GUIDELINES

GUIDELINE (EU) 2021/1759 OF THE EUROPEAN CENTRAL BANK

of 20 July 2021

amending Guideline ECB/2012/27 on a Trans-European Automated Real-time Gross settlement Express Transfer system (TARGET2) (ECB/2021/30)

THE GOVERNING COUNCIL OF THE EUROPEAN CENTRAL BANK,

Having regard to the Treaty on the Functioning of the European Union and in particular the first and fourth indents of Article 127(2) thereof,

Having regard to the Statute of the European System of Central Banks and of the European Central Bank and in particular Article 3.1 and Articles 17, 18 and 22 thereof,

Whereas:

(1) On 26 April 2007, the Governing Council of the European Central Bank adopted Guideline ECB/2007/2 ([1]) governing TARGET2, which establishes a single technical platform - the Single Shared Platform (SSP). That Guideline was recast in 2012 as Guideline ECB/2012/27 of the European Central Bank ([2]).

(2) It is necessary for effective regulation to clarify that TIPS DCA holders and T2S DCA holders will be connected to TARGET2 via the Eurosystem Single Market Infrastructure Gateway from November 2021 and June 2022, respectively.

(3) In order to ensure that TARGET2 continues to evolve to meet cyber security threats, the rules on the adherence to the TARGET2 endpoint security requirements need to be clarified and extended. Equally, in order to ensure a comprehensive and harmonised legal framework, the definitions should be amended.

(4) In order to ensure that instant payments are available throughout the Union, PM account holders, their indirect participants and addressable BIC holders which have adhered to the SCT Inst scheme by signing the SEPA Instant Credit Transfer Adherence Agreement should be and remain constantly reachable in the TIPS Platform via a TIPS DCA. The fund transfer services in central bank money for ancillary systems settling instant payments in their own books should be provided in the TIPS Platform.

(5) Once the T2-T2S Consolidation Project is operational, it is necessary to be transparent on the modalities of transfer of balances from participants' accounts in TARGET2 to the corresponding successor accounts in the future TARGET system so as to ensure legal certainty.

(6) In an effort to ensure effective application, it is also necessary to clarify and update other provisions of Guideline ECB/2012/27.

(7) The implementation of the T2-T2S Consolidation Project will also require changes to the applicable rules relating to contracts concluded with T2S network service providers, which should apply as of 13 June 2022.

(8) Therefore, the Guideline ECB/2012/27 should be amended accordingly,

([1]) Guideline ECB/2007/2 of the European Central Bank of 26 April 2007 on a Trans-European Automated Real-time Gross settlement Express Transfer system (TARGET2) (OJ L 237, 8.9.2007, p. 1).

([2]) Guideline ECB/2012/27 of the European Central Bank of 5 December 2012 on a Trans-European Automated Real-time Gross settlement Express Transfer system (TARGET2) (OJ L 30, 30.1.2013, p. 1).

HAS ADOPTED THIS GUIDELINE:

Article 1

Amendments

Guideline ECB/2012/27 is amended as follows:

1. Article 1, paragraph 1 is replaced by the following:

   '1. TARGET2 provides real-time gross settlement for payments in euro, with settlement in central bank money across PM accounts, T2S DCAs and TIPS DCAs. TARGET2 is established and functions on the basis of the SSP through which payment orders are submitted and processed and through which payments are ultimately received in the same technical manner. As far as the technical operation of the T2S DCAs is concerned, TARGET2 is technically established and functions on the basis of the T2S Platform. As far as the technical operation of the TIPS DCAs and TIPS AS technical accounts is concerned, TARGET2 is technically established and functions on the basis of the TIPS Platform.';

2. Article 2 is amended as follows:

   (a) point (58) is deleted;

   (b) point (62) is replaced by the following:

   '(62) "payment order" means a credit transfer order, a liquidity transfer order, a direct debit instruction, a PM to T2S DCA liquidity transfer order, a T2S DCA to PM liquidity transfer order, a T2S DCA to T2S DCA liquidity transfer order, a PM to TIPS DCA liquidity transfer order, a TIPS DCA to PM liquidity transfer order, a TIPS AS technical account to TIPS DCA liquidity transfer order, a TIPS DCA to TIPS AS technical account liquidity transfer order, an instant payment order, or a positive recall answer;';

   (c) point (78) is deleted;

   (d) point (81) is replaced by the following:

   '(81) "instant payment order" means, in line with the European Payments Council's SEPA Instant Credit Transfer (SCT Inst) scheme, a payment instruction which can be executed 24 hours a day any calendar day of the year, with immediate or close to immediate processing and notification to the payer and includes (i) TIPS DCA to TIPS DCA instant payment orders, (ii) TIPS DCA to TIPS AS technical account instant payment orders, (iii) TIPS AS technical account to TIPS DCA instant payment orders and (iv) TIPS AS technical account to TIPS AS technical account instant payment orders;';

   (e) the following points (87) to (90) are added:

   '(87) "European Payments Council's SEPA Instant Credit Transfer (SCT Inst) scheme" or "SCT Inst scheme" means an automated, open standards scheme providing a set of interbank rules to be complied with by SCT Inst participants, allowing payment services providers in SEPA to offer an automated, SEPA-wide euro instant credit transfer product;

   (88) "TIPS ancillary system technical account (TIPS AS technical account)" means an account held by an ancillary system or a CB on an ancillary system's behalf in the CB's TARGET2 component system for use by the ancillary system for the purpose of settling instant payments in its own books;

   (89) "TIPS DCA to TIPS AS technical account liquidity transfer order" means the instruction to transfer a specified amount of funds from a TIPS DCA to a TIPS AS technical account to fund the TIPS DCA holder's position (or the position of another participant of the ancillary system) in the books of the ancillary system;

   (90) "TIPS AS technical account to TIPS DCA liquidity transfer order" means the instruction to transfer a specified amount of funds from a TIPS AS technical account to a TIPS DCA to defund the TIPS DCA holder's position (or the position of another participant of the ancillary system) in the books of the ancillary system.';

3. Article 13 is replaced by the following:

'Article 13

Ancillary systems

1. The Eurosystem CBs shall provide fund transfer services in central bank money to ancillary systems in the PM accessed through the TARGET2 network service provider. Such services shall be governed by bilateral arrangements between the Eurosystem CBs and the respective ancillary systems.

2. Bilateral arrangements with ancillary systems that use the ASI shall be in conformity with Annex IV. In addition, the Eurosystem CBs shall ensure that in such bilateral arrangements the following provisions of Annex II apply mutatis mutandis:

(a) Article 8(1) (technical and legal requirements);

(b) Article 8(2) to (5) (application procedure), except that instead of being required to meet the access criteria in Article 4 the ancillary system shall be required to meet the access criteria in the definition of 'ancillary system' in Article 1 of Annex II;

(c) the operating schedule in Appendix V;

(d) Article 11 (requirements for cooperation and information exchange), except paragraph 8;

(e) Articles 27 and 28 (business continuity and contingency procedures and security requirements and control procedures), whereby the fee used as the basis for the calculation of the penalty charges for non-compliance with security requirements as laid down in Article 28 of Annex II is the fee referred to in paragraph 18(1)(a) of Annex IV;

(f) Article 31 (liability regime);

(g) Article 32 (evidence rules);

(h) Articles 33 and 34 (duration, termination and suspension of participation), except Article 34(1)(b);

(i) Article 35, where relevant (closure of PM accounts);

(j) Article 38 (confidentiality rules);

(k) Article 39 (Union requirements for data protection, prevention of money laundering and related issues);

(l) Article 40 (requirements for notices);

(m) Article 41 (contractual relationship with the TARGET2 network service provider);

(n) Article 44 (rules for governing law, jurisdiction and place of performance);

(o) Article 45a (1) (transitional clause).

3. Bilateral arrangements with ancillary systems that use the PI shall be in conformity with both of the following:

(a) Annex II, with the exception of Title V and Appendices VI and VII; and

(b) Article 18 of Annex IV.

For the purposes of point (a), the fee used as the basis for the calculation of the penalty charges for non-compliance with security requirements as laid down in Article 28 of Annex II shall be the fee referred to in paragraph 18(1)(a) of Annex IV.

4. By derogation from paragraph 3, bilateral arrangements with ancillary systems that use the PI, but only settle payments for the benefit of their customers, shall be in conformity with both of the following:

(a) Annex II, with the exception of Title V, Article 36 and Appendices VI and VII; and

(b) Article 18 of Annex IV.

For the purposes of point (a), the fee used as the basis for the calculation of the penalty charges for non-compliance with security requirements in Article 28 of Annex II shall be the fee referred to in paragraph 18(1)(a) of Annex IV.

5. Eurosystem CBs shall provide fund transfer services in central bank money for ancillary systems settling instant payments in their own books pursuant to the SCT Inst scheme only in TIPS Platform. Bilateral arrangements for the provision of such fund transfer services shall be in conformity with Annex IVa and shall only allow for the settling of instant payments pursuant to the SCT Inst scheme. In such bilateral arrangements, the following provisions of Annex IIb shall apply *mutatis mutandis*:

(a) Appendices I, II, and III;

(b) Article 4 (general description of TARGET2);

(c) Article 5 (access criteria), whereby the ancillary system shall be required to meet the access criteria in the definition of 'ancillary system' in Article 1 of Annex IIb;

(d) Article 6(1) (technical and legal requirements), except that instead of being required to have adhered to the SCT Inst scheme by signing the SEPA Instant Credit Transfer Adherence Agreement, the ancillary system shall be required to have announced its compliance with the SCT Inst scheme;

(e) Article 6(2) to (5) (application procedure), except that (i) instead of being required to meet the access criteria in Article 5 the ancillary system shall be required to meet the access criteria in the definition of 'ancillary system' in Article 1 of Annex IIb and (ii) instead of being required to submit evidence of their adherence to the SCT Inst scheme, the ancillary system shall submit evidence of the announcement of compliance with the SCT Inst scheme;

(f) Article 7 (accessing TIPS Platform);

(g) Article 8 (reachable parties);

(h) Article 9 (network service provider);

(i) Article 11 (TIPS directory);

(j) Article 11a (MPL repository);

(k) Article 12 (obligations of the CBs and the account holders), except paragraph 4;

(l) Article 14 (requirements for cooperation and information exchange);

(m) Article 16 (types of payment orders);

(n) Article 17 (acceptance and rejection of payment orders);

(o) Article 18 (processing of payment orders);

(p) Article 19 (recall request);

(q) Article 20 (moment of entry, moment of irrevocability);

(r) Article 21(security requirements and business continuity);

(s) Article 23 (liability regime);

(t) Article 24 (evidence rules);

(u) Articles 25 and 26 (duration, termination and suspension of participation), except Article 26(1)(b) and except the second subparagraph in paragraph 4 of Article 26;

(v) Article 27, where relevant (closure of accounts);

(w) Article 29 (confidentiality rules);

(x) Article 30 (Union requirements for data protection, prevention of money laundering and related issues);

(y) Article 31 (requirements for notices);

(z) Article 34 (rules for governing law, jurisdiction and place of performance);

(aa) Article 35a (transitional clause).';

4. Article 17, paragraph 4 is replaced by the following:

'4. Paragraphs 1 to 3a of this Article shall also apply in the event of suspension or termination of the use of the ASI or TIPS Platform by ancillary systems.';

5. The following Article 27a is inserted:

'Article 27a

Transitional provision

Eurosystem CBs may provide fund transfer services in central bank money for ancillary systems settling instant payments in their own books pursuant to the SCT Inst scheme using the Ancillary Systems Interface until 25 February 2022.';

6. Annex II to Guideline ECB/2012/27 is amended in accordance with Annex I to this Guideline;

7. Annex IIa to Guideline ECB/2012/27 is amended in accordance with Annex II to this Guideline;

8. Annex IIb to Guideline ECB/2012/27 is amended in accordance with Annex III to this Guideline;

9. Annex IV to Guideline ECB/2012/27 is amended in accordance with Annex IV to this Guideline;

10. A new Annex IVa to Guideline ECB/2012/27 is inserted in accordance with Annex V to this Guideline.

Article 2

Taking effect and implementation

1. This Guideline shall take effect on the day of its notification to the national central banks of the Member States whose currency is the euro.

2. The national central banks of the Member States whose currency is the euro shall take the necessary measures to comply with this Guideline from 21 November 2021, except for paragraphs 1(c), 7 and 9 of Annex II to this Guideline in respect of which they shall take the necessary measures and apply them from 13 June 2022. They shall notify the ECB of the texts and means relating to those measures by 9 September 2021 at the latest.

Article 3

Addressees

This Guideline is addressed to all Eurosystem central banks.

Done at Frankfurt am Main, 20 July 2021.

For the Governing Council of the ECB
The President of the ECB
Christine LAGARDE

ANNEX I

Annex II to Guideline ECB/2012/27 is amended as follows:

1. Article 1 is amended as follows:

   (a) point (a) of the definition of "group" is replaced by the following:

   '(a) a composition of credit institutions included in the consolidated financial statements of a parent company where the parent company is obliged to present consolidated financial statements under International Accounting Standard 27 (IAS 27), adopted pursuant to Commission Regulation (EC) No 1126/2008 (*) and consisting of either: (i) a parent company and one or more subsidiaries; or (ii) two or more subsidiaries of a parent company; or

   (*) Commission Regulation (EC) No 1126/2008 of 3 November 2008 adopting certain international accounting standards in accordance with Regulation (EC) No 1606/2002 of the European Parliament and of the Council (OJ L 320, 29.11.2008, p. 1).';

   (b) the definition of 'instant payment order' is replaced by the following:

   '— "instant payment order" means, in line with the European Payments Council's SEPA Instant Credit Transfer (SCT Inst) scheme, a payment instruction which can be executed 24 hours a day any calendar day of the year, with immediate or close to immediate processing and notification to the payer and includes (i) the TIPS DCA to TIPS DCA instant payment orders, (ii) TIPS DCA to TIPS AS technical account instant payment orders, (iii) TIPS AS technical account to TIPS DCA instant payment orders and (iv) TIPS AS technical account to TIPS AS technical account instant payment orders,';

   (c) the following definitions are added:

   '— "European Payments Council's SEPA Instant Credit Transfer (SCT Inst) scheme" or "SCT Inst scheme" means an automated, open standards scheme providing a set of interbank rules to be complied with by SCT Inst participants, allowing payment services providers in SEPA to offer an automated, SEPA-wide euro instant credit transfer product,

   — "TIPS ancillary system technical account (TIPS AS technical account)" means an account held by an ancillary system or a CB on an ancillary system's behalf in the CB's TARGET2 component system for use by the ancillary system for the purpose of settling instant payments in its own books,

   — "TIPS DCA to TIPS AS technical account liquidity transfer order" means the instruction to transfer a specified amount of funds from a TIPS DCA to a TIPS AS technical account to fund the TIPS DCA holder's position (or the position of another participant of the ancillary system) in the books of the ancillary system,

   — "TIPS AS technical account to TIPS DCA liquidity transfer order" means the instruction to transfer a specified amount of funds from a TIPS AS technical account to a TIPS DCA to defund the TIPS DCA holder's position (or the position of another participant of the ancillary system) in the books of the ancillary system,

   — "reachable party" means an entity which: (a) holds a BIC; (b) is designated as a reachable party by a TIPS DCA holder or by an ancillary system; (c) is a correspondent, customer or branch of a TIPS DCA holder or a participant of an ancillary system, or a correspondent, customer, or branch of a participant of an ancillary system; and (d) is addressable through the TIPS Platform and is able to submit instant payment orders and receive instant payment orders either via the TIPS DCA holder or the ancillary system or, if so authorised by the TIPS DCA holder or by the ancillary system, directly.';

   (d) the definition of "TIPS network service provider" is deleted;

2. Article 3 is amended as follows:

   (a) in paragraph 2, point (fc) is replaced by the following:

   '(fc) TIPS DCA to PM liquidity transfer orders and PM to TIPS DCA liquidity transfer orders;';

   (b) in paragraph 2, the following point (fd) is inserted:

   '(fd) TIPS DCA to TIPS AS technical account liquidity transfer orders and TIPS AS technical account to TIPS DCA liquidity transfer orders; and';

(c) paragraph 3 is replaced by the following:

'3. TARGET2 provides real-time gross settlement for payments in euro, with settlement in central bank money across PM accounts, T2S DCAs and TIPS DCAs. TARGET2 is established and functions on the basis of the SSP through which payment orders are submitted and processed and through which payments are ultimately received in the same technical manner. As far as the technical operation of the T2S DCAs is concerned, TARGET2 is technically established and functions on the basis of the T2S Platform. As far as the technical operation of the TIPS DCAs and TIPS AS technical accounts is concerned, TARGET2 is technically established and functions on the basis of the TIPS Platform.';

3. Article 5 is replaced by the following:

'Article 5

Direct participants

1. PM account holders in TARGET2 [insert CB/country reference] are direct participants and shall comply with the requirements set out in Article 8(1) and (2). They shall have at least one PM account with the [insert name of CB]. PM account holders that have adhered to the SCT Inst scheme by signing the SEPA Instant Credit Transfer Adherence Agreement shall be and shall remain reachable in the TIPS Platform at all times, either as a TIPS DCA holder or as a reachable party via a TIPS DCA holder.

2. PM account holders may designate addressable BIC holders, regardless of their place of establishment. PM account holders may designate addressable BIC holders that have adhered to the SCT Inst scheme by signing the SEPA Instant Credit Transfer Adherence Agreement only if such entities are reachable in the TIPS Platform, either as a TIPS DCA holder or as a reachable party via a TIPS DCA holder.

3. PM account holders may designate entities as indirect participants in the PM, provided that the conditions laid down in Article 6 are met. PM account holders may designate as indirect participants entities that have adhered to the SCT Inst scheme by signing the SEPA Instant Credit Transfer Adherence Agreement only if such entities are reachable in the TIPS Platform, either as a TIPS DCA holder with the [insert name of CB] or as a reachable party via a TIPS DCA holder.

4. Multi-addressee access through branches may be provided as follows:

(a) a credit institution within the meaning of Article 4(1)(a) or (b) of this Annex which has been admitted as a PM account holder may grant access to its PM account to one or more of its branches established in the Union or the EEA in order to submit payment orders and/or receive payments directly, provided that [insert name of the CB] has been informed accordingly;

(b) where a branch of a credit institution has been admitted as a PM account holder, the other branches of the same legal entity and/or its head office, in both cases provided that they are established in the Union or the EEA, may access the branch's PM account, provided that it has informed the [insert name of CB].';

4. in Article 12, paragraph 5 is replaced by the following:

'5. PM accounts and their sub-accounts shall either be remunerated at zero per cent or at the deposit facility rate, whichever is lower, unless they are used to hold minimum reserves or they are used to hold excess reserves.

In the case of minimum reserves, the calculation and payment of remuneration of holdings shall be governed by Council Regulation (EC) No 2531/98 (*) and Regulation (EU) 2021/378 of the European Central Bank (ECB/2021/1) (**) .

In the case of excess reserves, the calculation and payment of remuneration of holdings shall be governed by Decision (EU) 2019/1743 (ECB/2019/31) (***).

(*) Council Regulation (EC) No 2531/98 of 23 November 1998 concerning the application of minimum reserves by the European Central Bank (OJ L 318, 27.11.1998, p. 1).

(**) Regulation (EU) 2021/378 of the European Central Bank of 22 January 2021 on the application of minimum reserve requirements (ECB/2021/1) (OJ L 73, 3.3.2021, p. 1).

(***) Decision (EU) 2019/1743 of the European Central Bank of 15 October 2019 on the remuneration of holdings of excess reserves and of certain deposits (ECB/2019/31) (OJ L 267, 21.10.2019, p. 12).';

5. Article 28 is replaced by the following:

'Article 28

Security Requirements and Control Procedures

1. Participants shall implement adequate security controls to protect their systems from unauthorised access and use. Participants shall be exclusively responsible for the adequate protection of the confidentiality, integrity and availability of their systems.

2. Participants shall inform the [insert name of CB] of any security-related incidents in their technical infrastructure and, where appropriate, security-related incidents that occur in the technical infrastructure of the third party providers. The [insert name of CB] may request further information about the incident and, if necessary, request that the participant take appropriate measures to prevent a recurrence of such an event.

3. The [insert name of CB] may impose additional security requirements, in particular with regard to cybersecurity or the prevention of fraud, on all participants and/or on participants that are considered critical by the [insert name of CB].

4. Participants shall provide the [insert name of CB] with; (i) permanent access to their attestation of adherence to their chosen network service provider's endpoint security requirements, and (ii) on an annual basis the TARGET2 self-certification statement as published on the [insert name of CB]'s website and on the ECB's website in English.

4a. The [insert name of CB] shall assess the participant's self-certification statement(s) on the participants level of compliance with each of the requirements set out in the TARGET2 self-certification requirements. These requirements are listed in Appendix VIII, which in addition to the other Appendices listed in Article 2(1), shall form an integral part of these Conditions.

4b. The participant's level of compliance with the requirements of the TARGET2 self-certification shall be categorised as follows, in increasing order of severity: 'full compliance'; 'minor non-compliance'; or, 'major non-compliance'. The following criteria apply: full compliance is reached where participants satisfy 100% of the requirements; minor non-compliance is where a participant satisfies less than 100% but at least 66% of the requirements and major non-compliance where a participant satisfies less than 66% of the requirements. If a participant demonstrates that a specific requirement is not applicable to it, it shall be considered as compliant with the respective requirement for the purposes of the categorisation. A participant which fails to reach 'full compliance' shall submit an action plan demonstrating how it intends to reach full compliance. The [insert name of CB] shall inform the relevant supervisory authorities of the status of such participant's compliance.

4c. If the participant refuses to grant permanent access to its attestation of adherence to their chosen NSPs endpoint security requirements or does not provide the TARGET2 self-certification the participant's level of compliance shall be categorised as 'major non-compliance'.

4d. The [insert name of CB] shall re-assess compliance of participants on an annual basis.

4e. The [insert name of CB] may impose the following measures of redress on participants whose level of compliance was assessed as minor or major non-compliance, in increasing order of severity:

(i) enhanced monitoring: the participant shall provide the [insert name of CB] with a monthly report, signed by a senior executive, on their progress in addressing the non-compliance. The participant shall additionally incur a monthly penalty charge for each affected account equal to its monthly fee as set out in paragraph 1 of Appendix VI excluding the transaction fees. This measure of redress may be imposed in the event the participant receives a second consecutive assessment of minor non-compliance or an assessment of major non-compliance;

(ii) suspension: participation in TARGET2-[insert CB/country reference] may be suspended in the circumstances described in Article 34(2)(b) and (c) of this Annex. By way of derogation from Article 34 of this Annex, the participant shall be given three months' notice of such suspension. The participant shall incur a monthly penalty charge for each suspended account of double its monthly fee as set out in paragraph 1 of Appendix VI, excluding the transaction fees. This measure of redress may be imposed in the event the participant receives a second consecutive assessment of major non-compliance;

(iii) termination: participation in TARGET2-[insert CB/country reference] may be terminated in the circumstances described in Article 34(2)(b) and (c) of this Annex. By way of derogation from Article 34 of this Annex, the participant shall be given three months' notice of such termination. The participant shall incur an additional penalty charge of EUR 1 000 for each terminated account. This measure of redress may be imposed if the participant has not addressed the major non-compliance to the satisfaction of [insert name of CB] following three months of suspension.

5. Participants allowing access to their PM account by third parties as set out in Article 5(2), (3) and (4) shall address the risk stemming from allowing such access in accordance with the security requirements set out in paragraphs 1 to 4e of this Article. The self-certification referred to in paragraph 4 shall specify that the participant imposes the TARGET2 network service provider's endpoint security requirements on third parties who have access to that participant's PM account.';

6. Article 39(1) is replaced by the following:

'1. Participants shall be deemed to be aware of, shall comply with, and shall be able to demonstrate that compliance to the relevant competent authorities with all obligations on them relating to legislation on data protection. They shall be deemed to be aware of, and shall comply with all obligations on them relating to legislation on prevention of money laundering and the financing of terrorism, proliferation-sensitive nuclear activities and the development of nuclear weapons delivery systems, in particular in terms of implementing appropriate measures concerning any payments debited or credited on their PM accounts. Participants shall ensure that they are informed about the TARGET2 network service provider's data retrieval policy prior to entering into the contractual relationship with the TARGET2 network service provider.';

7. the following Article 45a is inserted:

'Article 45a

Transitional provisions

1. Once the TARGET system is operational and TARGET2 has ceased operation, PM account balances shall be transferred to the account holder's corresponding successor accounts in the TARGET system.

2. The requirement that PM account holders, indirect Participants and addressable BIC holders adhering to the SCT Inst scheme be reachable in the TIPS Platform pursuant to Article 5 shall apply as of 25 February 2022.';

8. in Appendix I, paragraph 8(4)(b) is replaced by the following:

'(b) User-to-application mode (U2A)

U2A permits direct communication between a participant and the ICM. The information is displayed in a browser running on a PC system (SWIFT Alliance WebStation or another interface, as may be required by SWIFT). For U2A access the IT infrastructure has to be able to support cookies. Further details are described in the ICM User Handbook.';

9. in Appendix IV, paragraph 6(g) is replaced by the following:

'(g) for contingency processing of payment orders, participants shall provide eligible assets as collateral. During contingency processing, incoming contingency payments may be used to fund outgoing contingency payments. For the purposes of contingency processing, participants' available liquidity may not be taken into account by the [insert name of CB].';

10. The text set out in Annex VI to this Guideline is added as a new Appendix VIII to Annex II of Guideline ECB/2012/27.

ANNEX II

Annex IIa to Guideline ECB/2012/27 is amended as follows:

1. Article 1 is amended as follows:

   (a) the definition of 'instant payment order' is replaced by the following:

   '— "instant payment order" means, in line with the European Payments Council's SEPA Instant Credit Transfer (SCT Inst) scheme, a payment instruction which can be executed 24 hours a day any calendar day of the year, with immediate or close to immediate processing and notification to the payer and includes (i) the TIPS DCA to TIPS DCA instant payment orders, (ii) TIPS DCA to TIPS AS technical account instant payment orders, (iii) TIPS AS technical account to TIPS DCA instant payment orders and (iv) TIPS AS technical account to TIPS AS technical account instant payment orders,';

   (b) the following definitions are added:

   '— "TIPS ancillary system technical account (TIPS AS technical account)" means an account held by an ancillary system or a CB on an ancillary system's behalf in the CB's TARGET2 component system for use by the ancillary system for the purpose of settling instant payments in its own books,

   — "TIPS DCA to TIPS AS technical account liquidity transfer order" means the instruction to transfer a specified amount of funds from a TIPS DCA to a TIPS AS technical account to fund the TIPS DCA holder's position (or the position of another participant of the ancillary system) in the books of the ancillary system,

   — "TIPS AS technical account to TIPS DCA liquidity transfer order" means the instruction to transfer a specified amount of funds from a TIPS AS technical account to a TIPS DCA to defund the TIPS DCA holder's position (or the position of another participant of the ancillary system) in the books of the ancillary system,

   — "Network Service Provider (NSP)" means an undertaking that has been awarded a concession with the Eurosystem to provide connectivity services via the Eurosystem Single Market Infrastructure Gateway.';

   (c) the definition of 'T2S network service provider' is deleted;

2. in Article 4(2), point (fc) is replaced by the following:

   '(fc) TIPS DCA to PM liquidity transfer orders and PM to TIPS DCA liquidity transfer orders;';

3. in Article 4(2), point (fd) is inserted:

   '(fd) TIPS DCA to TIPS AS technical account liquidity transfer orders and TIPS AS technical account to TIPS DCA liquidity transfer orders; and';

4. Article 4(3) is replaced by the following:

   '3. TARGET2 provides real-time gross settlement for payments in euro, with settlement in central bank money across PM accounts, T2S DCAs and TIPS DCAs. TARGET2 is established and functions on the basis of the SSP through which payment orders are submitted and processed and through which payments are ultimately received in the same technical manner. As far as the technical operation of the T2S DCAs is concerned, TARGET2 is technically established and functions on the basis of the T2S Platform. As far as the technical operation of the TIPS DCAs and TIPS AS technical accounts is concerned, TARGET2 is technically established and functions on the basis of the TIPS Platform. The [insert name of CB] is the provider of services under these Conditions. Acts and omissions of the SSP-providing NCBs and the 4CBs shall be considered acts and omissions of [insert name of CB], for which it shall assume liability in accordance with Article 21 of this Annex. Participation pursuant to these Conditions shall not create a contractual relationship between T2S DCA holders and the SSP-providing NCBs or the 4CBs when any of the latter acts in that capacity. Instructions, messages or information which a T2S DCA holder receives from, or sends to, the SSP or T2S Platform in relation to the services provided under these Conditions are deemed to be received from, or sent to, [insert name of CB].';

5. Article 8(3) is replaced by the following:

   '3. Where [insert name of CB] has granted a request by a T2S DCA holder pursuant to paragraph 1, that T2S DCA holder is deemed to have given the participating CSD(s) a mandate to debit the T2S DCA with the amounts relating to securities transactions executed on those securities accounts.';

6. Article 28(1) is replaced by the following:

'1. T2S DCA holders shall be deemed to be aware of, shall comply with, and shall be able to demonstrate that compliance to the relevant competent authorities with all obligations on them relating to legislation on data protection. They shall be deemed to be aware of, and shall comply with all obligations on them relating to legislation on prevention of money laundering and the financing of terrorism, proliferation-sensitive nuclear activities and the development of nuclear weapons delivery systems, in particular in terms of implementing appropriate measures concerning any payments debited or credited on their T2S DCAs. Prior to entering into the contractual relationship with its T2S network service provider, T2S DCA holders shall ensure that they are informed about its data retrieval policy.';

7. Article 30 is replaced by the following:

'Article 30

Contractual relationship with an NSP

1. T2S DCA holders shall either:

(a) have concluded a contract with an NSP within the framework of the concession contract with that NSP in order to establish a technical connection to TARGET2- [insert name of CB]; or

(b) connect via another entity which has concluded a contract with an NSP within the framework of the concession contract with that NSP.

2. The legal relationship between a T2S DCA holder and the NSP shall be exclusively governed by the terms and conditions of the separate contract concluded with an NSP as referred to in paragraph 1(a).

3. The services to be provided by the NSP shall not form part of the services to be performed by the [insert name of CB] in respect of TARGET2.

4. The [insert name of CB] shall not be liable for any acts, errors or omissions of the NSP (including its directors, staff and subcontractors), or for any acts, errors or omissions of third parties selected by participants to gain access to the NSP's network.';

8. The following Article 34a is inserted:

'Article 34a

Transitional provisions

Once the TARGET system is operational and TARGET2 has ceased operation, T2S DCA holders shall become T2S DCA holders in the TARGET system.';

9. The references to "T2S network service provider" (in singular or plural) in Articles 6(1)(a)(i), 9(5), 10(6), 14(1)(a), 22(1), 22(2), 22(3), 27(5), 28(1), 29(1) of Annex IIa and paragraph 1 of Appendix I are replaced with references to "NSP".

10. in Appendix I, paragraph 7(1)(b) is replaced by the following:

'(b) User-to-application mode (U2A)

U2A permits direct communication between a T2S DCA holder and the T2S GUI. The information is displayed in a browser running on a PC system. For U2A access the IT infrastructure has to be able to support cookies. Further details are described in the T2S User Handbook.'

ANNEX III

Annex IIb to Guideline ECB/2012/27 is amended as follows:

1. The references to "TIPS network service provider" (in singular or plural) in Articles 17(1)(a), 24(1), 24(2), 26(2)(d), 29(6), paragraph 1 of Appendix I, paragraph 6(1) of Appendix I and paragraph 3(3)(b) of Appendix II, shall be replaced with references to "NSP";

2. Article 1 is amended as follows:

   (a) the definition of 'reachable party' is replaced by the following:

   '— "reachable party" means an entity which: (a) holds a BIC, (b) is designated as a reachable party by a TIPS DCA holder or by an ancillary system; (c) is a correspondent, customer or branch of a TIPS DCA holder or a participant of an ancillary system or a correspondent, customer or branch of a participant of an ancillary system; and (d) is addressable through the TIPS Platform and is able to submit instant payment orders and receive instant payment orders either via the TIPS DCA holder or the ancillary system or, if so authorised by the TIPS DCA holder or by the ancillary system, directly,';

   (b) the definition of 'payment order' is replaced by the following:

   '— "payment order", except where used in Articles 16 to 18 of this Annex, means an instant payment order, a positive recall answer, a PM to TIPS DCA liquidity transfer order, a TIPS DCA to PM liquidity transfer order, a TIPS AS technical account to TIPS DCA liquidity transfer order or a TIPS DCA to TIPS AS technical account liquidity transfer order,';

   (c) the definition of 'instant payment order' is replaced by the following:

   '— "instant payment order" means, in line with the European Payments Council's SEPA Instant Credit Transfer (SCT Inst) scheme, a payment instruction which can be executed 24 hours a day any calendar day of the year, with immediate or close to immediate processing and notification to the payer and includes (i) TIPS DCA to TIPS DCA instant payment orders, (ii) TIPS DCA to TIPS AS technical account instant payment orders, (iii) TIPS AS technical account to TIPS DCA instant payment orders and (iv) TIPS AS technical account to TIPS AS technical account instant payment orders,';

   (d) the following definitions are added:

   '— "TIPS ancillary system technical account (TIPS AS technical account)" means an account held by an ancillary system or the CB on an ancillary system's behalf in the CB's TARGET2 component system for use by that ancillary system for the purpose of settling instant payments in its own books,

   — "TIPS DCA to TIPS AS technical account liquidity transfer order" means the instruction to transfer a specified amount of funds from a TIPS DCA to a TIPS AS technical account to fund the TIPS DCA holder's position (or the position of another participant of the ancillary system) in the books of the ancillary system,

   — "TIPS AS technical account to TIPS DCA liquidity transfer order" means the instruction to transfer a specified amount of funds from a TIPS AS technical account to a TIPS DCA to defund the TIPS DCA holder's position (or the position of another participant of the ancillary system) in the books of the ancillary system,

   — "European Payments Council's SEPA Instant Credit Transfer (SCT Inst) scheme" or "SCT Inst scheme" means an automated, open standards scheme providing a set of interbank rules to be complied with by SCT Inst participants, allowing payment services providers in SEPA to offer an automated, SEPA-wide euro instant credit transfer product,

   — "mobile proxy look-up (MPL) service" means a service which enables TIPS DCA holders, ancillary systems using TIPS AS technical accounts and reachable parties, who receive from their customers a request to execute an instant payment order in favour of a beneficiary identified with a proxy (e.g. a mobile number), to retrieve from the central MPL repository the corresponding beneficiary IBAN and the BIC to be used to credit the relevant account in TIPS,

   — "Network Service Provider (NSP)" means an undertaking that has been awarded a concession with the Eurosystem to provide connectivity services via the Eurosystem Single Market Infrastructure Gateway,

— "IBAN" means the international bank account number which uniquely identifies an individual account at a specific financial institution in a particular country.';

(e) the definition of "TIPS network service provider" is deleted;

3. In Article 3(1), the reference to "Appendix V: TIPS connectivity technical requirements" is deleted;

4. Article 4 is amended as follows:

(a) in paragraph 2, the following point (ia) is inserted:

'(ia) TIPS DCA to TIPS AS technical account liquidity transfer orders and TIPS AS technical account to TIPS DCA liquidity transfer orders; and';

(b) paragraph 3 is replaced by the following:

'3. TARGET2 provides real-time gross settlement for payments in euro, with settlement in central bank money across PM accounts, T2S DCAs and TIPS DCAs. TARGET2 is established and functions on the basis of the SSP through which payment orders are submitted and processed and through which payments are ultimately received in the same technical manner. As far as the technical operation of the TIPS DCAs and TIPS AS technical accounts is concerned, TARGET2 is technically established and functions on the basis of the TIPS Platform. As far as the technical operation of the T2S DCAs is concerned, TARGET2 is technically established and functions on the basis of the T2S Platform.';

5. Article 6(1)(a)(i) is replaced by the following:

'(i) install, manage, operate and monitor and ensure the security of the necessary IT infrastructure to connect to the TIPS Platform and submit payment orders to it. In doing so, applicant TIPS DCA holders may involve third parties, but retain sole liability. In particular, unless an instructing party is used, applicant TIPS DCA holders shall enter into an agreement with one or more NSPs to obtain the necessary connection and admissions, in accordance with the technical specifications in Appendix I; and';

6. Article 9 is replaced by the following:

'Article 9

Contractual relationship with an NSP

1. Participants shall either:

(a) conclude a contract with an NSP within the framework of the concession contract with that NSP in order to establish a technical connection to TARGET2-[insert CB/country reference]; or

(b) connect via another entity which has concluded a contract with an NSP within the framework of the concession contract with that NSP.

2. The legal relationship between a participant and the NSP shall be exclusively governed by the terms and conditions of their separate contract as referred to in paragraph 1(a).

3. The services to be provided by the NSP shall not form part of the services to be performed by the [insert name of CB] in respect of TARGET2.

4. The [insert name of CB] shall not be liable for any acts, errors or omissions by the NSP (including its directors, staff and subcontractors), or for any acts, errors or omissions by third parties selected by participants to gain access to the NSP's network.';

7. Article 10 is deleted;

8. The following Article 11a is inserted:

'Article 11a

MPL repository

1. The central MPL repository contains the proxy – IBAN mapping table for the purposes of the MPL service.

2. Each proxy may be linked to only one IBAN. An IBAN may be linked to one or multiple proxies.

3. Article 29 shall apply to the data contained in the MPL repository.';

9. Article 12(9) is deleted;

10. Article 15(5) is replaced by the following:

'5. TIPS DCAs, shall either be remunerated at zero per cent or at the deposit facility rate, whichever is lower, unless they are used to hold minimum reserves or they are used to hold excess reserves.

In the case of minimum reserves, the calculation and payment of remuneration of holdings shall be governed by Council Regulation (EC) No 2531/98 (*) and Regulation (EU) 2021/378 of the European Central Bank (ECB/2021/1) (**).

In the case of excess reserves, the calculation and payment of remuneration of holdings shall be governed by Decision (EU) 2019/1743 (ECB/2019/31) (***).

_____

(*) Council Regulation (EC) No 2531/98 of 23 November 1998 concerning the application of minimum reserves by the European Central Bank (OJ L 318, 27.11.1998, p. 1).

(**) Regulation (EU) 2021/378 of the European Central Bank of 22 January 2021 on the application of minimum reserve requirements (ECB/2021/1) (OJ L 73, 3.3.2021, p. 1).

(***) Decision (EU) 2019/1743 of the European Central Bank of 15 October 2019 on the remuneration of holdings of excess reserves and of certain deposits (ECB/2019/31) (OJ L 267, 21.10.2019, p. 12).';

11. Article 16 is replaced by the following:

'*Article 16*

Types of payment orders in TIPS DCA

The following are classified as payment orders for the purposes of the TIPS service:

(a) instant payment orders;

(b) positive recall answers;

(c) TIPS DCA to PM liquidity transfer orders;

(d) TIPS DCA to TIPS AS technical account liquidity transfer orders; and

(e) TIPS AS technical account to TIPS DCA liquidity transfer orders.';

12. Article 18(6) is replaced by the following:

'6. After a TIPS DCA to PM liquidity transfer order, a TIPS DCA to TIPS AS technical account liquidity transfer order or a TIPS AS technical account to TIPS DCA liquidity transfer order has been accepted as referred to in Article 17, the TARGET2-[insert CB/country reference] shall check whether sufficient funds are available on the payer's account. If sufficient funds are not available the liquidity transfer order shall be rejected. If sufficient funds are available the liquidity transfer order shall be settled immediately.';

13. Article 20(1)(b) is replaced by the following:

'(b) TIPS DCA to PM liquidity transfer orders, positive recall answers and TIPS DCA to TIPS AS technical account liquidity transfer orders are deemed entered into TARGET2-[insert CB/country reference] and irrevocable at the moment that the relevant TIPS DCA is debited. TIPS AS technical account to TIPS DCA liquidity transfer orders are deemed entered into TARGET2-[insert CB/country reference] and irrevocable at the moment that the relevant TIPS AS technical account is debited.';

14. Article 30(1) is replaced by the following:

'1. TIPS DCA holders shall be deemed to be aware of, shall comply with and shall be able to demonstrate that compliance to the relevant competent authorities with all obligations on them relating to legislation on data protection. They shall be deemed to be aware of, and shall comply with all obligations on them relating to legislation on prevention of money laundering and the financing of terrorism, proliferation-sensitive nuclear activities and the development of nuclear weapons delivery systems, in particular in terms of implementing appropriate measures concerning any payments debited or credited on their TIPS DCAs. TIPS DCA holders ensure that they are informed about their chosen NSP's data retrieval policy prior to entering into a contractual relationship with that NSP.';

15. The following Article 35a is inserted:

'Article 35a

Transitional provision

Once the TARGET system is operational and the TARGET2 has ceased operation, TIPS DCA holders shall become TIPS DCA holders in the TARGET system.';

16. in Appendix I, the table in paragraph 2 is replaced by the following:

'Message Type	Message Name
Pacs.002	FIToFIPayment Status Report
Pacs.004	PaymentReturn
Pacs.008	FIToFICustomerCreditTransfer
Pacs.028	FIToFIPaymentStatusRequest
camt.003	GetAccount
camt.004	ReturnAccount
camt.005	GetTransaction
camt.006	ReturnTransaction
camt.011	ModifyLimit
camt.019	ReturnBusinessDayInformation
camt.025	Receipt
camt.029	ResolutionOfInvestigation
camt.050	LiquidityCreditTransfer
camt.052	BankToCustomerAccountReport
camt.053	BankToCustomerStatement
camt.054	BankToCustomerDebitCreditNotification
camt.056	FIToFIPaymentCancellationRequest
acmt.010	AccountRequestAcknowledgement
acmt.011	AccountRequestRejection
acmt.015	AccountExcludedMandateMaintenanceRequest
reda.016	PartyStatusAdviceV01
reda.022	PartyModificationRequestV01'

17. in Appendix I, paragraph 6(1)(b) is replaced by the following:

'(b) User-to-application mode (U2A)

U2A permits direct communication between a TIPS DCA holder and the TIPS GUI. The information is displayed in a browser running on a PC system. For U2A access the IT infrastructure has to be able to support cookies. Further details are described in the TIPS User Handbook.';

18. in Appendix IV, paragraph 2 is deleted;

19. Appendix V is deleted.

ANNEX IV

Annex IV to Guideline ECB/2012/27 is amended as follows:

1. Paragraph 14(14)(d) is replaced by the following

   '(d) SWIFT orders using MT 103 messages may not be submitted.';

2. In paragraph 18(1)(b), the first line of the table is replaced by the following:

'Band	From (EUR million/ business day)	To (EUR million/business day)	Annual fee (EUR)	Monthly fee (EUR)'

3. in paragraph 18(1)(d), the final subparagraph is deleted.

ANNEX V

The following Annex IVa to Guideline ECB/2012/27 is inserted:

'ANNEX IVa

TIPS SERVICE FOR ANCILLARY SYSTEMS SETTLING INSTANT PAYMENTS

1. **Definitions**

For the purposes of this Annex and further to the definitions in Article 1 of Annex IIb:

(1) "ancillary system central bank (ASCB)" means the Eurosystem CB with which the relevant ancillary system settling instant payments in its own books has a bilateral arrangement for the settlement of ancillary system instant payments;

(2) "underlying gross volume" means the number of instant payments settled on the ancillary system's own books and enabled by funds held on the TIPS AS technical account. It does not include instant payments to or from TIPS DCAs or other TIPS AS technical accounts;

(3) "instructing party" means an entity which has been designated as such by an ancillary system and which is allowed to send payment orders to the TIPS Platform and/or receive payment orders from the TIPS Platform on behalf of that ancillary system or a reachable party of that ancillary system.

2. **Entry of payment orders into the system and their irrevocability**

The application of Article 20 of Annex IIb, regarding the moment of entry of instant payment orders, positive recall answers and TIPS DCA to TIPS AS technical account liquidity transfer orders and TIPS AS technical account to TIPS DCA liquidity transfer orders in the relevant TARGET2 component system shall not have any effect on any rules of ancillary systems which stipulate a moment of entry into the ancillary system and/or irrevocability of transfer orders submitted to such ancillary system at a point in time earlier than the moment of entry of the respective payment order in the relevant TARGET2 component system.

3. **Accounts to support settlement of instant payments in ancillary systems own books**

(1) To support the settlement of instant payments related to ancillary systems in TIPS, one TIPS AS technical account shall be opened.

(2) A TIPS AS technical account shall be identified by means of a unique account number of up to 34 characters and shall be structured as set out in the table:

	Name	Format	Content
Part A	Account type	1 char. exactly	'A' for AS technical account
	Country code of the central bank	2 char. exactly	ISO country code 3166-1
	Currency code	3 char. exactly	EUR
Part B	Account holder	11 char. exactly	BIC
Part C	Sub-classification of the account	Up to 17 char.	Free text (alphanumeric) to be provided by the account holder.

(3) TIPS AS technical accounts may only have a zero or positive balance during the day and may maintain a positive balance overnight. Overnight balance on the account shall be subject to the same remuneration rules that apply to Guarantee Funds pursuant to Article 11 of this Guideline.

4. **Settlement procedure**

(1) The ancillary system shall use a TIPS AS technical account to collect the necessary liquidity set aside by their clearing members to fund their positions.

(2) Upon request, the ancillary system shall be notified of the crediting and debiting of their TIPS AS technical account.

(3) An ancillary system may send instant payment orders, and positive recall answers to any TIPS DCA holder or TIPS ancillary system. An ancillary system shall receive and process instant payment orders, recall requests and positive recall answers from any TIPS DCA holder or TIPS ancillary system.

5. **User interface**

(1) The TIPS AS technical account holder shall access the TIPS Platform in A2A mode and may also connect in U2A mode either directly or via one or more instructing parties.

(2) Access to the TIPS Platform allows TIPS AS technical account holders to:

(a) access information relating to their accounts and to manage CMBs;

(b) initiate TIPS AS technical account to TIPS DCA liquidity transfer orders; and

(c) manage certain static data.

6. **Fee schedule and invoicing**

(1) An ancillary system in TIPS, shall be subject to both of the following:

(a) a transaction fee calculated on the same basis as the schedule established for TIPS DCA holders in Appendix IV to Annex IIb;

(b) a fee based on the underlying gross volume of instant payments settled in the ancillary system's own platform and enabled by the pre-funded positions on the TIPS AS technical account. The fee shall be EUR 0.0005 per instant payment.

(2) The underlying gross volume of the ancillary system's instant payments shall be calculated by the ASCB each month on the basis of the underlying gross volume during the previous month rounded down to the nearest ten thousand and reported by the ancillary system at the latest by the third business day of the following month. The calculated gross volume shall be applied for calculating the fee during the following month.

(3) Each ancillary system shall receive an invoice from its ASCB for the previous month based on the fees referred to in point (1) of this paragraph, no later than the ninth business day of the following month. Payments shall be made no later than the 14th business day of the month in which the invoice is issued to the account specified by the ASCB or shall be debited from an account specified by the ancillary system.

(4) For the purposes of fee schedules and invoicing pursuant to this Annex:

(a) an ancillary system that has been designated as a system under Directive 98/26/EC shall be treated as a separate ancillary system, notwithstanding that it is operated by a legal entity that operates another ancillary system;

(b) an ancillary system that has not been designated as a system under Directive 98/26/EC shall be treated as a separate ancillary system where it fulfils the following criteria:

(i) it is a formal arrangement, in the form of a contract or a legislative instrument;

(ii) it has more than one [member] [participant] [excluding the system operator of that system];

(iii) it is established for the purposes of clearing, netting and/or settlement of payments and/or securities between the participants; and

(iv) it applies common rules and standardised arrangements to the clearing, netting and settlement of payments and securities between the participants.

(5) The fees, for the purposes of invoicing pursuant to this Article for the period from 1 December 2021 to 28 February 2022, shall amount to the average of the total fees invoiced for the months of September, October and November 2021.'.

ANNEX VI

The following Appendix VIII to Annex II to Guideline ECB/2012/27 is added:

'Appendix VIII

Requirements regarding information security management and business continuity management

Information security management

These requirements are applicable to each participant, unless the participant demonstrates that a specific requirement is not applicable to it. In establishing the scope of application of the requirements within its infrastructure, 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 SWIFT (e.g. SWIFT VPN Box) or Internet (with the latter applicable to Internet-based Access).

Requirement 1.1: Information security policy

The 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 organisation, 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. The management shall coordinate and review the establishment of the information security framework to ensure the implementation of the information security policy (as per Requirement 1.1) across the organisation, including the allocation of sufficient resources and assignment of security responsibilities for this purpose.

Requirement 1.3: External parties

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 external parties or products/services of external parties are required to access the organisation's information processing facilities, 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 owner can delegate the implementation of specific controls as appropriate, but remains accountable for the proper protection of the assets.

Requirement 1.5: Information assets classification

Information assets shall be classified in terms of their 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 the information asset in the relevant business processes and shall also take into consideration the underlying IT components. An information asset classification scheme approved by the management shall be used to define an appropriate set of protection controls throughout the information asset lifecycle (including removal and destruction of information assets) and to communicate the need for specific 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 handling security breaches shall be established for employees. Responsibilities shall be in place to ensure that 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 shall be granted only to individuals who fall within the 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 equipment 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 of equipment or information. 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 all the underlying systems in the Payment Transaction Chain end-to-end.

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 by the management; those recovery policies 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 events relevant to information security shall be recorded. Operator logs shall be used to ensure that information system problems are identified. Operator logs shall be regularly reviewed on a sample basis, based on the criticality of the operations. 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, carried out in line with exchange agreements among the involved parties and shall be compliant with any relevant legislation. Third party software components employed in the exchange of information with TARGET2 (like software received from a Service Bureau in scenario 2 of the scope section of the TARGET2 self-certification arrangement document) 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 ([1])) and according to the established framework of corporate policies (including the information security policy). Clear access control rules shall be defined based on the principle of least privilege ([2]) 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 (e.g. encryption, personal data anonymisation).

Formal and documented procedures shall be in place to control the allocation of access rights to information systems and services that fall within the scope of the Payment Transaction Chain. The procedures shall cover all stages in the lifecycle 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 abuse of those access rights could lead to a severe adverse impact on the operations of the participant (e.g. access rights allowing system administration, override of system controls, direct access to business data).

Appropriate controls shall be put in place to identify, authenticate and authorise 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 organisational controls shall be 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.

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).

([1]) 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.

([2]) The principle of least privilege refers to tailoring a subject's access profile to an IT system in order to match the corresponding business role.

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 of 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 a timely fashion.

Requirement 1.11: Information security in supplier ([3]) 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 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 organisation's established framework of policies (e.g. information security policy, cryptographic control policy).

Requirement 1.14: Virtualisation

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). Centralised 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.

([3]) 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 TARGET2 self-certification.

Business continuity management (applicable only to critical participants)

The following requirements (2.1 to 2.6) relate to business continuity management. Each TARGET2 participant classified by the Eurosystem as being critical for the smooth functioning of the TARGET2 system shall have a business continuity strategy in place comprising the following elements.

Requirement 2.1:	Business continuity plans shall be developed and procedures for maintaining them are in place.
Requirement 2.2:	An alternate operational site shall be available.
Requirement 2.3:	The risk profile of the alternate site shall 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 shall 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 shall be able to resume normal operations from the alternate site, where it shall be possible to properly close the business day and open the following business day(s).
Requirement 2.5:	Procedures shall 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 shall be tested at least once a year and critical staff shall be aptly trained. The maximum period between tests shall not exceed one year.'.