Document initial messages per organisation

Fictional case data and worked reasoning

On May 10, 2028, a failed warning function of a networked device disrupts two regulated customers. The manufacturer knows about 09:20 UTC a confirmed serious safety incident with effect on the safety of his product. The German water operator gains knowledge of its own significant security incident at 10:30 UTC. A bank knows its ICT-related incident around 10:10 UTC and considers it serious by 13:00 UTC based on their own criteria. The three documented decisions are case assumptions. They are executed by the responsible parties each time.

Test point Purpose or comparison Observation Decision		
Manufacturer CRA-Kntnis on May 10 around 09:20	Serious product incident confirmed	Early warning no later than 11 May 09:20 UTC
Water operator BSIG-Knisse um 10:30 Own significant evidence		Early first notification no later than 11 May 10:30 UTC
Bank knowledge 10:10, classification 13:00 Four hours after classification are first reached		First notification no later than 10 May 17:00 UTC

Expected result

Separate reporting files per legal entity with time, competent authority, receipt and reference to common chronology.

The information provided shall be recorded on the same time basis and, where appropriate, on the same classification.

Matching your own competent transmission and calculated plan mark.

Secure receipts and follow-up tasks for each reporting track.

Counter-test and next decision

Do not accept the confirmed DORA classification and keep track of the incident. The bank has an open placement order and no calculated first mark for a case considered serious. The confirmed CRAand BSIG reporting channels and their time-receipts remain valid.

Document initial messages per organisation

For your observation, specify a findable document.

Calculate the first registration marks for three confirmed decision-making paths and secure their charges.

Verification identification, legal entity and date of processing and responsible body

Product, event identifier and actual entity

Own knowledge, classification and location of the documents

Triggers, calculated first mark and competent body

Actual charge with condition and recipient

Document of transmission, follow-up order and previous status

Document initial messages per organisation

Refer remedial and post-test to the original test order.

Findings and supporting evidence

Required updating of the joint event file

Tested follow-up test with date, observation and version documentation

Full proof of dispatch and decision

Release by and on the open order and date