EUROPEAN CENTRAL BANK

EUROSYSTEM

Information Guide for TARGET participants

Part 2 – CLM & RTGS

Version R2024.JUN

June / 2024

Contents

1 Introduction

1.1 Purpose of the Information Guide for TARGET participants

The Information Guide for TARGET participants (hereinafter referred to as the "Infoguide") aims to provide TARGET participants (credit institutions, ancillary systems, other entities settling in TARGET[1]) with a comprehensive set of information regarding the functioning and operational procedures of TARGET settlement services during both normal and abnormal situations.

The Infoguide consists of four parts:

1. Fundamentals
2. **CLM & RTGS**
3. TIPS and
4. T2S Cash

The Fundamentals part describes the aspects that apply similarly across TARGET settlement services, the **CLM & RTGS** part describes the specific procedures applicable to the operation of central liquidity management (CLM) and RTGS services, the TIPS part describes the specific procedures applicable to the TARGET Instant Payment Settlement (TIPS) service, and the T2S Cash part describes the specific procedures applicable to T2S dedicated cash accounts (T2S DCAs).

while TARGET was developed to offer multi-currency services, this Infoguide describes all relevant procedures for the euro currency. For other currencies, the central bank making its currency available in TARGET[2] is responsible for the relevant operational procedures, which are not covered in the Infoguide.

Scope of the **Infoguide PART 2: CLM & RTGS** (hereinafter referred to as the **CLM & RTGS Infoguide**) excludes functional/technical descriptions of CLM and RTGS, as well as the internal process of Level 3 NCBs[3] (hereinafter referred to as the 4CB).

Note: the CLM & RTGS Infoguide complements the Fundamentals Infoguide and is not to be used as a stand-alone document.

All references throughout this document to "CLM and/or RTGS participants" refer to participants as well as other entities authorised to access their account (e.g. co-managers for CLM). All references throughout this document to "TARGET users"

---

1 Additional information may be found in Chapter 2.4 of Fundamentals Infoguide.

2 By signing a Currency Participation Agreement (CPA).

3 Level 3 NCBs means the Deutsche Bundesbank, Banque de France, Banca d'Italia and Banco de España (4CB) in their capacity as the CBs developing and operating TARGET for the Eurosystem's benefit.

refer to an individual or an application that can log into a service with a login name and password.

All times in this document refer to the local time at the seat of the European Central Bank (ECB), i.e. Central European Time (CET) / Central European Summer Time (CEST).

1.2 Structure of the CLM & RTGS Infoguide

The CLM & RTGS Infoguide starts with an introductory part (**Chapter 1**) to explain to the reader the purpose and structure of the Infoguide.

Chapter 2 contains CLM & RTGS-specific information on participation in CLM and RTGS and communication flows.

Chapters 3 and 4 describe the CLM and RTGS-related operational procedures to be respectively applied under normal and abnormal situations.

Chapter 5 deals with how service continuity is assured by the use of different tools and business continuity measures.

Chapter 6 enlists and describes the testing activities for CLM and RTGS.

Chapter 7 covers the receipt and payment of invoices for participants.

Chapter 8 describes the change, release and deployment management procedures for CLM & RTGS for the annual releases and for other emergency changes and what are known as “hotfixes”.

Chapter 9 describes the processes for gathering and sharing information about the endpoint security of RTGS participants.

1.3 CLM & RTGS Infoguide change management

The CLM & RTGS Infoguide is reviewed and updated in line with the chapter titled “Infoguide change management” (see Chapter 1.4 of the Fundamentals Infoguide).

2 General information

2.1 Types of participation

TARGET participants are entities that have at least one main cash account (MCA) and may additionally hold one or more dedicated cash accounts (DCAs) in TARGET or ancillary systems.

Note that reference is made in this chapter to both participants (holding one or more TARGET accounts in CLM and/or RTGS) and other actors that have a direct technical interaction with CLM and/or RTGS.

Central bank

Central banks are responsible for maintaining the reference data of their respective banking community and may act on behalf of their registered participants in contingency.

2.1.1 CLM

MCA holder (participant)

The access criteria for holding an MCA, or any other TARGET cash account, are set out in the Guideline (EU) of the European Central Bank on a new-generation Trans-European Automated Real-time Gross settlement Express Transfer system (TARGET) and repealing Guideline ECB/2012/27 (hereafter referred to as “TARGET Guideline”) (Annex I, Part I, Article 4).

MCAs are opened by the competent central banks and are used to settle central bank operations and liquidity transfers (for overnight deposit accounts, to/from all TARGET settlement services and between two MCAs belonging to the same MCA liquidity transfer group).

Co-management

MCA holders may authorise another MCA holder or their responsible central bank (if such service is offered by the central bank) to act as co-manager of their MCA.

The aim of co-management is to allow participants to delegate all or some of the activities in CLM to a co-manager. Participants with only MCA(s) choosing to co-manage their MCA(s) do not need to establish their own technical connection to access CLM as activities can be delegated to the co-manager. For example, banks only fulfilling their reserve requirement directly can delegate cash flow management – transferring excess liquidity from its MCA to a different account – to another bank (co-manager).

Note: MCA holders choosing to designate a co-manager are still bound by any action taken by the co-manager.

More details about co-management can be found in Chapter 3.2.3 “Functionalities” of the CLM UDFS.

2.1.2 RTGS

RTGS DCA holder (participant)

The access criteria for holding an RTGS DCA, or any other TARGET cash account, are set in the TARGET Guideline, Annex I, Part I, Article 4.

The RTGS DCAs are opened by the responsible central bank and are used to settle payment orders to or from RTGS DCAs, cash transfer orders to ancillary systems (AS) guarantee fund accounts, cash transfer orders related to AS (may also settle on RTGS sub-accounts) and liquidity transfers to or from all TARGET settlement services.

Note: RTGS DCA holders are required to also open an MCA with the same central bank.

AS technical account holder (participant)

TARGET provides **ancillary systems (AS)** with functionality to settle AS transfer orders in central bank money.

As defined in the TARGET Guideline, AS are systems operated by entities established in the European Union or the EEA that are subject to supervision and/or oversight by a competent authority and comply with the oversight requirements for the location of infrastructures offering services in euro, as amended from time to time and published on the ECB’s website, in which payments and/or financial instruments are exchanged and/or cleared or recorded with (a) the monetary obligations resulting in transfer orders which are settled in TARGET and/or (b) funds held in TARGET.

Examples of AS include retail payment systems (RPS), large-value payment systems (LVPS), foreign exchange systems, money market systems (MMS), automated clearing houses (ACH), central counterparties (CCP) and securities settlement systems (SSS).

Optional: in contrast to other participants, AS are not required to hold an MCA but may ask to open one, such as for the payment of TARGET settlement services-related invoices. It is important to note that an AS will need to open an MCA if it wishes to have a contingency account in ECONS II for supporting settlement via “clean” payments.

Required: the Eurosystem requires AS to make use of the AS settlement procedures in the RTGS due to the criticality and specificity that they represent as system participants as well as the benefits identified compared to AS settlement via

“clean” payments. These benefits include technical, liquidity and information efficiencies. However, the Eurosystem also allows an AS to request a derogation whereby an AS could open an RTGS DCA (i.e. in addition to or instead of an AS technical account) in order to make use of “clean” payments. In this case, the AS wishing to benefit from a derogation and open an RTGS DCA should turn to its responsible central bank for further information. Note that if an AS requests a derogation to open an RTGS DCA, then an MCA must also be opened. The responsible national central bank will make an initial assessment on whether to grant a derogation based on the existence the following factors:

- a temporary reason relating to a change in the AS’s operating model;
- the use of standard payments procedures for an AS’s secondary activity (e.g. activity that does not directly relate to the settling of monetary obligations of its clearing members that arise within its system from the clearing of different instruments);
- where the AS carries out two different businesses (i.e. AS and banking business).

Once assessed by the NSD, a derogation request must be endorsed by the Eurosystem.

According to the settlement procedures used by the AS, the following type of accounts for AS settlement can be opened:

1. Sub-account
2. Guarantee funds account
3. AS technical account

Addressable BIC holder

RTGS DCA holders may register their correspondents or customers or branches as addressable BIC holders. Cash transfer orders to/from an addressable BIC holder can be sent and received only by the respective RTGS DCA holder on the addressable BIC holder’s behalf. These cash transfers are settled on the RTGS DCA holder’s account. Addressable BICs are eligible to be listed in the RTGS Directory irrespective of their place of establishment.

Note: it is the responsibility of the RTGS DCA holder to forward the relevant information to the respective central bank so that it can perform the necessary reference data configuration for the set-up of the addressable BIC holders and include the addressable BIC in the RTGS Directory.

Multi-addressee access

RTGS DCA holders may authorise branches and credit institutions belonging to their group to channel payments through their RTGS DCA, without their involvement, by submitting/receiving cash transfers directly to/from RTGS. This offers affiliate banks

or groups of banks efficient features for liquidity management and payment business.

In practice, a multi-addressee bank is able to send and receive cash transfers from/to its own BIC address. However, cash transfers are booked on the account of its RTGS DCA holder.

Note: it is the responsibility of the RTGS DCA holder to forward the relevant information to the respective central bank so that it can perform the necessary reference data configuration for the set-up of the multi-addressee access users and include the multi-addressee access BIC in the RTGS Directory.

2.2 Monetary policy eligible counterparty (MPEC) configured as multiple parties in a TARGET component system

In order to allow for the correct computation of automatic marginal lending for a monetary policy eligible counterparty (MPEC), each MPEC should be configured as one party in the Common Reference Data Management (CRDM). This allows the CLM to sum up the cash balances of all accounts opened under this party. If the total amount is negative, the liquidity required to bring it to zero is pulled from the marginal lending account[4] of the participant into its MCA (automatic marginal lending).

However, at the time of the TARGET go-live, a few cases were identified of MPECs that had multiple parties opened within one national TARGET component system. Therefore, for these participants, the CLM computation of automatic marginal lending cannot be executed correctly, as the CLM cannot compute the sum of all accounts across different parties.

Required actions

- All MPECs modelled as several parties are encouraged to merge their parties into one.
- In order to comply with the TARGET Guideline conditions on credit extension for intraday credit (marginal lending), the responsible central banks of these participants must ensure, on a daily basis, that all TARGET account balances of one MPEC are taken into account for the purpose of calculating the amount of the entity's recourse to the automatic marginal lending facility.
- MPECs modelled as several parties in TARGET have only one of those parties configured as eligible for marginal lending (i.e. set up with "marginal lending indicator=Yes" in CRDM). These participants must set up daily standing orders for each of their accounts under the parties with "marginal lending indicator=No" transferring all liquidity on these accounts to the accounts under the party with

[4] Or from the CLM CB account after the go-live of ECMS.

"marginal lending indicator=Yes".[5] The standing orders should be set to be executed with event "cut-off for CLM RTS (CCII)".[6] Note that if TIPS DCAs are not opened under the party with "marginal lending indicator=Yes", it could be preferable not to empty the account at the end of each day. In this case, participants are advised to close that specific TIPS DCA and open another TIPS DCA under the party with "marginal lending indicator=Yes".

- NSDs with these participants in their community monitor the execution of these standing orders daily, ensuring that liquidity is swept to the party eligible for marginal lending at the end of the day. If the standing order is not executed properly, on the next business day the NSD will perform manual corrections to the participant's recourse to automatic marginal lending for the impacted day.

- MPECs may, according to their business needs, decide on how to ensure that the "emptied" account is funded again. These participants may choose to: (i) set up a standing order/rule-based liquidity transfer order to be executed with event "Execution of standing orders in CLM (CESO)" for a fixed amount that they consider to be sufficient; (ii) manually instruct an immediate liquidity transfer order for the required amount once "CESO" has taken place; or (iii) put in place a standing order which can be amended to the exact amount prior to settlement (i.e. before "CESO").

- In accordance with the relevant decision by the Market Infrastructure Board, each MPEC should be set up as one party per national TARGET component system by 1 March 2024. This deadline was extended to 30 June 2024.

- These rules should also be followed for new TARGET participants.

Cases eligible derogations from the rules

- Legal reasons: In some cases, MPECs are required under legal acts (e.g. in the case of cover pools for covered bonds) or court decisions to keep some of their funds outside of the scope of automatic marginal lending.

- Technical reasons: there are two scenarios under which it is impossible to merge parties:

    - Where an ancillary system (AS) uses both AS settlement procedures C and D. In this case, the AS technical account linked to AS settlement procedure D (which can hold overnight liquidity) should fall under the party eligible for marginal lending, whereas the AS technical account linked to AS settlement procedure C should be linked to the other party. Since that account does not hold overnight liquidity, it may be held by a different party, without affecting the marginal lending.

---

5 As the end-of-day balances cannot be predicted, the standing orders should be set for extremely high amounts. This way, the standing orders will be partially settled by moving the entire amount into the specific DCA account.

6 Scheduled at 18:00.

- Where an AS owns a T2S DCA, because it needs both an AS party (for billing purposes, and if it uses AS settlement procedures) and a payment bank party, (as only payment banks may own T2S DCAs).

If these technical constraints apply, the relevant central bank monitors on a daily basis that liquidity is swept to the party eligible for marginal lending at the end-of-day.

- **Critical MPECs:** If a critical MPEC has a complex account structure with multiple levels of self-collateralisation in T2S and complying with the one-party rule would entail a significant operational risk due to the need to recreate the entire account structure in T2S.

- **MPECs with branches or different business areas**: if defined as one party, it is currently not possible to configure separate access rights for the accounts set-up for headquarters and the ones set-up for branches or, in another case, to separate the access rights for the accounts set-up for different business areas of a MPEC. As this represents an operational risk, a derogation from the one-party rule is granted until the implementation of the change request[7] which will allow that access rights are separated at account level (and no longer at party level). Following the implementation of the CR, derogations granted for this reason will no longer be applicable.

- **MPECs which need to send the account statement message (camt.053) to different entities**: T2 only allows for account statement messages (for all the accounts) of one party to be sent to one distinguish name (DN). A derogation from the one-party rule is granted until the change request *T2-0096-SYS (Account statement report configuration at account level)* is implemented[8]. The implementation of this change request will allow that the account statement messages are sent to different DNs for different accounts, which will remove the need for a derogation from the one-party rule.

- **Mergers of different MPECs**: if different parties still need to exist for an interim period while a merger is taking place, a derogation can be granted for one year from the start of the merger process, allowing time for successful completion of a merger.

2.3 Configuration of DN-user link

Each person or application connects to TARGET making use of a unique distinguished name (DN). The functionality of CRDM allows for a person's DN to be linked to more than one system user, as well as one system user being linked with multiple DNs.

[7] Implementation of the change request is foreseen at the occasion of the T2 release R2025.NOV, at the earliest.

[8] Implementation of the change request is foreseen at the occasion of the T2 release R2025.NOV, at the earliest.

However, a **risk may arise under the following scenario**: if one person has more than one system users in the same party linked to more than one DNs (where the DNs are each issued by different NSPs), the four-eyes principle could be bypassed (i.e. if the user creates and approves an action using a different NSP's DN for each step). It is noted that this risk does not materialise in case of multiple DNs being linked to the same system user.

It is noted that the participants are responsible for the proper management of their reference data including their system users' configuration and linked DNs.

This risk will be eliminated with the deployment of the change request *T2-0124-URD Prevent four-eye bypass with NSP check.*

2.4 Distinguished names in the Common Reference Data Management

Depending on the NSP naming conventions, it should be noted that for personal tokens and personal HSM users, the DN might need to stand for a person and to follow a format such as "firstname-lastname", which means that personal data will be visible in the CRDM.

This risk will be eliminated at the occasion of the T2 R2025.JUN release with the deployment of the change request *T2-0129-URD CRDM admin users access rights scope limitation*.

2.5 Communication flows

Note that, in general, the contact point for CLM and/or RTGS participants is the National Service Desk (NSD). The communication flows and tools used for CLM and RTGS are the same as for all TARGET settlement services and are described in detail in Infoguide Fundamentals (Chapter 2.3).

3 Operational procedures during normal operations

3.1 Daily operations

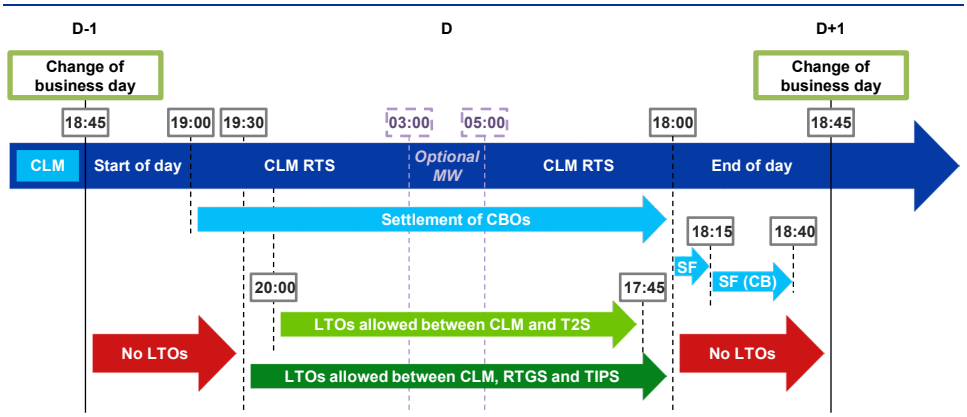
3.1.1 CLM daily operations

3.1.1.1 CLM business day overview

The schedule of a CLM business day comprises the following main periods:

- Start of day (SoD)
- CLM real-time settlement (CLM RTS)
- Maintenance window (MW), if activated
- End of day (EoD)

Figure 1
CLM business day schedule with optional MW – euro



The table below provides an overview of the different periods and the related CLM settlement events and processes.

Table 1

Overview of CLM business day

CLM Period	CLM Settlement day events	Time/Predecessor	CLM Processes
CLM SoD	**Change of business day (CSOD)**	Approx. 18:45 Following completion of CCOS – End of day close of service	• Change of business day • Revalidation of warehoused payments • Execution of standing order reservations for the settlement of CBOs
CLM RTS	**Start of CLM RTS (CRTI)**	19:00 Following completion of CSOD – Change of business day	• Reimbursement of marginal lending, calculation and posting of interest • Refunding of overnight deposit, calculation and posting of interest • Creation of automated LTOs to pull missing liquidity from linked RTGS DCAs in case of queued/pending CBOs • Creation of rule-based liquidity transfers in case of floor or ceiling breach • Start of processing of CBOs (including SFs) sent by CBs
	Execution of standing orders in CLM (CESO)	19:30	• Processing of standing order liquidity transfers defined for this specific event • Start of processing of immediate, rule-based and automated liquidity transfers • Note: liquidity transfers in T2S are settled after 20:00 (with C1S0)
CLM Maintenance Window (MW)	**Start of MW (CSMW)**	02:30 for mandatory MW 03:00 for optional MW	
	End of MW (CEMW)	02:30 for mandatory MW 05:00 for optional MW	
CLM RTS	**Cut-off for CLM RTS (CCII)**	18:00	• Processing of standing order liquidity transfers defined for this specific event • Closure of settlement of immediate, rule-based, automated liquidity transfers and CBOs (except SFs, connected payments and credit line modifications) • Note: liquidity transfers to T2S after 17:45 are rejected by T2S • Reservation modifications, payment orders and task queue orders (except SFs, connected payments and credit line modifications) with non-final status are rejected
	Data propagation for CLM and RTGS (T2DP)**	18:00	• Propagation of all already captured CLM and RTGS reference data from CRDM to CLM and RTGS
CLM EoD	**Start of end of day (CEOD)**	Approx. 18:00 Following completion of CCII – Cut-off for CLM RTS	• Collection of General Ledgers (GL) from RTGS, TIPS and T2S • Sending of GLs to the central banks • Calculation of cross-CB turnover
	General cut-off for SF (CCSF)	18:15*	• Cut-off for the use of standing facilities (for participants)
	CB cut-off for SF (CCML)	18:40*	• Cut-off for the use of standing facilities (by central banks)*** • Closure of settlement of connected payments and credit line modifications • Credit line modifications and task queue orders with non-final status are rejected • Check of cash accounts to be closed as of the next business day and processing of emergency liquidity transfer in case of need • Calculation of aggregated EoD balance of participants (considering liquidity positions received via GLs from RTGS, TIPS and T2S) • Settlement of automatic marginal lending • Calculation of running average and adjustment balance for minimum reserve • Calculation of interest for accounts subject to interest calculation • Creation of reports scheduled for EoD • Sending of CLM GL to central banks
	End of day - Close of service (CCOS)	Approx. 18:45** Following completion of CCML	

* Postponed by 15 minutes on the last business day of the minimum reserve maintenance period.
** Reference data valid as of the next business day must be captured before event data propagation, scheduled for 18:00.
*** Until ECMS go-live.

The following sections describe the procedural tasks during a normal operational day.

3.1.1.2 Start-of-day period (18:45-19:00)

The start-of-day (SoD) process is launched after successful completion of CLM EoD (see paragraph 3.1.1.5) and not before 18:45. It runs until around 19:00 (when the "CLM RTS" event is launched).

During the SoD period:

- change of business day in CLM takes place;
- processing of standing order reservations for the settlement of CBOs takes place;
- reference data valid as of the new business day are activated;
- revalidation of warehoused payments is performed;
- no settlement takes place;
- payment orders will be parked until the CLM RTS period is reached (except for liquidity transfer orders, which will be parked from 19:00 onwards and not before);
- local reference data maintenance instructions (e.g. blocking of an account) may be processed;
- queries are processed immediately.

3.1.1.3 CLM real-time settlement period (19:00-18:00)

The **CLM real-time settlement (RTS)** period starts after the successful completion of the SoD period (at around 19:00). The scheduled duration is until 18:00 and it is interrupted by the maintenance window, if activated.

The main goal of CLM RTS is the settlement of central bank operations (CBOs). CBOs include any payment order or liquidity transfer order initiated by a CB on an MCA opened in any TARGET component system. CBOs therefore include the following operations: update of credit line (cash side), marginal lending and overnight deposits (summarised as standing facilities), cash withdrawals and cash lodgements, monetary policy operations other than standing facilities (e.g. open market operations such as main refinancing operations or longer-term refinancing operations), debiting of the invoiced amount, interest payment orders linked to marginal lending, overnight deposits, minimum reserves, excess reserves and for accounts subject to other purposes of interest calculation, and any other activity that

a CB initiates in its capacity as CB of issue. If any of these operations is queued or pending, it will trigger an automated liquidity transfer.

During the CLM RTS period, the following processes take place.

- Marginal lending and overnight deposits are reimbursed and all related interest is settled.
- CBOs are settled.
- The following liquidity transfers are settled from 19:30 onwards:
    - immediate, standing order, rule-based liquidity transfers within CLM;
    - immediate, standing order, rule-based and automated liquidity transfers between CLM and RTGS (including RTGS sub-accounts);
    - immediate and standing order liquidity transfers between CLM and TIPS.
- Immediate and standing order liquidity transfers between CLM and T2S are settled with the start of NTS in T2S (starting at 20:00 normally), even though their settlement in CLM may take place earlier from 19:30 onwards. Liquidity transfers to/from T2S can be processed until 17:45.
- Local reference data maintenance instructions (e.g. blocking of a participant) may be processed.
- Queries are processed immediately.

CLM RTS is closed by the event "Cut-off for CLM RTS[9]", scheduled for 18:00. The cut-off implies the closure of settlement for liquidity transfers and CBOs, except standing facilities, connected payments and credit line modifications.

3.1.1.4 Maintenance window

System maintenance processes take place during the maintenance window.

During the maintenance window (MW), it is not possible to access the CLM, RTGS or T2S GUIs, the CRDM, or the DWH. Files and messages sent in A2A mode during this time are parked in the NSP queues until the maintenance window is closed. Queries (including admi.005) are rejected.

Non-optional MW: the maintenance window is activated every weekend and on TARGET closing days: it starts with the event "Start of non-optional maintenance window (CSMW)" (scheduled for 02:30 of the closing day) and ends with the event "End of non-optional maintenance window (CEMW)" (scheduled for 02:30 of the next TARGET business day). Note that, on an exceptional basis, the duration of the non-optional maintenance window may be shortened. The procedure to be followed is the

[9] Operations arriving later than the scheduled or revised time linked to the cut-off event are rejected.

same as in case of optional maintenance window activation, described in Chapter 4.1.2.10 “Activation of the optional maintenance window”.

Optional MW: on all other TARGET business days the maintenance window can be activated on an optional basis. Its scheduled timing is from 03:00 to 05:00. It starts with the event “Start of optional maintenance window (CSOM)” and ends with the event “End of optional maintenance window (CEOM)”. The relevant procedure to be followed in case of activation of the optional MW is described in Chapter 4.1.2.10 “Activation of the optional maintenance window”.

3.1.1.5 End-of-day period (18:00-18:45)

The end-of-day (EoD) period starts with the event “Start-of-EoD processing” and ends with the event “EoD – close of service”. It is scheduled to run from 18:00 to 18:45.

During the EoD period, the following processes take place.

- Standing facilities, connected payments and credit line modifications continue to settle until the relevant cut-offs.
- Counterparties may instruct standing facilities until 18:15[10] (“Cut-off for standing facilities”).[11]
- Central banks may input requests for the use of standing facilities until 18:40[12] (“CB cut-off for standing facilities”). A liquidity transfer crediting an overnight deposit account can be instructed intra-service and inter-service. In the case of intra-service (i.e. from an MCA), it can be instructed until 18:15. For inter-service, this is only allowed from RTGS[13]/TIPS to the overnight deposit account. In this case, the relevant liquidity transfer cut-off of RTGS/TIPS applies (i.e. 18:00).
- Daily propagation of reference data from the CRDM takes place.
- Every CRDM opening day[14], the event “Data propagation for T2” triggers the propagation of all CLM reference data from CRDM to CLM (and RTGS). The event takes place at 18:00 for CLM (and RTGS) in order to ensure a smooth and complete reference data propagation before the change of business day. Reference data valid as of the next business day must therefore be captured before the event is triggered at 18:00. The set of reference data that CLM

---

10 A liquidity transfer crediting an overnight deposit account can be instructed inter-service. In such case, the relevant liquidity transfer cut-offs of each settlement service apply (i.e. for liquidity transfers from T2S the cut-off is at 17:45 and for liquidity transfers from RTGS/TIPS the cut-off is at 18:00).

11 Until 18:30 on the last day of the minimum reserve maintenance period.

12 Until 18:55 on the last day of the minimum reserve maintenance period.

13 This is not applicable from an RTGS ancillary system technical account.

14 CRDM follows the CLM calendar and scheduling.

receives on business day T includes all the active data on the mentioned business date.

- In the event of a contingency, the TARGET operator may trigger an ad hoc propagation (contingency propagation) from CRDM to CLM (and RTGS). The contingency propagation is an additional daily propagation (all reference data available in CRDM at the time of the ad hoc propagation will be propagated) triggered intraday if an immediate change of a set of data (not manageable directly into CLM) must be performed.
- local reference data maintenance instructions (e.g. blocking of an account) may be processed.
- queries are processed immediately.

After the event “CB cut-off for standing facilities” (18:40):

- the settlement of connected payments and credit line modifications is closed;
- the aggregated end-of-day balance of CLM account holders is calculated taking into account the balances of RTGS/T2S/TIPS DCAs;
- for counterparties subject to minimum reserve, CLM calculates the running average and the adjustment balance;
- interest is calculated (for accounts subject to interest calculation) and the relevant interest payment orders are created (but not yet settled);
- the reports scheduled for the EoD are created.

Note: queries in the CLM Graphical User Interface (GUI) are unavailable between the events CCOS (EOD close of service) and CSOD (change of business day).

3.1.2 RTGS daily operations

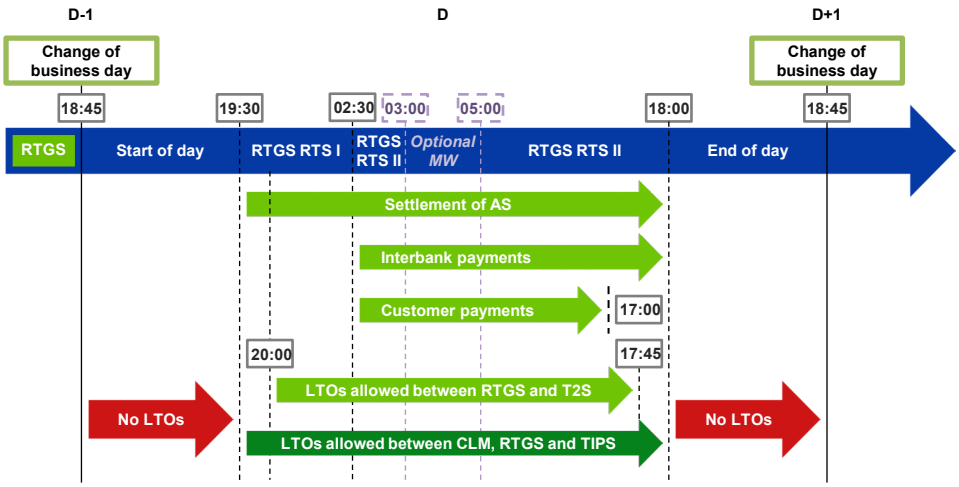
3.1.2.1 RTGS business day overview

The schedule of a RTGS settlement day comprises the following main periods:

- Start of day (SoD)
- Real-time settlement I (RTS I)
- Maintenance window (MW), if activated
- Real-time settlement II (RTS II)
- End of day (EoD)

Figure 2

RTGS business day schedule with optional MW – euro



The table below provides an overview of the different periods and the related RTGS settlement events and processes.

Table 2

Overview of RTGS settlement business day

RTGS Period	RTGS Settlement day events	Time/Predecessor	RTGS Processes
RTGS SoD	**Change of business day (RSOD)**	Approx. 18:45 Following completion of RCOS – EoD close of service	• Change of business day • Processing of standing order reservations and standing order limits • Revalidation of warehoused payments
RTGS RTS I	**Start of RTS I (RRTI)**	19:30 Following completion of RSOD	• Settlement of AS transfer orders for procedures A, B and E • Execution of automated liquidity transfer orders from RTGS to CLM due to pending/queued CBOs. • Execution (in RTGS) of liquidity transfer orders from CLM to RTGS
	Execution of standing orders (RESO)	Approx. 19:30 Following completion of execution of standing orders in CLM (CESO)	• Processing of standing order liquidity transfers in favour of sub-accounts (AS settlement procedure C) and technical accounts (AS settlement procedure D) • Settlement of AS transfer orders for procedures C and D • Processing of standing order liquidity transfers defined for this specific event • Processing of immediate liquidity transfers • Creation of rule-based liquidity transfers
RTGS Maintenance Window (MW)	**Start of RTGS MW (RSMW)**	02:30 for mandatory MW 03:00 for optional MW	
	End of RTGS MW (REMW)	02:30 for mandatory MW 05:00 for optional MW	
RTGS RTS II	**Start of RTGS RTS II (RRII)**	02:30	• Processing of AS transfer orders and liquidity transfer orders
	Start of settlement window for interbank and customer payments (RSIC)	02:30	• Processing of interbank payment orders • Processing of customer payment orders • Processing of standing order liquidity transfers defined for this specific event
	Cut-off for customer payments (RCOC)	17:00	• Closure of settlement of customer payment orders
	Cut off for RTS II (RCII)	18:00	• Closure of settlement of interbank payment orders, AS transfer orders and liquidity transfers • Liquidity remaining on sub-accounts is transferred to the linked RTGS DCAs • Limit and reservation modifications with non-final status are rejected
	Execution of standing orders after last settlement attempt in RTGS (RLSO)	Approx. 18:00 - After all cash transfers are in a final status	• Processing of standing order liquidity transfers defined for this specific event in RTGS
RTGS EoD	**Start of end of day (REOD)**	Approx. 18:00 Following completion of RLSO	• Creation of reports scheduled for EoD • Upon request by CLM, sending to CLM of the RTGS general ledger
	End of day – close of service (RCOS)	Following completion of REOD	

The following sections describe the procedural tasks during a normal operational day.

3.1.2.2 Start-of-day period (18:45-19:30)

The start-of-day (SoD) process is launched after successful completion of RTGS EoD close of service (RCOS) (see Chapter 3.1.2.6), and not before 18:45. It runs until around 19:30 (when the event “RTGS RTS I” is launched).

During the SoD period:

- change of business day in RTGS takes place;
- processing of standing order reservations and standing order limits takes place;
- reference data valid as of the new business day are activated;
- revalidation of warehoused payments is performed;
- no settlement takes place;
- liquidity transfer orders can be submitted from 19:00 onwards (start of CLM RTS);
- Note: in RTGS, liquidity transfers are parked at 19:00 and only processed at the beginning of the RTGS RTS I period; i.e. “Execution of standing orders in RTGS” (RESO) event at 19:30;
- local reference data maintenance instructions (e.g. blocking of an account) may be processed;
- queries are processed immediately.

3.1.2.3 RTGS real-time settlement I period (19:30-02:30)

RTGS real-time settlement (RTS) I starts after the successful completion of the SoD period (at around 19:30) and is followed by the non-optional maintenance window (if activated) and the RTGS RTS II period.

RTGS RTS I opens at 19:30 to support ancillary system settlement. It is at this time that the settlement window for AS transfer orders starts in the RTGS. For more information on ancillary systems settlement procedures and settlement times, please see Chapter 3.1.2.7.

The planned duration is until 02:30. During the RTGS RTS I period:

- the execution of automated liquidity transfer orders (transferring liquidity from RTGS to CLM due to pending CBOs) takes place;
- AS transfer orders for settlement procedures A, B and E are settled;
- local reference data maintenance instructions (e.g. blocking of an account) may be processed;
- queries are processed immediately.

Furthermore, (with the start of event “Execution of standing orders in RTGS”)[15]:

[15] The event “Execution of standing orders in RTGS” starts after successful completion of the execution of standing orders liquidity transfers to RTGS in CLM.

- immediate and standing order liquidity transfers within RTGS are settled;
- immediate, standing order, rule-based and automated liquidity transfers between RTGS and CLM are settled;
- immediate and standing order liquidity transfers between RTGS and TIPS are settled;
- immediate and standing order liquidity transfers between RTGS and T2S are settled with the start of NTS in T2S (starting at 20:00 normally), even though their settlement in RTGS may take place earlier from 19:30 onwards.
- Note: liquidity transfers to/from T2S can be processed until 17:45;
- AS transfer orders for settlement procedures C and D are settled;
- standing order liquidity transfers from RTGS and TIPS DCAs to sub-accounts and technical accounts are settled.

3.1.2.4 Maintenance window

Please see Chapter 3.1.1.4 of this document.

3.1.2.5 RTGS real-time settlement II period (02:30-18:00)

RTGS real-time settlement (RTS) II starts after the successful completion of the RTGS RTS I period (at around 02:30). It is scheduled to run until 18:00.

If the optional maintenance window is activated, RTGS RTS II is interrupted from 03:00 to 05:00.

During the RTS II period:

- AS transfer orders and liquidity transfers (already started at RTS I) are settled until 18:00;
- customer payments are settled until 17:00;
- interbank payments are settled until 18:00.

The ECB's website is updated at 02:30, confirming that T2 is operating normally..

3.1.2.6 End-of-day period (18:00-18:45)

The end-of-day (EoD) period starts with the event "Start-of-EoD processing" and ends with the event "EoD – close of service". It is scheduled to run from 18:00 to 18:45.

During the EoD period, the following processes take place.

- The reports scheduled for EoD are created.
- Daily propagation of reference data from the CRDM takes place.
- Every CRDM opening day[16], the event “Data propagation for T2” triggers the propagation of all CLM reference data from CRDM to RTGS (and CLM). The event takes place at 18:00 for RTGS (and CLM) in order to ensure a smooth and complete reference data propagation before the change of business day. Reference data valid as of the next business day must therefore be captured before the event is triggered at 18:00. The set of reference data that CLM receives on business day T includes all the active data on the mentioned business date.
- Local reference data maintenance instructions (e.g. blocking of a participant) may be processed.
- Queries are processed immediately.
- **Note**: queries in the RTGS Graphical User Interface (GUI) are unavailable between the events RCOS (EOD close of service) and RSOD (change of business day).

3.1.2.7 Ancillary systems settlement procedures and settlement times

AS settlement procedures

The RTGS offers various AS settlement procedures for the settlement of AS transfer orders that support:

- technical efficiency (e.g. AS are in full control of the payment flows);
- liquidity efficiency (e.g. prioritisation of AS settlement transactions in RTGS over other transactions);
- information efficiency (e.g. AS have full visibility on the status of payments/net balances submitted at any time throughout the entire settlement process).

Table 3 below provides an overview of the AS settlement procedures and Table 4 provides an overview of the account types in relation to the account holder that may open such accounts and the relevant AS procedures they are used for.

Table 3
Overview of AS settlement procedures

Procedures	Description
AS settlement procedure A	**Settlement information:** • AS can send for settlement a set of multilateral balances (debits and credits) in batch mode.

[16] CRDM follows the CLM calendar and scheduling.

Procedures	Description
	• The sum of debits must be equal to the sum of credits in each AS batch message. • All debits are settled first, followed by credits. **Type of account used:** • **AS technical account:** it is mandatory to use a dedicated AS technical account that cannot be reused for other AS settlement procedures. • **Guarantee fund account:** can be used to limit the negative impact of failed settlement. **Note:** the same guarantee account can be used for both AS settlement procedures A and B, though it is also possible to use two different guarantee accounts. **Optional connected mechanisms:** • Information period • Settlement period ("till") • Guarantee fund mechanism
AS settlement procedure B	**Settlement information:** • AS can send for settlement a set of multilateral balances (debits and credits) in batch mode. • The sum of debits must be equal to the sum of credits in each AS batch message. • All debit and credit AS transfer orders are settled simultaneously if possible (i.e. settlement on an "all-or-nothing" basis). If not possible, no settlement takes place and the orders remain in the queue. **Type of account used:** • **AS technical account:** a dedicated AS technical account must be used. • **Guarantee fund account:** can be used to limit the negative impact of failed settlement. **Note:** the same guarantee account can be used for both AS settlement procedures A and B, though it is also possible to use two different guarantee accounts. **Optional connected mechanisms:** • Information period • Settlement period ("till") • Guarantee fund mechanism

AS settlement procedure C	**Settlement information:**
	• Settles AS transfers (initiated by AS) between the AS settlement banks' sub-accounts and the AS technical account held by the ancillary systems.
	• The sum of debits does not necessarily equal the sum of credits in each AS batch message. As it is based on bilateral settlement, each batch message could include one or more AS transfer orders.
	• Allows an AS settlement bank to dedicate liquidity for the settlement of AS transfer orders from a specific ancillary system by opening at least one sub-account per ancillary system they are settling with.
	Note: it is possible to open several sub-accounts for one AS.
	• Uses the mandatory procedure (opened by the RTGS every business day at 19:30[17]) and allows ancillary systems to execute optional procedure(s) with the mandatory procedure closed earlier (otherwise closed by the RTGS every business day at 18:00).
	• Once a cycle is opened and for as long as it remains open, the liquidity on the sub-accounts cannot be decreased. Any immediate liquidity transfer order on the sub-account is executed only in case of a liquidity increase.
	• Settlement starts once the necessary liquidity is available on the sub-accounts. Only on an exceptional basis (e.g. an error on AS side) may AS transfers be queued on sub-accounts due to missing liquidity. For example, if a wrong amount was initiated by the AS the transfer would be queued and rejected at the end of the cycle and could then be re-instructed by the AS with the correct amount.
	• Liquidity is dedicated by the AS settlement banks on the sub-accounts opened for the AS settlement.
	• With each closure of the procedure, the remaining liquidity on the sub-accounts is swept back to the linked RTGS DCA/RTGS CB account.
	Type of account used:
	• **AS technical account:** a dedicated AS technical account must be used for AS settlement procedure C.
	Note: this technical account may be reused only for AS settlement procedure E.
	• **Sub-account:** this AS settlement procedure settles AS transfer orders on sub-accounts. These are used to set aside liquidity for the exclusive settlement of a specific ancillary system and are linked to an RTGS DCA or RTGS CB account.
	The settlement takes place:
	  • from the sub-accounts towards the AS technical account (debits) and
	  • from the AS technical account towards the sub-accounts or RTGS DCAs or RTGS CB accounts (credits).

AS settlement procedure D	**Settlement information:** • Settles AS liquidity transfers (initiated by AS or the AS settlement banks) between the AS settlement banks' RTGS DCAs or RTGS CB accounts and the AS technical account held by the ancillary systems. • For AS settlement procedure D, the settlement phase is an internal process of the ancillary system and therefore no details are provided here.

[17] Procedure start time subject to RESO event start.

Procedures	Description
	• Allows an AS settlement bank to dedicate liquidity for the settlement from a specific ancillary system by allocating (pre-funding) the necessary liquidity to the respective AS technical account. • Uses a mandatory procedure (opened by the RTGS every business day at 19:30) and does not allow ancillary systems to close it. • At the cut-off for EoD no re-transfer of liquidity from the AS technical account to the RTGS DCAs/RTGS CB accounts takes place. Therefore, the AS technical account can have a non-zero balance. **Type of account used:** • **AS technical account:** a dedicated AS technical account must be used to settle AS transfer orders (i.e. liquidity transfers).
AS settlement procedure E	**Settlement information:** • AS can benefit from the bilateral settlement of simultaneously sent debits and credits that shall be processed independently from each other. • The sum of debits does not necessarily equal the sum of credits in each AS batch message. As it is based on bilateral settlement, each batch message could include one or more AS transfer orders. • The ancillary system may use AS settlement procedure E also to settle multilateral balances by using a technical account. This can be achieved by creating debits first (debit RTGS DCA or RTGS CB account and credit technical account) and then sending the batch of credits (debiting technical account and crediting RTGS DCA or RTGS CB account) only after successful settlement of the debits. **Type of account used:** • **AS technical account:** it is recommended to use a dedicated AS technical account that cannot be reused for other AS settlement procedures. **Note:** the technical account used for AS settlement procedure C may be reused for AS settlement procedure E. **Optional connected mechanisms:** • Information period • Settlement period (“till”)

Note: Optional connected mechanisms can be used to fine-tune the AS settlement procedure to the needs of the ancillary systems, by defining information periods or settlement periods or by attaching guarantee mechanisms to ensure the settlement of multilateral balances.

Table 4

AS account types in relation to account holders and relevant AS procedures

Account type	Account holder	Description	Procedure
Sub-account	AS settlement bank	Used to set aside liquidity for exclusive settlement of a specific ancillary system and is linked to an RTGS DCA/RTGS CB account	AS settlement procedure C only
Guarantee funds account	Guarantor (CB, payment bank or ancillary system*)	Used if the optional guarantee mechanism has to be activated by an ancillary system or the CB on its behalf. The same guarantee account can be used for both procedures (AS settlement procedure A and B), though it is also possible to use two different ones.	AS settlement procedures A and B
AS technical account	Ancillary system or CB	Used as: • intermediary account for the collection of debits and credits resulting from the settlement of AS transfers related to settlement procedure A, B, C and E • for pre-funding in the context of AS settlement procedure	One dedicated AS technical account is to be opened for each AS settlement procedure used Only for AS settlement procedure E is it possible to reuse the technical account from AS settlement procedure C

Note: Source: RTGS UDFS.

AS settlement times

The overall planned duration for the settlement window for AS transfer orders (covering RTGS RTS I and II) is from 19:30 until 18:00, with a possible interruption due to the maintenance window. (See Figure 2 – RTGS business day schedule with optional MW – euro in Chapter 3.1.2.1 “RTGS business day overview”).

The settlement window for AS transfer orders starts at two different events, depending on the settlement procedure:

- **For AS settlement procedures A, B and E:** the settlement window is started by the event “Start of RTGS RTS I”, with a scheduled start time of 19:30. The settlement window resumes in RTGS RTS II.
- **For AS settlement procedures C and D:** the settlement window is started by the event “Execution of standing orders in RTGS”, with a scheduled start time of 19:30. The event is processed after the successful completion of execution of standing order liquidity transfer orders to RTGS in CLM. The settlement window resumes in RTGS RTS II.

3.1.2.8 Algorithms used for dissolution of the payment queue

Certain algorithms (algos) are used for the:

- continuous settlement of queued cash transfer orders;
- processing of AS transfers;
- optimisation of the processing of AS transfer orders on the sub-accounts of settlement banks.

A description of the various algorithms and their usage can be found in the table below.

Table 5
Algorithms and their usage

Algo type	Algorithm name	Usage
Algo 2	“Partial optimisation”	Algorithm 2 resolves queued normal cash transfer orders. The queues for cash transfers orders with urgent or high priority are continuously resolved by the sequential run of algorithms for the resolving of normal cash transfer orders (i.e. Algo 2,3,4). If the run of this algorithm fails, the algorithm “multiple optimisation” is activated.
Algo 3	“Multiple optimisation”	Algo 3 resolves queued normal cash transfer orders. The queues for cash transfers orders with urgent or high priority are continuously resolved by the sequential run of algorithms for the resolving of normal cash transfer orders (i.e. Algo 2,3,4). The aim of this algorithm is to resolve the queues with the highest possible settlement volume and low liquidity demand.
Algo 4	“Partial optimisation with ancillary system”	Algorithm developed to support the simultaneous multilateral settlement of an ancillary system (AS procedure B), thus ensuring an efficient and fast processing of the related AS transfer orders. Furthermore, in order to keep the whole settlement process running smoothly in RTGS, Algo 4 also resolves payments with priority urgent, high and normal.
Algo 5	“Optimisation on sub-accounts”	This algorithm aims at resolving AS transfer orders using dedicated liquidity on sub-accounts in RTGS. The algorithm only checks sub-accounts instead of RTGS DCAs and only covered AS transfer orders are settled. For each RTGS sub-account, the total position is calculated (the sum of actual balance on one sub-account plus incoming AS transfers minus outgoing AS transfers for this sub-account.) If all total positions are covered, all AS transfers are settled on the sub-accounts.

Note: Two algorithms cannot run in parallel to each other. A description of the main characteristics of each algorithm, as well as their sequence, can be found in the RTGS UDFS[18].

3.2 Liquidity transfers

CLM and RTGS provide inter-service liquidity transfer orders and intra-service liquidity transfer orders.

Inter-service liquidity transfer orders can be inbound liquidity transfer orders moving liquidity from another TARGET settlement service to CLM or RTGS, or outbound from CLM or RTGS to any other TARGET settlement service.

Intra-service liquidity transfers are used to move liquidity between accounts within CLM or within the RTGS.

3.2.1 Liquidity transfers in CLM – euro

Inter-service liquidity transfer orders

Inbound liquidity transfer orders move liquidity from another TARGET settlement service (RTGS, T2S, TIPS) to CLM, while outbound liquidity transfer orders move liquidity from CLM to any other TARGET settlement service (RTGS, T2S, TIPS).

Note: all inter-service liquidity transfers, regardless of type, are settled by moving the liquidity through the relevant transit accounts in CLM, RTGS, T2S and TIPS. Since the liquidity transfers move technically via the CLM transit account across the different settlement services, no liquidity transfers can take place between RTGS, T2S and TIPS if CLM encounters an outage.

Intra-service liquidity transfer orders

Intra-service liquidity transfer orders move liquidity between two MCAs in CLM and between an MCA and a CLM CB account.

Note: for the settlement of liquidity transfer orders between MCAs, both MCAs must be part of the same MCA Liquidity Transfer Group[19]. Each MCA may be part of one or more Liquidity Transfer Groups. The set-up of a Liquidity Transfer Group is required even if the MCA to be debited and the MCA to be credited belong to the same party.

The following types of liquidity transfer orders can be executed in CLM:

---

[18] See Chapter 5.3.9.3.2. Settlement of queued normal payments and Chapter 5.3.9.3.3. Algorithm Optimisation on sub-accounts

[19] An MCA Liquidity Transfer Group is an optional group of MCAs. Upon request of an MCA, the central bank shall create an MCA Liquidity Transfer Group to enable the processing of MCA-to-MCA liquidity transfer orders (not for liquidity monitoring purposes).

Table 6

CLM liquidity transfer order types

Liquidity transfer order type	Initiated	Note	Intra-/Inter-service
Immediate liquidity transfer order Enabling the immediate transfer of liquidity to or from an MCA	By the CLM/RTGS participant	• Available in A2A and U2A • No partial settlement	Both
Standing order liquidity transfer order (within CLM, between CLM and RTGS, between CLM and T2S, from CLM to TIPS) Recurring transfer of a fixed amount processed every business day at certain business day events	Automatically by the system	• To be configured in CRDM • Partial settlement allowed and no further attempts	Both
Automated liquidity transfer order (from RTGS to CLM) Transferring liquidity from a pre-defined RTGS DCA to an MCA due to a queued/pending central bank operation (CBO)	Automatically by the system	• Must be configured in CRDM for participants owning at least one RTGS DCA • Partial settlement and further attempts allowed	Inter-service
Rule-based liquidity transfer order (between RTGS and CLM, or within CLM) Initiated upon the breach of a pre-defined limit (floor or ceiling)	Automatically by the system	• May be configured in CRDM at the participant's discretion • Partial settlement allowed and no further attempts	Both

Liquidity transfer orders other than automated liquidity transfer orders are never queued in CLM; they are either:

- settled immediately (fully or partially); or
- rejected.

An automated liquidity transfer order triggered in CLM can be queued in RTGS only.

Liquidity windows

Liquidity transfers to/from CLM are not available:

- from 18:00 until 19:30 for CLM/RTGS/TIPS on all TARGET business days:
- from 17:45 until 20:00 for T2S[20] on all TARGET business days: and
- during the maintenance window/TARGET closing days.

Upon the occurrence of any abnormal event causing changes to the operational day of CLM, the liquidity provisioning windows will be impacted accordingly for all settlement services.

Liquidity transfers sent during the maintenance window are queued and processed afterwards.

[20] Liquidity transfers between CLM and T2S are settled with the start of NTS in T2S (starting at 20:00 normally), even though their settlement in CLM may be instructed and settled earlier from 19:30 onwards.

3.2.2 Liquidity transfers in RTGS – euro

Inter-service liquidity transfer orders

Inbound liquidity transfer orders move liquidity from another TARGET settlement service (CLM, T2S, TIPS) to RTGS, and outbound from RTGS to any other TARGET settlement service (CLM, T2S, TIPS).

Note: all inter-service liquidity transfer orders, regardless of type, are settled by moving the liquidity through the relevant transit accounts in CLM, RTGS, T2S and TIPS. Since the liquidity transfer moves technically via the CLM transit account across the different settlement services, no liquidity transfers can take place between RTGS, T2S and TIPS if CLM encounters an outage.

Intra-service liquidity transfer orders

Intra-service liquidity transfer orders in the case of RTGS include liquidity transfers between two RTGS DCAs (within a RTGS Liquidity Transfer Group), liquidity transfers between an RTGS DCA and a linked sub-account dedicated to an AS for AS settlement procedure C, and liquidity transfers between an RTGS DCA and a technical account dedicated to an AS for AS settlement procedure D. More information can be found in the relevant chapters of the RTGS UDFS.

Note: for the settlement of liquidity transfers between two RTGS DCAs, both accounts must be part of the same Liquidity Transfer Group[21]. The set-up of an RTGS Liquidity Transfer Group is required even if the RTGS DCA to be debited and the RTGS DCA to be credited belong to the same party.

Liquidity transfer orders can be executed via the following types in RTGS:

[21] An RTGS Liquidity Transfer Group is an optional group of DCAs. On the request of an RTGS DCA holder, the central bank shall create an RTGS Liquidity Transfer Group to enable the processing of RTGS DCA-to-RTGS DCA liquidity transfer orders (not for liquidity monitoring purposes).

Table 7

RTGS liquidity transfer order types

Liquidity transfer order type	Initiated	Note	Intra/Inter-service
Immediate liquidity transfer order Enabling the immediate transfer of liquidity to or from an RTGS DCA	By the RTGS/CLM participant	• Available in A2A and U2A • If initiated by an RTGS DCA holder or NCB: ⇨ No partial settlement • If initiated by AS: ⇨Partial settlement allowed and no further attempts	Both
Standing order liquidity transfer order (within RTGS, from RTGS to CLM, from RTGS to TIPS, and from RTGS to T2S) Recurring transfer of a fixed amount processed every business day at certain business day events	Automatically by the system	• To be configured in CRDM • Partial settlement allowed and no further attempts	Both
Automated liquidity transfer order (from RTGS to CLM) Transferring liquidity from a pre-defined RTGS DCA to an MCA due to a queued/pending central bank operation (CBO)	Automatically by the system	• Must be configured in CRDM for participants owning at least one RTGS DCA • Partial settlement and further attempts allowed	Inter-service
Rule-based liquidity transfer order (between RTGS and CLM) Initiated: (a) upon the breach of a pre-defined limit (floor or ceiling) or (b) due to a pending urgent payment order, or AS transfer order or high priority payment order	Automatically by the system	• May be configured in CRDM at the participant's discretion • Partial settlement allowed and no further attempts	Both

Note: Intra-service in the case of RTGS includes liquidity transfers between two RTGS DCAs (within a Liquidity Transfer Group), liquidity transfers between an RTGS DCA and a linked sub-account dedicated to an AS for AS settlement procedure C, and liquidity transfers between an RTGS DCA and a technical account dedicated to an AS for AS settlement procedure D. More information can be found in the relevant chapters of the RTGS UDFS.

Liquidity transfer orders other than automated liquidity transfer orders are never queued in the RTGS; they are either:

- settled immediately (fully or partially); or
- rejected.

Only an automated liquidity transfer order triggered in CLM can be queued in RTGS. In such a scenario, any incoming liquidity (up to the required amount) on the RTGS DCA is transferred to the MCA in CLM until the original amount of the automated liquidity transfer (i.e. the amount needed to settle the pending/queued CBO(s) in CLM) is settled in full. **Note**: whenever such an automated liquidity transfer is queued, it must be settled prior to any other payment order and does not allow for the earlier settlement of any other payment order.

Liquidity windows

Liquidity transfers to/from RTGS are not available:

- from 18:00 until 19:30 for CLM/RTGS/TIPS on all TARGET business days;
- from 17:45 until 20:00 for T2S on all TARGET business days; and
- during the maintenance window/TARGET closing days.

Upon the occurrence of any abnormal event causing changes to the operational day of RTGS, the liquidity provisioning windows will be impacted accordingly for all settlement services.

Liquidity transfers sent during the maintenance window are queued and processed afterwards.

3.2.2.1 Dedicated liquidity for ancillary system settlement

Depending on the AS settlement procedure the ancillary system is using, the liquidity may need to be provided on different accounts:

- sub-account for AS settlement procedure C (account owner = RTGS DCA holder)
- AS technical account for AS settlement procedure D (account owner = ancillary system or its NCB)

Moreover, the RTGS DCA holder can open a dedicated RTGS DCA to be used for ancillary system settlement only.

To transfer liquidity to the RTGS account holder's sub-account or to the AS technical account, the following options exist:

- Setting-up of standing order liquidity transfer orders by the RTGS account holder in CRDM. These become effective as of the next business day.
- Immediate liquidity transfer orders initiated by the RTGS account holder.
- Immediate liquidity transfer orders initiated by the ancillary system.

Liquidity transfers to/from RTGS sub-accounts for AS settlement procedure C

Liquidity transfer orders are executed in the following ways:

- Standing order liquidity transfer orders crediting the RTGS sub-accounts:
  - executed upon the start of the mandatory/optional procedure
  - initiated by the AS settlement banks
- Immediate liquidity transfer orders executed during the open mandatory/optional procedure:
  - outside the cycle, may be initiated by the AS settlement banks or the ancillary systems debiting/crediting the RTGS sub-account

- during the open cycle, may be initiated only by the AS settlement banks crediting the RTGS sub-account. When an order debits the RTGS sub-account, the order is stored until the cycle is closed.

More information can be found in the relevant chapter of the RTGS UDFS.

Liquidity transfers to/from AS technical accounts for AS settlement procedure D

AS settlement procedure D is based on liquidity transfers between the AS settlement banks' RTGS DCAs/RTGS CB accounts and the AS technical account.

Liquidity transfer orders are executed in the following ways:

- Standing order liquidity transfer orders crediting the AS technical account:
  - executed upon the start of the mandatory procedure
  - initiated by the AS settlement banks
- Immediate liquidity transfer orders crediting the AS technical account:
  - executed during the open mandatory procedure
  - initiated by the AS settlement banks or the ancillary systems (or their CB on their behalf)
- Immediate liquidity transfer orders debiting the AS technical account:
  - executed during the open mandatory procedure
  - initiated by the ancillary systems (or their CB on their behalf)

More information can be found in the relevant chapter of the RTGS UDFS.

4 Operational procedures during abnormal situations

4.1 Operational incidents and operational procedures to be followed

This section lists potential operational issues (non-exhaustive list) and provides a mapping of these against applicable operational procedures. The operational procedures are described in detail in the following section. The application of such operational procedures is triggered via incident and/or crisis management. Failures affecting CLM and/or RTGS can result in the complete or partial unavailability of the services (e.g. settlement continues, but with no U2A visibility).

4.1.1 Overview of operational issues and applicable procedures for each business day period

Table 8
CLM operational issues and procedures

#	Period	Key activities	Relevant operational issues	Possible measures to address operational failure scenarios
1	CLM SoD 18:45-19:00	• Change of business day in CLM	Failure affecting CLM	Rescheduling of CLM and/or RTGS events (Chapter 4.1.2.1)
				Intra-region failover (Chapter 4.1.2.5.1)
			CLM revalidation of instructions against reference data updates leads to unexpected results	Last--level intervention on request (Chapter 4.1.2.11)
			Wide-scale regional disruption	Inter-region failover (Chapter 4.1.2.5.2)
			One or more CLM actors are unable to access CLM	Failure at central bank level (Chapter 4.1.2.6)
				Failure at participant level (non-AS) (Chapter 4.1.2.8)
2	CLM RTS 19:00-18:00	• Settlement of CBOs (19:00-18:00) • Settlement of liquidity transfers (19:30-18:00)	Failure affecting CLM	Rescheduling of CLM and/or RTGS events (Chapter 4.1.2.1)
				Contingency processing in ECONS II (Chapter 4.1.2.4)
				Intra-region failover (Chapter 4.1.2.5.1)
			Central bank requesting a delay	Rescheduling of CLM and/or RTGS events (Chapter 4.1.2.1)
			Failure of a network service provider	Failure at NSP level (Chapter 4.1.2.7)
			Wide-scale regional disruption	Inter-region failover (Chapter 4.1.2.5.2)
			4CB request to activate the optional maintenance window	Activation of optional maintenance window (Chapter 4.1.2.10)
			One or more CLM actors are unable to access CLM	Failure at central bank level (Chapter 4.1.2.6)

				Failure at participant level (non-AS) (Chapter 4.1.2.8)
3	CLM EoD 18:00-18:45	• Settlement of standing facilities • Sending of general ledger (GL) files	Failure affecting CLM	Rescheduling of CLM and/or RTGS events (Chapter 4.1.2.1)
				Intra-region failover (Chapter 4.1.2.5.1)
			CLM has not received the GL files from RTGS/TIPS/T2S or CLM failure in sending the GL files to the central banks	Procedure in case of missing GL files (Chapter 4.1.2.3)
			Central bank requesting a delay in the cut-offs for standing facilities due to failures impacting central bank collateral management systems	Delay in the cut-offs for standing facilities (Chapter 4.1.2.2)
			Failure of a network service provider	Failure at NSP level (Chapter 4.1.2.7)
			Wide-scale regional disruption	Inter-region failover (Chapter 4.1.2.5.2)
			One or more CLM actors are unable to access CLM	Failure at central bank level (Chapter 4.1.2.6)
				Failure at participant level (non-AS) (Chapter 4.1.2.8)

Table 9

RTGS operational issues and procedures

#	Period	Key activities	Relevant operational issues	Possible measures to address operational failure scenarios
1	RTGS SoD 18:45-19:30	• Change of business day in RTGS	Failure affecting RTGS	Rescheduling of CLM and/or RTGS events (Chapter 4.1.2.1)
				Intra-region failover (Chapter 4.1.2.5.1)
			RTGS revalidation of instructions against reference data updates leads to unexpected results	Last-level intervention on request (Chapter 4.1.2.11)
			Wide-scale regional disruption	Inter-region failover (Chapter 4.1.2.5.2)
			One or more RTGS actors are unable to access RTGS	Failure at central bank level (Chapter 4.1.2.6)
				Failure at participant level (non-AS) (Chapter 4.1.2.8)
				Failure at ancillary system level (Chapter 4.1.2.9)
2	RTGS RTS I 19:30-02:30	• Settlement of AS transfer orders • Settlement of liquidity transfers	Failure affecting RTGS	Rescheduling of CLM and/or RTGS events (Chapter 4.1.2.1)
				Intra-region failover (Chapter 4.1.2.5.1)
			Wide-scale regional disruption	Inter-region failover (Chapter 4.1.2.5.2)
			One or more RTGS actors are unable to access RTGS	Failure at central bank level (Chapter 4.1.2.6)
				Failure at participant level (non-AS) (Chapter 4.1.2.8)
				Failure at ancillary system level (Chapter 4.1.2.9)
			Failure of a network service provider	Failure at NSP level (Chapter 4.1.2.7)
			Central bank requesting a delay	Rescheduling of CLM and/or RTGS events (Chapter 4.1.2.1)

3	RTGS RTS II 02:30-18:00	• Settlement of AS transfer orders • Settlement of liquidity transfers • Settlement of interbank and customer payments	Failure affecting RTGS	Rescheduling of CLM and/or RTGS events (Chapter 4.1.2.1)
				Intra-region failover (Chapter 4.1.2.5.1)
				Contingency processing in ECONS II (Chapter 4.1.2.4)
			Wide-scale regional disruption	Inter-region failover (Chapter 4.1.2.5.2)
			One or more RTGS actors are unable to access RTGS	Failure at central bank level (Chapter 4.1.2.6)
				Failure at participant level (non-AS) (Chapter 4.1.2.8)
				Failure at ancillary system level (Chapter 4.1.2.9)
			Central bank requesting a delay	Rescheduling of CLM and/or RTGS events (Chapter 4.1.2.1)
			4CB request to activate the optional maintenance window	Activation of optional maintenance window (Chapter 4.1.2.10)
4	RTGS EoD 18:00-18:45	• Creation of RTGS reports • Sending of GL file to CLM	RTGS failure in creating/sending GL file to CLM	Procedure in case of missing GL files (Chapter 4.1.2.3)
			Failure affecting RTGS	Rescheduling of CLM and/or RTGS events (Chapter 4.1.2.1)
				Intra-region failover (Chapter 4.1.2.5.1)
			Failure of a network service provider	Failure at NSP level (Chapter 4.1.2.7)
			Wide-scale regional disruption	Inter-region failover (Chapter 4.1.2.5.2)
			One or more RTGS actors are unable to access RTGS	Failure at central bank level (Chapter 4.1.2.6)
				Failure at participant level (non-AS) (Chapter 4.1.2.8)

Note: Customer payments are settled until 17:00.

4.1.2 Possible measures to address operational failure scenarios

4.1.2.1 Rescheduling of CLM and/or RTGS events

Various situations can occur during a CLM and RTGS business day, possibly requiring a delay in closing CLM and RTGS[22] and/or the postponement of one or more events of the CLM/RTGS operational schedule. This can happen if CLM and/or RTGS are, for one reason or another (e.g. a software bug), unable to continue with any phase of their respective operational schedule. Issues outside CLM and/or RTGS can also have an impact on their operating schedules.

The following non-exhaustive list of causes might lead to a delay:

- CLM and/or RTGS failure (including CLM and/or RTGS GUI failure);
- failure of a TARGET common component;

[22] "Delayed closing" means a delay in the CLM RTS cut-off and RTGS RTS II cut-off (scheduled for 18:00).

- TIPS failure;
- T2S failure;
- NSP failure;
- Other reasons, such as business continuity events, turmoil, or market turbulence.

A failure of one single bank never leads to a delay in the closing of CLM and RTGS.

In the unlikely event of a critical AS failure that could have a significant impact on the smooth operations of TARGET, the central bank of the critical AS may request the delayed closing of CLM and RTGS to give the AS more time to resolve the failure or lessen its impact. It is noted that the decision for a delayed closing of CLM and RTGS is not automatically granted as it is subject to the assessment of the crisis managers appointed by their central banks. As part of the decision-making process, consideration is given not only to the criticality of the relevant AS, but most importantly to the criticality of the pending transactions.

Additionally, a delayed closing might be performed in response to a banking crisis, especially if the whole market is affected, or a large part of it.

In the event of any situation that might require a delay in the closing of CLM and RTGS and/or the postponement of one or more events on the CLM/RTGS operational schedule, Eurosystem internal incident and crisis management procedures will be invoked to assess the situation and to agree on the next steps. Once a delayed closing or a postponement of a CLM/RTGS event is decided, an external communication will be shared with TARGET participants without undue delay:

1. on the ECB's website;
2. via a GUI broadcast;
3. via the communication channels used at national level by the NSDs.

4.1.2.2 Delay in cut-offs for standing facilities

A central bank may request a delay in the cut-offs for standing facilities in the event of failures affecting that central bank's collateral management system resulting in its inability to collateralise participants' marginal lending requests. Such a delay may be considered specifically on the last days before the end of a minimum reserve maintenance period.

4.1.2.3 Procedure in case of missing general ledger files

For the preparation of the general ledger (GL) files, CLM sends a camt.019 to RTGS, TIPS and T2S with the information needed to start creating the GL file with the end-of-day balances on the relevant accounts. A scenario leading to problems in the end-of-day procedures could affect this process and subsequently result in the postponement of certain CLM and RTGS end-of-day cut-offs.

Immediately after the decision to apply the shortened operational timeline has been taken, the information will be published on the ECB's website under TARGET and shared via a GUI broadcast. Based on this communication, the NSDs will also inform their market participants accordingly via local communication channels.

4.1.2.4 Contingency processing in ECONS II

Contingency processing means the manual processing of cash transfer orders during a failure of CLM and RTGS. The failure implies that the banks' payment capacity would be blocked in CLM and RTGS.

ECONS II supports the settlement of very critical and critical cash transfer orders in the event that CLM and/or RTGS are unavailable. (please see Chapter 4.1.2.4.3.1 "Concept of (very) critical payments in TARGET").

Connection to ECONS II is mandatory for all central banks in TARGET, for participants considered critical and for participants settling very critical transactions in CLM and RTGS, as well as for critical ancillary systems. In the medium term (i.e. two years after TARGET commenced live operations) connectivity to ECONS II will become mandatory for all TARGET participants.[23]

It is noted that in case of co-managed MCAs, the co-manager will not be able to manage the contingency accounts linked to the co-managed MCAs as the co-manager has no visibility over them in ECONS II. Therefore, co-managed participants shall ask their responsible NSD to act on their behalf in ECONS II for the execution of cash transfer orders and monitoring of balances of their contingency accounts.

Activation procedure

If the running of Eurosystem internal incident and crisis management processes concludes that contingency processing should be initiated, the NSDs inform participants via the relevant communication channels used at national level and the ECB's website is updated accordingly.

[23] As of March 2025, all RTGS DCA holders and AS using RTGS are required to establish a direct connection to ECONS II.

As a general rule, ECONS II should be activated between 07:00[24] and 18:00, unless otherwise agreed by the crisis managers.

Provision of liquidity to contingency accounts

Contingency accounts in ECONS II start with a zero balance. Hence, participants wishing to make contingency payments must first inject liquidity to ECONS II to create new payment capacity in ECONS II. The possible sources for such liquidity may depend on local arrangements at a national level and are listed below:

- provision of eligible assets collateral (only applicable to participants eligible for intra-day credit);[25]
- use of already available collateral that has not been used for other purposes (only applicable to participants eligible for intra-day credit and dependent on national collateral management practices);
- use of collateral specifically dedicated for contingency purposes (only applicable to participants eligible for intra-day credit, and dependent on national collateral management practices);
- movement of liquidity from T2S (if T2S is available);
- incoming payments within ECONS II;
- other, dependent on national collateral management practices.

In the event a participant relies on T2S for the mobilisation of collateral and T2S is also unavailable, other local means may be used instead (e.g. mobilisation of non-marketable assets).

Payments processing and monitoring

Processing of payments/AS files

- Once **fresh liquidity is available** (injected by the central bank or via incoming payments) for a participant in its contingency account, contingency processing may start for that participant.
- **The participant or central bank may insert payment instructions directly in the ECONS II GUI.**

---

24 In the event of an overnight incident presenting a risk for CLS settlement at 08:00, ECONS may be activated shortly before 07:00, e.g.15 minutes prior, to ensure it is operational by 07:00.

25 ECONS credit is collateralised in the same manner as monetary policy credit operations and hence, the existing rules and procedures of the Eurosystem collateral framework also apply for ECONS. In other words, no dedicated eligibility criteria and rules have to be developed to form a dedicated collateral framework for ECONS ("ECONS collateral framework"). The rules and procedures of the existing Eurosystem valuation framework remain applicable.

- **Note I:** if a participant is unable to insert a payment (e.g. the participant is unable to connect to ECONS II) or is not required[26] to establish a connection to ECONS II, it may request its central bank – using the respective national communication channels – to instruct a contingency payment on its behalf.

- **Note II:** If, before the start of the contingency session, a participant has transmitted a payment to RTGS that has been queued and the participant processes that payment again via ECONS II, a "double processing" of the payment (once in the ECONS II and afterwards in the RTGS upon its restart) is not preventable.

- **The central bank of a sending participant agrees or disagrees to the processing** of a payment (in the ECONS II GUI), ensuring that very critical payments (as defined by the Eurosystem) are processed. Critical payments are agreed/disagreed on a best effort basis.

  - A (very) critical payment in TARGET means a payment that is considered systemically important and thus eligible for contingency processing. Chapter 4.1.2.4.3.1 "Concept of (very) critical payments in TARGET" explains which payments must (very critical) or may (critical) be processed via ECONS II in such a scenario.

- **A central bank (or the relevant TARGET Service Desk acting on its behalf) may upload AS files upon the request of the AS,** in A2A mode.

  - An AS shall use bilaterally agreed transmission channels to submit the files to the responsible central bank. ECONS II supports AS settlement procedure A with the use of a contingency technical account.

    Note: the aforementioned "agree/disagree" functionality on the processing of each payment is not applied to payments entered via file upload by the central bank on behalf of an AS, nor to payments entered directly by the central bank.

In order to reduce the number of contingency payments, participants are encouraged to make use of bulking.

Monitoring

Participants can monitor their contingency account balances and the related transactions in ECONS II via the dedicated GUI.

The relevant central bank and the receiver of a payment, if connected to ECONS II, can see all incoming payments sorted by time and amount. However, not all participants will have established their own connection to ECONS II. Therefore, it is advisable for the sender of the payment to inform the receiver outside of ECONS II

[26] As of March 2025, all RTGS DCA holders and AS using RTGS are required to establish a direct connection to ECONS II.

about the settled transaction. The relevant central bank may also inform this participant, on a best effort basis, about the incoming payment.

Concept of (very) critical payments in TARGET

Prevailing principles:

- ECONS II contingency processing primarily focuses on cash transfer orders that need to be processed to avoid systemic risk during an incident.
- Owing to technical and operational volume limitations related to contingency processing, the overall number of contingency payments should be minimised.

The following individual categories of cash transfer orders are subject to contingency processing:

1. **Very critical cash transfer orders** must be processed in contingency and are characterised by their:

   (a) propensity to cause a spillover effect to other markets if not settled; and

   (b) need to be settled at specific times.

This category includes:

- payments related to CLS Bank International-related payments operated on CLS settlement;
- central counterparty margin calls (pay-ins).

2. **Critical cash transfer orders** – central banks may decide to process them in a contingency and they are, characterised by their:

   (a) possibility of creating systemic risk if not settled; and

   (b) need to be settled during the business day, though not necessarily at specific times.

This category includes but is not limited to:

- cash transfer orders related to the settlement of other systemically important payment systems (i.e. EURO1, STEP2-T, STET, Mastercard);
- liquidity transfers from ECONS II to T2S or TIPS;
- liquidity transfer orders and payments (re)distributing liquidity that are indispensable to the execution of very critical cash transfer orders or to other critical cash transfer orders.

3. **Other cash transfer orders** may also be processed under the following conditions:

(a) the participant has enough liquidity on its contingency account;

(b) their processing will not impede the processing of (very) critical payments.

Note: the criticality of other cash transfer orders might change depending on the duration and characteristics of the incident. In order to address this aspect, TARGET participants may connect to ECONS II and insert payments assessed as important according to their specific business needs via a graphical user interface (GUI) in U2A mode.

Aspects to be taken into consideration when selecting contingency payments for processing

In addition to the two basic principles explained in Chapter 4.1.2.4.3.1 "Concept of (very) critical payments in TARGET" (i.e. avoidance of systemic risk and the limitation on volumes processed), the following aspects might support the NSDs in their selection of the contingency payments to be processed:

- The failure situation, in particular:
  - the time of occurrence. Besides the beginning of the day and the end of the day, the settlement times of ancillary systems could be considered as more critical;
  - the possible spillover effect to other ancillary systems; and
  - its duration and expected recovery time.
- The business day – it could be of relevance whether an incident occurs at the end of the minimum reserve maintenance period, on a public holiday or on a day where particularly high volumes are expected.
- The communicated needs of participants and other central bank business areas (e.g. for monetary policy operations).
- Liquidity constraints – contingency processing would require additional collateral, i.e. the more payments that would be processed in contingency, the more additional collateral would have to be provided by a participant and, depending on the time of occurrence, the provision of additional collateral might be difficult.
- The principle of prioritisation – very critical payments should generally be processed before critical payments (as long as the critical payments are not required to release a "business gridlock" of very critical payments).

The incident handling measures might alleviate the need for processing contingency payments. For instance, major ancillary systems might choose to delay their settlement to the same extent as the delay in RTGS's closing and queued payments would be processed at the moment of the RTGS's recovery instead of settling in ECONS II.

The market's alternative contingency means (arrangements at the disposal of each individual participant) might also ease the need to process contingency payments.

Liquidity movements between ECONS II and T2S

Direct liquidity transfers (including movements for the purpose of reimbursing the auto-collateralisation provided in T2S) between ECONS II and T2S are not possible, in either way. Transferring liquidity from ECONS II to T2S or from T2S to ECONS II is only possible in an indirect way, by processing transfers between the **participant's and the central bank's accounts in T2S and in ECONS II**.

Central banks offer this service so their participants can manage their liquidity needs in T2S even in case of an unavailability of CLM and RTGS. The processing details of these liquidity movements should be arranged between a participant and its relevant central bank.

Liquidity movements between ECONS II and TIPS

Direct liquidity transfers between ECONS II and TIPS are not possible in either way. Transferring liquidity from ECONS II to TIPS or from TIPS to ECONS II in an indirect way will become available with future enhancements of the service.

Use of ECONS II for more than one day.

ECONS II may be used for contingency processing for several consecutive days, allowing to close a business day/change the value date.[27]

Operating hours of ECONS II:

If ECONS II is used for several business days, a decision is taken on the operating hours for each day according to the business needs and the crisis at hand. In principle, the operational day runs from 07:00 until 18:00 (with standard support hours running from 07:00 to 18:15).

Change of business day in ECONS II:

The decision to close a business day in ECONS II, and the continuation of the ECONS II processing on the following business day (if CLM and RTGS remain unavailable) is agreed following Eurosystem internal incident and crisis management procedures.

External communication:

[27] Liquidity transfers between ECONS II and TIPS will be possible upon deployment of CR TIPS-0011-URD.

If it is decided to continue contingency processing on the following business day, the participants are informed via the relevant national communication channels and the ECB's website.

Collateral aspects:

If ECONS II is open for several subsequent business days, processing of participant payments will continue to be based on liquidity provided and/or incoming payments. In the event that the collateral previously provided by a participant is no longer enough to cover the credit granted in ECONS II (at the end of the business day), a central bank shall request the participant to make an adjustment of the granted credit for ECONS II purposes (margin call) at the beginning of the new ECONS II business day. The request may be combined with a suspension of further processing of the participant's payments until additional collateral is provided.

Remuneration aspects:

End-of-day balances during ECONS II activation

- The end-of-day balances to be considered for each day of contingency settlement in ECONS II will be remunerated retroactively once CLM has resumed operations. The balances to be remunerated will be based on the information available from TARGET prior to the incident, i.e. the last trustworthy balance.[28] ECONS II balances are excluded from the remuneration calculation.

- During an incident lasting longer than one business day, central banks shall report the balances they have in ECONS II to the ECB as part of their daily current account holdings reporting. These balances will not reflect the full liquidity overview, but this will be the only information available during an incident and the reporting can be corrected only once normal operations have resumed.

Minimum reserve requirements

- Remuneration for minimum reserve requirement (MRR) and exempt holdings will take place retroactively after CLM and RTGS resume. The remuneration calculation takes into account all the days of the reserve maintenance period (i.e. including the days of ECONS II activation). The end-of-day balances to be considered for each day of contingency settlement in ECONS II are according to best information available to the ECB. Any balances held in ECONS II are remunerated at an interest rate of zero.

- Excess reserves beyond the MRR and exempt holdings for the period of the CLM outage are remunerated at deposit facility rate (DFR).

Marginal lending facility and intraday credit

[28] This balance is also used at the re-start of CLM and RTGS before the ECONS II balances are transferred to CLM.

- Marginal lending facility (MLF) and interest on MLF needs to be repaid only after CLM and RTGS resume. The interest calculation excludes the days run in ECONS II.
- Outstanding credit in MLF at the time of ECONS II activation granted the day before the incident shall be charged an interest rate of zero over the entire duration of the outage.
- Outstanding intraday credit in CLM prior to ECONS II activation shall be remunerated at an interest rate of zero over the entire duration of the outage.
- Any MLF credit granted and already settled in real time on the day of the incident in CLM but prior to ECONS II activation shall be treated as credit granted at the day of restart of CLM and RTGS.

Closing of ECONS II processing

Procedure for closing ECONS II

Once the incident has been resolved and TARGET can resume normal business operations, the decision will be taken to close ECONS II following the application of the Eurosystem internal incident and crisis management procedures.

Participants receive information on the processed data:

1. via the ECONS II GUI over the entire duration of the ECONS II session;
2. via the ECONS II GUI, a statement of accounts can be downloaded via “export function” for each business day of the contingency session. The download can be performed at any point[29], even after the contingency session has been closed. In the event of a contingency session spanning across several business days, these are available in U2A only via a dedicated screen for each ECONS II business day;

The information available in ECONS II refers only to transactions settled in ECONS II (i.e. transactions previously settled in RTGS cannot be queried in ECONS II).

In the event of a prolonged CLM/RTGS outage lasting multiple business days, the affected days of the contingency session will be set as closing days in the TARGET calendar in CRDM.

With the closing of ECONS II, its total balances will be transferred and booked in the CLM (no transfer of the individual underlying payments).

The NSDs inform the participants about the successful closure of the contingency session via the relevant communication channels used at national level and the TARGET coordinator updates the ECB’s website accordingly.

[29] Except for the time when ECONS II GUI is unavailable (i.e. maintenance window)

4.1.2.5 Service continuity (failover to the second site or second region)

Smaller issues are covered by redundant elements within the same region, while **major failures or disasters** (e.g. disruption of major hardware caused by fire, flood or terrorist attacks, or by telecommunications faults) require **failover to the second site in the same region (intra-region failover) or activation of a site in the second region (inter-region failover)**. **The main aim** is to recover full processing capacity as quickly as possible.

Communication: throughout the failover process, updates are provided via the ECB's website and the participants are also informed by their respective NSD using the agreed local communication channels.

Intra-region failover

- An intra-region failover means the failing over from site A to site B within the same region. As a synchronous copy is applied, the databases at both sites are exactly the same, and no reconciliation is required after the failover.
- An intra-region failover ensures the continuation of normal business within a maximum of one hour after the decision to recover from the other site is taken.
- Payment processing is interrupted during the failover and therefore TARGET participants will be advised as to whether or not they should keep on sending messages/files to the CLM and RTGS. The NSDs will disseminate this information to their respective communities.
- The GUI interfaces will be unavailable during the recovery.
- The activation of intra-region recovery could cause the unavailability of the test environments. Test environments are resumed on a best effort basis.

Inter-region failover

A wide-scale regional disruption that causes a severe interruption of transportation, telecommunication, power or other critical infrastructure across a metropolitan or a geographical area will require the failing over to the second region (inter-region failover). Such a disruption is expected to impact all production environments operating in the affected region (i.e. CLM, RTGS, T2S).

An inter-region failover means failing over from Region 1 to Region 2. As an asynchronous copy is applied, the databases in the two regions show the processing status with a time discrepancy of no longer than two minutes. Loss of data following an inter-region failover when both sites within Region 1 become unavailable is possible. In this situation, there is no alternative but to fail over to Region 2 and reconcile the missing traffic. Still, the resumption of operations in Region 2 should be enabled within two hours of the decision-making process.

Note that during the failover:

- the sending of new instructions both in A2A and U2A is prevented; for this reason, the participants should stop sending messages/files during the failover;
- the GUI interfaces will be unavailable during the recovery.

Rebuilding process

Rebuilding process in Region 2 is only required in the event that both sites in Region 1 become unavailable at the same time and there is a consequential loss of data. The aim of the rebuilding is to ensure that all messages processed in Region 1 are also shown in Region 2. In order to achieve this, all messages processed in Region 1 in the two minutes preceding the incident are retrieved and reconciled against what is shown in Region 2 to identify any missing cash transfer orders.

This includes:

1. Payment orders sent by banks, central banks and ancillary systems and AS transfer orders (other than payments) sent by an ancillary system;
2. Intra-service and inter-service liquidity transfers.

Identification of inter-service missing liquidity transfers:

If missing liquidity transfers are identified, the participants concerned shall be informed by their NSDs about the affected liquidity transfers and the actions to be carried out.

Rebuilding of liquidity transfers:

CASE A) Liquidity transfers from MCA/RTGS DCA accounts to T2S DCAs booked on T2S and on CLM & RTGS (Region 1) before the disaster **but not on CLM & RTGS (Region 2)** after the disaster:

The central bank shall provide the MCA/ RTGS DCA holder concerned with information concerning the T2S reference, the Users Reference[30], the debited MCA/RTGS DCA and the amount.

1. For liquidity transfers from MCAs to T2S DCAs:

(a) The central bank responsible for the debited MCA holder will debit the relevant MCA, after receiving authorisation from the MCA holder via camt.050, and credit the ECB's CB account in CLM.

(b) ECB will debit ECB's CB account in CLM and credit the T2S transit account in CLM.

2. For liquidity transfers from RTGS DCAs to T2S DCAs:

[30] The "Users reference" corresponds to the field end-to-end ID in the GUI. It can be used to identify the transaction from end-to-end along the entire chain.

(a) The central bank responsible for the debited RTGS DCA holder will debit the relevant RTGS DCA, after receiving authorisation from the RTGS DCA holder via camt.050, and credit the ECB's CB account in RTGS;

(b) ECB will debit ECB's CB account in RTGS and credit the CLM transit account in RTGS.

(c) ECB will debit the RTGS transit account in CLM and credit the T2S transit account in CLM.

CASE B) Liquidity transfers from T2S DCAs to MCA or RTGS DCAs booked on T2S and in CLM & RTGS (Region 1) before the disaster **but not in CLM & RTGS (Region 2)** after the disaster:

The central bank responsible for the debited T2S DCA should identify the outbound messages related with the liquidity transfers and resend them.

CASE C) Liquidity transfers from MCA or RTGS DCAs to TIPS DCAs booked on TIPS and in CLM & RTGS (Region 1) before the disaster **but not in CLM & RTGS (Region 2)** after the disaster:

The central bank will provide the MCA or RTGS DCA holder concerned with information regarding the instruction reference, the debited MCA or RTGS DCA and the amount.

1. For liquidity transfers from MCAs to TIPS DCAs:

(a) The central bank responsible for the debited MCA holder will debit the relevant MCA, after receiving authorisation from the MCA holder via camt.050, and credit the ECB's CB account in CLM.

(b) ECB will debit ECB's CB account in CLM and credit the TIPS transit account in CLM.

2. For liquidity transfers from RTGS DCAs to TIPS DCAs:

(a) The central bank responsible for the debited RTGS DCA holder will debit the relevant RTGS DCA, after receiving authorisation from the RTGS DCA holder via camt.050, and credit the ECB's CB account in RTGS;

(b) ECB will debit the ECB's CB account in RTGS and credit the CLM transit account in RTGS.

(c) ECB will debit the RTGS transit account in CLM and credit the TIPS transit account in CLM.

CASE D) Liquidity transfers from TIPS DCAs to MCA or RTGS DCAs that are booked on TIPS and in the CLM & RTGS (Region 1) before the disaster **but not in the CLM & RTGS (Region 2)** after the disaster:

The central bank will provide the participants concerned with information regarding the TIPS instruction reference, the debited TIPS DCA, the credited MCA or RTGS DCA and the amount.

1. For liquidity transfers from TIPS DCAs to MCA:

ECB shall use intra-service LT to debit the TIPS transit account in CLM and credit the relevant MCA.

2. For liquidity transfers from TIPS DCAs to RTGS DCAs:

ECB shall use:

(a) Intra-service LT to debit the TIPS transit account in CLM and credit ECB's CB account in CLM

(b) Inter-service LT to debit the ECB's CB account in CLM and credit the relevant RTGS DCAs.

CASE E) Liquidity transfers between **MCAs and RTGS DCAs** booked on CLM and in RTGS (Region 1) before the disaster but **not in RTGS (Region 2)** after the disaster:

The central bank(s) will provide the MCA/RTGS DCA holder concerned with information regarding the liquidity transfer reference[31], involved MCA and RTGS DCAs and the amount.

1. For liquidity transfers from RTGS DCA to MCA:

(a) The central bank responsible for the debited RTGS account holder will debit the relevant RTGS DCA via camt.050, after receiving authorisation from the RTGS account holder, and credit the ECB's CB account in RTGS;

(b) ECB will debit ECB's CB account in RTGS and credit the CLM transit account in RTGS.

CASE F) Liquidity transfers between **MCA and RTGS DCAs** booked on CLM and in RTGS (Region 1) before the disaster but **not in CLM (Region 2)** after the disaster:

The central bank(s) will provide the MCA/RTGS DCA holder concerned with information regarding the liquidity transfer reference[32], the MCA and RTGS DCAs involved and the amount.

1. For liquidity transfers from MCA to RTGS DCA:

[31] Instruction reference of the underlying camt.050.

[32] Instruction reference of the underlying camt.050.

(a) The central bank responsible for the debited MCA holder will debit the relevant MCA via camt.050, after receiving authorisation from the MCA holder, and credit the ECB's CB account in CLM;

(b) ECB will debit ECB's CB account in CLM and credit the RTGS transit account in CLM.

2. For liquidity transfers from RTGS DCA to MCA:

ECB will debit the RTGS transit account in CLM and credit MCA.

The above steps must be completed within two hours after the decision to failover.

4.1.2.6 Failure at central bank level

Even though a partial or complete failure of a central bank will not prevent access to CLM and RTGS for the respective community, it might prevent the central bank from exercising its functions and responsibilities in supporting its community in aspects related to CLM and RTGS. Hence, adequate measures are in place to cope with any malfunctioning at central bank level and properly serve the respective community and avoid any risk of a spillover effect due to a central bank problem beyond their own national community (e.g. where the central bank is unable to settle transactions related to monetary policy operations).

As a general rule, a problem at a central bank that could have an impact on RTGS, CLM or the banking community must be assessed via the Eurosystem internal incident and crisis management procedures.

Communication of failure

Depending on the problem and its potential impact on CLM/RTGS, a communication may be published on the ECB's website and NSDs may inform the national banking community via the bilaterally agreed communication channels.

If the problem does not carry any implications for CLM/RTGS and depending on national rules and procedures, the affected NSD may inform the national banking community directly about national problems.

Failure at ECB level

In the event of a failure at ECB level, all the preceding measures that are available to a central bank will apply.

4.1.2.7 Failure at NSP level

In the event of an NSP failure, no alternative contingency network is available. However:

1. the TARGET Service Desks may act on behalf of the central bank(s), as described in the section above; or

2. if there is a failure affecting only one of the NSPs, the other one could be used, in case the participant has opted to have a second NSP connection as a back-up (U2A or A2A[33]).

4.1.2.8 Failure at participant level (excluding AS)

Communication of failure

Any operational or technical failure of a participant that is known to have lasted for longer than ten minutes should be reported to the respective NSD as soon as possible.

Procedures for handling a failure at participant level

In the event that a participant encounters a problem that prevents it from processing cash transfer orders to/from its MCAs and/or RTGS DCAs, including problems with its NSP, it shall use its own contingency means to the fullest extent possible. This includes in-house solutions as well as the GUI functionality to process liquidity transfers in CLM and the GUI functionality to process liquidity transfers and exceptional payments in RTGS (for more information, see Chapter 4.1.2.8.3).

If its own contingency means are not enough, the participant can rely on the support offered by its NSD. The detailed contingency means are according to the bilateral relationship between a participant and its central bank.

In the case of a failure of a participant which acts as a co-manager, it is noted that the co-managed participants may turn to their responsible NSD (not the NSD of the co-manager) for supporting them.

---

[33] A central bank or a participant that has procured two different NSPs for ESMIG connectivity may initiate transactions via both NSPs in A2A by using different Distinguished Names (DNs). In order to concretely do so, two DNs (each registered by one NSP) must be authorised as Technical Sender and also authorised for the network service; the System User Reference in the BAH must have been associated by the User Certificate DN Link to two (other) Business Sender DNs, each registered by one NSP. On the receiving side, this central bank/participant can only receive (if subscribed) credit/debit notifications to a single DN that is reflected in the CRDM as the default routing. E.g. a participant may receive (if subscribed) a pacs.002 to the same DN from which it sent the related pacs.008 debiting its RTGS DCA. However, a participant whose account will be credited by a CLM payment will receive (if subscribed) the camt.054 to its default routing only.

Note: a single participant's failure should never lead to a delayed closing of CLM and RTGS.

Exceptional payments functionality in RTGS GUI

The exceptional payments functionality (previously referred to as "backup payments") applies in a harmonized way across all participants and aims at allowing them to process payment orders even in the case of a major incident on their side. It provides the affected participants a possibility to reduce the business impact of a potential technical failure by entering payment orders in the GUI. It is entirely at the discretion of the participant to use this functionality for instructing pacs.008 (customer payment orders) and/or pacs.009 (interbank payment orders).

When doing so, the following aspects shall be taken into consideration:

1. **Activation needed:** the exceptional payments functionality is blocked by default and can only be used once the responsible NSD has authorised the affected RTGS participant to use it. Only participants with U2A access may use this functionality. Upon the participant's request (following the bilateral procedures in place), the NSD will activate the functionality with immediate effect.

2. **Activation parameters:** when activating the exceptional functionality, the central bank must indicate if it is for pacs.008, pacs.009 or both, as requested by the participant.

3. **The ability to enter payment orders is subject to necessary privileges:** exceptional payments are inserted via the same GUI screens as "normal" payment orders, and the users of the participant may enter normal and/or backup payments according to the privileges granted to them. More precisely, two different sets of privileges exist for entering pacs.008 and pacs.009 in U2A. For this reason, during the registration process, the participants are required to decide whether they will allow their users to insert a given message type in the GUI, either permanently (i.e. NSD grants role with normal U2A privilege to this participant) or as an exceptional functionality only (i.e. NSD grants role with backup payment U2A privilege to this participant). As a second step, the participant is responsible for assigning the necessary roles and privileges to its users as it sees fit.

4. **Four/two eyes principle:** the four eyes principle is mandatory for entering exceptional payments.

5. **Debit notification:** the sender of an exceptional payment order (i.e. interbank payment with code word "BACP" Backup payment) via pacs.009 can receive a debit notification, via a camt.054 – BankToCustomerDebitCreditNotification, with the code word "BACP" if it has included such code word in element Local Instrument Code and provided also that the participant has previously subscribed to receive such messages. The sender of the exceptional payment

order receives the debit notification once its major incident is resolved and its connection to RTGS is operational again. Participants may only use “BACP” upon activation of the “Exceptional payments” functionality by its relevant NSD and subject to having the dedicated privileges for the usage of the "Enter Payment Order" functionality.

6. **Credit notifications:** the receiver of an exceptional payment (sent via pacs.009) will receive a pacs.009 – FinancialInstitutionCreditTransfer (CORE) with the code word “BACP” if the sender has included such code word in element Local Instrument Code.

7. **NCBs acting on behalf:** In the unlikely event that any TARGET participant is unable to use the “Exceptional payments” functionality in RTGS, it can request its relevant central bank to act on its behalf. When executing the credit transfer order, the central banks may use the relevant code word “BACP”.

8. **Returning to normal operations on the same day:** if the participant resumes normal operations during the same business day it may request the NCB to deactivate the exceptional payment and process cash transfer orders by standard means.

9. **De-activation:** once the participant has resumed normal operations, it may ask the central bank to deactivate the functionality. Otherwise, it will be deactivated automatically at the end of the business day.

10. **Failure lasting more than one day:** if the participant resumes normal operations on the following business day or later, it may submit payment orders with value date of that (current) business day or with a past (original) value date. Notwithstanding, the cash transfer orders will always be settled on the current business day (even if a different value date is indicated).

If a participant opts to submit payment orders from a previous business day, with a past (original) value date, it must ask the respective central bank to deactivate the value date check (which verifies that a payment order specifies a value date that is the same as the current business day). The deactivation is valid only for the current business day and will be automatically reactivated at the end of the business day. Hence, if such deactivation is needed beyond the current business day (i.e. if it is required to deal with unprocessed cash transfer orders with an old value date), the deactivation of the value date check for consecutive business days must be requested separately at the beginning of each business day and implemented by the central bank. Once the participant has completed the sending of payment orders with original (past) value date(s), it must inform the central bank accordingly so that it can reactivate the value date check with immediate effect.

In this situation, the participant may ask its central bank to send a broadcast to inform other TARGET participants about the bank’s use of cash transfer orders with previous value date.

4.1.2.9 Failure at ancillary system level

Communication of failure

Any operational or technical failure of an ancillary system (AS) lasting for more than ten minutes should be reported to the respective NSD as soon as possible.

In the event of a problem, an AS must inform its respective central bank and both need to agree on the contingency processing. Moreover, the AS must inform its settlement members separately about the procedure to be followed. If, following its initial assessment, the responsible central bank believes that the failure of the AS might have originated from a TARGET failure, the normal Incident Management process is initiated.

Available contingency means

If an AS encounters a problem, it is encouraged to use its own contingency means as much as possible while the problem persists. If need be, the respective central bank may act on behalf of the AS. The level of support provided to an AS outside standard support hours is at the discretion of each central bank.

The following contingency means may be used:

- the AS makes payments via pacs.009/pacs.010 (only for ancillary systems owning an RTGS DCA);
- the central bank processes AS files on behalf of the AS using the RTGS GUI ("Upload files" screen) or in A2A mode;
- the central bank makes payments on behalf of the AS (payments can involve only RTGS DCAs and AS technical accounts for procedure D, meaning it is not possible to settle payments on other AS technical accounts);
- if neither the AS nor its responsible central bank are able to process the AS files (e.g. if they are unable to connect to the relevant NSP), the relevant TARGET Service Desk may be asked to upload AS files on behalf of the central bank and the AS.

The contingency means to be used are subject to the bilateral agreement between the AS and its central bank.

Note: in the unlikely event of an AS failure when there may be a significant impact on the smooth operations of TARGET, the home central bank of the AS may request the delayed closing of CLM and RTGS (see Chapter 4.1.2.1 "Rescheduling of CLM and or RTGS events") to give the AS more time to resolve the failure or lessen the impact. The central banks in TARGET will collectively decide on whether a delayed closing should be granted.

Specific aspects for ancillary systems using AS settlement procedures

The contingency processing makes a distinction between AS credits (where a settlement bank funds its short position by making a payment to the AS) and AS debits (where an AS makes payment to a settlement bank with a long position).

Note: the availability of the options described may differ from one case to another.

AS credits may be processed using one of the following methods:

- the home central bank sends, on behalf of the AS, an ASTransferInitiation message/file to the RTGS using the RTGS GUI ("Upload file" functionality) or in A2A mode;
- the AS sends a pacs.010 message if its NSP connection is still up and running (on the preconditions that the AS has an RTGS DCA and the necessary configuration has been implemented in the CRDM; otherwise it is not possible to process direct debits);
- the home central bank sends a pacs.010 message on behalf of the AS (only available for AS settlement procedure D or where the AS owns an RTGS DCA and on the precondition that the necessary configuration has been implemented in the CRDM; otherwise it is not possible to process direct debits); or
- the settlement bank is requested to make payments (i.e. pacs.009) in favour of the AS (only available for AS settlement procedure D or where the AS owns an RTGS DCA).

AS debits may be processed using one of the following methods:

- the home central bank sends, on behalf of the AS, an ASTransferInitiation message/file to the RTGS using the RTGS GUI ("Upload file" functionality) or in A2A mode;
- the AS makes payments (pacs.009) (only available for settlement procedure D or for ancillary systems that own an RTGS DCA).

If the central bank does not process AS message/files on behalf of the AS (i.e. if payments are used), the order of settlement becomes important for AS settlement procedures A and B:

- AS settlement procedure A: the central bank checks in coordination with the AS that all credits are settled before opening the debits phase. If some credits remain unsettled, the central bank reverses them by issuing an opposite payment from the ancillary system's RTGS DCA to the settlement bank's RTGS DCA (for those credits already settled) or by revoking the payment (for unsettled payments that remain pending).
- AS settlement procedure B: this is processed in the same way as AS settlement procedure A.

- For AS making use of the guarantee mechanism, AS settlement procedure A applies, except that, if necessary, the central bank debits the guarantee account in coordination with the AS, rather than making a credit.

For AS settlement procedure C, the home central bank may, on behalf of the ancillary system, open optional procedures, open/close cycles and close procedures directly via the RTGS GUI[34] or via A2A mode.

Simulation of the receipt of a technical notification message

A problem in delivering or processing a technical notification message (e.g. ASTransferNotice, ASInitiationStatus, Receipt, ReturnAccount) may result in a blockage of current and subsequent settlement processes on the AS side. Accordingly, it is strongly recommended that AS are able to simulate the receipt of such messages. This should be done on the AS' own initiative following a check in the RTGS GUI or on the basis of a confirmation of the settlement result received from the NSD via the local communication means in place. Ultimately, the AS can choose the most appropriate solution in agreement with its NSD, i.e. opt for the simulation of receipt or deal with non-receipt via an alternative solution.

Specific aspects for ancillary systems not using AS settlement procedures

As a general rule, ancillary systems should make use of AS settlement procedures. However, in exceptional cases some ancillary systems may be granted a derogation and open an RTGS DCA.

Pay-ins: a failure at the level of ancillary systems that do not make use of AS settlement procedures should not impact the processing of pay-ins to the ancillary system's accounts, although the central bank might have to inform the ancillary system via national communication channels about the incoming payments.

Pay-outs may be processed by the ancillary system using one of the following methods:

1. By making payments or via the RTGS GUI if it can still access it (not allowed for payments to and from AS guarantee funds account, AS mirror account, or AS technical account).

2. By requesting its central bank to send a mandated payment (a payment sent by the central bank debiting the ancillary system's RTGS DCA and crediting the settlement bank's RTGS DCA). The central bank may inform the ancillary system via national communication channels about the processed payments.

[34] See RTGS User Handbook (UHB), Chapter 5.4.6 "AS Procedures and cycles - List screen".

4.1.2.10 Activation of optional maintenance window

Description

From Monday to Friday, CLM and RTGS do not go in maintenance window (MW). The daily MW in CLM and RTGS is optional and activated from 03:00 to 05:00 only upon request. Activation of the MW occurs only:

- in case an urgent activity needs to be performed in CLM and/or in RTGS; and
- upon approval by the central banks in TARGET.

CLM and RTGS will send, upon subscription, a "Status of the CLM and RTGS settlement day notification" message to communicate the start at 03:00 and the end at 05:00 of the optional MW. The specific ReturnBusinessDayInformation message is sent in push mode via camt.019 to communicate the relevant business day events linked to CLM (CSOM "Start of optional maintenance window", CEOM "End of optional maintenance window") and to RTGS (RSOM "Start of optional maintenance window", REOM "End of optional maintenance window").

The decision to activate the MW will be made by the central banks in TARGET by 18:00 at the latest. Following the decision, a communication is also released on the ECB's website to inform the market about the activation of the daily MW.

4.1.2.11 Last-level intervention on request

The TARGET Service Desks can apply last level interventions (LLIs) to address endogenous issues arising in one of the TARGET settlement services without delay to assure the continuity of the service.

In extraordinary cases (i.e. when the current functionalities do not allow modifications due to a bug in the system), central banks may request a last-level intervention from one of the TARGET Service Desks to address an issue on the side of the central bank or one of the participants within its community.

4.2 Suspension and extraordinary termination procedures – euro

A central bank shall immediately terminate[35] or suspend the entire participation of a TARGET participant or some of its cash accounts (MCA, RTGS DCA, TIPS DCA or T2S DCA) separately in its TARGET component, without prior notice, if:

1. insolvency proceedings are opened in relation to the participant; and/or

[35] The conditions under which a central bank shall or may suspend or terminate a participant are laid down in the TARGET Guideline, Annex I, Part I, Article 25.

2. the participant no longer meets the access criteria for participation in that component system.

The central bank may terminate without prior notice or suspend the participant's participation in its TARGET component if:

- one or more events of default (other than those referred to above) occur;
- the participant is in material breach of the harmonised conditions for Participation in TARGET;
- the participant fails to carry out any material obligation to the central bank;
- the participant ceases to have a valid agreement with an NSP to provide the necessary connection to TARGET;
- any other participant-related event occurs which, in the central bank's assessment, threatens the overall stability, soundness and safety of any TARGET component system, or which jeopardises the central bank's performance of its tasks, as described in the respective national law and the Statute of the European System of Central Banks and of the European Central Bank; and/or carries risks on the grounds of prudence;
- an NCB suspends or terminates the participant's access to intraday credit pursuant to Article 13, Part II, Annex I of the TARGET Guideline.
- the participant is excluded or otherwise ceases to be a member of the NSP CGU for the relevant service.

If a central bank suspends or terminates a participant's participation in TARGET, all other central banks must be notified via broadcast of all the relevant services in which the suspended/terminated participant was active.

4.2.1 Suspension or extraordinary termination of a participant in CLM & RTGS

In the event of suspension or extraordinary termination of a TARGET participant, the following actions are performed by the central bank concerned:

1. Blocking:

(a) Block the party. The blocking becomes effective for all the TARGET settlement services the party is linked to and all TARGET accounts[36] owned by that participant across all services are blocked; or

(b) Block the various TARGET accounts of the participant separately; either "Block for credits and debits", "Block for credits" or "Block for debits".

[36] Please note that overnight deposit accounts and marginal lending accounts are not automatically blocked when blocking a party in CRDM. They must therefore be blocked separately.

In both cases, the responsible central bank may reverse the situation by unblocking the party or the cash accounts.

Blocking is possible at any time when CRDM is running. If the “valid from” date and time is specified as immediate, the blocking of a party, for example, becomes effective immediately in all settlement services the party is linked to. The same goes for the unblocking of parties or will be effective in the future if a specific “valid from” date is indicated.

If the suspended participant still needs to remain in the RTGS directory and CLM repository, the respective central bank shall take the necessary actions.

If the suspension takes place outside standard support hours (e.g. at the weekend), each central bank must ensure that appropriate procedures are in place so that the necessary action can be taken.

2. Actions between central banks and the affected participants

The responsible central bank checks whether it is necessary to amend the CRDM set-up to replace the active links between the suspended/terminated participant’s CLM and RTGS accounts and other participants’ accounts (i.e. link for the direct debit of fees, link to T2S DCA, link for Floor/Ceiling Rule-based liquidity transfer orders, leading CLM account holder). The responsible central bank informs other affected participants (due to the existence of such links), asking them to provide the necessary information in order to proceed with the replacement of those links. If cross-border links exist, the relevant central banks coordinate the actions over all impacted accounts.

The following table shows the relevant CRDM parameters to be considered:

Table 10

CRDM parameters to be considered

CRDM set-ups to be checked by CB	Needs to be replaced (yes/no)	Clarification
Overnight deposit	No (except limitation of access to monetary policy tools)	
Marginal lending	No (except limitation of access to monetary policy tools)	
Automated and rule-based LT	No	MCA and RTGS DCA belong to the same party
RTGS sub-account	No	RTGS DCA and sub-account belong to the same party
Direct debit of fees	No	For invoicing only
Floor/Ceiling Rule-based LTO	Yes	LT cross-participant and cross-border can be done
T2S DCA	Yes	LT cross-participant and cross-border can be done
Auto-collateralisation	No (except limitation to auto-collateralisation procedure)	
ECONS II accounts	No	
Leading CLM account holder	No	For remuneration or MR requirements only
TIPS CMB	No	TIPS DCA set-up amending if necessary
Co-manager	Yes	Co-manager is responsible for its own account (even if the account is co-managed by another participant) and thus holds the responsibility to appoint a new co-manager. During the period prior to the appointment of a new co-manager, the central banks may act on behalf of the affected co-managee on a best effort basis.
Leader of a Liquidity Transfer Group or Account Monitoring Group	No	
Leader of minimum reserve pool or indirect (Leading CLM account holder)	Yes	Participants in the minimum reserve pool/indirect holders will need to assign a new leader

External communication: a broadcast message is sent immediately (a pop-up alert) to all TARGET users and all relevant TARGET settlement services (i.e. CLM, RTGS, TIPS[37], T2S) to communicate the suspension or termination of the party and/or the blocking of its TARGET accounts. Separate broadcasts will be visible in CLM and RTGS via the respective GUIs.

If the suspension takes place outside standard support hours (e.g. at the weekend), the relevant broadcasts will be visible when the CLM/RTGS GUIs are available.

Further actions in the event of termination. In addition to the above steps, the responsible central bank must delete the related reference data via the CRDM. As a consequence, the reactivation of a party requires the re-creation of all the correspondent reference data in CRDM.

It should be noted that:

[37] The broadcast functionality in TIPS is subject to the approval and deployment of Change Request CR-0014.

- As concerns liquidity transfer groups, central banks, as responsible actors, exchange all necessary information for the performance of their duties and obligations under the liquidity transfer groups agreement. These central banks immediately notify the managing central bank of any enforcement event of which they become aware relating to the group or any group member, including the head office or any of its branches.
- When suspending a party, the central bank can choose whether the suspended participant should still be published in the RTGS directory.
- If the suspended party is an ancillary systems settlement bank, it is treated according to the rules that apply to participants. The central bank of the settlement bank must confirm its transactions. As concerns specifically AS settlement procedure C, if a participant is declared insolvent while a settlement cycle is still open, the central bank of the settlement bank is obliged to manually process all earmarked transactions relating to that AS, up to the amount frozen in the participant's sub-account.
- If an ancillary system is suspended or terminated from CLM and or RTGS, it is treated according to the rules that apply to participants. The central bank of the ancillary system must confirm its transactions.

Effects of the suspension of a participant in CLM and or RTGS/blocking of MCA/blocking of RTGS DCA:

- No new cash transfer orders (depending on whether debit/credit or both have been blocked) can be settled automatically on a blocked account (MCA, RTGS DCA). For settlement to proceed, the respective CB must confirm them.
- In RTGS, cash transfer orders involved in a running algorithm are not directly affected by the blocking.
- In principle, all queued cash transfer orders sent by the suspended participant are set to "earmarked" after the blocking becomes effective and each cash transfer order requires explicit confirmation by the CB before any further settlement attempt can take place.
- Cash transfer orders sent to the suspended participant, following its suspension, are also set to "earmarked" pending approval by the central bank. If they are not approved by the end of the business day, they will be rejected automatically. The basis on which the central bank confirms cash transfer orders depends on both European Union regulations and national rules.
- Liquidity transfer orders, with the exception of automated liquidity transfer orders, are rejected after the unsuccessful settlement attempt.
- Warehoused payment orders need to be confirmed by the responsible CB on the intended settlement day before they can run through the entry disposition.
- Standing order liquidity transfer orders debiting the blocked MCA or RTGS DCA are no longer generated. Standing order liquidity transfer orders crediting the

blocked MCA or RTGS DCA are set to “earmarked” pending approval by the responsible CB.

- For inter-service standing order liquidity transfer orders, the blocking status of the cash account to be credited is not checked by the CLM and RTGS and the detailed handling is up to the respective receiving settlement service.
- Intra-service standing order liquidity transfer orders are not created if:
  - the cash account to be debited is blocked for debits;
  - the cash account to be credited is blocked for credits; or
  - the standing order liquidity transfer order is related to an AS and the AS is blocked.

4.2.2 Suspension or termination of MCA designated for T2S purposes

If a central bank suspends or terminates a participant (following the procedures described above) with an MCA to which a T2S DCA is linked to, the central bank(s) responsible for the linked T2S DCA shall:

Change the MCA:

- if the MCA is blocked as a result of the suspension/termination of a participant due to insolvency proceedings or other events of default and the T2S DCA does not belong to the same party as the MCA; or
- if the participant has been suspended/terminated due to reasons other than insolvency proceedings or other events of default and there are no reasons to suspend or terminate the linked T2S DCA.

Suspend the T2S DCA(s):

- if the participant has been suspended/terminated due to insolvency proceedings or other events of default and the T2S DCA(s) belong(s) to the same party as the participant; or
- if the participant has been suspended/terminated due to reasons other than insolvency proceedings or other events of default and there are also reasons to suspend or terminate the linked T2S DCA.

4.2.3 Limitation, suspension or termination of intraday credit

Suspension/termination of intraday credit

A national central bank shall suspend or terminate access to intraday credit if one of the following events of default occurs:

- the participant's primary[38] MCA with the central bank is suspended or closed;
- the participant concerned ceases to meet any of the requirements for the provision of intraday credit, as laid down in Annex I, Part II, Article 10 of the TARGET Guideline;
- a decision is made by a competent judicial or other authority to implement a procedure for the winding-up of the entity or the appointment of a liquidator or analogous officer over the entity or any other analogous procedure;
- the participant becomes subject to the freezing of funds and/or other measures imposed by the European Union restricting the participant's ability to use its funds;
- the participant's eligibility as a counterparty for Eurosystem monetary policy operations has been suspended or terminated.

A national central bank **may** suspend or terminate access to intraday credit if a national central bank suspends or terminates the participant's participation in TARGET as per the TARGET Guideline Part I, Article 25(2).

A central bank **may** decide to suspend or terminate a participant's access to intraday credit if the participant is deemed to pose risks on the grounds of prudence, i.e. if a national central bank has good grounds to suspect that allowing a participant further unrestricted access to TARGET would constitute a risk for the ESCB.

In case of suspension or termination of intraday credit, the credit line of the MCA holder should be set to zero.

Limitation of intraday credit

A central bank **may** decide to limit a participant's access to intraday credit if the participant is deemed to pose risks on the grounds of prudence.

In case of limitation to intraday credit, the credit line of the MCA holder should be adjusted accordingly to the limit defined.

Note that **if an NCB decides to suspend, limit, or terminate a Eurosystem monetary policy counterparty's access to intraday credit**:

1. the national central bank shall implement that decision pursuant to the relevant provisions in the contractual or regulatory arrangements applied by that national central bank.
2. such decision will not take effect until the Governing Council of the ECB has approved it. Where appropriate, the Governing Council shall decide upon uniform implementation of the measures taken in all TARGET settlement services.

[38] Primary MCA is the legal term according to the TARGET Guideline definitions. Note that Primary MCA is also referred to as Default MCA in the Functional Documentation.

4.2.4 Technical suspension of a participant

Technical suspension is a temporary means to protect CLM and RTGS from massive and uncontrolled message inflows. It is a purely technical measure that is triggered when a participant sends a presumably uncontrolled and extraordinarily high number of messages. As this is a measure to protect the functioning of the service, the related procedures are very time-critical and should receive the highest priority attention.

If massive inflows are detected compared to the normal inflow expected by a participant, the responsible NSD and its participant will work together to investigate whether the messages were sent unintentionally, asking them to cease the abnormal behaviour without delay. If the participant is unable to resolve the issue rapidly and stop the inflow of traffic, a decision will be made on whether to technically suspend the participant. If the investigation performed by the participant reveals a security incident (e.g. cyber issue), then the procedures described in Chapter 4.3 "Operational procedures related to information security events (e.g. cyberattack)" should be followed. If it is considered that the ongoing issue threatens the stability or resilience of TARGET, the technical suspension will be applied.

Messages sent by the technically suspended participant will no longer reach CLM/RTGS. Any messages sent to a technically suspended participant will be processed by CLM/RTGS.

4.3 Operational procedures related to information security events (e.g. cyberattack) at the level of the participant

In the unlikely case a CLM MCA and/or RTGS DCA holder is affected by an information security event (such as a cyberattack), at first instance it is the responsibility of the CLM MCA and RTGS DCA holder to implement all local measures to contain the issue internally and avoid any spillover to CLM and/or RTGS. A key measure could be the disabling of the local connection by the CLM MCA and/or RTGS DCA holder (or its instructing party).

The CLM MCA and/or RTGS DCA holder should inform its responsible NSD of the event without undue delay.

4.3.1 Information gathering

Upon being notified of the information security event detected by a CLM MCA and/or RTGS DCA holder, the decision on further actions by the responsible central bank would largely depend on the availability of relevant information. Gathering such information is primarily within the prerogatives of the home central bank of the participant concerned and the process may be based on the data provided by the participant or obtained from other available sources (e.g. CLM & RTGS Service Desk reports). Relevant information may encompass the following aspects:

- **Impacted transactions:** the type and details of the fraudulent messages together with the total number, value, time of submission/settlement and receivers of the impacted messages.
- **Impacted connectivity channel:** information on the participant's connection type (NSP) and possible use of a service bureau, with all related details.
- **Parties already informed:** seeking confirmation that the participant's banking supervisor and relevant law enforcement authorities were notified. If this is not the case, the CLM MCA and/or RTGS DCA holder should be reminded/advised to inform them accordingly.
- **Cross-border aspects:** information on whether the same infrastructure is used to connect to several TARGET component systems and other cross-border considerations (if relevant).
- **Information on the cash transfer orders initiated by the participant in the period preceding the instance of fraud:** the data can be obtained via ex-post scrutiny of the payments and liquidity transfers initiated by the participant before the information security breach occurred. The investigation could help to identify when the fraud/fraud attempt took place in comparison to when it was detected.

Any other relevant information, including initial assumptions as to the source of the fraud.

4.3.2 Mitigation measures

Should the local containment measures of the CLM MCA and/or RTGS DCA holder prove insufficient to mitigate the event, the responsible NSD may offer to apply the following measures:

1. A reservation of all funds for urgent payments may be introduced in the GUI.
2. To safeguard the funds, the liquidity can be transferred to a CLM MCA or RTGS DCA of the responsible NCB through an inter-service liquidity transfer.
3. The CLM MCA(s) and/or RTGS DCA(s) may be blocked.
4. Exclusion of the participant from the NSP Closed Group of Users (CGU) by the NSP. Following a request from the responsible central bank to the TARGET Service Desk, the latter will ask the NSP to remove the TARGET participant from the CGU.

4.3.3 Additional support for the affected participant

In addition to the mechanisms described above, the respective central bank may also provide further assistance to a participant affected by a fraud event. Depending

on the circumstances and assessment of the fraud event, the following measures may be considered:

- **Support in recovering fraudulently processed cash transfer orders:** the support provided to the participant may include, for example, assistance in collecting the contact details and other relevant information of the recipients of cash transfer orders (if necessary, in collaboration with other central banks).
- **Immediate investigation on the source of the fraud:** the central bank may provide further support in identifying the source, spreading and impact of the fraudulent activity.

5 Business continuity management

For a general description of business continuity management, please see Chapter 7 of the Infoguide – Fundamentals.

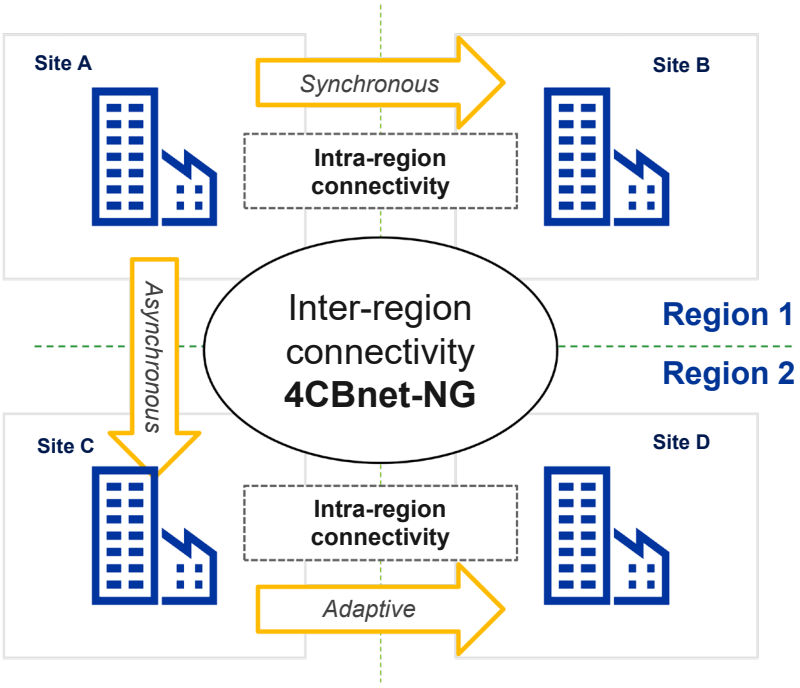
5.1 CLM and RTGS business continuity management model

The CLM and RTGS business continuity model envisages an operational model based on **service continuity arrangements** (i.e. “two regions, four sites”) and **contingency arrangements**.

5.1.1 CLM and RTGS service continuity arrangements

The CLM and RTGS architecture provides a high level of resilience thanks to application redundancy and its self-healing capability. The architecture of the CLM, RTGS (and T2S) is based on the concept of “two regions, four sites”. The four sites are fully equivalent and each of them is equipped with the same technical resources: processor, storage, network interface, software, etc. The two sites in each region are located at a distance that is sufficient to have a distinct risk profile. The two regions are located several hundreds of kilometres apart.

Figure 3
Service continuity arrangements – “*Two regions, four sites*”



5.1.1.1 Arrangements for CLM & RTGS local disaster

Each region has the capability of a local recovery; the two sites in each region are located at a distance of a few kilometres from each other. The recovery within a region is assured by Synchronous Remote Copy (SRC) activated on the whole environment between the two sites of the same region. The SRC guarantees real-time data updates at both sites, i.e. each write operation is completed only when both sites are updated. Major failure or disaster indicates a serious service interruption which is solved by the relocation of CLM and RTGS operations to a second site (**intra-region failover**), physically separate from the primary site. As a synchronous mode is applied, the databases at both sites are the same, and no reconciliation is required after a failover.

An **intra-region failover** can be conducted if deemed necessary following an appropriate technical assessment. The relevant procedure to be followed if a local disaster occurs can be found in Chapter 4.1.2.5 “Service continuity (failover to the second site or second region)”.

An intra-region failover ensures the continuation of normal business within a maximum of one hour.

5.1.1.2 Arrangements for CLM & RTGS regional disaster

A wide-scale disaster having a high impact on the region operating CLM, RTGS and T2S might trigger an inter-region failover. To be effective even in a worst-case scenario, the plan to recover the operating region avoids any dependency between the two regions (decisional, personnel, technical, etc.), thus allowing the alternate region to take over the operation without relying at all on the impacted region.

If both sites within Region 1 become unavailable at the same time or if the asynchronous copy facility encounters problems, then a loss of data would occur. In such a situation, the only option would be a failover to Region 2 (**inter-region failover**) and to reconcile the missing traffic. The resumption of business in Region 2 should be enabled within two hours, excluding the time between informing service users and the service users’ response, i.e. the time they need to reconcile the lost data.

Should the type of incident allow for an orderly and progressive external connections closure and so to complete smoothly the asynchronous copy towards Region 2, the inter-region failover and the resumption of operations in Region 2 would result in no loss of data. This is to be completed within two hours.

5.1.2 CLM and RTGS contingency arrangements

CLM and RTGS contingency arrangements are in place to mitigate the impact on participants of failures at different levels. ECONS II is activated in response to a failure at the level of the CLM and/or RTGS. The *exceptional payment functionality*

and the *acting on behalf* arrangements aim to mitigate technical failures at participant level.

5.1.2.1 ECONS II

ECONS II aims to address the situation where the CLM and/or RTGS are not available. Once activated, ECONS II will always replace both CLM and RTGS for contingency settlement. The settlement of transactions in a contingency session shall be performed on specific accounts opened in ECONS II, dedicated for contingency settlement, with a starting balance of zero. The liquidity used for processing in ECONS II may be obtained from other available sources or be based either on already available collateral or newly provided collateral.

When activated, ECONS II provides:

- real-time gross settlement in central bank money for payment orders and ancillary systems;
- transactions submitted by ECONS II actors, in the event of unavailability of CLM and/or RTGS;
- liquidity management functionalities to support the contingency settlement;
- queries and reporting tools to support monitoring and reconciliation activities;
- contingency session opened for several business days (up to five business days).

Account structure

Central banks open contingency accounts for all CLM CB accounts and all participant MCAs in CRDM. Additionally, the central banks open AS contingency technical accounts in CRDM for ancillary systems that wish to make use of contingency processing in ECONS II under AS settlement procedure A. All these contingency accounts have the same BIC as the respective account in CLM and are propagated daily during the end-of-day propagation from CRDM to ECONS II.

Most participants are expected to use the same BIC for opening a CLM account as for opening an RTGS DCA. Therefore, participants can rely on a general assumption that in a contingency situation they can make payments to the same recipient BICs that they use also for normal wholesale payments in the RTGS or for central bank operations processing in CLM. However, it is also important to note the limitations of this general assumption. For example, if a participant has opened multiple RTGS DCAs but holds only one MCA then only the BIC of the MCA will be reachable in ECONS II. Similarly, no multi-addressee BICs are reachable in ECONS II.

ECONS II supports the following contingency processing options for AS:

AS settlement procedure A

- ECONS II supports only the settlement of AS files that fulfil AS settlement procedure A file format and content requirements. Therefore, an AS should only request its central bank to open an AS contingency technical account in CRDM (to be propagated to ECONS II) if the AS is in a position to make use of AS settlement procedure A.

- Also, an AS that would not need a technical account normally (e.g. if the AS makes use of bilateral settlement via AS settlement procedure B) but wishes to settle in ECONS II by making use of AS settlement procedure A, will have to open an AS technical account in RTGS, requesting its central bank to also open the relevant AS contingency technical account in CRDM (to be propagated to ECONS II).

AS settlement based on U2A payment orders

- If an AS does not wish to settle in ECONS II by making use of AS settlement procedure A, it may instead settle on a contingency account by making use of individual U2A payment orders. In order for the central bank to open a contingency account in CRDM, the AS must hold an MCA in CLM.

- For AS settling normally under settlement procedure B, C and E, this contingency processing approach would require a change to their standard operational set-up: these AS would need to rely on settlement banks initiating the payment orders themselves (i.e. settlement cannot be initiated by the AS) or on central banks initiating the payment orders on behalf of the settlement banks (if not all the settlement banks are connected to ECONS II).

- AS making use of AS procedure D could continue settlement in their own books based on the liquidity on the RTGS technical account before the failure, even when the RTGS service is unavailable. Funding and defunding procedures while ECONS II is open are subject to bilateral agreements between the AS and its settlement banks.

Each AS that joins the RTGS settlement service, or intends to add a new settlement procedure, shall communicate to its responsible central bank whether, in the event of a CLM/RTGS outage, it would use procedure A or U2A payment orders. An AS may decide to amend its contingency processing set-up and shall inform its central bank accordingly.

On an exceptional basis, a contingency (technical) account in ECONS II during a contingency situation can be opened. However, this exceptional opening of an account is only possible in a contingency situation lasting multiple business days and for those accounts that are already reflected in CRDM and, without a prolonged incident, would have also become active during a business day covered by the incident.

Connectivity

ECONS II is accessible via an instance of ESMIG that is distinct from the instance serving the CLM and RTGS production environments. Therefore, unavailability of the ESMIG connection to CLM and RTGS will not impact the ESMIG connection to ECONS II. Consequently, participants must join a separate CGU for ECONS II.

The following channels are available for connecting to ECONS II via ESMIG:

- Application-to-application (A2A) channel, which is application-oriented and available only to central banks;
- User-to-application (U2A) channel, which is user-oriented and available to central banks and participants.

The option for participants to connect to ECONS II stems from the acknowledgement that the criticality of payments might change depending on the duration of the incident. Therefore, participants may insert payments assessed as critical for their specific business via a graphical user interface (GUI) in U2A mode. In addition, a direct connection to ECONS II limits the number of manual steps required for processing payments in a contingency situation.

As of go-live of CLM and RTGS, all critical participants (RTGS DCA holders and AS settling in the RTGS component or in TIPS) and those having very critical business (i.e. settling CLS payments or CCP margin calls) must connect via U2A to ECONS II. Connectivity remains optional for all other participants.

This rule also applies to participants connecting via connected central banks (Out CBs). Connectivity to ECONS II is optional for connected central banks, unless they have a participant that must, or requests to be connected to ECONS II.

As of March 2025 (i.e. two years from CLM and RTGS go-live), all participants holding an RTGS DCA as well as all AS settling in the RTGS will be required to connect to ECONS II via U2A. Connectivity remains optional for all other participants.

Just as a participant may outsource its ESMIG connectivity to a third party for normal operations, it may also outsource its connectivity to ECONS II (via ESMIG) to a third party. In order to avoid issues stemming from this outsourcing in a contingency situation, the same third party providing the connectivity for normal operations should also provide the connection to ECONS II.

5.1.2.2 Exceptional payments functionality

In a contingency situation, a participant that normally sends payments via A2A may no longer be able to send payment orders to RTGS as a consequence of a major incident on its site. The participant can request the activation of the exceptional payments functionality from its responsible central bank and should already have U2A access in place. This functionality provides the participant with the means to

introduce interbank and/or customer payment orders via the RTGS GUI in a contingency situation.

These exceptional payments can be either normal U2A payment orders during a contingency (flag activation for pacs.008 and pacs.009) or backup interbank payment orders (only pacs.009) if the code word BACP is entered by the participant in the GUI.

A detailed description of the operational procedures can be found in Chapter 4.1.2.8.3 “Exceptional payments functionality in RTGS GUI”.

5.1.2.3 Acting on behalf (NCB and 4CB)

A CLM or RTGS participant may request the support of its responsible NSD if it is confronted with an issue that cannot be mitigated through its own contingency measures or using the GUI that allows it to instruct, in U2A mode: (i) liquidity transfers in CLM and (ii) liquidity transfers and exceptional payments in RTGS.

Acting on behalf is a contingency arrangement that can be applied in CLM and RTGS as well as in ECONS II.

For AS files

- Ancillary systems that are not able to process AS files can request their responsible NSD to process files on their behalf following the bilaterally agreed procedures between the AS and its NSD. The NSD can process the files in A2A mode or via a dedicated RTGS GUI screen.
- If both the AS and its responsible NSD are not able to process the AS file, the relevant central bank may request support from the TARGET Service Desk to upload the file on its behalf.
- In ECONS II, an NSD or the TARGET Service Desk will be able to upload only AS files that satisfy the format and content requirements of AS settlement procedure A on behalf of an AS, as it is the only AS file format that ECONS II supports.

For cash transfer orders

- NSDs may process cash transfer orders upon request from their participants. The instructions are sent to the NSD using the contingency communication procedures agreed beforehand between the NSD and its participants.
- The cash transfer orders to be processed can be payments, liquidity transfer orders or clean payments for ancillary systems (subject to potential limitations at local level; for example, an NSD might not support the processing of pacs.008 messages).

- In turn, NSDs may ask the TARGET Service Desk to process cash transfer orders on their own behalf or on behalf of their participants if the NSD's connection to CLM and RTGS or ECONS II is unavailable.

6 Testing activities for CLM and RTGS

6.1 Overview of testing activities for CLM and RTGS

The following table provides an overview of the tests to be performed.

Table 11
Overview of testing activities for CLM and RTGS

Test name	Environment	Participation for critical participants	Participation for non-critical participants
BCM testing			
Service/business continuity			
Inter-region failover	PROD	N/A	N/A
Intra-region failover	PROD	Fulfilled without additional testing activities required	Fulfilled without additional testing activities required
Contingency arrangements			
ECONS II regular testing	UTEST	Mandatory	Mandatory for participants (excluding AS) settling very critical cash transfer orders
ECONS II live trial	PROD	Mandatory	
ECONS II two-day test involving T2S	UTEST	Mandatory	
Exceptional payment functionality	PROD/alternatively UTEST	Mandatory	Mandatory for participants settling (very) critical cash transfer orders;
Acting on behalf	PROD/alternatively UTEST	Mandatory if this support is offered by their central bank	Mandatory for participants settling (very) critical cash transfer orders; if this support is offered by their central bank.
Business continuity at the level of participants			
For critical participants (secondary site test)	PROD	Mandatory	N/A
Other operational procedures tested			
TC2 connectivity test and simulation exercise (xMatters)	N/A	Optional	N/A
TC2 connectivity test and simulation exercise (CISCO)	N/A	Optional	N/A

6.2 BCM tests

6.2.1 Service/business continuity tests

Intra-regional failover

The intra-regional failover test covers the scenario of a site recovery moving from site A to site B within the same region.

Intra-regional recovery sessions are organised by the TARGET Service Desk once every six months. The test is performed in the production environment over a week as follows: the intra-regional failover is performed moving from site A to site B within the same region on the pre-agreed date on a Saturday morning. Normal operations are run by the second site for an entire week, with the return to site A one week later, on Saturday morning. Since full T2 operations are run for an entire week, there are no further additional testing activities required for critical participants.

Description of the intra-regional recovery can be found in Chapter 5.1.1.1 "Arrangements for CLM and RTGS local disaster" of this document.

Inter-regional failover

The inter-regional failover test covers the scenario of a regional recovery moving from region 1 to region 2.

Inter-regional recovery sessions are to be organised by the TARGET Service Desk once every six months. The test is to be performed in the production environment during weekends. During normal business days and hours, similar exercises can be conducted in UTEST. Participants do not participate in the test as the system is in maintenance window.

Description of the inter-regional recovery can be found in Chapter 5.1.1.2 "Arrangements for CLM and RTGS regional disaster" of this document.

6.2.2 Contingency arrangements tests

The tests described below consist of:

1. Injecting liquidity into the participants' contingency accounts:

   (a) by the NSD injecting the liquidity directly into the ECONS II participants' contingency accounts that will participate in the test; or

   (b) by making liquidity movements from T2S DCAs.

2. Central banks uploading AS files for AS Settlement Procedure A on behalf of their participants (if applicable).

3. MCA/RTGS DCA holders (or the responsible NSD acting on their behalf for those participants not required to have a direct connection to ECONS II) inputting cash transfer orders into the ECONS II GUI. The NSD then agrees/disagrees with the cash transfer orders on behalf of its participants.

Participants are expected to find counterparts with whom they can exchange payments. Where inter-Member State payments form part of the scenario and the

counterparty is not available for testing, the respective central bank is to replace the external counterpart with one of its own accounts.

ECONS II regular testing

Regular testing of ECONS II should be completed at least every six months by central banks and those TARGET participants that are obliged to have a connection to ECONS II (critical participants as well as those participants that process very critical cash transfer orders in the RTGS). These tests are performed in the UTEST environment.

For this purpose, ECONS II is activated in UTEST on Wednesdays from 10:00 to 12:00. Testing outside this time frame may be provided upon request.

In cooperation with their national user community, central banks may organise these tests on specific dates and for a specific time frame or may choose to use the permanent weekly option. If the test schedule is constrained to specific dates, central banks are to provide critical participants with sufficient opportunities (e.g. one test day per quarter) to complete this test at the required frequency.

ECONS II live trial

At least once a year, the ECB coordinates one-day live trial sessions for ECONS II in the production environment.

Participation in these live trial sessions is required for all central banks and those participants that are obliged to have a connection to ECONS II (critical participants, as well as those participants[39] that process very critical cash transfer orders in the RTGS). For the live trial, ECONS II is activated in the PROD environment in parallel with normal operations. Volume testing is not carried out.

ECONS II two-day test involving T2S

Once a year, the scenario of a two-day opening in ECONS II is tested. The test is organised in UTEST and also involves T2S.

Participation in this two-day test is required for all central banks and those participants[40] that are obliged to have a connection to ECONS II (critical participants, as well as those participants that process very critical cash transfer orders in the RTGS).

Exceptional payment functionality

Critical participants and participants that process (very) critical cash transfer orders in RTGS, and that intend to use the exceptional payment functionality, must perform this test at least twice a year in live operations (i.e. PROD environment). The test

[39] Excluding non-critical AS.

[40] Excluding non-critical AS.

date is to be agreed with the relevant central bank in advance[41]. In cooperation with their national user community, central banks may either limit the number of days and time frame for these tests or may keep it open as a permanent option, i.e. available on all days when the respective environment is in operation. If the test schedule is constrained to specific dates, central banks are to provide critical participants with sufficient opportunities to perform this test at least every three months.

Each participant is to request activation of exceptional payment functionality via its central bank. Participants may then execute exceptional low value payments of different amounts (less than €10) to pre-agreed accounts. Central banks may allow participants to use their accounts as the addressee for cash transfer orders if no other test counterparty is available.

If the risk of testing the above scenario is considered to be too high in the PROD environment, the test may be performed in UTEST. In this case, no limits apply to the amount.

Acting on behalf

Each critical participant, as well as those participants that process (very) critical cash transfer orders in the RTGS, which intend to use an additional arrangement offered by its central bank[42] (e.g. mandated payments, contingency upload of A2A files and messages in U2A) must test the following scenarios in live operations (i.e. PROD environment). The test must be performed at least twice a year (one test every six months) on a date agreed with the relevant central bank.

If the risk of testing these scenarios is considered to be too high in PROD, tests may be performed in UTEST.

In cooperation with their national user community banks, central banks may decide to limit the number of days and time frame for these tests or may keep it open as a permanent option, available on all days when the respective environment is in operation. If the number of days or the time frame is constrained, central banks are to provide sufficient opportunities for each critical participant to schedule respective tests at least every three months.

Scope

- Central banks are expected to execute critical payments on behalf of their critical participants and participants setting (very) critical cash transfer orders using the exceptional payment functionality and to test it together with them.
- Central banks that offer their critical participants and participants setting (very) critical cash transfer orders the option of instructing cash transfer orders (i.e. mandated payments) are expected to test its operational functionality.

---

41 For A2A -only RTGS account holders, the exceptional payment functionality is subject to central bank activation. For RTGS account holders under a mixed scenario with the option of creating payment orders (interbank and customer) in U2A outside of the contingency situation, central bank activation is only necessary for interbank payments with the code word: BACP (backup payment).

42 Depending on the support offered by their respective NCB.

- Central banks that offer their participants the option of uploading A2A files and messages in U2A are expected to test its operational functionality.

Although not mandatory, non-critical participants may arrange similar testing activities with their NSD at regular intervals.

6.2.3 Business continuity at the level of participants

For critical participants (secondary site test)

To ensure the smooth functioning of the TARGET system, participants that qualify as critical participants must have a business continuity strategy that includes the following elements.

- Business continuity plans and procedures for maintaining them.
- An alternate operational site must be available.
- The risk profile of the alternate site must be different from that of the primary site (significant distance between the sites, different power grid, different central telecommunications, etc.).
- In the event of a major operational disruption rendering the primary site inaccessible and/or critical staff unavailable, critical participants must be able to resume normal operations from the alternate site, where it must be possible to properly close the business day and open again the following business day(s).
- Procedures must be in place to ensure that the most critical business transactions can be performed while business is being moved from the primary to the alternate site.
- The ability to cope with operational disruptions must be tested at least once a year and all critical staff must be suitably trained. There should be no more than one year between tests.

The business continuity testing requirements can therefore be summarised as follows.

- Critical participants must test their business continuity procedures by performing critical business transactions in the production environment and closing the business day from the secondary site at least once a year.

6.3 Other operational procedures tested

TC2 communication tools - connectivity test and simulation exercise

At least once a year, a TC2 connectivity test and simulation exercise is to be organised to test the primary and secondary communication tools.

Participation is optional for the appointed representatives of the critical participants, but strongly recommended.

7 Financial management

The process of collecting CLM & RTGS revenues takes place once a month.

More details regarding the receipt and payment of the relevant invoices can be found in Chapter 9 “Financial management” of the Infoguide – Fundamentals.

8 Change, release and deployment management

8.1 Purpose and scope

The change, release and deployment management process (hereafter referred to as CRM) defines how functional changes to CLM and RTGS are managed. The CRM covers the life cycle of change requests (CR), from the moment a change is formally requested to its release in the production environment, including planning and agreement on the content of a release, and the consequent design, build, configuration and testing of the new software and hardware components. Management of non-functional changes (emergency and others) is also covered in this chapter.

8.2 CRM procedures for CLM & RTGS

Change and release management processes govern the procedure for managing modifications and enhancements requested to CLM & RTGS during its life cycle, from the time a change request is formally requested until it reaches its final status (i.e. withdrawn, rejected or implemented in a release).

8.2.1 Main applicable deadlines

Change requests can be raised at any point in time. However, in order to ensure that a change request can be considered for implementation in a particular release, under normal circumstances, a change request shall be raised at the latest approximately 19 months before the planned go live of its target release. The NSDs shall inform their CLM & RTGS participants of the applicable deadline.

Change requests and solutions to problems are allocated to a release scope at least 12 months ahead of the planned go-live of that specific release. The content of the release including the assigned change requests and the main milestones of the release are published on the ECB's website.

8.2.2 Change management

Change management governs the life cycle of requested modifications and enhancements that may result in functional or non-functional changes.

The ECB, central banks (euro and non-euro), CLM & RTGS participants and the 4CB are entitled to formally **submit a change request** (see form in Annex III). Change requests raised by CLM & RTGS participants must be submitted via their

respective central banks. Other stakeholders can initiate a change request only if they are sponsored by one of the former actors.

8.2.3 Release management

Release management is a specific process for assessing and ranking change requests and production problems and for defining the scope and the proposed target implementation date of a new CLM & RTGS release. This ensures that all aspects of a change, both technical and non-technical, are taken into account, including coordination aspects with other TARGET services, if needed. Release management addresses all types of possible releases:

A yearly major release during the second weekend in June.

- includes a set of software changes affecting CLM and RTGS functionality, as well as fixes or resolution of identified production problems.

A yearly minor release during the third weekend of November.

- includes a set of software changes to align CLM and RTGS with the regularly scheduled update of the ISO 20022 message standards, as well as resolution of identified production problems.

Changes to common components (may happen outside the standard CLM & RTGS annual release schedule).

8.2.4 Deployment management

Deployment management organises the rollout of CLM & RTGS software releases[43], configurable parameter changes and/or any associated operational service changes to the pre-production environment and the production environment.

8.2.4.1 Standard deployment path

The standard deployment path for a release follows a phased approach, meaning it starts with a deployment in the Eurosystem acceptance (EAC) environment, followed by the user testing (UTEST) environment and lastly the production (PROD) environment. Except as otherwise agreed by the Eurosystem, the releases are deployed to production on a rolling basis during the weekend when the release is planned.

[43] CLM & RTGS software releases include changes (change requests and fixes/resolutions to production problems/release defects) to the dedicated CLM & RTGS components as well as all changes to common components.

Prior to the deployment, the new release is first tested by the Eurosystem in the EAC environment. That is followed by user testing in the UTEST Environment.

Figure 4
CLM & RTGS environments for release deployment

8.2.4.2 Post deployment activities

In general, in order to evaluate release and deployment effectiveness, a post implementation review is undertaken to capture experiences and feedback on the satisfaction with the deployment and the potential lessons learnt.

8.2.4.3 Operating schedule of CLM and RTGS during release weekends

During any CLM and RTGS release deployment weekend, the start of the following CLM and RTGS business day will be aligned with the start of the business day in T2S. More specifically, the Eurosystem will close business day D on the Friday (prior to new release deployment) and will not open business day D+1 as usual. Instead, it will open business day D+1 after the successful deployment of the new release. As a result, the start of CLM RTS and RTGS RTS I periods usually taking place at 19:00 and 19:30 respectively on the evening of Friday, will be postponed to Saturday. Furthermore, the start of the maintenance window (MW) will be aligned with that of T2S (usually taking place on Sunday morning at 11:00).

Communication

The estimated time for Start of Day, start of CLM RTS and start of RTGS RTS I following the successful release deployment will be shared with the TARGET participants well in advance for each release.

8.3 Emergency changes and hotfixes

Emergency change means deployment of a change directly to the production environment to resolve or avoid a major incident that could potentially result in the complete unavailability of some or all services for which no workaround is available.

The following categories of changes are discussed in the following sections:

- Emergency changes

- Urgent production problems to be implemented as a “hotfix”.

Any other changes shall be considered as part of the normal change and release management procedures applicable for the annual releases.

8.3.1 Emergency change deployment

In the event of system difficulties, it may be decided to execute an immediate change in order to resume the normal operations of CLM and RTGS. This emergency change is performed directly in the PROD environment and does not go through all testing stages before its deployment.

8.3.2 Hotfix deployment

A hotfix is a change that includes all software corrections to be delivered in advance of a normal release due to the urgency of the fix (i.e. a fix for production problems that could lead to substantial operational issues, require heavy workarounds and/or lead to any other clear increase in the operational risk level). Due to time constraints, the change management process or the standard release management process cannot be followed for these changes and only the hotfix release management process shall be applied.

Contrary to an emergency change, a hotfix is tested – to the extent possible – in the UTEST environment prior to its deployment to PROD.

9 Gathering and sharing information about endpoint security of RTGS participants

To ensure the security and operational reliability of participants, the following four main tasks and responsibilities can be distinguished:

- **framework-setting by the Eurosystem**: producing guidelines to be followed by all those involved and specifying common requirements that should be met by participants;
- **compliance check by central banks**: checking whether participants comply with the measures laid down in the framework;
- **provision of information by participants:** providing central banks with relevant information, as specified in the framework; and
- **monitoring and follow-up activities by central banks:** identifying weaknesses and monitoring follow-up actions taken to address these weaknesses.

To ensure that all participants meet the same criteria and that compliance checks are carried out in a harmonised manner, consistent and effective guidelines and procedures need to be in place. The responsibility for establishing and maintaining this framework is assumed by the Eurosystem.

As regards compliance checks, the guiding principle is that the customer relationship remains under the full responsibility of the central bank with which the participant has a legal relationship. In this context, it must be stressed that the decisive criterion is not whether the participant is located inside or outside the euro area. Rather, it has to be considered whether its responsible central bank is participating in TARGET.

Example: Denmark has not adopted the euro, however, Danmarks Nationalbank is participating in TARGET. Consequently, direct participants with their head office in Denmark will typically establish a legal relationship with Danmarks Nationalbank.

In general, if the head office of a participant is maintaining a technical connection to TARGET, all information is to be collected by whichever central bank has the legal relationship with the head office.

If the head office is not maintaining a technical connection to TARGET, the information is to be collected by whichever central bank has a legal relationship with the entity of the group (branch or subsidiary) that is maintaining a technical connection to TARGET and that channels the largest volume of this entity's traffic to TARGET.

There might be an exception to the rule for service bureaus (see the section entitled “Service bureau and member/concentrator”). It is conceivable that a number of low-volume participants located in different countries share the same technical infrastructure provided by this type of organisation. However, service bureaus do not establish legal relationships with central banks. Rather, they only have legal relationships with those customers that use their technical infrastructure to route transactions to TARGET. However, participants with a service bureau are legally bound by the “Harmonised conditions” to provide their central bank with information of any failure of this type of organisation. In such a case, and in order to avoid identical information being collected through different participants, the respective central bank shall oversee its legal relationship with the largest participant – in terms of value of those participants using the same service bureau to verify whether it complies with the measures laid down in the framework for ensuring the security and operational reliability of participants (see Chapter 9.3.1. “Measures applies to critical participants and non-critical participants”).

Whenever participants use a member/concentrator, there are two possible scenarios: either the member/concentrator is a direct participant itself, in which case the central Bank that has the legal relationship with this participant will assume the responsibilities set out in this Infoguide; or the member/concentrator is only a connectivity service provider with no legal relationship with a central bank. In this case, the central bank with which the largest participant (in terms of value of those participants using the same member/concentrator) has a legal relationship is responsible for checking compliance with the relevant security requirements.

To ensure that these checks can be effectively performed, and upon request, participants are to provide their central banks with the requisite information and documentation.

Any weaknesses identified will need to be carefully assessed, based on a harmonised approach. Follow-up actions to address these weaknesses are to be agreed and implementation monitored. This is also a task to be performed by the central banks.

The Eurosystem has introduced the following processes to identify, monitor and manage risks that participants may create for RTGS operations:

1. identification of critical RTGS participants;

1. participants’ incident reporting

2. reporting about the compliance with information security and business continuity requirements

9.1 Identification of critical participants

9.1.1 Background

The impact of a security failure that affects the internal systems of a participant can vary depending on the market share that this participant holds in terms of value and/or the type of transactions processed (e.g. settlement transactions of systemically important ancillary systems). In this respect, the Eurosystem makes a distinction between critical participants and non-critical participants.

For the smooth operation of the CLM and RTGS, it is useful to have a comprehensive overview of which participants are classified as critical. For example, in the event of an operational disruption affecting the CLM and RTGS, this information may be used for the prioritisation of measures that need to be taken in order to limit the impact of such an incident.

Furthermore, while all participants will need to abide with certain minimum level of security measures and reporting, critical participants will have to implement some additional measures. This is in recognition of the vital importance that critical participants have for the smooth functioning of the CLM and RTGS system.

As a result, the Eurosystem agrees on a list of critical participants based on information provided by central banks on an annual basis. The criteria for determining which entities are considered to be critical are described below.

9.1.2 Credit institutions

General considerations and rationale

The guiding principle applied when establishing criteria to determine whether a credit institution is a critical participant is that organisations with a sufficient market share in terms of value are eligible, as well as those where their inability to meet their obligations could result in the inability of other participants or of financial institutions in other parts of the financial system to meet their obligations as they become due[44]. This means, in particular, that an operational disruption[45] could result in the accumulation of liquidity on a participant's account, which in turn could prevent other participants from making payments and thus potentially create systemic risk.

Criteria

Defining the criteria to distinguish critical credit institutions from non-critical credit institutions depends on the statistical distribution profile of the respective credit institution's turnover figures in terms of value.

---

[44] Principles for financial market infrastructures, Bank for International Settlements, April 2012.

[45] As opposed to balance sheet problems.

As a general guideline, the Eurosystem considers a credit institution to be a critical TARGET (CLM and RTGS) participant if it consistently settles at least 1% of the value of the CLM and RTGS turnover[46] as a daily average in the first quarter of the year. This includes interbank payments, customer payments, payments to central banks, liquidity transfers and ancillary system related transactions where (i) the initiator is the debited participant and (ii) the debited and credited parties are not the same or do not belong to the same technical platform. In addition, criticality also depends on the previous year's classification, both for critical and non-critical participants. This implies that, once classified as critical, a participant stays as such for a minimum of two years.

This criterion is to be reviewed at regular intervals. The review clause described in Chapter 9.8 "Review clause" is the mechanism to be used to ensure that this criterion is brought into line with evolving business practices given the experience gained during TARGET operations over time.

It is possible for two or more credit institutions to share the same technical infrastructure in order to participate in the CLM and RTGS. If the overall value of the transactions settled by these credit institutions in the shared environment is equal to or greater than 1% in terms of value, the organisation (for instance a transaction bank) operating the infrastructure in the legal sense is to be classified as a critical participant.

In addition to turnover, the Eurosystem applies simulation techniques in order to assess the impact of the technical failure of a participant based on measurable criteria.[47] More specifically, a technical failure of a credit institution is simulated and the impact this failure might have on the settlement of payments in CLM and RTGS is measured. As a general rule, a credit institution may be (re)classified as critical if the simulation proves that, on average, 1.5% of the overall CLM and RTGS turnover could not be settled owing to the outage of the respective credit institution's technical infrastructure.

In addition to the aforementioned key criteria commonly agreed by the Eurosystem, central banks may also take into account their own specific national features when classifying the credit institutions with which they have a business relationship. As a result, central banks may propose to classify direct participants as critical participants even if the main criterion is not met. The relevant central bank is to inform the ECB of this reclassification and is to explain the rationale behind it. The ECB will then form an opinion as to whether this reclassification is reasonable.

The opinion formed by the ECB is to be submitted to the relevant Eurosystem committee[48] for further consideration.

---

46 The TARGET turnover also includes transfers to/from T2S DCAs but not the securities-related settlements (e.g. DvP).

47 The Simulation tool used for the simulations developed by the Bank of Finland and adapted to replicate the CLM and RTGS functionalities

48 The relevant committee is the Market Infrastructure Board (MIB), "which assists the decision-making bodies of the Eurosystem in the fulfilment of the ESCB's basic tasks, more specifically to promote the smooth operation of payment systems".

9.1.3 Ancillary systems

The group of ancillary systems is CLM and RTGS composed of organisations in the field of securities clearing and settlement, retail payment systems (systemically important retail payment systems (SIRPS), prominently important retail payment systems (PIRPS) and other retail payment systems), and other large-value payment systems (e.g. CLS and EURO1).

As with credit institutions, for ancillary systems there is no empirical evidence on what exactly could cause systemic risk. Therefore, criteria for determining the criticality of ancillary systems were defined based on the results of a consultation of the relevant Eurosystem entities and available documentation.

Retail and large-value payment systems

Large-value payment systems are by definition classified as systemically important. Given that a failure to settle payments for these large-value payment systems in CLM and RTGS could transmit shocks across the financial system (and in the case of CLS even globally), these systems are classified as critical participants.

Following the same logic, SIRPS settling via CLM and RTGS are also classified as critical participants.

As regards PIRPS and other retail payment systems, it was felt that a failure to clear the net balances in central bank money would not have systemic implications for the CLM and RTGS or its participants. Therefore, these systems are classified as non-critical participants.

Organisations in the field of securities clearing and settlement

Organisations in the field of securities clearing and settlement are central securities depositories (CSDs), international central securities depositories (ICSDs) and central counterparties (CCPs).

In the opinion of the Eurosystem, all these systems are of systemic importance and the failure of a (I)CSD/CCP would have knock-on effects on the smooth functioning of TARGET. Consequently, all organisations in the field of securities clearing and settlement are considered to be critical participants.

In order to avoid over-regulation, the relevant central bank, on a case-by-case basis, may need to assess whether a particular organisation in the field of securities clearing and settlement should indeed be classified as a critical participant. If the outcome of this assessment were to demonstrate that the failure of such a participant would not have systemic implications for CLM and RTGSor its participants, this relevant central bank could classify it as a non-critical participant. The relevant central bank is to inform the ECB of this reclassification and to explain the rationale behind it. The ECB is to form an opinion on whether the reclassification is reasonable. This opinion is to be submitted to the relevant Eurosystem committee for further consideration and this committee may decide that the new criteria used by this central bank should be commonly used.

9.1.4 Service bureaus and Group hubs

Apart from sharing the connection to the NSP of another participant, there are two other ways for a participant to connect indirectly,[49] as described below:

- outsourcing the day-to-day operation to a third party, called a service bureau[50]; and
- in addition to the technical connectivity (see previous bullet point), using a Group Hub which provides supplementary business services, e.g. taking care of the SWIFT administration and invoicing on behalf of the participant.

Credit institutions and potentially also ancillary systems could decide to use one of these connectivity models. Considering that these organisations obtain a BIC for addressing through the NSP of their choice and take responsibility for their messages, they are participants, although they are only indirectly connected. Since the payments traffic of multiple users would be routed via an indirect connection, an operational failure of the service bureaus' or Group Hubs' technical infrastructure might have systemic implications.

Although the Eurosystem has provisionally concluded that service bureaus are not as such considered critical participants at this stage, it seems advisable that, if the total payments traffic routed via such an organisation exceeds the 1% criterion applicable to credit institutions, it is treated like a critical participant. Like for credit institutions, criticality also depends on the previous year's classification, i.e. once classified as critical, service bureaus and Group Hubs will keep this status for a minimum of two years.

Since service bureaus and Group hubs do not have a legal relationship with the Eurosystem, the legal basis for such entities to meet the requirements laid down in this Infoguide can only be created through the direct participants.

9.2 Participants' incident reporting

9.2.1 Background

A participant's capability to prevent liquidity accumulation on its account is of crucial importance for the smooth functioning of TARGET. Therefore, monitoring the availability of a participant's technical infrastructure and incident reporting are two means that can – in the longer run – contribute to the stability and robustness of TARGET.

---

[49] An indirect connection to SWIFTNet is typically used by smaller institutions seeking a cost-effective SWIFTNet connectivity solution.

[50] A service bureau is defined as a "A SWIFT user or non-user organisation registered under the Shared Infrastructure Programme that provides services to connect SWIFT users that are not affiliated with such organisation", SWIFT Glossary, September 2019.

Once a participant goes live in TARGET, it is closely monitored[51] by the relevant central bank. The participant is to inform the responsible central bank of any internal incident as soon as possible if the internal system of this participant is affected by an operational or technical disruption that lasts more than ten minutes. Once the participant has resumed operations, the central bank may send an incident report form (Annex II) to this participant for completion. This report requires the participant to describe the root cause of the problem, the impact, the steps taken to resolve the issue and any mitigating action that should prevent the incident from reoccurring.

A participant must provide an incident report under the following scenarios.

1. **Critical participants:** the duration of the incident exceeds 30 minutes. If the duration is below this threshold, an incident report is, in principle, not required. However, if an incident adversely affects the smooth operations of the RTGS, the central bank should request the report even if the duration is below the 30-minute threshold.

2. **Non-critical participants:** it is up to the relevant central bank to decide whether an incident report is required. The decisive factor is whether the incident has an impact on the smooth functioning of the RTGS or other participants.

Note that an incident report is not required if a participant makes a conscious decision to suspend payment processing activities for a certain period of time, even though it does not face any technical issues. However, participants are advised to inform the relevant central bank of any such action in order to avoid confusion.

If a central bank observes repetitive, short service interruptions by a participant that last less than 30 minutes, it shall contact that participant and request clarification, which could ultimately result in the need for a formal response.

Incidents affecting a participant's availability are probably the only types that can be identified by the system operator itself by comparing actual payment processing with normal patterns. Whenever a central bank notices a deviation from the normal pattern and suspects that a participant may be experiencing potentially serious availability problems it has not been informed about, the participant is to be contacted, and an explanation is to be requested. However, participants are encouraged to carry out regular, and possibly intraday account reconciliations, using the different tools and features offered by the system, such as daily account statements (camt053) and sender notification (pacs.008) messages.

In addition, participants should actively research and use available market tools, such as those provided by messaging networks or other third parties that could enhance their capabilities to prevent and detect fraudulent payments.

Apart from those incidents affecting the availability of a participant's internal system, participants shall also report security problems concerning confidentiality and

[51] CP VII (7.7.4): System operator activities should also involve "monitoring the security and operational reliability of the participants, for example the availability of their components during normal business hours".

integrity, such as a security-related incident in their technical infrastructure and, where appropriate, security-related incidents that occur in the technical infrastructure of the third-party providers. Reporting such cases as quickly as possible is essential for ensuring that meaningful and concise communication can be prepared, and possibly other measures, to reassure financial markets and the public. These types of incidents may not always be visible to the respective central bank. Instead, in accordance with the TARGET Guideline, Annex I, Part I, Article 20, a participant is to proactively report these to its respective central bank.

Moreover, if necessary, as provided in Chapters 4.1.2.8 "Failure at participant level (excluding ASs)" and 4.1.2.9 "Failure at ancillary system level", the relevant NSD may also support the participant in handling the incident, assisting, for example, in the implementation of measures to protect the participant's funds and to stop further fraudulent activity.

9.2.2 Procedure

Once a central bank requests its participant to complete an incident report (Annex II), participants must return the incident report to the relevant central bank within three business days of the occurrence. Depending on whether the incident:

- was already evaluated at that time, this first incident report is considered to be the final evaluation report.
- is still under investigation, the initial information that can already be provided should be considered to be an interim report. The final evaluation report, which complements the information provided in the interim report, should be sent to the central bank no later than one month after the incident occurred.

Once the incident report is marked final, the central bank is to assess its completeness. The central bank is to contact the participant if any information appears to be missing.

9.3 Measures to ensure the security and operational reliability of participants

The CPMI-IOSCO Principles for Financial Market Infrastructures[52] (PFMI) set out certain responsibilities that must be fulfilled by an operator of a payment system. More specifically, Principle 17 relates to issues concerning the security and operational reliability of financial market infrastructures such as systemically important payment systems.

To manage the operational risks associated with its participants, Principle 17 states that "[a]n FMI should consider establishing minimum operational requirements for its

[52] See a full description of the international standards for financial market infrastructures on the BIS's website: https://www.bis.org/cpmi/info_pfmi.htm.

participants. For example, an FMI may want to define operational and business continuity requirements for participants in accordance with the participant's role and importance to the system." The objective of these requirements is to address potential operational vulnerabilities for the FMI stemming from these participants and, in line with the related CPMI strategy, to reduce the risk of wholesale payment fraud related to endpoint security.[53]

The measures used to ensure the security and operational reliability of participants should be commensurate with their criticality. The previous sections outlined the criteria for determining critical participants. Chapter 9.4 describes the measures that are applied to both critical and non-critical participants. Chapter 9.4.4 outlines the procedures that are applied to critical participants only.

9.3.1 Measures applied to critical and non-critical participants

One measure to address security issues from a general perspective is the insertion of a clause in the legal arrangements between the central banks and their participants.

In particular, Article 20, Part I, Annex I of the "Harmonised conditions" for participation in TARGET of the TARGET Guideline defines security-related requirements and clearly states that the user is fully responsible for ensuring that the confidentiality, integrity and availability of its system are adequately protected (Article 20, Part I, Annex I of the TARGET Guideline).

Moreover, Article 22 (4), Part I, Annex I of the TARGET Guideline also states, inter alia, that central banks shall not be liable if a loss is caused by a TARGET participant. This implies that if the smooth functioning of TARGET is affected by an incident caused by the malfunction of a participant's system, the TARGET system operator will not accept any liabilities towards this participant. Moreover, the participant that caused the problem would have to reimburse the central bank (subject to the conditions set out in the "Harmonised conditions" and under applicable law) if this central bank had needed to compensate other participants on account of this incident.

9.3.1.1 Annual self-certification

Principle 17 of the CPSS/IOSCO Principles for Financial Market Infrastructures (PFMI)[54] recalls that "there are many relevant international, national, and industry-level standards, guidelines, or recommendations that an FMI may use in designing its operational risk-management framework." Conformity with such commercial standards can help to ensure a high degree of security and operational reliability.

---

[53] See a full description of the CPMI strategy for reducing the risk of wholesale payment fraud related to endpoint security on the BIS's website: https://www.bis.org/cpmi/publ/d178.htm.

[54] See a full description of the international standards for financial market infrastructures via the BIS website: https://www.bis.org/cpmi/info_pfmi.htm

Taking this into account, the Eurosystem asks RTGS DCA holders and ASs to self-certify that they meet the security requirements laid down by the Eurosystem and that security within their organisation is addressed in line with internationally recognised standards such as the “Code of practice for information security management” (ISO 27001). Compliance with other standards on information security may also be acceptable.

The Eurosystem needs to be reassured that the security of TARGET RTGS DCA holders and ASs components continues to meet the requirements specified by the Eurosystem even when new threats, new business requirements or newly identified vulnerabilities change the risk profile of a particular user operated internal system. Therefore, the Eurosystem asks RTGS DCA holders and ASs to self-certify compliance with the Eurosystem’s requirements on a yearly basis.

For this purpose, a C-level executive of the TARGET participants is to submit a self-certification statement to the relevant central bank (see Annex I). This statement is to indicate the level of compliance with the Eurosystem’s requirements and the used standard. Central banks will send the self-certification form to their TARGET participants, which have until the end of the respective year to self-certify their compliance with the Eurosystem’s requirements.

In the event of non-compliance with the Eurosystem’s requirements, TARGET participants shall complement the self-certification statement with a description of the major risks associated with this situation. Furthermore, TARGET participants shall set-up an action plan to rectify the situation, including the dates envisaged for implementing the respective measures. The responsible central bank is to evaluates the mitigation measures and compliance status of its TARGET participants. Those users that do not achieve full compliance with a specific year’s self-certification arrangement may be subject to certain measures to incentivise the participant to achieve full compliance in a timely manner.

Procedure

Central banks are to send the self-certification form to all RTGS participants (RTGS DCA holders and ancillary systems) with which they have a business relationship. RTGS participants have until the end of the respective year to self-certify their compliance with the Eurosystem’s requirements. The form must be signed by a senior executive (e.g. C-level executive). Critical participants need to make sure that the form is also signed by an internal or external auditor.

Central banks are to monitor whether the signed form is returned by the end of the respective year and, if not, are to contact the relevant participant to clarify the situation. A participant may submit a form that indicates that it also covers other RTGS participants (i.e. ‘‘reporting on behalf of’’).

In the event of non-compliance with the self-imposed information security standard or the business continuity requirements, the participant shall complement the self-certification form with a description of the major risks associated with this situation. Furthermore, the participant shall submit an action plan for rectifying the situation,

including the dates envisaged for implementing the respective measures. The relevant central bank is to assess this information and to monitor the implementation of these mitigation measures.

9.3.1.2 NSP endpoint security requirements

Participants are to provide their respective central bank with permanent access to their attestations of adherence with their NSP endpoint security requirements. If the participant refuses to grant permanent access to its attestation of adherence with their chosen NSP endpoint security requirements, the participant's level of compliance is to be categorised as "major non-compliance".

9.3.2 Measures applied to critical participants only

Business continuity

On 31 May 2006 the Governing Council of the ECB approved the Business continuity oversight expectations for systemically important payment systems (SIPS) (hereinafter referred to as the "oversight expectations"). This report sets out new oversight expectations in respect of business continuity for systemically important payment systems in euro.

The oversight expectations include a section dedicated to system participants since "the technical failure of critical participants in the system may induce systemic risk". In according with this, participants identified as critical by the system operator need to meet certain minimum requirements to ensure that business can be continued in the event of an operational disruption. The oversight expectations designate the system operator with the responsibility for verifying whether these requirements have met.

In particular, critical participants are required to confirm that:

- business continuity plans are produced and procedures for maintaining them are in place;
- there is an alternate site in place; and
- the risk profile of the alternate site is different from that of the primary sites. A different risk profile means that the alternate site must be a significant distance away from, and does not depend on, the same physical infrastructure components[55] as the primary business location. This minimises the risk that both could be affected by the same event. For example, the alternate site

[55] It should be noted that there is no obligation to use different hardware brands and/or software components, e.g. to install an MS Windows infrastructure in the primary site but UNIX systems in the alternate location. The statement "[…] should not depend on the same physical infrastructure […]" means that alternate sites should not rely on the same infrastructure components (e.g. transportation, telecommunications, water and electricity supply) as those used by the primary site.

should be on a different power grid and central telecommunication circuit from the primary business location[56].

In this context, it is acknowledged that critical participants can only be responsible for what is within their immediate sphere of control. There is an element of reliance on suppliers and critical participants cannot be held liable if the resilience of a service provided by a third party is less robust than expected. However, critical participants should make efforts to ensure that an appropriate level of resilience is stipulated in the contract with these suppliers. For example, a telecom provider should commit to multiple routing facilities and this should be laid down in the contractual arrangements.

- in the event of a major operational disruption rendering the primary site inaccessible and/or rendering critical staff unavailable, a critical participant is able to resume normal operations from the alternate site where the business day can be properly closed and reopened the following business day;
- in order to bridge the time needed for moving business from the primary to the alternate site, procedures are in place to ensure that the most critical business transactions can be performed; and
- the ability to cope with operational disruptions is tested at least once a year and critical staff are adequately trained.

Critical participants should confirm their level of compliance with the Oversight expectations by way of the self-certification process (see Section 8.3). Central banks are to check whether the oversight expectations are being met. A testing programme is to verify whether the provisions for business continuity are effective (see the section below on “Testing”).

Testing

In order to verify that business continuity arrangements are effective, they need to be tested at regular intervals.

Principle 17 of the principles for financial market infrastructures stipulates that any testing of the documented business continuity arrangements should also involve the system’s participants.

Testing activities can, in principle, be broken down into different scenarios. One category comprises bilateral testing of contingency arrangements between critical participants and a central bank. These activities already form an integral part of the user testing programme that TARGET participants need to perform prior to joining TARGET.

For critical participants, it is mandatory to take part in all testing activities. The relevant central bank is to monitor the successful completion of the tests.

[56] “High-level principles for business continuity”, The Joint Forum, Bank for International Settlements, August 2006.

Self-certification to be signed by internal or external auditor

As mentioned in Chapter 9.3.1.1.1, the self-certification statement must be signed by a C-level executive. For critical TARGET participants, the self-certification statement must be additionally signed by an internal or external auditor.

Contingency connections

In order to limit the impact of a prolonged outage affecting one of the two NSPs, all TARGET critical participants are required to put in place a dual connection to ESMIG (i.e. with both NSPs) at the latest by March 2026.

The second connection shall be a “contingency” U2A connection and not a fully-fledged connection to TARGET.

Moreover, this contingency/dual connection is to be regularly tested to ensure timely and smooth activation in the event of a prolonged NSP outage. The operational testing procedures are to be updated accordingly in due course.

9.4 Implementation

9.4.1 Legal enforceability

The “Harmonised conditions” for participation in TARGET, more specifically Article 20, Part I, Annex I of the TARGET Guideline, define high-level security requirements and therefore also the framework for the legal enforceability of the detailed measures specified in this Infoguide. However, each individual central bank is responsible at the national level for the practical and legal implementation of these individual measures that are to be made binding for all participants. Consequently, the central banks are responsible for deciding how to integrate the security measures for participants into their legal arrangements with their users (e.g. annexes to the contractual or regulatory arrangements, publications on the website with reference to these contractual or regulatory arrangements, letters from the respective central bank, etc.). Since legislation varies across countries, to ensure that the measures are legally enforced in a harmonised manner and in accordance with the provisions of the “Harmonised conditions” for participation in TARGET across all countries participating in TARGET, central banks report through which means this has been achieved.

9.4.2 Interim period

The measures for critical participants also ideally need to be met by any new critical participant prior to joining TARGET. New critical participants need to self-certify that information security requirements have been met in accordance with internationally recognised standards and that the business continuity requirements specified in the

section “Business continuity” are also met. Moreover, business continuity arrangements also need to be successfully tested in accordance with the aforementioned testing programme (see Chapter 6 “Testing activities for CLM&RTGS”).

A critical participant will have 18 months to comply with specific requirements that apply to its security and operational reliability. This period will start from the time of its designation as critical participant.

Finally, once a critical participant has been identified, the relevant central bank should contact it and ask it to indicate its level of preparedness given the aforementioned deadline for implementation. If significant gaps between the requirements outlined in this guide and the actual situation are identified, a workaround plan should be established. This plan should be monitored by the relevant central bank to ensure that the required measures are implemented by the aforementioned deadline.

9.4.3 Constructive approach

It should be emphasised that the objective of the legal enforceability framework is, of course, not to prevent institutions from participating in TARGET. Rather, the specified measures aim to strengthen the resilience and robustness of the TARGET system as a whole, thus contributing to the stability of financial markets.

If a TARGET participant fails to meet one of the requirements, the relevant central bank is to raise awareness about the risks arising from the identified weaknesses. In close cooperation with the TARGET participant in question, the respective central bank is to develop a programme to gradually improve the situation. If a situation of unwillingness and bad faith persists and therefore prevents any such gradual improvement, the TARGET participant in question is normally no longer permitted to participate in the TARGET system. However, a final decision will only be made following a careful evaluation of the situation at the Eurosystem level.

9.5 Communication and coordination

A sound organisational structure is essential for the communication and coordination of security issues between central banks and their participants to be managed in an effective and trustworthy manner. Each central bank, together with its participants, are responsible for ensuring that the necessary activities within the respective organisations are organised in a proper and efficient way. Whenever sensitive information is exchanged between the parties involved, it must be ensured that this information is properly labelled and receives an appropriate level of protection.

9.6 Confidentiality

All information provided by the participants will be treated as confidential by the Eurosystem. It will only be used to assess whether participants are in compliance with the measures required by the Eurosystem in order to fulfil its system operator responsibilities, as required by the PFMIs.

If participants receive sensitive information in the context of the overall framework, they must treat this information as confidential.

9.7 Reporting

The central banks are responsible for collecting the required information and monitoring any follow-up measures/actions. For example, if a participant's provisions for business continuity are considered to be ineffective, measures for resolving the identified shortcomings need to be put in place, including deadlines for implementing such mitigating measures.

Since the Eurosystem, as a whole, assumes payment system operator responsibilities, any information about incidents which could have an impact on the smooth functioning of TARGET received by central banks is to be made available to the relevant committee at the Eurosystem level. Given the sensitivity of this information, it is crucial that this be treated as strictly confidential/in strict confidence. Anonymising the information is highly recommended.

The committee is to review the information and consider on a case-by-case basis which measures should be taken in order to ensure that a particular participant does not compromise the smooth functioning of TARGET and its other participants.

The Eurosystem determines the reporting format and defines the detailed procedures for submitting such information to the responsible committee.

9.8 Review clause

Regular reviews of the overall framework are required to ensure that it remains appropriate.

For example, the criteria used to determine critical participants may need to change over time. The Eurosystem is responsible for adjusting these criteria in the light of the experience gained with TARGET business operations or new research evidence on systemic risk.

Another reason for adjusting the criteria could be that the payment traffic generated by the individual credit institutions also changes over time. If, for example, following a merger, a credit institution suddenly starts processing more than 1% of the value of transactions in TARGET, this credit institution may need to be classified as a critical participant and therefore need to meet the requirements specified for that type of

participant. Equally, if the payments' value of a critical participant drastically decreases and remains below the given threshold for a sufficiently long period, this participant may need to be reclassified as a non-critical participant.

Therefore, the criteria for determining critical participants and the classification of critical participants are to be reviewed on at least an annual basis but, if required, this can also be done on an ad hoc basis. In addition to this, participants are obliged to inform their central banks well in advance of any significant changes to their business practices.

9.9 Compliance implementation framework

9.9.1 Compliance methodology

The central banks use a quantitative approach to assess the overall compliance of RTGS DCA holders or ASs against their self-certification statement (compliance with business continuity requirements is only assessed for critical participants). Consequently, participants may be categorised under three levels of compliance, as follows.

- **Full compliance:** RTGS participants that fully meet the requirements at the level of 100%, meaning all 15 information security and (applicable to critical participants only) all six business continuity requirements.
- **Minor non-compliance:** RTGS participants that meet less than 100% but at least 66% of the requirements, meaning no less than ten information security and (applicable to critical participants only) no less than four business continuity requirements.
- **Major non-compliance:** RTGS participants that meet less than 66% of the requirements, meaning less than ten information security and (applicable to critical participants only) four or less business continuity requirements.

An RTGS participant that is able to demonstrate that a specific requirement is not applicable in its individual case will, however, be considered compliant with the respective requirement.

9.9.2 Implementation measures

If an RTGS participant does not fully comply, as assessed against the RTGS self-certification statement, , the relevant central bank should implement the measures described below in this section. However, it should be emphasised that the compliance implementation framework is not a one-size-fits-all which central banks can automatically/mechanistically apply to all RTGS participants that have not been

fully compliant. Instead, it should be used as general guidance for the measures to be applied to any non-compliant participants on a case-by-case basis.

Active dialogue (moral suasion)

This involves the central bank making both formal and informal contact with a non-compliant participant so that it becomes fully compliant as soon as possible. These types of contact could include the following.

- A participant is to provide an action plan indicating the measures that it will take to rectify its situation. This action plan is also to specify the envisaged dates for implementing each of these measures. The respective central bank is to evaluate the measures described by the participant and is to request additional information/clarification, if necessary.
- The respective central bank is to send an official letter signed by a senior official and addressed to a C-level executive of a non-compliant participant. This letter is to remind the participant of its responsibility and obligation to ensure that it operates its local infrastructure (used for submitting transactions to the RTGS) with a high level of security and operational reliability.
- This letter should also outline the additional compliance implementation measures that a central bank must apply if the measures indicated in the action plan appear inadequate or the deadlines for their implementation do not meet the expectations of the Eurosystem. In this respect, this letter should also recall the implications that a blocking/termination will entail.
- The respective central bank should also inform the C-level executive of a non-compliant participant via an official letter each time a participant's compliance status warrants additional compliance implementation measures.
- The respective central bank should also inform the relevant supervisory authority of the participant's compliance status. The respective central bank is also to keep the relevant supervisory authority informed each time a participant's compliance status warrants additional compliance implementation measures.

Should further compliance implementation measures be necessary, further enquires are to be made for a case-by-case assessment of whether to suspend this participant/terminate its account.

Enhanced monitoring and penalties charged

Participants are to provide their central banks with a monthly report on their progress in addressing their non-compliance. This is to be done in writing and is to be signed by a senior executive (e.g. C-level executive) of the participant in question.

In addition to monitoring these action plans, central banks will apply enhanced monitoring measures of a participant's activity in the RTGS in terms of the value and volume so that any changes to the participant's payment behaviour are flagged as early as possible. It is left to the discretion of each central bank to decide how

exactly to enhance their monitoring, depending on the size and business model of the participant.

Furthermore, the participant will incur a monthly penalty charge of €1,000 for each affected account. This measure of redress can be imposed as soon as the participant receives a second consecutive assessment of "minor non-compliance" or a first assessment of "major non-compliance", which serves two purposes. First, it incentivises the participant to become fully compliant as soon as possible. Second, it is meant to compensate the respective central bank for its additional enhanced monitoring measures.

Suspension of RTGS account(s) and penalties charged

A central bank will need to separately approve each payment that a suspended participant receives and/or sends in the RTGS (a participant's MCA[s] will not be suspended). This will only be approved once the central banks receives separate confirmation from the participant in question via the means agreed at the local level (e.g. phone confirmation, email verification, etc.). The participant will be given three months' notice of such suspension.

Should a participant be suspended in the RTGS, it will be required to pay a monthly penalty charge for each suspended account of €2,000. This is to incentivise the participant to become fully compliant as soon as possible time and to compensate the respective central bank for the additional work involved in the suspension.

Termination of RTGS account(s) and penalties charged

Should a participant's RTGS account(s) be suspended, the respective central bank should in parallel also give the participant three months' notice of termination of the RTGS account(s) unless significant progress is seen to be made by the participant to become fully compliant (this notice of termination does not apply to a participant's MCA[s]).

A participant will be required to pay a one-off penalty charge of €1,000 for each terminated account. This charge is to compensate the respective central bank for the additional work involved in the termination.

9.9.3 Timeline for applying measures

These measures are applied to participants which have not become fully compliant despite using a staggered approach and whose compliance status is severe. The table below shows the measures to be applied to participants that fall under the categories of "minor non-compliance" and "major non-compliance".

The first stage of measures apply to a participant at the end of the respective year's exercise round (e.g. at the end of 2022 against the outcome of the 2022 endpoint security exercise round). The second stage of measures would follow at the end of the following year (e.g. at the end of 2023 as against the 2022 endpoint security exercise round) should a participant still not fully comply at this stage.

Table 12

Timeline for applying the measures

	First stage implementation measures: 31 December of year *X*	Second stage implementation measures: 31 December of year *X + 1*
Minor non-compliance	Active Dialogue →	Enhanced Monitoring
Major non-compliance	Active Dialogue + Enhanced Monitoring →	Suspension + Termination of account*

This framework is not a one-size-fits-all which the central banks can automatically apply to all RTGS participants that have not reached full compliance. Instead, it is to be used as general guidance for the measures that should be applied to a non-compliant participant following a case-by-case assessment. This applies in particular to measures such as the suspension or termination of an account of an RTGS participant. A participant's compliance with its NSP endpoint security requirements should also be taken into account as additional information supporting the application/non-application of the different measures that comprise the compliance implementation framework.

10 Annex

10.1 Annex I – Self-certification statement

TARGET Self-certification arrangement for RTGS DCA holders and Ancillary Systems[57] - Security requirements and self-certification statement -

10.1.1 Introduction

The CPMI-IOSCO Principles for Financial Market Infrastructures[58] (FMI) set out certain responsibilities that must be fulfilled by an operator of a payment system. More specifically, Principle 17 relates to issues concerning the security and operational reliability of Financial Market Infrastructures such as systemically important payment systems.

To manage the operational risks associated with its participants, principle 17 states that "[a]n FMI should consider establishing minimum operational requirements for its participants. For example, an FMI may want to define operational and business continuity requirements for participants in accordance with the participant's role and importance to the system." The objective of these requirements is to address potential operational vulnerabilities to the FMI stemming from the participants and, in line with the related CPMI strategy, to reduce the risk of wholesale payments fraud related to endpoint security.[59]

In this light, the Eurosystem, in its capacity as TARGET system operator, has developed a set of requirements addressing information security and cyber resilience[60] risks with which currently all RTGS DCA holders and Ancillary Systems (critical and non-critical participants)[61] must comply with taking into account their internal systems in relation to the Payment Transaction Chain as defined in this document. Moreover, RTGS DCA holders allowing access to their RTGS DCA by third parties [i.e. via multi-addressee access] or registering addressable BIC holders, shall be deemed to have managed the risk stemming from allowing such access by

---

57 The "Information guide for TARGET participants" (hereinafter Infoguide) defines TARGET participants (including the RTGS ones) as credit institutions, ancillary systems and other entities settling in TARGET. The Infoguide also includes the concept of critical and non-critical participants which can be credit institutions and ancillary systems. The terms "participant" and "user" will be used interchangeably for the purpose of this note.

58 See a full description of the international standards for financial market infrastructures via the BIS website: https://www.bis.org/cpmi/info_pfmi.htm.

59 See full description on the CPMI strategy of Reducing the risk of wholesale payments fraud related to endpoint security via the BIS website: https://www.bis.org/cpmi/publ/d178.htm.

60 According to the CPMI-IOSCO "Guidance on Cyber Resilience for Financial Market Infrastructures", June 2016, Cyber Resilience is an FMI's ability to anticipate, withstand, contain and rapidly recover from a cyber-attack.

61 Central banks are also covered by the TARGET Self-Certification arrangement and therefore must comply with the requirements addressing information security and cyber resilience risks defined in this document.

third parties or having registered addressable BIC holders in accordance with the security requirements imposed upon them.

In addition, the Eurosystem has developed a set of requirements that address business continuity risk and that are exclusively applicable to the internal systems of those participants classified as critical in accordance with the rules laid down in the Information Guide for TARGET participants. All RTGS DCA holders and Ancillary Systems[62] have to self-certify their level of compliance with the requirements specified in the following section.

10.1.2 Requirements regarding information security management and business continuity management

Information security management (applicable to all RTGS DCA holders and Ancillary Systems)

The set-up of the internal systems (i.e. back office systems, front office systems, middleware, internal networks and external network connectivity infrastructure) used by participants for submitting transactions to TARGET may vary significantly, due to different architectures that can be used to connect to TARGET.

Consequently, the scope of security requirements may differ based on the specific architecture implemented by the participant. In establishing the scope, the participant should identify the elements that are part of the Payment Transaction Chain (PTC). Specifically, the PTC starts at a Point of Entry (PoE), i.e. a system involved in the creation of transactions (e.g. workstations, front-office and back-office applications, middleware), and ends at the system responsible to send the message to the Network Service Provider (NSP).

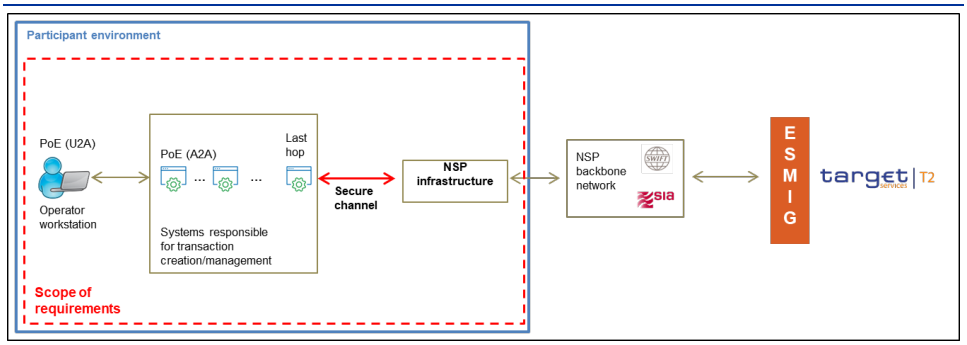
It is up to the individual organisations to assess whether all or only a subset of the security requirements is applicable to them. It should also be noted that the wording of the requirements references the ISO 27000/2018(en) Vocabulary.

In the following, a description of two possible architectures along with an indication of the Payment Transaction Chain and possible Point of Entries is provided for illustrative purposes.

Participant with NSP infrastructure within its environment

The NSP infrastructure used to connect to TARGET is within the participant environment, as represented in the figure below.

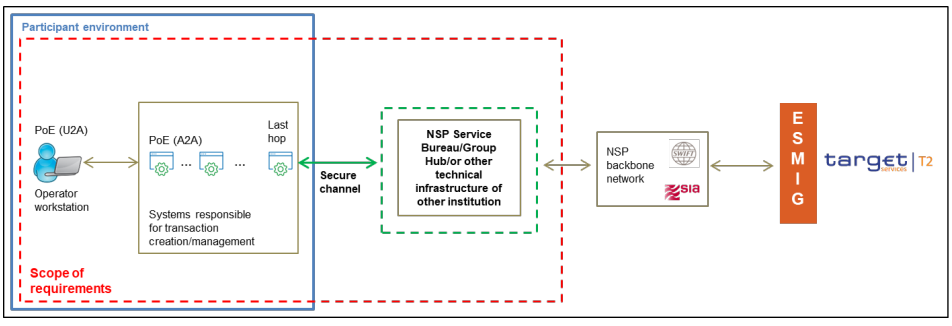
[62] All the ancillary systems have to self-certify their level of compliance with the requirements specified in this document regardless of the adopted TARGET accounts.



The scope includes (i) the workstation used by the operator; (ii) systems that are responsible for transaction generation or transaction management (e.g. middleware, front office/back office application); (iii) the secure channel established between the NSP infrastructure and the last hop; (iv) the NSP infrastructure; (v) the participant's physical environment.

Participant connected via NSP Service Bureau, via Group Hub or other technical infrastructure of other institution

No NSP infrastructure component is hosted in the participant environment; hence middleware and back-office applications communicate directly with the NSP Service Bureau, Group Hub or other technical infrastructure of other institution using a secure channel provided by it (e.g. GUI application, middleware product).



The scope includes (i) the workstation used by the operator, (ii) systems that are responsible for transaction generation or transaction management (e.g. middleware, front office/back office application); (iii) the secure channel established between the NSP infrastructure hosted by the Service Bureau/Group Hub/other technical infrastructure of other institution and the last hop; and (iv) the participant's physical environment.

Some of the security requirements that are applicable may be provided by the respective *NSP Service Bureau or Group Hub other technical infrastructure of other institution*. In this respect, those signing the self-certification statement are still

responsible for the compliance with the security requirements, i.e. they must seek assurance that compliance is being achieved “on their behalf”. In general, RTGS DCA holders and Ancillary Systems must ensure that their signed self-certification statement reflects a true and accurate picture of the security situation of their organisation, including services that may be externally provided.

In case of multi-country credit institution, the Head-Office may host and operate the technical infrastructure used to connect to TARGET and share it with a number of local branches, within a certain group hub.

In this case, the scope mentioned under the architecture “*Participant with NSP infrastructure within its environment*” applies to the Head-Office, but some security requirements are still applicable also for local branches[63]. For example, the controls related to physical security have to be met by both the TARGET participant hosting the shared technical infrastructure and the branch. The TARGET participant hosting the shared technical infrastructure will have to implement controls protecting the data centre while a branch will have to make sure that the components used for connecting to the shared technical infrastructure are properly protected (e.g. the workstation used by the operator).

In respect to RTGS DCA holders or Ancillary Systems being provided by a NSP Service Bureau, the same principles hold, meaning the participant still needs to access which controls fall under its scope and which do not (seeking assurance in this case that the respective NSP Service Bureau is compliant with these requirements).

Requirement 1.1: Information security policy

Management shall set a clear policy direction in line with business objectives and demonstrate support for and commitment to information security through the issuance, approval and maintenance of an information security policy aiming at managing information security and cyber resilience across the organisation in terms of identification, assessment and treatment of information security and cyber resilience risks. The policy should contain at least the following sections: objectives, scope (including domains such as organization, human resources, asset management etc.), principles and allocation of responsibilities.

Requirement 1.2: Internal organisation

An information security framework shall be established to implement the information security policy within the organisation. Management shall coordinate and review the establishment of the information security framework to ensure the implementation of the policy across the organisation, including the allocation of sufficient resources and assignment of security responsibilities for this purpose.

Requirement 1.3: External parties

[63] The same rules and scope apply if the technical infrastructure used to connect to TARGET is managed by a non-EEA (European Economic Area) Head Office.

The security of the organisation’s information and information processing facilities should not be reduced by the introduction of and/or the dependence on an external party/parties or products/services provided by them. Any access to the organisation’s information processing facilities by external parties shall be controlled. When access by external parties or products/services from external parties is/are required, a risk assessment shall be carried out to determine the security implications and control requirements. Controls shall be agreed and defined in an agreement with each relevant external party.

Requirement 1.4: Asset management

All information assets, the business processes and the underlying information systems, such as operating systems, infrastructures, business applications, off-the-shelf products, services and user-developed applications, in the scope of the Payment Transaction Chain shall be accounted for and have a nominated owner. The responsibility for the maintenance and the operation of appropriate controls in the business processes and the related IT components to safeguard the information assets shall be assigned. NOTE: The implementation of specific controls can be delegated by the owner as appropriate, but the owner remains accountable for the proper protection of the assets.

Requirement 1.5: Information assets classification

Information assets shall be classified in terms of criticality to the smooth delivery of the service by the participant. The classification shall indicate the need, priorities and degree of protection required when handling it in the relevant business processes and by the underlying IT components. An information asset classification scheme approved by the management shall be used to define an appropriate set of protection controls across the information asset lifecycle, including removal and destruction, and communicate the need for special handling measures.

Requirement 1.6: Human resources security

Security responsibilities shall be addressed prior to employment in adequate job descriptions and in terms and conditions of employment. All candidates for employment, contractors and third-party users shall be adequately screened, especially for sensitive jobs. Employees, contractors, and third-party users of information processing facilities shall sign an agreement on their security roles and responsibilities. An adequate level of awareness shall be ensured among all employees, contractors and third-party users, and education and training in security procedures and the correct use of information processing facilities shall be provided to them, to minimise possible security risks. A formal disciplinary process (for employees) for handling security breaches shall be established. Responsibilities shall be in place to ensure an employee’s, contractor’s or third-party user’s exit from or transfer within the organisation is managed, and that the return of all equipment and the removal of all access rights are completed.

Requirement 1.7: Physical and environmental security

Critical or sensitive information processing facilities shall be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They shall be physically protected from unauthorised access, damage and interference. Access should be granted only to individuals who are in scope of Requirement 1.6. Procedures and standards shall be established to protect physical media containing information assets when in transit.

Equipment shall be protected from physical and environmental threats. Protection of equipment (including that used off-site) and against the removal of property is necessary to reduce the risk of unauthorised access to information and to guard against loss or damage. Special measures may be required to protect against physical threats and to safeguard supporting facilities such as the electrical supply and cabling infrastructure.

Requirement 1.8: Operations management

Responsibilities and procedures shall be established for the management and operation of information processing facilities covering end-to-end all the underlying systems in the Payment Transaction Chain.

As regards operating procedures, including technical administration of IT systems, segregation of duties shall be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse. Where segregation of duties cannot be implemented due to documented objective reasons, compensatory controls shall be implemented following a formal risk analysis. Controls shall be established to prevent and detect the introduction of malicious code for systems in the Payment Transaction Chain. Controls shall be also established (including user awareness) to prevent, detect and remove malicious code. Mobile code shall be used only from trusted sources (e.g. signed Microsoft COM components and Java Applets). The configuration of the browser (e.g. the use of extensions and plugins) shall be strictly controlled.

Data backup and recovery policies shall be implemented, and it shall include a plan of the restoration process which is tested at regular intervals at least annually.

Systems that are critical for the security of payments shall be monitored and relevant information security events shall be recorded. Operator logs shall be used to ensure that information system problems are identified. Operator logs shall be regularly reviewed based on the criticality of the operations, on a sample basis. System monitoring shall be used to check the effectiveness of controls which are identified as critical for the security of payments and to verify conformity to an access policy model.

Exchanges of information between organisations shall be based on a formal exchange policy and carried out in line with exchange agreements among the involved parties and shall be compliant with any relevant legislation. Third-parties software components employed in the exchange of information with TARGET (e.g. software received from a Service Bureau in scenario 2 of the scope section) must be used under a formal agreement with the third-party.

Requirement 1.9: Access control

Access to information assets shall be justified on the basis of business requirements (need-to-know[64]) and according to the established framework of corporate policies (including the information security policy). Clear access control rules shall be defined based on the least-privilege principle[65] to reflect closely the needs of the corresponding business and IT processes. Where relevant (e.g. for backup management), logical access control should be consistent with physical access control unless there are adequate compensatory controls in place (i.e. encryption, personal data anonymization).

Formal and documented procedures shall be in place to control the allocation of access rights to information systems and services in the scope of the Payment Transaction Chain. The procedures shall cover all stages in the life-cycle of user access, from the initial registration of new users to the final deregistration of users that no longer require access.

Special attention shall be given, where appropriate, to the allocation of access rights of such criticality that the use of them could lead to a severe adverse impact on the operations of the participant (e.g. system administration, override of system controls, direct access to business data).

Appropriate controls shall be put in place to identify, authenticate and authorize users at specific points in the organisation's network, e.g. for local and remote access to systems in the Payment Transaction Chain. Personal accounts shall not be shared in order to ensure accountability.

For passwords, rules shall be established and enforced by specific controls to ensure that passwords cannot be easily guessed, e.g. complexity rules and limited-time validity. A safe password recovery and/or reset protocol shall be established.

A policy shall be developed and implemented on the use of cryptographic controls to protect the confidentiality, authenticity and integrity of information. A key management policy shall be established to support the use of cryptographic controls.

There shall be policy for viewing confidential information on screen or in print (e.g. a clear screen, a clear desk policy)" to reduce the risk of unauthorised access.

When working remotely, the risks of working in an unprotected environment shall be considered and appropriate technical and organizational controls are applied.

Requirement 1.10: Information systems acquisition, development and maintenance

Security requirements shall be identified and agreed prior to the development and/or implementation of information systems.

---

64 The need-to-know principle refers to the identification of the set of information that an individual needs access to in order to carry out her/his duties.

65 The least-privilege principle refers to tailoring a subject's access profile to an IT system in order to match the corresponding business role.

Appropriate controls shall be built into applications, including user-developed applications, to ensure correct processing. These controls shall include the validation of input data, internal processing and output data. Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical information. Such controls shall be determined on the basis of security requirements and risk assessment according to the established policies (e.g. information security policy, cryptographic control policy).

The operational requirements of new systems shall be established, documented and tested prior to their acceptance and use. As regards network security, appropriate controls, including segmentation and secure management, should be implemented based on the criticality of data flows and the level of risk of the network zones in the organisation. There shall be specific controls to protect sensitive information passing over public networks.

Access to system files and program source code shall be controlled and IT projects and support activities conducted in a secure manner. Care shall be taken to avoid exposure of sensitive data in test environments. Project and support environments shall be strictly controlled. Deployment of changes in production shall be strictly controlled. A risk assessment of the major changes to be deployed in production shall be conducted.

Regular security testing activities of systems in production shall also be conducted according to a predefined plan based on the outcome of a risk-assessment, and security testing shall include, at least, vulnerability assessments. All the shortcomings highlighted during the security testing activities shall be assessed and action plans to close any identified gap shall be prepared and followed-up in timely fashion.

Requirement 1.11: Information security in supplier[66] relationships

To ensure protection of the participant's internal information systems that are accessible by suppliers, information security requirements for mitigating the risks associated with supplier's access shall be documented and formally agreed upon with the supplier.

Requirement 1.12: Management of information security incidents and improvements

To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses, roles, responsibilities and procedures, at business and technical level, shall be established and tested to ensure a quick, effective and orderly and safely recover from information security incidents including scenarios related to a cyber-related

[66] A supplier in the context of this exercise should be understood as any third party (and its personnel) which is under contract (agreement), with the institution, to provide a service and under the service agreement the third party (and its personnel) is granted access, either remotely or on site, to information and/or information systems and/or information processing facilities of the institution in scope or associated to the scope covered under the exercise of the TARGET self-certification.

cause (e.g. a fraud pursued by an external attacker or by an insider). Personnel involved in these procedures shall be adequately trained.

Requirement 1.13: Technical compliance review

A participant's internal information systems (e.g. back office systems, internal networks and external network connectivity) shall be regularly assessed for compliance with the organization's established framework of policies (e.g. information security policy, cryptographic control policy).

Requirement 1.14: Virtualization

Guest virtual machines shall comply with all the security controls that are set for physical hardware and systems (e.g. hardening, logging). Controls relating to hypervisors must include: hardening of the hypervisor and the hosting operating system, regular patching, strict separation of different environments (e.g. production and development). Centralized management, logging and monitoring as well as managing of access rights, in particular for high privileged accounts, shall be implemented based on a risk assessment. Guest virtual machines managed by the same hypervisor shall have a similar risk profile.

Requirement 1.15: Cloud computing

The usage of public and/or hybrid cloud solutions in the Payment Transaction Chain must be based on a formal risk assessment taking into account the technical controls and the contractual clauses related to the cloud solution.

If hybrid cloud solutions are used, it is understood that the criticality level of the overall system is the highest one of the connected systems. All on-premises components of the hybrid solutions must be segregated from the other on-premises systems.

Business continuity management (applicable only to critical participants)

The following requirements (2.1 to 2.6) relate to business continuity management. Each RTGS DCA holder or Ancillary System classified by the Eurosystem as being critical for the smooth functioning of the RTGS service must have a business continuity strategy in place comprising the following elements.

Requirement 2.1: Business continuity plans have been developed and procedures for maintaining them are in place.

Requirement 2.2: An alternate operational site must be available.

Requirement 2.3: The risk profile of the alternate site must be different from that of the primary site, in order to avoid that both sites are affected by the same event at the same time. For example, the alternate site should be on a different power grid and central telecommunication circuit from those of the primary business location.

Requirement 2.4: In the event of a major operational disruption rendering the primary site inaccessible and/or critical staff unavailable, the critical participant must be able

to resume normal operations from the alternate site, where it must be possible to properly close the business day and open the following business day(s).

Requirement 2.5: Procedures must be in place to ensure that the processing of transactions is resumed from the alternate site within a reasonable timeframe after the initial disruption of service and commensurate to the criticality of the business that was disrupted.

Requirement 2.6: The ability to cope with operational disruptions must be tested at least once a year and critical staff must be aptly trained. The maximum period between tests shall not exceed one year.

10.1.3 Self-certifying institution

RTGS DCA holders and Ancillary Systems can technically connect to TARGET either directly or via a shared technical infrastructure. However, in case of the latter it is ultimately the key responsibility of the respective RTGS DCA holders or Ancillary Systems to thoroughly assess which security requirements are applicable to the specific and unique technical infrastructure as well as the organisational set-up of its institution.

Each RTGS DCA holder and Ancillary System (i.e. critical and non-critical participants) must submit a self-certification statement to the central bank with which it is having a business relationship. If parts of the operations and/or technical infrastructure used for the TARGET access are shared by different RTGS DCA holders or Ancillary Systems, each participant should submit its own self-certification statement to its respective central bank.

Such a shared technical concept would include also setups where several participants use e.g. the same technique or application to create/process cash transfers orders to be sent to TARGET. The usage of such shared technical infrastructures is to be also reported as part of the self-certification statement.

In the event a RTGS DCA holder or Ancillary System has outsourced (parts of) its operations to a third party (for example a NSP Service Bureau, a Group Hub or other technical infrastructure of other institution), it must seek assurance that the third party is compliant with the security requirements set-up by the Eurosystem for RTGS DCA holders and Ancillary Systems.[67]

In case one or more security requirements are not applicable, the RTGS DCA holders or Ancillary Systems should indicate this in the compliance check table below. Moreover, it should be explained in the relevant box included in the self-

[67] A *Service Bureau* is a NSP user or non-user organisation that connects non-affiliated NSP users. The services offered by a service bureau include sharing and operating of NSP messaging and/or connectivity components on behalf of NSP users. A *Group Hub* is a user or non-user organisation connecting affiliated users within its corporate group. O*ther institution* is any institution that provides a technical infrastructure for the RTGS DCA holder or Ancillary System.

certification statement (labelled “towards compliance”) why a specific security requirement is not applicable.

In case of doubt, the RTGS DCA holders or Ancillary Systems are kindly invited to contact the central bank with which they are having a contractual relationship in order to clarify the scope of their self-certification statement.

10.1.4 Signatory

The self-certification statement should be signed by a C-Level executive[68] responsible/accountable for the information security risk management function within the RTGS DCA holder’s or Ancillary System’s organisation.

For critical participants the self-certification statement should also be signed by the (external or internal) auditor of the critical RTGS DCA holder or Ancillary System.

10.1.5 Compliance check

For each of the requirements specified by the Eurosystem the RTGS DCA holders and Ancillary Systems must report in the self-certification statement whether it is compliant or non-compliant against the control or if the control is not applicable.

In the event of non-compliance against a specific requirement, a description of the major risks[69] should be included in the relevant box included in the self-certification statement (labelled “towards compliance”). Furthermore, an action plan for rectifying the situation and the planned dates for implementing each particular measure should be included. This information must be evaluated and the timely implementation of risk-mitigating measures monitored by the central bank responsible. Finally, it should be noted that the Eurosystem governance body responsible for the secure and reliable operations of TARGET is informed about the outcome of self-certification exercise and the progress being made with respect to the implementation of risk-mitigating measurers, as relevant.

Level of compliance

RTGS DCA holders and Ancillary Systems are required to indicate whether they are compliant or non-compliant against the requirements regarding information security management specified by the Eurosystem in its capacity as TARGET system operator.

---

68 A C-level executive is a high-ranking executive of a company in charge of making company-wide decisions. The "C" stands for "chief." Some best-known C-level executives include the chief executive officer (CEO), chief operating officer (COO) and chief information officer (CIO). Provided equivalent competencies have been assigned the signatory could also be a chief risk officer (CRO) or a chief information security officer (CISO).

69 A major risk could be, for instance, insufficient measures against denial of service attacks, uninterruptible power supply not in place, etc.

The TARGET operator applies a quantitative approach for assessing the overall compliance of RTGS DCA holders and Ancillary Systems (compliance against business continuity requirements is only assessed for critical participants). The following criteria apply:

- **Full compliance:** RTGS DCA holders and Ancillary Systems satisfying 100% of the requirements (all 15 information security and all 6 business continuity requirements (critical participants only)).
- **Minor non-compliance:** RTGS DCA holders and Ancillary Systems satisfying less than 100% but at least 66% (i.e. 10 information security and 4 business continuity requirements (critical participants only)).
- **Major non-compliance:** RTGS DCA holders and Ancillary Systems satisfying less than 66% of the requirements (i.e. less than 10 information security or less than 4 business continuity requirements (critical participants only)).

A RTGS DCA holder or Ancillary System that demonstrates that a specific requirement is not applicable for itself will be considered as compliant against the respective requirement with regard to the above-described assessment.

10.1.6 Reporting on behalf of other RTGS DCA holders/ Ancillary Systems

A RTGS DCA holder or Ancillary System may submit a self-certification statement to its respective Central Bank while at the same time also reporting the compliance status on behalf of other RTGS DCA holders/Ancillary Systems. This ‘’reporting on behalf’’ is possible if the two following conditions are met:

1. **All participants belong to the same ‘’banking group’’ as defined in the TARGET Guideline and use the same technical infrastructure for submitting payments**

Irrespective of whether the RTGS DCA holder or Ancillary System covered by a single self-certification statement have established their business relationship with the same Central Bank or not, the participants are using the same infrastructure for submitting payments to TARGET.

Should a banking group include a critical participant, then this critical participant needs to be the one who submits the self-certification statement to the respective Central Bank while reporting also on behalf of other participants belonging to the same group.

2. **All participants covered by the single self-certification statement are fully compliant with all the applicable requirements**

It may be that some of the RTGS DCA holders and Ancillary Systems within one banking group are classified as critical participant while others are non-critical. Therefore, the self-certification statement makes a distinction as to which

participants have to meet the information security requirements and which ones have to comply with both the information security as well as the business continuity management requirements (''reporting on behalf'' boxes after each requirement type in the statement).

If some participants comply with a specific control while for others the same control may not be applicable, both boxes for this requirement (i.e. ''Compliant with the requirement'' and ''Requirement not applicable'') should be ticked in the self-certification statement. More detailed information as to why a certain requirement is not applicable for a specific participant shall then be separately described in the respective box in the statement.

If any RTGS DCA holder or Ancillary System that is not compliant with one/any of the individual requirements, this specific participant needs to submit its own self-certification statement to its respective Central Bank. This process (i.e. each non-compliant participant within a ''group'' needs to submit a separate self-certification statement) needs to be followed even if the missing control would be the same across all participants within the ''group''.

10.1.7 Self-certification statement

Contact details

In the following the name of the RTGS DCA holder or Ancillary System submitting the self-certification statement and contact details of a person to be contacted in case further information is required should be provided.

Name of the RTGS DCA holder or Ancillary System	
Address	
BIC	
Contact person (name) (print)	
Contact person (telephone)	
Contact person (e-mail)	

Use of NSP Service Bureau or Group Hub or other technical infrastructure of other institution

Apart from establishing a technical direct connection to TARGET, participants can connect through a NSP Service Bureau or Group Hub or other technical infrastructure of other institution.

Is your organisation connected to TARGET via a NSP Service Bureau?	Yes ☐	No ☐

If yes, please indicate the name and BIC of the NSP Service Bureau	

Is your organisation connected to TARGET via a Group Hub?	Yes ☐	No ☐
If yes, please indicate the name and BIC of the Group Hub		

Is your organisation connected to TARGET via a technical infrastructure of another institution (not being categorized NSP service bureau/Group Hub)?	Yes ☐	No ☐
If yes, please indicate the name and BIC of the other institution(s)		

Information security management requirements (section applicable to all RTGS DCA holders and Ancillary Systems[70])

	Compliant with the requirement	Non-compliant with the requirement	Requirement not applicable
Requirement 1.1	☐	☐	☐
Requirement 1.2	☐	☐	☐
Requirement 1.3	☐	☐	☐
Requirement 1.4	☐	☐	☐
Requirement 1.5	☐	☐	☐
Requirement 1.6	☐	☐	☐
Requirement 1.7	☐	☐	☐
Requirement 1.8	☐	☐	☐
Requirement 1.9	☐	☐	☐
Requirement 1.10	☐	☐	☐
Requirement 1.11	☐	☐	☐

[70] I.e. all RTGS DCA holders and Ancillary Systems shall fulfill the requirements in this table covering the different information security management requirements (tick-boxes) and shall respond to the questions thereafter in this section.

Requirement 1.12	☐	☐	☐
Requirement 1.13	☐	☐	☐
Requirement 1.14	☐	☐	☐
Requirement 1.15	☐	☐	☐
Which information security management standard (e.g. ISO 27001, COSO, ISACA COBIT, NIST) is applied in your organisation?			
Is your organisation using services that are relevant for the PTC from a Cloud Service Provider (i.e. public and hybrid clouds or external document repositories)?			

Reporting **information security management requirements** on behalf of other RTGS DCA holders or Ancillary Systems (if applicable)	
BIC of the participant	Respective Central Bank of the participant

Business continuity management requirements (section applicable to critical participants only)

	Compliant with the requirement	Non-compliant with the requirement	Requirement not applicable
Requirement 2.1	☐	☐	☐
Requirement 2.2	☐	☐	☐

Requirement 2.3	☐	☐	☐
Requirement 2.4	☐	☐	☐
Requirement 2.5	☐	☐	☐
Requirement 2.6	☐	☐	☐

Reporting **business continuity management requirements** on behalf of other RTGS DCA holders or Ancillary Systems (if applicable)	
BIC of the participant	Respective Central Bank of the participant

Towards compliance

The following section must be completed if a participant has (i) identified a case of non-compliance against any of the security requirements; or (ii) labelled any requirement as ‘’not applicable’’.

For each requirement indicated as “not applicable” in the table above, please provide a short explanation why it is not applicable. Comments:
Which risks have been identified resulting from non-compliance with requirements 1.1 to 1.15 and 2.1 to 2.6 (please respond separately for each requirement indicated as ‘’non-compliant’’)? Comments:
What steps will be taken to achieve full compliance with all requirements (please respond separately for each requirement indicated as ‘’non-compliant’’)?

Comments:
By when will full compliance be achieved? Comments:

Certification

The signatories confirm that they have read and understood the requirements outlined in this self-certification statement. The statement will be renewed annually. Meanwhile, any identified non-compliance needs to be reported to the responsible central bank without undue delay.

The signatories certify that the information contained in the statement represents a true and accurate picture of the current situation. They further certify that the statement has been prepared under their direction and supervision and that qualified personnel properly gathered and evaluated the information provided. The submitted information is, to the best of the signatories' knowledge and belief, true, accurate and complete. The signatories are aware that the submission of this information is a material obligation and that submitting false, inaccurate or misleading information constitutes a breach of Article 25 (2) (c) of the Part I, Annex I of the TARGET Guideline, which is one of the grounds for termination of an institution's participation in TARGET.

Finally, the signatories confirm that their organisation has a mechanism in place to ensure that it will remain in compliance over the coming year. If full compliance has not yet been achieved, the signatories confirm that appropriate measures will be taken to achieve full compliance at the very latest by the end of the next calendar year.

In the event that a participant submits the statement and report on behalf of other RTGS DCA holders or Ancillary Systems, the signatories confirm the above-mentioned aspects covering all participants mentioned in the statement. The signatories are aware that the submission of this information is a material obligation of the participant on behalf of which they sign and that submitting false, inaccurate or misleading information constitutes a breach of Article 25 (2) (c) of the Part I, Annex I of the TARGET Guideline, which is one of the grounds for termination of an institution's participation in TARGET.

Signature

Name of official (print)	

Title/function (C-level executive)	
Date	
Signature	

Auditor signature – for completion by critical participants only

Name of Auditor (print)	
Title (indicate whether internal or external auditor)	
Date	
Signature	

This self-certification statement should be returned to:

Name of central bank	
Address	
Contact person	

10.2 Annex II – Incident report for TARGET participant

Confidentiality The information included in this document will only be used by the Eurosystem to further strengthen the resilience of the TARGET system as a whole. Within the Eurosystem, access to this information is only granted to those with a business-related need to know

Name of the central bank responsible	Click or tap here to enter text.

Point of contact (POC) information	
Name of the TARGET participant	Click or tap here to enter text.
Name of the contact person	Click or tap here to enter text.
Title/function	Click or tap here to enter text.
Telephone number	Click or tap here to enter text.
E-mail address	Click or tap here to enter text.

General incident information	
Incident ID (to be assigned by the central bank responsible)	Click or tap here to enter text.
Status	☐ Interim ☐ Final[71]
Type of failing component	☐ Hardware ☐ Software[72] ☐ Network[73] ☐ Infrastructure[74] ☐ Human error
Date and time the incident started (CET)	Click or tap to enter a date.
Date and time the incident ended (CET)	Click or tap to enter a date.

[71] An incident report is considered "final" when the implementation date of the remedial measure is indicated.

[72] Software comprises system software (including DB systems) and application software.

[73] Network comprises only the internal network. External network failures should be listed under infrastructure.

[74] Infrastructure comprises premises, supporting services (e.g. air conditioning, power supply, telecommunication (including NSP)).

Duration	Click or tap here to enter text.

Description of the incident The summary should be a high-level description suitable for senior management and avoiding technical language to the extent possible. The summary should include for instance the following elements: • basic description of the events and their impact • services/systems affected by the incident and • external effects (e.g. other TARGET participants affected).
Click or tap here to enter text.

Details of the cause of the incident Specifically, the root cause of the incident - who, what, where, when, how.
Click or tap here to enter text.

Remedial action This section should include for instance the following elements: • action taken to resolve the incident and • measures taken to prevent the incident from reoccurring/implementation scheduled for.
Initial resolution: Click or tap here to enter text. *Long term solution:* Click or tap here to enter text.

Date and signature: _____

Name of the signatory (Print): _____

Title: _____

This form should be returned to the central bank mentioned above:

Address	
Contact person	

10.3 Annex III – Market Infrastructure and Application Change Request form

General Information (Origin of request) ☐ User Requirements Document (URD) ☐ User Detailed Functional Specification (UDFS) ☐ User Handbook (UHB) ☐ Other User Functional or Technical Documentation (SYS)		
Request raised by:	Institution:	Date raised:
Request title:		Request ref. no[75]: [filled in by ECB]
Request type		
1. Legal/business importance parameter:	2. Market implementation efforts parameter – Stakeholder impact:	
3. Operational impact:	4. Financial impact parameter:	
5. Functional/ Technical impact:	6. Interoperability impact:	
Requestor Category:	Status:	

Reason for change and expected benefits/business motivation
Description of requested change
Submitted annexes / related documents
Proposed wording for the change request

[75] XXXX = ECMS /TIPS / CONS, NNNN = 9999, DDDD = URD/UDFS/UHB

High level description of impact
Impacts on other projects and products
Outcome/decision

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.ecb.europa.eu

For specific terminology please refer to the ECB glossary (available in English only).