EUROPEAN CENTRAL BANK

EUROSYSTEM

Directorate General Market Infrastructure and Payments

MARKET INFRASTRUCTURE MANAGEMENT DIVISION

ECB-PUBLIC

20 June 2022

TARGET Self-certification arrangement for RTGS DCA holders and Ancillary Systems[1]
- Security requirements and self-certification statement -

Introduction

The CPMI-IOSCO Principles for Financial Market Infrastructures[2] (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.[3]

In this light, the Eurosystem, in its capacity as TARGET system operator, has developed a set of requirements addressing information security and cyber resilience[4] risks with which currently all RTGS DCA holders and Ancillary Systems (critical and non-critical participants)[5] 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

---

1 The "Information guide for TARGET users" (hereinafter Infoguide) defines TARGET users (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. This suggests that the terms "participant" and "user" can be used interchangeably for the purpose of this note.

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

3 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.

4 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.

5 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.

such access by 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 users. All RTGS DCA holders and Ancillary Systems[6] have to self-certify their level of compliance with the requirements specified in the following section.

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).

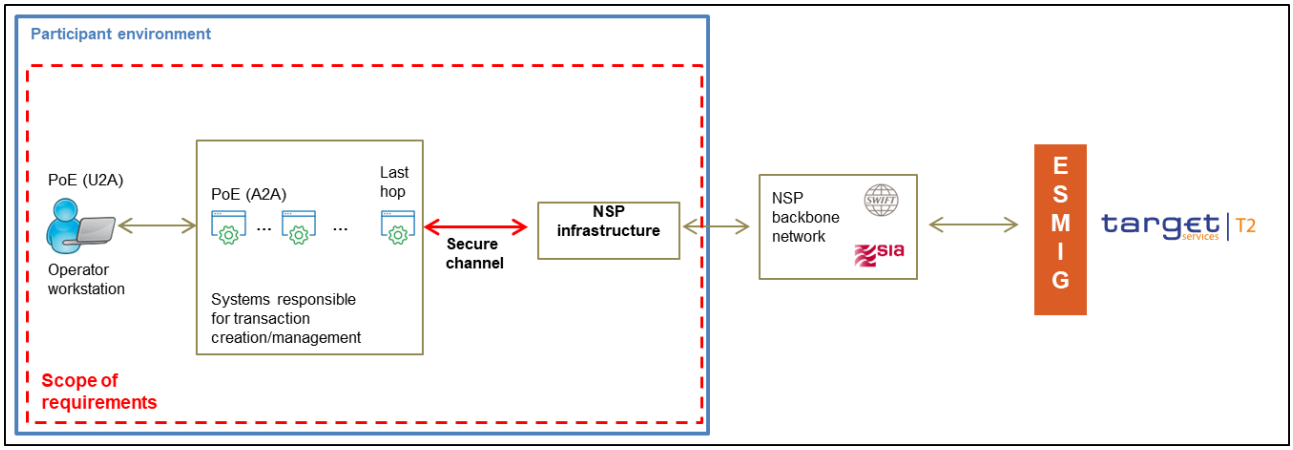
It is up to the individual organisations to assess whether all or only a subset of the security requirements is applicable to them. It should also be noted that the wording of the requirements references the ISO 27000/2018(en) Vocabulary.

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.

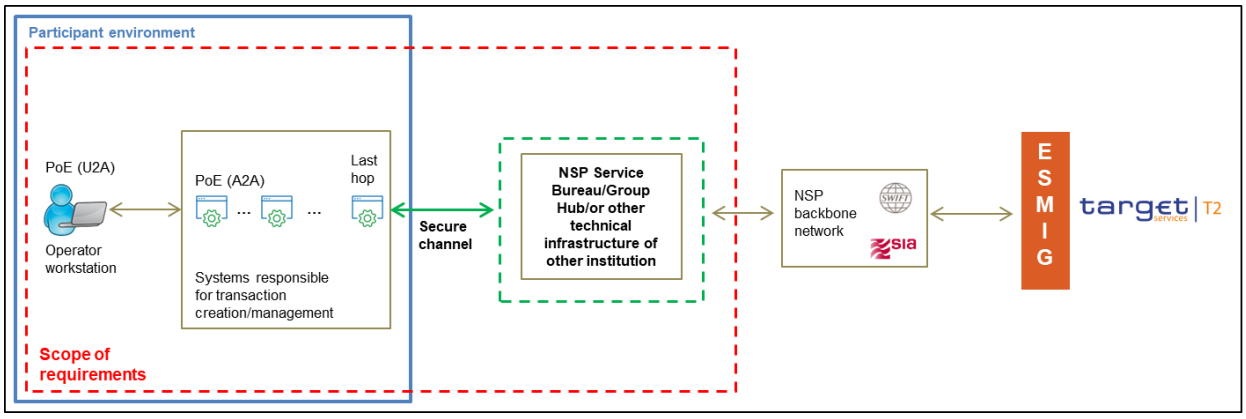
[6] All the ancillary systems have to self-certify their level of compliance with the requirements specified in this document regardless of the adopted TARGET accounts.



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[7]. 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.

[7] 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.

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 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[8]) 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[9] 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.

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.

---

8 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.

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

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[10] 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.

[10] 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.

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.

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.[11]

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

[11] 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.

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.

Signatory

The self-certification statement should be signed by a C-Level executive[12] 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.

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[13] 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

[12] 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).

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

Eurosystem in its capacity as TARGET system operator.

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.

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:

(i) 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.

(ii) 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''.

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[14])

	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	☐	☐	☐
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			

[14] 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.

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	