

17 December 2021

## **Action plan to address recommendations following incidents affecting TARGET Services in 2020**

In 2020 TARGET Services encountered a number of major incidents affecting in particular TARGET2 and TARGET2 Securities (T2S). Owing to the frequency of the incidents as well as their relevance, the ECB announced the launch of an [independent review](#) in November 2020 in order to draw all possible lessons from these incidents and properly address them.

Deloitte GmbH (“Deloitte”) was appointed on 21 December 2020 to conduct this review. On 28 July 2021 the ECB [announced](#) the publication of the report presenting the results of [Deloitte’s independent review](#) and the [Eurosystem response](#) in which it accepted Deloitte’s general conclusions and recommendations made in the review and committed to decisively implement them as soon as possible.

The Eurosystem has prepared this action plan to address Deloitte’s recommendations. The action plan also includes recommendations issued by the Eurosystem oversight function and the Internal Audit Committee in relation to the TARGET Services incidents in 2020. This approach provides a solid basis for addressing all recommendations related to the 2020 incidents in a comprehensive and complete manner.

Measures addressing several recommendations have already been agreed or implemented. For some recommendations, market participants have also been involved to ensure that their views are well understood and can be taken into account. For that purpose, dedicated sessions were organised with the Advisory Group on Market Infrastructures for Payments (AMI-Pay), the Advisory Group on Market Infrastructures for Securities and Collateral (AMI-SeCo) and the CSD Steering Group (CSG). The ECB will update these groups regularly on the progress of implementation of the action plan until its completion.

The action plan, a summary of which can be found below, has been structured according to the six workstreams of the Deloitte review, i.e. (I) Change and Release Management; (II) Business Continuity Management; (III) Failover and recovery tests; (IV) Communication protocols; (V) Governance; and (VI) Data centre and IT operations.

## **Workstream I: Change and Release Management**

In response to the recommendations received from Deloitte, as well as from the Eurosystem oversight function and the Internal Audit Committee, the current change management processes will be thoroughly reviewed. The review will encompass all phases of Change and Release Management. As regards the recommendations related to the technical implementation of changes, the applicable procedures will be standardised – from the drafting of the change to the phases of implementation, deployment and testing. The revised change management process will also encompass security assessments and dedicated risk analyses aiming at minimising disruptions to business processes. All changes scheduled outside the maintenance window are already required to be formally approved at the highest level by means of a letter of authorisation, and this will be reflected in the relevant documentation. The service management processes will also be recast based on ITIL 2011 V3 (together with some elements of the ITIL 4 framework) and will be subject to a regular revision process in line with continual service improvement. The completion of this review phase is scheduled for the second quarter of 2022, ahead of the go-live of the T2-T2S consolidation project. In parallel, in order to maintain the documentation of the processes, a common document management system will be implemented by the first quarter of 2022 which will centralise document sharing and data storage among the 4CB<sup>1</sup>.

Furthermore, the change deployment management tool, which follows the whole lifecycle of a technical change, will be reviewed by the second quarter of 2022 to ensure full consistency with the process requirements, e.g. mandatory roll-back checklist, respect of the scheduled installation time, change execution time. Improving change and release management will also entail a transversal enhancement of the 4CB governance and processes. A new process framework (based on ITIL V3 principles) will define common process architectures and align interfaces among the 4CB. A new non-functional change management process will also be implemented by the second quarter of 2022. In addition, a new transversal governance framework, which will be established by the fourth quarter of 2022, will set out the 4CB obligations, organisational structures and responsibilities in detail.

The recommendation to enhance the system resilience in the event of incidents at network level could be carried out by establishing a test environment for the network (4CB-Net NG). The 4CB will conduct a comprehensive analysis on the benefits of establishing a dedicated test environment with a view to improving the overall network resilience and availability.

Already implemented actions include strengthening the local technical change management with training sessions offered to external staff and ensuring strict application of the instructions included with the relevant changes. In addition, unsupervised work in secure areas is avoided by following a well-defined process that governs access to such areas.

---

<sup>1</sup> The TARGET Services are operated by the four service-providing national central banks (the “4CB”): Deutsche Bundesbank, Banque de France, Banco de España and Banca d'Italia.

## **Workstream II: Business Continuity Management**

With regard to the area of Business Continuity Management (BCM), a new technical procedure for activating the Enhanced Contingency Solution (ECONS) was implemented by the 4CB in the fourth quarter of 2021 and included in the relevant processes and testing activities. The 4CB have also ensured that operational staff are fully trained and knowledgeable about the ECONS activation procedures in all situations. The decision-making processes and the procedures for handling major incidents will also be reviewed and updated by the first quarter of 2022 in order to manage incidents more effectively and efficiently while limiting the downtime to the two-hour Recovery Time Objective (RTO). The documentation will include inter alia a separate document for crisis managers, which will provide general recommendations as well as concrete suggestions as to how to approach specific scenarios, drawing lessons from past incidents. It will serve as training material for newly appointed crisis managers as well as support material during crisis managers' calls. In this review, further clarification will also be introduced on the detailed steps to be followed when testing the different business continuity and contingency scenarios. By the end of 2022 the BCM framework will also be reviewed in a holistic manner and according to international standards and best practices to ensure that the related processes are in place and properly documented. Information security and cyber security aspects will be defined and integrated into the BCM and the IT Service Continuity Management (ITSCM) processes. This exercise will, in addition, include a cartography of all the current processes, and a complete review of the Business Impact Analysis (BIA) and the Business Continuity Plan (BCP) with a view to assessing them at least once a year thereafter, for instance on the occasion of major releases. The regular review of the BIA and BCP will also take into account the interfaces with other processes (e.g. from crisis management to BCM, ITSCM), the specific roles and responsibilities of the stakeholders involved, the related detailed process steps and the enhancement of the testing scenarios.

## **Workstream III: Failover and recovery tests**

While failover and recovery tests are already taking place for all TARGET Services on a regular basis, the documentation for the relevant processes, policies and procedures should be enhanced to better define the roles and responsibilities of the different actors in the planning of these tests, as well as during their execution and reporting the outcome. The technical documentation supporting the operational recovery tests and the test calendar have already been amended. Further improvements are planned to be in place by the first quarter of 2022, in particular as regards the frequency of intra-region and inter-region failover tests and the fine-tuning of the Business Continuity Plan, which would clarify the period after which a failover will be considered in the event of an incident. The feasibility of operating the TARGET Services for an entire week from the secondary site will also be assessed by the third quarter of 2022.

With regard to improvement of contingency procedures testing, the operational documentation will be updated by the last quarter of 2021 to require all TARGET2 central banks to check on a monthly basis their technical ability to connect to the Enhanced Contingency Solution (ECONS) and to the contingency network. The relevant documentation will also be updated by the first quarter of 2022 such that all

TARGET2 central banks will have to carry out transactions in the test environment at least every six months and report the outcome of the test to the TARGET Coordinator.

Furthermore, by the first quarter of 2022, an overarching document will be prepared for TARGET2 and T2S outlining all three levels of operational tests, i.e. those performed by the 4CB, by the TARGET2 central banks and by participants. The document will describe, in a holistic way, the respective processes to ensure the effectiveness of the development, execution and assessment of operational tests. A revision of the legacy testing scenarios will also be part of this exercise, while a new document management process will be designed to ensure that the processes are regularly reviewed.

The operational documentation will be improved to describe more precisely what is expected from participants during intra-region and inter-region failovers as well as during long-lasting incidents. Participants will be given opportunities to train their operational staff and to familiarise themselves with the procedures during simulation exercises, which will be organised regularly once the new consolidated platform has gone live.

Finally, from the second quarter of 2022 onwards, all failover tests will be reported using the same template irrespective of the TARGET Service affected and the testing of the IT Service Continuity procedures will also be reviewed by the end of 2022.

#### **Workstream IV: Communication protocols**

The external communication protocols have already been improved following discussions with market participants held in February 2021. It is now, for example, easier for participants to access the RSS-feed notification service, and the TARGET Services section of the ECB website has been streamlined to show the operational status of the three services (TARGET2, T2S and TIPS) clearly on a single page along with a link to past communications (historical overview). Further improvements are planned for 2022. The service used to inform participants about incidents affecting TARGET Services, which currently uses RSS feeds, will be migrated to a new technology that is more user-friendly and more flexible. Crisis communication procedures will also be modified and will allow the Eurosystem crisis managers to establish direct contact with key participants to ensure that the communication during major outages is adequately addressing participants' needs. For TARGET2, this group will be composed of the most critical institutions, designated in accordance with a methodology that has already been in place for several years. The T2S governance has also been invited to consider the most adequate composition for an equivalent group of T2S users. The opportunity to merge those two groups in the medium term will also be assessed.

The internal Eurosystem procedures for incident management will be improved. TARGET Services crisis managers will be reminded about the necessity to comply with the Recovery Time Objective (RTO) defined for each TARGET Service and, in the event of an incident, consider as one of their first possible actions the activation of the available contingency tools (Enhanced Contingency Solution – ECONS). The TARGET2 central banks and the central securities depositories (CSDs) will align their communications on operational incidents with the updates agreed at Eurosystem level and published on the ECB website. Last,

each incident requiring the involvement of crisis managers will be the subject of an ex-post assessment with the objective to identify and implement all lessons learned. These changes will be implemented at the latest in the first quarter of 2022.

### **Workstream V: Governance**

Work is being launched to identify ways to reduce the overall organisational complexity of TARGET Services and to improve the effectiveness of its governance.

The groups that may be dismantled once the migration to the T2-T2S consolidated platform is completed will be identified by the second quarter of 2022. The outcome of this review will also be used to set up a framework to ensure that the mandate of each committee and each group is kept up to date, with a review at least every two years, and that the membership lists are well-defined.

In addition, a Eurosystem Task Force will be established to “perform a full organisational review covering relevant good governance principles, all involved parties and levels with the goal to formulate an updated target operating model, as well as addressing the current and future organisational, resource and governance needs”<sup>2</sup>. This Task Force, which will be supported by external consultants, will be invited to report to the ECB decision-making bodies with concrete proposals by the second quarter of 2022. Based on the Task Force’s proposals, it will also be considered whether responsibility for documents such as the Manual of Operations for TARGET2 and T2S, which have both governance and operational content, could be reallocated to an appropriate operational level. The revised governance structure should ideally take effect after the scheduled go-live of the European Collateral Management System (ECMS) in November 2023. As part of the governance review, an inventory of legal documents will be created, giving a central and up-to-date overview of the relevant legal documentation in place.

In addition, full implementation of the second line of defence is envisaged by the last quarter of 2021. The TARGET Services Risk Management Framework will ensure that specific criteria for the necessary independence, transparency and information sharing and participation in decision-making are implemented in line with the expectations set out in Annex 1 of the TARGET2 Guideline (ECB/2012/27).<sup>3</sup>

### **Workstream VI: Data centre and IT operations**

To prevent the occurrence of incidents as far as possible and reduce their impact, the existing IT-related structures, processes and procedures will be enhanced and strengthened.

Several measures will focus on developing the Technical Monitor facility, which has been identified as the most suitable instrument for a timely and accurate detection of adverse factors that could hamper or even disrupt the TARGET Services normal operations. The measures envisage integrating the Technical Monitor with other tools/processes, along with drafting additional checklists for managing alerts in view of the go-

---

<sup>2</sup> See [Deloitte’s independent review](#)

<sup>3</sup> Guideline of the European Central Bank of 5 December 2012 on a Trans-European Automated Real-time Gross settlement Express Transfer system (TARGET2) (ECB/2012/27) (OJ L 30, 30.1.2013, p. 1).

live of the T2-T2S consolidation project in the fourth quarter of 2022. A gap analysis will also be performed by the first quarter of 2022 to review the current checklists and identify the additional ones necessary.

To ensure continuous availability of the monitoring tools, a study was carried out after the incident of 23 October 2020 with the aim of extending accessibility to the domestic infrastructures of the alternate region in the event of loss of connectivity in one region. In addition, by the last quarter of 2022, increased auditability of the Technical Monitor will be possible, and the retention policy will be reviewed accordingly.

With regard to the management of recurring incidents, identified issues will be better documented in internal data repositories and guidelines as well as in the problem management process by the second quarter of 2022. From a security standpoint, the relevant documentation will be updated by the second quarter of 2022 to clarify the rules related to the TARGET Services-providing organisation's security requirements taking into account the TARGET2/T2S security requirements and controls (SRC) dealing with third-party management. By the fourth quarter of 2022, an overarching guideline covering the third parties that have access to TARGET2 and/or T2S information should be in place.

As for the IT inventories relevant for TARGET Services (hardware and software), a new state-of-the-art Configuration Management Database (CMDB) is in its procurement phase and the related TARGET2/T2S Asset and Configuration Management process, already in the review phase, is scheduled to be completed in the second quarter of 2022, prior to the go-live of the T2-T2S consolidation project. The new CMDB will ensure that asset owners are clearly identified, as required in the relevant documentation, which will also be reviewed.

From a change-management perspective, the current processes describing the release upgrades will be reviewed by the third quarter of 2022, and the impact on the internal control system will also be assessed before deploying the upgrade in the different environments.

From an infrastructure perspective, a wide range of actions is underway to ensure that all market infrastructures have adequate resources to maximise their activities and production output under any conditions in the short, medium and long-term. An integrated system management platform will be provided within the T2-T2S consolidation project, with the aim of managing the numerous virtualised open system servers providing critical services for back-end applications. The study and procurement phases are planned to be finished by the fourth quarter of 2021, while their implementation is planned for the fourth quarter of 2022.

Finally, the recruitment process at the 4CB, which encountered difficulties in recruiting new staff owing to the outbreak of the coronavirus (COVID-19) pandemic, has started again and aims to ensure that there is an adequate number of qualified staff across all functions of the 4CB, with a special focus on day-to-day operations.