能单独证明信任恢复。管理层应把传播观察与服务数据、获授权团队反馈相互核对，而不是仅根据舆情音量下结论。

正式确认管理决定

明确情况报告责任、备用渠道和结束沟通的条件。要求一次演练复盘展示发现了什么错误、作出了什么决定，以及落实了什么改进。在下一次事故发生前，让机制得到实际检验。

可信传播应让人们能够理解和行动，即使服务仍然受到影响。

资料来源与参考

[1] ESMA, EBA, EIOPA — First report on DORA major ICT-related incidents

[2] Google Search Central — AI features and your website

分析与建议由Belief System提出。报告中的情景仅用于示例推演。所引资料用于说明背景，不代表来源机构认可本报告的建议。