EUROPEAN CENTRAL BANK
EUROSYSTEM

DG-MIP/MIM

Managing long-lasting TARGET2 incidents

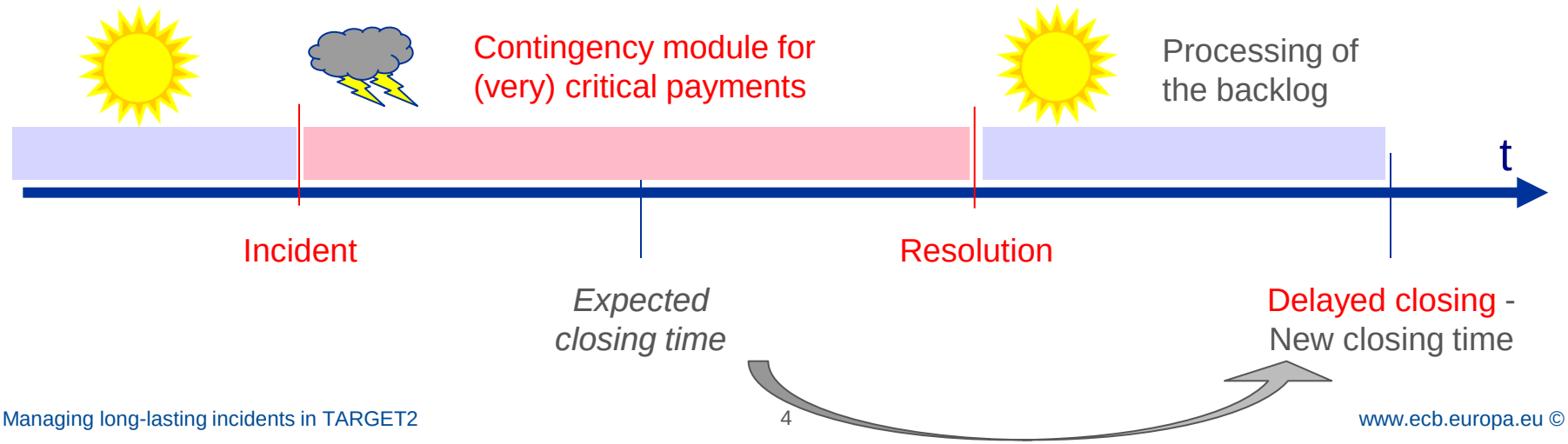
AMI-Pay, 29 September 2017

Overview

Overview

Current situation

- **Assumption:** possible to resume full TARGET2 single shared platform (SSP) processing capabilities on the day of the disruption
- Recovery Time Objective (RTO) ≤ 2 hours
- Recovery by 22:15 would still ensure a start of the day trade phase at 07:00 on the following business day
- Response to disruptive events severely affecting TARGET2 availability
  - consists of using the contingency module (for very critical and critical payments)
  - possibly combined with a delayed closing



Limitation of current arrangements

- Contingency Module: ability to perform contingency payments only on the same business day
- A very late closing (technically feasible) may create severe disruptions to Central Banks, banks and markets, in particular if it goes beyond midnight
- No effective response to new challenging scenarios going along with the changed threat landscape (e.g. cyber attack resulting in the corruption of data)
- Not appropriate to meet new oversight requirements (e.g. CPMI-IOSCO guidance on cyber resilience for FMIs)

Overview

General considerations, definitions and assumptions

- **Scope**
  - Work based on the existing technical and operational set-up
  - Development of a “throw-away” solution should be avoided
- **Long-lasting incident**
  - No scenario-based approach
  - Definition: “an event preventing the timely start of the day trade phase of the following business day”
- **Impact**
  - TARGET2 SSP is considered unusable by the TARGET2 Crisis Managers
  - It can be reasonably assumed that normal operations cannot be resumed and the day trade phase of the following business day cannot start in a timely manner
  - Maximum duration: five business days
  - Network service provider is not impacted/is available

General considerations, definitions and assumptions

- Oversight requirements
  - resumption requirement specified in the Principles for Financial Market Infrastructure (Key consideration 17.6)
  - Guidance on cyber resilience (section 6.2.3) specifies an additional requirement. Accordingly, an FMI
    - *"…should also plan for scenarios in which the* [two-hour recovery time] *objective is not achieved."*
    - *"…should analyse critical functions, transactions and interdependencies to prioritise resumption and recovery actions, which may, …, facilitate the processing of critical transactions."* This includes planning for situations where *"…systems may be unavailable for significant periods"*.

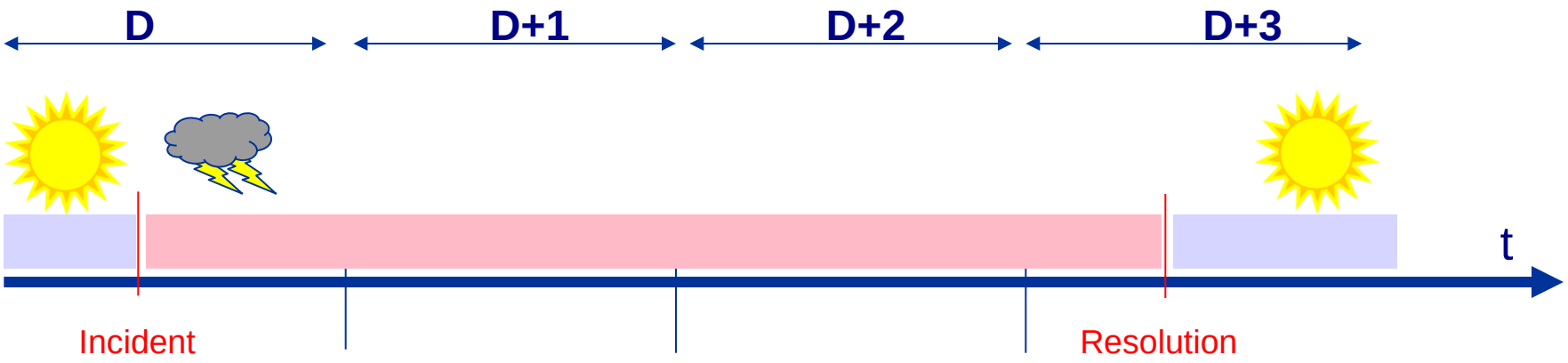
General considerations, definitions and assumptions

- Critical transactions
  - Definition:
    - Clean payments
      - Concept of very critical and critical payments remains unchanged
      - Challenging to set-up objective criteria for categorising interbank and customer payments
      - Banks are best positioned to assess criticality of payments
    - Ancillary systems:
      - importance/criticality increases the longer the system is unusable
      - generally to be supported

Overview

Objective

- Define requirements to increase the preparedness of TARGET2 to cope with a long-lasting incident



Requirements

- Degraded service
- Capacity
  - Clean payments
  - Ancillary systems
    - ASI procedure 4 should be supported
    - No night time settlement
- Functional
  - Starting balance zero
  - Connectivity: banks access to the GUI (U2A mode)
  - Mechanism to allow CBs to control/prioritise payments flow

Requirements

- Non-Functional
  - Segregated from the one hosting the TARGET2 SSP
  - TARGET2 operating day with the exception of night time settlement
  - Number of concurrent users: the same as supported for U2A access today
  - TARGET2 accounts main accounts mirrored
  - Reconciliation after recovery
- Information security
  - in principle be compliant with TARGET2 security requirements and controls

Next steps

- Eurosystem internal consultations
- Preparing change request for cost and feasibility assessment

Questions?