

When service stops, trust is on the line

Banking, finance & insurance / 8 pages / 3 October 2026

Proposed decision: treat information for customers as a component of continuity of service.

What weakens trust

A service interruption leaves customers with immediate decisions: wait, try again, call or look for an alternative. If the information does not help them choose, a technical breakdown also becomes a experience of abandonment. Communication must be linked to operations and customer relationship as soon as the resilience arrangements are prepared.

Recommended decision

The committee validates a single factual baseline, publication responsibilities and an update frequency adapted to the situation. The competent teams determine regulatory obligations; communication organizes the consistency of explanations to the public. The priority is not to produce a reassuring formula, but to provide accurate, useful and reviewable information.

Decisions expected

To designate a person responsible for the situation report, a customer information officer and a spokesperson. To define the emergency channels, the modalities of assistance to vulnerable customers and the procedure for correcting erroneous messages. To provide for a post-incident review which distinguishes service restoration, resolution of individual consequences and preventive actions.

DECISION POINT

Can a customer understand what to do without knowing the internal organization of our group?

Resilience is also a public experience

System availability, business continuity and client understanding need to be reviewed together.

A challenge beyond cyberattack

The first overview of the major incidents reported under DORA, published by the European authorities in 2026, highlights the role of system failures, external events and provider dependencies [1]. Preparation should therefore not be limited to an intrusion scenario. Migration, third-party failure or configuration error may also call for a coordinated response.

Different consequences for the public

The same unavailability may prevent an individual from paying, a company from carrying out a transaction or an employee from responding to a request. The general message must be supplemented by instructions relevant to these situations. The bank or insurer must also distinguish the persons actually affected from those who are worried but not affected.

Do not confuse reassurance with certainty

A formula such as "everything is secure" can go beyond what the investigation can establish. It is more useful to indicate the features involved, the elements checked and the course to be followed. The communications team can acknowledge uncertainty while showing an organization: who is responding, what information will be updated and how to access help.

DECISION POINT

Trust also depends on the ability to make an uncertain situation workable for the client.

A situation report, several useful answers

Consistency does not consist in sending the same text to all recipients.

Build the common base

The situation report records the time of detection, the services affected, the confirmed scope, the measures taken and the unknowns. It is versioned and its validation is assigned. Employees who respond to customers must access an up-to-date version without waiting for an informal flow of emails.

Adapt the answer without altering the facts

Clients need guidance and assistance. Employees need to know what to say and where to guide. The media expect a public explanation and a possibility of follow-up. The authorities receive the information determined by the applicable procedures. Validations and timetables must be coordinated, without presenting a public communication as a substitute for a regulatory notification.

Provide operation in disrupted conditions

The usual site, application or mailing tool may not be available. It is necessary to test the emergency channels and means of authenticating messages. Incident communications can be exploited by fraudsters: instructions must direct to known contact points and avoid inviting customers to transmit secrets or codes.

Audience	Priority need	Coordination owner
Customers	Impact and action to take	Customer relations and operations
Employees	Instructions and referral routes	Internal communications
Media	Facts and next update	Media relations
Authorities	Required information	Compliance and authorised teams

DECISION POINT

A single reference chronology; messages tailored to the needs of each audience.

Test responses to three situations

The scenarios below are illustrative and are used to prepare an organization without describing a real incident.

Unavailable payments, cause still unknown

The first answer explains the impact observed, the alternatives actually available and the time of the next point. It does not promise an unconfirmed resolution deadline. The committee decides on the level of mobilization of assistance, the audiences to be contacted directly and the information that can be published before the technical conclusion.

A rumor of leaking data accompanies the breakdown

Service unavailability alone does not establish data exfiltration. The authorized teams assess the situation and communication avoids confirming without proof as well as denying prematurely. Messages must specify the scope of each statement: "we have not identified" is not synonymous with "there is no risk". The persons concerned are given appropriate instructions where the facts permit.

Unpopular business decision revives criticism

A tariff change announced after an incident can be seen as disconnected from the customer experience. The committee must examine the schedule, economic explanation and possibilities of recourse or accompaniment. The communication cannot resolve only a contradiction between the service rendered and the decision taken. It must make this contradiction visible before publication.

DECISION POINT

Does the public discourse remain defensible in the face of the client who has suffered the most concrete consequence?

Preserving the relationship after the return of service

The end of the technical incident is not always the end of the incident for those concerned.

Distinguish three steps

The recovery describes the return of features. Remediation deals with individual consequences, transactions to verify or complaints. Learning is about causes and prevention actions. Mixing these steps can lead to announcing a complete resolution while clients are still waiting for an answer.

Explain a sensitive decision

A branch closure, a change in coverage or a change in service must be presented with its reasons, timetable and practical consequences. The legal or contractual nature of a decision is not sufficient to make it understandable. Field teams must be able to respond to specific situations or direct them towards a clearly defined procedure.

Giving a place to public affairs

Institutional relations help to understand the territory's expectations, the issues of access to services and the concerns of public decision-makers. They must be linked with real customer experience and local communication. The committee is better able to distinguish between obligations, voluntary commitments and choices on which dialogue remains possible.

DECISION POINT

A resolution announcement must specify what is being re-established and what remains to be addressed.

Make trust verifiable

A strong reputation requires information that the public can retrieve, understand and verify.

Prepared media relations

The spokesperson must have a common chronology, perimeter and vocabulary with the experts. Replies to journalists must separate established facts from assumptions. After the incident, an explanation of the actions taken may be useful; it must not disclose elements that would facilitate an attack or announce absolute guarantees.

A digital presence without contradictions

Help pages, application messages, institutional site and social publications should refer to reference information. Previous incident instructions must be dated and closed. A search engine or AI service can otherwise present a past situation as current. GEO work begins with the accuracy, availability and consistency of these contents [2].

Observe what is useful

Test the questions that audiences really ask: service available, assistance procedure, distinction between brands, contact details. Identify the wrong answers and sources used, without using personal data in tests. The frequency of citation of a brand does not tell whether a customer receives safe, actionable instructions.

DECISION POINT

The correct, dated information on the right perimeter and accessible from the channels that the customer uses.

90 days to make the process operational

The proposed programme should be coordinated with existing continuity and incident management procedures.

Days 1 to 30 - Mapping variances

Compare the official procedures with a client's actual journey during an interruption. Identify unavailability of channels at the same time, owners without designated backups and contradictory messages. Also consider the latest grounds for complaint and repeated questions to field teams. The diagnosis must lead to a list of assigned corrections.

Days 31 to 60 - Simulate pressure

Conduct an exercise combining operations, security, compliance, customer relationship, human resources and communication. Introduce evolving information during the session. Verify the publication of a first message, its correction and channel coordination. Assess the ability to decide with partial information rather than recitation of a learned scenario.

Days 61 to 90 - Installing follow-up

Updating instructions, training replacements and testing back-up means. Prepare a review template distinguishing customer consequences, quality of information and operational improvements. The committee follows outstanding gaps and validates the means that are lacking. Subsequent exercises must vary situations so as not to create an illusion of preparation.

DECISION POINT

The process works even when the usual tool or a key role holder is unavailable.

Measuring what protects the relationship

Indicators should shed light on public experience as well as on the speed of publication.

Recommended measures

Follow the time between confirmation of an impact and useful information, consistency between channels, repeated requests for lack of explanation and treatment of individual consequences. Keep calculation bases and distinguish incidents according to their perimeter. An overall average should not mask a serious situation for a restricted public.

Interpret with caution

An increase in contacts may indicate concern, but also a greater visibility of the assistance. A decrease in public discussion alone does not lead to a return of confidence. The committee combines communications observations with the service data and the feedback from authorised teams.

The decision to formalize

Validate the responsibilities of the situation report, emergency channels and closing rules. Request a debrief of an exercise showing an error detected, a decision made and an improvement actually implemented. The aim is to make the process testable before the next incident.

Trusted communication empowers people to understand and act, including when service is weakened.

Sources and reference points

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

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

Analysis and recommendations by Belief System. Scenarios are illustrative. Sources provide context; they do not constitute endorsement of our recommendations.