

Hold harmless agreement

By clicking on the button “I accept the conditions of access”, you (third party) agree to the following terms and conditions to the benefit of Deloitte GmbH Wirtschaftsprüfungsgesellschaft:

1. Our engagement was performed solely for our client European Central Bank and not with regard to possible interests of any third parties.
2. We do not assume any responsibility towards third parties as to the completeness and accuracy of our report and its suitability and sufficiency for the purposes of any third party. It is solely the responsibility of third parties to augment or verify the report through its own examinations. Should any third party decide to rely upon the report, it does so entirely and solely at its own risk.
3. Our liability towards any third party in connection with the disclosure of the report is excluded. Third party agrees that we are not liable towards them in contract (particular information contract (*Auskunftsvertrag*)), in quasi-contract, or in any other way obliged to compensate loss, damages or costs of any kind (except for damages arising from the injury of life, body or health) which are caused by the reliance of third party on the report. Our liability for willful misconduct (*Vorsatz*) remains unaffected.
4. Third party will treat the information strictly confidential except where information has to be disclosed by law, regulation or legal or regulatory order.

Document accessibility notice

Please note that in certain circumstances this document may not fully be accessed when opened via a mobile device. This will depend on the used mobile operating system, e.g. Android or iOS, and installed application to open the document. The document can fully be accessed via devices that use operating systems like Windows or macOS.

European Central Bank

Report on the external review of TARGET Services in the context of the incidents in March, May, August, October, and November 2020

This document is an abridged excerpt from our report on the external review of TARGET Services in the context of the incidents in March, May, August, October, and November 2020. The European Central Bank has decided, for reasons of information security and client-specific detailed information, to abridge and redact parts of the report. The initiation and responsibility for the abridgement and redaction of the sections lies with the European Central Bank. Redactions are indicated in the outline and in the text via [REDACTED].

We accept no responsibility towards third parties that the information in this abridged excerpt from the report is correct, complete, and suitable or sufficient for their purposes. It is solely the responsibility of the third parties to expand or verify the information through their own investigations. If third parties decide to rely on the information, they do so entirely at their own risk. The provision of the information contained in this document is not deemed to be an offer for conclusion of a contract to provide information or for any other contractual or quasi-contractual relationship.

This abridged excerpt from the report may only be read after a hold harmless agreement has been accepted.

Table of Contents		Page
1	Scope of the review	3
2	Executive summary	7
3	Overview of the TARGET Services and description of the incidents	10
3.1	Introduction	10
3.2	TARGET Services	10
3.3	Incident on 16 March 2020	12
3.4	Incident on 25 May 2020	13
3.5	Incident on 11 August 2020	13
3.6	Incident on 23 October 2020	14
3.7	Incident on 13 November 2020	15
4	Review procedures performed, findings, and recommendations	16
4.1	Change and release management	16
4.1.1	Review procedures performed and applicable review criteria	16
4.1.2	Process description	17
4.1.3	Findings	17
4.1.4	Recommendations	18
4.2	Business Continuity Model and approach	19
4.2.1	Review procedures performed and review criteria applied	19
4.2.2	Process description	19
4.2.3	Findings	20
4.2.4	Recommendations	21
4.3	Fail-over and recovery tests	21
4.3.1	Review procedures performed and review criteria applied	21
4.3.2	Process description	22
4.3.3	Findings	23
4.3.4	Recommendations	24
4.4	Communication protocols	24
4.4.1	Review procedures performed and review criteria applied	24
4.4.2	Process description	25
4.4.3	Findings	26
4.4.4	Recommendations	27
4.5	Governance	27
4.5.1	Review procedures performed and review criteria applied	27
4.5.2	Process description	28
4.5.3	Findings	28
4.5.4	Recommendations	29

4.6	Data centre and IT operations	29
4.6.1	Review procedures performed and review criteria applied	29
4.6.2	Process description	30
4.6.3	Findings	31
4.6.4	Recommendations	32
5	Practitioner's conclusion	34
	Appendix A: List of abbreviations	35

1 Scope of the review

1 By order dated 21 December 2020, the executive management of the

**European Central Bank,
Frankfurt am Main**

– hereinafter also referred to as "ECB" for short –

engaged us to review the backgrounds and causes of the incidents on 16 March 2020, 25 May 2020, 11 August 2020, 23 October 2020, and 13 November 2020 in relation to the TARGET Services regarding the following topics:

- Phase I – Planning, preparation, and initial analysis of root causes of the incidents relevant for the review: In the first phase, the initial work sessions were held with those responsible for the relevant processes (process owners), applications, and underlying infrastructure to get an understanding of the overall situation of the incidents that occurred in 2020 which were in scope for this review. This phase included the review of the initial documents on the individual incidents provided to us, and to structure and document the review procedures for the following phase.
- Phase II – Deep dives root cause analysis of the incidents and initial analysis of the related as-is processes: During the second phase, the review and analysis of the existing and additionally provided documentation was continued. This phase included deep dives on the root cause analysis of the incidents and the initial analyses on the as-is processes related to the incidents.
- Phase III – Deep dive as-is processes, design and implementation as well as operating effectiveness testing, derivation of findings and recommendations: In the third phase, we performed deep dives on the as-is processes relevant for the incidents via walk-throughs with relevant personnel and reviewed additionally requested documents. We performed tests of design and implementation, as well as tests of operating effectiveness within the work streams for our review conclusions. This phase included drawing more general lessons and proposing recommendations for improvements in the following areas, reflecting the functional and technical interdependencies as well as between the TARGET Services:
 - **Work stream I. Change & release management:** The efficiency and effectiveness of the change and release management procedures applicable to functional and infrastructural changes, including the deployed test protocols.
 - **Work stream II. Business Continuity Management:** The robustness and adequacy of the TARGET2, TIPS and T2S business continuity model and approach. The analysis included an assessment of the appropriateness of the structures and processes as well as measures deployed to monitor the infrastructures, to detect and to mitigate major incidents and crises. This comprised an assessment of the deployed resources (number and qualifications) as well as management/operational structures within the different TARGET2, TIPS and T2S operations' groups and teams within the infrastructure providing national central banks as well as in the ECB.

- **Work stream III. Fail-over and recovery tests:** The adequacy and effectiveness of the regularly performed intra- and inter-regional fail-over and recovery tests. This comprised, but was not limited to, an assessment of the intra- and inter-regional fail over and recovery tests, including the identification of any potential single point of failure in these processes, an assessment of the implemented testing protocols as well as preparedness and training of TARGET2, TIPS and T2S clients.
 - **Work stream IV. Communication protocols:** The deployed communication protocols for
 - (1) Eurosystem-internal communication (1.a. within Level3 governance structure – service-providing national central banks and ECB – as well as 1.b. between Level3 and Level2 of the governance structure) as well as
 - (2) Communication with the TARGET2, TIPS, T2S clients including e.g., the CSDs service desks within the national central banks, central clearing counterparties (CCPs).
 - **Work stream V. Governance:** Efficiency of the governance (with a focus on the timeliness and appropriateness of the information provided and the decision-making processes) to ensure a smooth operation and effective risk management of TARGET2, TIPS, T2S.
- 2 After the conclusion of the second phase, it was decided to expand the external review on 19 February 2021 to include the following topic:
- **Work stream VI. Data Centre & IT Operations:** Review and evaluation of the efficiency and effectiveness of the IT operations procedures across work streams I to V. The additional work stream evaluated the activities for the operation and maintenance of the IT systems (amongst others hardware and software) used within the TARGET2, TIPS and T2S services. This included various service management processes such as change, release, and access processes, test procedures, IT-related business continuity approaches, and IT governance structures.
- 3 Our review covered the structural and procedural organisation as well as the IT systems of the TARGET Services that are closely related to the aforementioned incidents. The external review did not cover the regulatory and internal control system (ICS) related processes or the IT systems that were not directly affected by the aforementioned incidents.
- 4 We have aligned our review procedures, in particular our enquiries, evaluations, and analyses, with the auditing standard "International Standard on Assurance Engagements (ISAE) No. 3000 (Revised): Assurance Engagements Other than Audits or Reviews of Historical Financial Information". The choice of review work is subject to the practitioner's professional judgment.

5 In addition, we have based our further review procedures and our assessment of the regular processes and measures on the following industry standards and guidelines (as far as reasonable and applicable) as a benchmark for the assessment of the review results:

- ECB specific regulation and guidance, such as:
 - ECB Regulation on oversight requirements for systemically important payment systems (SIPS Regulation), amended in 2017
 - Cyber resilience oversight expectations for financial market infrastructures (CROE)
 - Business continuity oversight expectations for systemically important payment systems (SIPS)
- CPMI-IOSCO Principles for financial market infrastructures (CPMI Papers No. 101) and associated CPMI-IOSCO guidance documents, such as:
 - Guidance on cyber resilience for financial market infrastructures (CPMI Papers No. 146)
 - Application of the "Principles for financial market infrastructures" to central bank FMIIs (CPMI Papers No. 130)
 - Principles for financial market infrastructures: Assessment methodology for the oversight expectations applicable to critical service providers (CPMI Papers No. 123)
 - Principles for financial market infrastructures: disclosure framework and assessment methodology (CPMI Papers No. 106)
- European Banking Authority (EBA) Guidelines, such as:
 - Guidelines on ICT and security risk management (EBA/GL/2019/04)
 - Guidelines on outsourcing arrangements (EBA/GL/2019/02)
 - Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2017/11)
- generally accepted industry standards, such as:
 - ISO/IEC 20000 IT service management
 - ISO 22301 business continuity management systems
 - ISO/IEC 27001/2 information security management systems
 - ISO/IEC 27005 information security risk management
 - ISO/IEC 27031 information and communications technology readiness for business continuity
 - ISO 31000 risk management guidelines
 - ITIL v3

6 In selecting and carrying out our review, we have chosen a risk-based approach to assess the processes and measures introduced. We obtained our results based on structural and functional reviews, as well as on testimonial review procedures. The review was conducted on the basis of information provided by employees involved in the matter and submitted documents, including corresponding documentation and process descriptions. In doing so, we retraced facts, validated information obtained by testing random samples and used industry-specific key figures for the review. We received clarifications and evidence, the required documents, and the necessary support in the performance of our work to the extent requested. We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our conclusion.

- 7 We want to emphasize, that due to the nature of a review, there are always certain inherent limitations regarding the conclusion that can be drawn from the results of our review. This includes, inter alia, that it is generally impossible to ensure that complex processes, systems, tooling or other such structures are completely free from error or inadequacies. Additionally, we would like to call attention to the fact that this review is not suitable for the provision of general compliance with the frameworks and standards mentioned above. These inherent limitations of the review need to be considered when using our report.
- 8 Our audit firm applies the Quality Assurance Standard: Quality Assurance Requirements in Audit Practices (IDW QS 1) promulgated by the Institut der Wirtschaftsprüfer (IDW). We have fulfilled the professional responsibilities in accordance with the German Public Auditor Act (WPO) and the Professional Code of Conduct for German Public Auditors and Sworn Auditors (BS WP/vBP) including the requirements on independence.
- 9 This report is based on the review results obtained during the period from 28 December 2020 to 26 March 2021. We conducted the review predominantly remotely.
- 10 ECB's management has provided us with a representation letter in writing dated 1 June 2021. Thereafter, instructions have been issued to provide us with all documents and information relating to the scope of the review to be examined in full.
- 11 The results of the report were presented and aligned in several meetings with the audited entities as well as the representatives of the Market Infrastructure Board (MIB) as well as the service-providing national central banks.
- 12 This report is intended exclusively for the executive management of the European Central Bank, Frankfurt am Main, and may not be passed on to third parties or used by third parties without our prior consent. We do not assume any responsibility towards third parties in this respect.
- 13 We issue this report in reference to the engagement agreement concluded with ECB. Our responsibility is solely to the European Central Bank, Frankfurt am Main, and our liability is limited in accordance with the engagement agreement dated 21 December 2020. By taking note of and using the information contained in this report, each recipient confirms that they have taken note of the provisions made therein (explicitly the limitation of liability for negligence to EUR 4 million in No. 9 of the IDW-AAB) and acknowledges their validity in relation to us.

2 Executive summary

- 15 In March, May, August, October, and November 2020 several major information technology (IT) related incidents occurred in functional and technical processes and infrastructures, which affected the payment transactions and securities processing of the TARGET Services under the responsibility of ECB and the service-providing national central banks (NCBs: Deutsche Bundesbank, Banco de España, Banque de France, and Banca d'Italia).
- 16 Two services were involved in the incidents, TARGET2 and TARGET2-Securities (T2S). TARGET2 is a real-time gross settlement service (RTGS) for payment processing, T2S is a securities settlement system.
- 17 For a more detailed description of the technical background and the consequences of the incidents, we refer to section 3 of this report.
- 18 After carrying out their root cause analyses, the management of the TARGET Services took various measures to address identified weaknesses in a timely manner. At the time of our review (28 December 2020 to 26 March 2021), these measures were either designed and planned, or in the process of being implemented. However, we identified a total of 40 findings. Of those, 17 findings are categorised with a high, 17 with a medium, and 6 with low severity rating. Based on our findings, further measures have already been initiated.
- 19 We did not identify any individual finding with a “very high” severity rating¹. We noted findings with a “high” severity rating in the areas of change management, business continuity management, fail-over and recovery testing, communication protocols, governance, as well as in data centre and IT operations.
- 20 Based on the detailed findings, we identified six major overarching issues. These overarching issues either directly or indirectly contributed to the occurrence of the incidents or had an impact on the incidents’ severity during their resolution.
- 21 We concluded that two overarching issues concerning change management and testing, as well as communication had a more direct and closer relationship to the incidents and their resolution.
- 22 The first overarching issue concerns deficiencies related to the planning and implementation of changes. We noted that the change-planning process does not include a comprehensive risk-based assessment and planning approach with defined minimum information requirements as well as objective criteria for decision-making. Additionally, the test management approach – based on an infrastructure staging concept – does not appropriately reflect the scope, complexity, potential service interruptions, timely recoverability, and underlying risk of a

¹ We categorised our findings according to the risk rating procedure of the ECB, which considers the impact on business objectives and reputation as well as the likelihood, i.e. frequency of risk event occurrence. Likelihood includes qualitative criteria such as complexity, system resilience, skill sets or awareness. The combination of impact and likelihood determines the overall severity level of our findings. These severity ratings are “very high”, “high”, “medium” and “low”.

change to derive an adequate extent of testing. We provide more detailed information in sections 4.1, 4.2, and 4.6.

- 23 Communication during incident resolution is the second overarching issue we identified. Due to the limited usability of the ECB website, as well as unclear roles and responsibilities during the incident resolution, market participants perceived the information availability as inadequate. In addition, we noted that NCBs provide information regarding incident resolution via their respective websites, which differ from the information provided by ECB. Finally, market participants expressed a need for a more bidirectional information exchange to provide their feedback towards ECB. We provide more detailed information in section 4.4.
- 24 Separate from the above described two directly affected issues, we have identified four additional overarching issues that had – due to their nature – an indirect, contributory effect on the incidents. These issues are regarding continuous improvement processes, documentation, the internal control system, as well as governance, and will be explained in the following.
- 25 Within the mentioned different processes, we noted a third overarching issue: The lack of a structured continuous improvement process or a formal process to incorporate lessons learned. While lessons learned were identified and documented in the incident reports, they were not necessarily incorporated into the affected processes in a timely manner. Also, results from fail-over and recovery testing were not used as input towards the improvement of existing processes. We provide more detailed information in sections 4.4 and 4.5.
- 26 The fourth overarching issue that we noted concerns the adequacy, consistency, and clarity of the documentation of processes, policies, and procedures. In part, documentation is not structured in a clear document hierarchy, but split into many separate documents, dependencies between the latter are partially unclear, references are not fully consistent, and the depth of the process description is at times insufficient. Also, in some critical areas, roles and responsibilities are not fully defined, terms and definitions are not consistent and complete. Additionally, we noted that the documentation review is not consistently performed leading to instances of out-of-date documentation. Technical documentation in form of a Configuration Management Database (CMDB) does not exist. We provide more detailed information in sections 4.1 to 4.6.
- 27 As a fifth overarching issue we identified shortcomings regarding an overarching internal control system. Various organisational, procedural, and technical controls have been installed throughout the service-providing central banks for operational processes including change and release management, business continuity management, fail-over and recovery tests, data centres and IT operations. We noted that these operational IT controls are sometimes not well-defined, especially regarding technical monitoring. In some cases, control evidence is not fully available. Moreover, we noted that existing controls are not linked to an overarching internal control system, managed by a central second line-of-defence (LoD) function with decision-making power for the TARGET system. We provide more detailed information in section 4.6.

- 28 Finally, the sixth overarching issue concerns governance. In our review, we noted that the TARGET Services governance structure relies heavily on an overly complex organisational structure including a large number of committees and working groups, while decision-making power is allocated only at high levels in the organisational structure, limiting responsiveness and speed of decision-making. Also, a second LoD, covering inter alia risk management and internal control has not yet been fully implemented. Current activities are mainly focused on information security and cyber resilience, while a new, comprehensive risk management framework is expected to be implemented in the summer of 2021. We provide more detailed information in section 4.5.
- 29 Besides the above described overarching issues, we have noted a significant issue regarding major limitations in fail-over procedures and testing in certain scenarios. We provide more detailed information in section 4.3.
- 30 We strongly recommend significantly improving certain aspects of TARGET Services:
- Implement risk assessments within relevant processes, especially in change management, and deciding criticality of processes and IT elements, in particular business impact analyses (see paragraphs 19 and 24);
 - Improve relevant processes, inter alia communications with external stakeholders and continuous improvement /incorporation of lessons learned (see paragraphs 20 and 22);
 - Improve documentation by inter alia introducing umbrella documents for complex processes, implementing a CMDB spanning all TARGET systems' IT elements and requiring more stringent documentation of roles and responsibilities (see paragraph 23);
 - Enhance organisational and governance structures, including implementing a common second LoD, responsible for implementing and running a comprehensive risk management and overarching internal control system spanning all platforms and services with adequate staffing (see paragraphs 24 and 25).

Detailed recommendations can be found in sections 4.1 to 4.6.

- 31 TARGET Services today have evolved considerably since the time their structures and governance were set up. New products, new groups of users, added processes and technologies result in additional requirements and challenges that need to be adequately addressed. Therefore, improvements based on our recommendations are necessary and should be addressed urgently. TARGET Services should be proactive about these developments and aim for meaningful improvements. We recommend performing 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 current and future organisational, resource, and governance needs.

3 Overview of the TARGET Services and description of the incidents

3.1 Introduction

32 In this section of the report, we provide a brief description of the TARGET Services and describe the relevant facts and issues leading up to the incidents, during the incidents themselves and because of the incidents. Any issues observed in our review of the incidents were further investigated within the work streams (see section 4).

3.2 TARGET Services

33 The TARGET Services are a number of post-trading services developed and operated by the Eurosystem, which ensure the free flow of cash, securities, and collaterals across Europe. The services, which are in scope of the external review of TARGET Services, are the RTGS system TARGET2, the TARGET Instant Payment Settlement (TIPS), and the European platform for securities settlement in central bank money T2S.

34 **TARGET2** is the real-time gross settlement system of the Eurosystem. The system is based on an integrated central technical infrastructure called the Single Shared Platform (SSP), which is run by the 3CB, Deutsche Bundesbank (BBk), Banque de France (BdF), and Banca d'Italia (BdI). It is the leading European platform for processing large-value payments and is used by both national central banks and commercial banks to process payments in Euro in real-time. National central banks and commercial banks can submit payment orders in Euro to TARGET2, where they are processed and settled in central bank money, i.e., money held in an account with a central bank.

35 **TIPS** is a harmonised and standardised pan-European service for the settlement of instant payments in central bank money. It enables payment service providers to offer fund transfers to their customers in real-time and around the clock, every day of the year. This means that individuals and firms can transfer money between each other within seconds, irrespective of the opening hours of their local bank. TIPS is built on a modern and advanced technical solution that was specifically developed for the purpose of settling instant payments. It is designed to secure an end-to-end processing time of ten seconds or less, support the expected large volumes of transactions and meet scalability requirements, secure availability around the clock without maintenance windows, and to enable a deployment process with no interruption in the service.

36 **T2S** is a platform for securities settlement in central bank money which is designed to support Central Security Depositories (CSDs) by providing core, borderless, and neutral settlement services. The platform is run by the 4CB, BBk, BdF, BdI, and Banco de España (BdE). The objective of T2S is to achieve harmonised and commoditised delivery-versus-payment settlement in central bank money in Euro, and also possibly other currencies, in substantially all securities in Europe. This is performed in a single technical platform integrated with the national central banks' real-time gross settlement systems for all participating currencies. The following figure shows a high-level architectural setup and operational responsibilities of the TARGET Services.

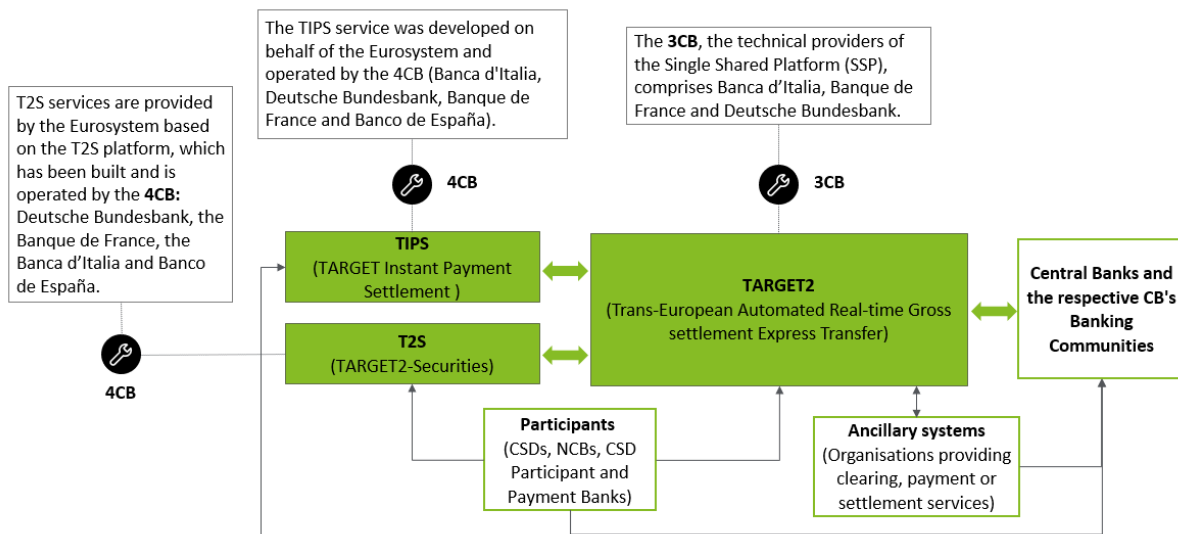
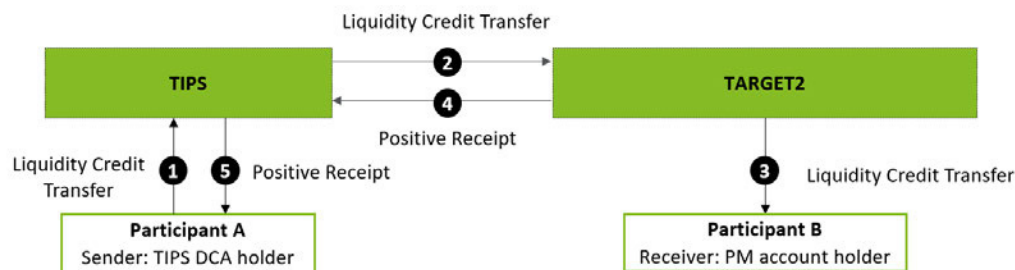


Figure 1: Architectural setup and operational responsibilities of TARGET Services

- 37 From a legal perspective, these platforms are (for cash settlement services) governed by the TARGET2 Guideline and (for securities settlement services) by two multilateral agreements, the T2S Framework Agreement (FA) with the CSDs and the Currency Participation Agreement (CPA) for the non-Euro currencies whose national central banks have agreed for these currencies to be a T2S settlement currency. The following figure shows the flow of information between the TARGET Services participants. The interconnection between the applications is based on an application-to-application approach (A2A) and is ensured by the respective interfaces, which mainly facilitates the exchange of liquidity.

Liquidity transfers from TIPS to TARGET2 (ISO 20022 message flows)



Liquidity transfers from T2S to TARGET2 (ISO 20022 message flows)

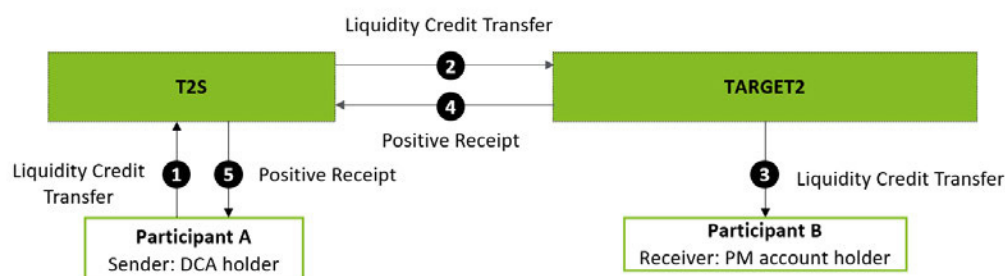


Figure 2: Information flow between participants of TARGET Services

3.3 Incident on 16 March 2020

- 38 On 16 March 2020 at 11:06 CET, the communication between the TARGET2 payment and accounting processing services systems (PAPSS) components in charge of the web applications (Web application server - WAS) and the internal messages exchange (Message Queue - MQ) was interrupted. The automatic restart of these components was not successful and hence some of the TARGET2 functionalities became unavailable. This in turn impacted the connection between the TARGET2 system and SWIFT. The system downtime was approximately two hours.
- 39 The root cause was connected to the introduction of a mandatory SWIFT security feature called local authentication (LAU), which provides internal identification mechanisms between the SWIFT appliance and the backend application. The SWIFT security feature was implemented in February 2020. Due to the high volumes experienced on 16 March, the configuration proved not to be adequately sized, which led to the interruption.
- 40 The incident had an impact on the availability of the TARGET2 Information Control Module (ICM), the processing of the SWIFT message types, the liquidity transfers between TARGET2 and T2S and TIPS, and the processing of application server files. This affected the settlement of customer, interbank, ancillary system and CLS related payments during the system downtime. Once the issue was resolved, cumulated settlement picked up again and then returned to a level in line with a normal business day.

3.4 Incident on 25 May 2020

- 41 On 25 May 2020, following a request of a customer to allow the settlement of an exceptional peak of instructions, a night-time-settlement (NTS) job got stuck during the running of a specific event in the T2S system due to lack of memory. This was the result of a combination of high volumes (740,000 transactions vs 340,000 transactions on average in 2019 and a maximum of 590,000 transactions during the COVID-19 peak period) and high cash concentration (almost 70,000 transactions debiting). The NTS job tried to allocate 53GB of memory when only 50GB were available. Because of this mismatch the NTS job terminated out of order. When the issue was identified and the allotted memory increased, the job restarted and completed orderly. Shortly thereafter and because of the high volumes and cash concentrations noted, the so-called Mathematical Optimisation Module (MOM) algorithm as part of a specific event reached its timeout and had to be aborted. The next operation of the event (Gross algorithm) was also not successful and terminated out of order. The system downtime was approximately twelve hours.
- 42 The root cause could be identified in the Gross algorithm that aborted due to the number of so-called “Indirect Use of Restrictions (UoR)” which exceeded the allowed number of 250. In such a case, the software generates a memory breach when reaching the limit of 250 connections. This high number of indirect UoR was reached because the MOM algorithm, which usually settles most of the transactions, ended up in a loop condition and could not be closed automatically when reaching its time limit. Therefore, the Gross algorithm was started as usual, but with a higher number of transactions, specifically more than 250 UoR.
- 43 The incident impacted the services provided by the T2S system in a way that updates to 22 cash balances and 1,835 securities positions were not applied due to the error whereas the associated postings were correctly updated. Due to these outdated cash balances and securities positions, some transactions settled which should not have been the case. Under normal circumstances, they would not have settled as there would not have been cash balances and securities positions in the accounts as expected.

3.5 Incident on 11 August 2020

- 44 On 11 August 2020, TARGET2 got disconnected from the network, becoming unreachable by the three service-providing NCBs and external users. After several unsuccessful attempts to restore the service in the primary site, the 3CB decided to proceed with the site recovery around 15:40 CET. The site recovery started at 15:45 CET and the system was then available at 16:43 CET. The traffic for the SWIFT message type FIN, which transmits financial information from one financial institution to another, was working, but it was not possible to reach the ICM neither via A2A nor via user-to-application (U2A) connections. Additionally, the connection with T2S was unavailable. The so-called store and forward traffic were not available upon opening the system and consequently the ancillary system interface. Internet Access was available at 16:58 CET. Nonetheless, the national central banks were able to connect to ICM via the contingency network at 18:15 CET. As a result, the crisis managers decided

to delay the settlement day procedures twice. The T2S settlement day was also delayed. The TARGET2 functionalities were progressively restored, the last impacted one was inherent to the Standing Facility refunds that took 18 hours to be fully recovered.

- 45 The investigations on the root cause revealed that an incorrect configuration of a data centre power supply component during a maintenance activity performed closely before the incident resulted in the loss of power to several IT systems including to the mainframe that hosts the TARGET2 production environment. When the intra-region fail-over was performed, the A2A traffic was not immediately available due to an incorrect configuration on the secondary site. The U2A access to the ICM via SWIFT was not available because of a missing firewall rule on one of the subsystems on the secondary site.
- 46 The incident impacted the services provided by the TARGET2 system that the processing and reception of payments, the processing of liquidity transfers from and to T2S and TIPS, the business day closing, and the change of the business day were delayed, respectively.

3.6 Incident on 23 October 2020

- 47 On 23 October 2020, the connection access to all TARGET2 applications as well as access to the ICM was lost on the primary site [REDACTED]. Also, all settlement services became unavailable to participating national central banks. This resulted in the loss of processing for payments, ancillary system transactions, internet access transactions and liquidity transfers from and to TIPS and T2S. The system downtime was approximately eleven hours.
- 48 The root cause of the TARGET2 incident was identified as a network issue. The switches in the so-called 4CBnet-NG network (private network interconnecting the Italian, German, French, and Spanish national central banks) are aggregated in couples, using the so-called [REDACTED], and maintain this aggregation and interaction between each other through a specific protocol [REDACTED]. A configuration parameter triggered a bug that created an instability, which caused the switches to lose each other, and eventually produced the domino effect on both sites of the [REDACTED] region. The configuration parameter applied on the 4CBnet-NG switches triggered the software bug which was known to the vendor's technical assistance centre since May 2020. The problem report describing this bug was neither described in the product manuals nor in the relevant release notes.
- 49 The incident impacted the services provided by the TARGET2 and T2S systems that a change of the business appointment, expected for 04:15 CET, took place at 05:20 CET. The incident in TARGET2 also had an impact on the other TARGET Services, in T2S, the intraday delivery versus payment (IDVP) cut-off was postponed until 21:30 CET. Start of the NTS had to be postponed to 06:00 CET on the following day. The impact for TIPS was limited to the delay in notifying TARGET2 of the trade date change.

3.7 Incident on 13 November 2020

- 50 On 13 November 2020, an incident occurred on the TARGET2 system in the evening that prevented the provision of liquidity in the T2S system. Only liquidity in Danish Krone (DKK) was injected into T2S and settled during that evening.
- 51 The root cause of the incident was a mismatch in the message-schema between TARGET2 and T2S. In preparatory activities for the release 14.0, two message-schema versions were installed in parallel. During the Change Coordination Meeting on Wednesday, 11 November 2020, a verbal misunderstanding between the involved entities occurred. Because of this misunderstanding, the message-schema change to the latest version on the TARGET2 system was applied prior to the business day change. This resulted in a mismatch between the TARGET2 and T2S message-schema versions.
- 52 The incident impacted the services provided by TARGET2 and the availability of liquidity from TARGET2 to T2S right before the T2S NTS.

4 Review procedures performed, findings, and recommendations

4.1 Change and release management

4.1.1 Review procedures performed and applicable review criteria

53 Regarding the area of change and release management, we have performed review activities to assess the appropriateness (design and implementation) of implemented change management processes. Our review procedures focussed on the change initiation by T2S Actors (which includes NCBs, European Central Bank (ECB), CSDs and Directly Connected Parties (DCPs)), by the National Central Banks in the context of TARGET2 and the 3/4CB in their respective roles as TARGET2 and T2S Operators, the change design, change implementation and change delivery on 3CB level for TARGET2, respectively on 4CB level for T2S in order to assess if the written policies and procedures define accountable roles and responsibilities, are up-to-date, cover proper risk measurements for assessing risks associated with a specific change or bundle of changes (release), define controls in order to manage changes depending on their risk classification and specify adequate documentation requirements for changes. In addition, we performed a test of operating effectiveness of the implemented change management processes based on a sample of implemented changes.

54 These review procedures included, amongst others, the following:

- Inquiries of employees responsible for change design, change implementation and change delivery on 3/4CB level
- Inquiries of employees responsible for infrastructure changes related to TARGET Services on BBk level
- Inspection of internal policies, processes and procedures related to change management
- Inspection of contracts that form the legal basis of the TARGET system
- Observation of how the change management process will be supported by tools
- Review of the implemented change management process based on drawn samples
- On-site visit of BBk's primary data centre
- Inspection of implemented security measures at BBk's primary data centre during the on-site visit

55 Our evaluation of the underlying subject matter is based on the general criteria as described, and on specific criteria suitable for assessment of the relevant change and release management processes:

- Information Technology Infrastructure Library version 3 (ITIL V3) published by Central Computing and Telecommunications Agency (CCTA)
- ISO/IEC 27002:2015 Information technology – Security techniques – Code of practice for information security controls (ISO/IEC 27002) published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

4.1.2 Process description

56 The Change and Release Management (CRM) process is designed to ensure consistent standards for proposing, assessing, scheduling, approving, and documenting functional change requests by TARGET2 and T2S participants that apply prior to the submission of approved functional changes to 3/4CB for building and implementing changes. The 3/4CB internal change management processes are designed to ensure consistent requirements for building, testing, and implementing functional and technical changes to TARGET2's and T2S' soft- and hardware as well as to the underlying infrastructure. Essential control measures include, among others, an assessment of proposed changes regarding their business impact, security impact, functional and technical impact, costs and risks, request and documentation of approvals, schedule of changes, and personnel planning. The change management and release management frameworks as well as the different process descriptions include definitions of accountabilities and responsibilities of the involved parties (NCBs, ECB, 3/4CB, Steering Committees), process steps, and task descriptions and roles.

4.1.3 Findings

57 Our review of the processes for change and release management identified weaknesses in the design and implementation on the process, policy, and procedural level as well as the operative effectiveness of these processes, policies, and procedures.

58 Regarding the overall design of the written policies and procedures for change management, we noted that the change and release management process for TARGET2 and T2S is comprised of a total of 13 documents covering processes, policies, and procedures for both level 2 (ECB) and level 3 (3/4CB). These 13 documents are enhanced by local processes and procedures for changes to the cooling and power supply of the data centres of BBk and Bdl. Next to this, we noted that TARGET2 and T2S have separate change and release management processes, policies and procedures that vary in detail and extent. An overarching umbrella document for change and release management that defines the hierarchy of the different processes, policies, and procedures and their dependencies does not exist and therefore the hierarchy and interaction of the processes, policies, and procedures are not comprehensible. In addition, some process descriptions on 3CB and 4CB level were last reviewed in 2007 (TARGET2) and 2015 (T2S) respectively, and therefore it is not ensured that the process descriptions are up to date.

59 Identified weaknesses in the design of the change and release management process concern a missing description of the risk assessment approach as well as appropriate test management. The assessment of risks associated with a specific change or a bundle of changes (release) lacks a definition of the information required to conduct an impact assessment, a description of objective criteria which serve as a foundation of the impact analysis, and process of the risk assessment. Next to this, mandatory risk mitigation measures, i.e. roll-back procedures, are not defined. With regard to test management, we noted that no objective criteria are defined to serve as a foundation for the decision on the scope and extent of required test activities. Finally, no sufficient methods are in place to assess the validity of technical test cases in comparison to the production environment.

60 With regard to the operating effectiveness of the change and release management we noted that changes were assessed with “no business impact” without the provision of information on the derivation of this result. Next to this, no test documentation was provided to validate the appropriateness of test cases and the appropriate test coverage for the introduced change. Additionally, we noted that changes were implemented during operational hours without considering the risks associated with the change. Furthermore, we noted that BBk classifies all changes to hardware, IT systems, and C/S databases, based on long-term experience, as a standard change with low risk independent of the risk determined by the defined risk assessment matrix, which also applies for changes to the power supply and cooling of BBk’s data centres for the hosting of TARGET Services.

61 We also noted that for network changes there is no functional test environment. Therefore, changes are applied directly to the production environment, without prior testing in a separate environment. Without testing, critical faults or failures may not be identified which can negatively impact operational availability and stability.

4.1.4 Recommendations

62 Based on the results of our review, we conclude that the number of process descriptions and procedures for change and release management on 3/4CB level should be reduced. Focus areas for the reduction are the sub processes change design, change implementation, and change delivery. Next to this, an umbrella document shall be created to define and document the hierarchy of the processes and documentation as well as their interaction to improve the transparency of the change and release management process. Furthermore, performed reviews shall be documented in a document history in order to ensure that process descriptions are up-to-date, even if no changes are necessary.

63 In order to ensure a uniform application of the risk assessments, the risk assessment approach for assessing risks associated with a specific change or a bundle of changes (release) shall be defined considering objective criteria. Depending on the assessed risk of a change or a bundle of changes mandatory risk mitigation measures shall be defined and taken into account in the approval process.

64 Additionally, objective criteria as well as risk mitigation measures considering the results of the risk assessment shall be defined for the implementation of changes during operational hours in order to avoid an interruption and unavailability of TARGET Services. Furthermore, the classification of technical changes as a standard change shall be re-designed by BBk in order to ensure that the risk associated with a change will be managed in an appropriate way.

65 Regarding the test management, objective criteria shall be defined to increase transparency for third parties on which basis it is decided whether changes require tests. In addition, the test documentation shall ensure that test results are reliable and that conducted tests are able to proof the behaviour of tested systems, modules or components in the test environment also apply to the production environment. For this reason, test cases shall cover unit, system, and integration tests, negative test scenarios in order to validate the correct handling and processing of errors by the system as well as end to end test cases.

4.2 Business Continuity Model and approach

4.2.1 Review procedures performed and review criteria applied

66 Regarding the area of Business Continuity Management, we have reviewed and assessed the procedures and controls for Business Continuity Management (BCM), including IT Service Continuity Management (ITSCM). The focus of our review related to the assessment of the appropriateness of the BCM / ITSCM guidelines including the assessment of the appropriateness of the process for the transition of the Business Impact Analysis (BIA) to the BCM. In addition, we checked the derivation of the maximum tolerable downtime (Recovery Time Objective - RTO) and the maximum tolerable data loss (Recovery Point Objective - RPO), the procedure for planning and controlling the test requirements, as well as the implementation of emergency tests on a random basis. To this end, we reviewed the internal specifications and documentation provided, conducted workshops and in-depth discussions with the specialist departments, and randomly checked the effectiveness of selected procedures.

67 These review procedures included, amongst others, the following:

- Inquiries of employees responsible for BCM and ITSCM at the ECB and 3CB/4CB
- Inspection of internal policies, processes and procedures related to BCM and ITSCM
- Review of the implemented BCM and ITSCM processes based on training documentation

68 Where the requirements of the ECB regarding the design of the Business Continuity Model and approach were not adequately designed, BCM/ITSCM best practices and principles were considered for the review. These best practices have been drawn in particular from:

- Business continuity oversight expectations for systemically important payment systems (SIPS), European Central Bank, 2006.
- ISO/IEC 27031:2011-03 - Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity
- ISO/TS 22317:2015-09 - Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)
- BS 11200:2014 - Crisis management – Guidance and good practice

4.2.2 Process description

69 The TARGET system covers both business continuity and IT service continuity for TARGET2 and T2S with its Business Continuity Management process, consisting of the Business Area Continuity Management (BACM) and ITSCM processes.

70 BCM is dedicated to the analysis and prevention of risks which, if materialised, could lead to a disruption of business processes. BCM strives to reduce the risk likelihood to an acceptable level and to develop measures

that will guarantee the resumption of business operations by a predefined deadline. To solve business interruptions quickly, appropriate corrective measures based on various interruption scenarios must be developed, tested, and documented. BACM serves the overarching process of BCM by ensuring that, even in the event of a disaster, all necessary business-area-related resources are available to resume business processes at a predetermined level. ITSCM defines the structure, control actions, and countermeasures to carry out to face disasters. Its aim is to guarantee the availability of IT services. It does so by supporting BCM, defining conditions for training and testing, minimising the duration of service interruptions, ensuring the agreed service levels for TARGET2 and T2S.

- 71 BCM measures can also be activated by the TARGET system's crisis management process in case the broader impacts of incidents and events exceed a pre-agreed severity threshold. The crisis management process can activate other management disciplines if necessary.

4.2.3 Findings

- 72 During the review, we identified key issues related to the BCM for TARGET2 and T2S in particular about the documentation of BCM, ITSCM and Crisis Management in an overarching umbrella document [REDACTED].
- 73 Regarding the documentation, we noted the lack of an overarching umbrella document which defines the interrelations and interfaces of BCM, ITSCM, Crisis Management, Contingency Management and non-IT emergency management. The review of the existing documents regarding BCM, ITSCM, Crisis Management and Contingency Management showed that these documents loosely fit together and are not designed based on best practices or international standards. We noted that inconsistencies between terms and definitions exists, relevant description of roles and responsibilities are lacking sufficient level of detail, regarding the different plans (ITSCM plan, Business Continuity Plan (BCP), crisis plan) significant details according to best practices and international standards were missing, proof for sufficient qualifications and trainings of the relevant personnel was not provided. Insufficient definitions and documents may lead to the risk that TARGET2 and T2S continuity is not managed as effectively and efficiently as the criticality of TARGET2 and T2S systems requires, due to an inconsistent and incoherent BCM approach. Furthermore, the risk exists that the implemented BCM measures are not effective due to an inappropriate training for relevant employees e.g. during testing and exercises.
- 74 With respect to the BIA, we noted a lack of a valid BIA for TARGET2 and T2S. The provided BIA was for T2S only and dated 17 April 2015, authored by ECB. We noted that this BIA was drafted before the go live of T2S. Afterwards, no updates were conducted even though this is recommended by best practices and international standards, and which is also necessary from a technical perspective to incorporate all changes that occurred since then. Furthermore, significant content of the BIA was missing. A complementary risk assessment was also missing. Due to the lack of a complete and updated BIA, a BCP as well as an IT Service Continuity Plan (ITSCP) was not provided. Lack of or outdated documentation bears the risk of insufficient BCM and ITSCM execution during service interruptions which might lead to further escalation of an incident or a crisis.

75

[REDACTED]

4.2.4 Recommendations

76

Taking a holistic view of the findings identified during the review of Business Continuity model and approach, we conclude that the overall concept of BCM, including ITSCM, Crisis Management, Contingency Management, and non-IT emergency management should be re-designed and internationally acknowledged best practices as well as relevant international standards should be the foundation of this re-design. This concept built on an overarching BCM framework must ensure a consistent and coherently aligned BCM approach regarding the processes and their governance for Incident Management, Contingency Management, BCM, ITSCM, Crisis Management, which also depict the interfaces to other processes (e.g. risk management). Next to this, we recommend defining specific roles and responsibilities for parties involved and the related detailed process steps.

77

Furthermore, we recommend establishing a BIA for TARGET2 and T2S according to international standards (e.g., ISO/TS 22317:2015) and performing a periodic review of TARGET2 and T2S BIAs according to the defined requirements. Similar to BIAs, also BCPs should be updated at least annually based on testing results, current threat intelligence, and lessons learned from previous events. Any changes in recovery objectives (including RTOs and RPOs) and/or changes in business functions, supporting processes, and information assets should also be considered, where relevant, as a basis for updating the BCPs.

78

[REDACTED]

4.3 Fail-over and recovery tests

4.3.1 Review procedures performed and review criteria applied

79

Regarding the area of fail-over and recovery tests, we reviewed and assessed the documented fail-over and recovery procedures and controls as provided in the respective documents. We focussed on the TARGET2 security

requirements and their controls, the TARGET2 and T2S Business Continuity Management, and IT Service Continuity Management Process. We also assessed the continuity plan handbook, the documented system architecture, and the 3CB/4CB Business Continuity Security guideline, as well as all provided IT Service Continuity, Business Continuity, and operationally related test calendars, plans, and reports for 2019 and 2020. To this end, we reviewed the internal specifications and documentation provided, conducted workshops and in-depth discussions with the specialist departments, and randomly checked the effectiveness of selected procedures.

80 These review procedures included, amongst others, the following:

- Inquiries of employees responsible for fail-over and recovery testing at the ECB and 3CB/4CB
- Inspection of internal policies, processes, and procedures related to fail-over and recovery testing
- Review of the relevant fail-over and recovery testing calendars

81 Our evaluation of the underlying subject matter is based on the general criteria as described, and on specific criteria suitable for assessment of fail-over and recovery testing:

- Business continuity oversight expectations for systemically important payment systems (SIPS), European Central Bank, 2006.
- ISO/IEC 27031:2011-03 - Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity
- ISO/TS 22317:2015-09 - Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)
- BS 11200:2014 - Crisis management – Guidance and good practice

4.3.2 Process description

82 The Business Service Continuity Management concept in the fail-over and recovery section provides the approach to providing continuous IT services and continuity management criteria in the business areas. BCM is dedicated to the analysis and prevention of risks which could lead to a disruption of business processes. The business continuity process is considered as a whole regarding both TARGET2 and T2S. An IT Service Continuity process is in place to minimise the probability and impact of a major IT service interruption in key business functions and processes. ITSCM ensures that the IT services along with the underlying infrastructures required for supporting basic business processes are available even in the event of an emergency. The objective of the BCM/ITSCM process is to determine the required resilience of the infrastructure, and to drive the development of disaster recovery and IT contingency plans. The processes also address the organisational structure for continuity management, covering the roles, tasks, and responsibilities of their management and customers. The ITSCM plans are based on a risk assessment of potential infrastructural impacts. Response and recovery requirements are defined in various documents. IT continuity plans and BCM plans are tested with a few exceptions on a regular basis to ensure that IT systems can be effectively recovered, and shortcomings are addressed. The process of preparation, documentation, reporting of test results and, according to the results, implementation of an action plan is defined. The actions are explicitly specified to be taken for the period when IT is recovering

and resuming. This includes activation and initiation of alternative sites, customer and stakeholder communication, and resumption procedures. In the case of a short continuity failure, major failure, or disaster, scenarios are defined to configure critical components in a fully redundant manner.

83 Apart from the BCM/ITSCM process, the process of preparation, execution, and following up on the operationally related tests is implemented as well. Some of these tests according to the test descriptions are also performed together with the CSDs/NCBs participation.

4.3.3 Findings

84 During our review of fail-over and recovery testing, we noted weaknesses regarding the documentation of processes, policies and procedures, roles and responsibilities of ECB during fail-over and recovery testing, as well as the planning, execution, and reporting of fail-over and recovery tests.

85 Regarding the documentation of processes, policies, and procedures, we noted that various approaches and scenarios for fail-over and recovery testing are in place. These approaches and scenarios are outlined separately in different documents, whereas dependencies and interactions between the tests and incident scenarios are not defined. An overarching umbrella document providing a central view on the execution of the planned tests as well as a central definition of roles and responsibilities during testing does not exist. Next to this, the interaction with other processes, as for example information security as well as communication of test results, including rescheduling of tests, is not comprehensively defined.

86 Next to this, we noted inconsistencies and lack of comprehensibility towards terms, definitions, and documents of fail-over and recovery testing. Referenced sections in other documents are not fully consistent or do not exist in the referenced documents. In some cases, documentation of which tests are covered, how tests are performed, and whether they were executed was not comprehensive. In addition, the absence of details and background of test scenarios hamper comprehensibility. Lastly, inconsistencies in defined test frequencies for the same test, as well as in documentation of test approaches in the test reports, were noted.

87 We noted that the documented roles and responsibilities of ECB during fail-over and recovery testing differ from the actual roles and responsibilities. The provided documents state that ECB has a coordination role, however, during the review we noted that ECB is responsible for the execution of two tests.

88 Regarding the development, execution, and reporting of fail-over and recovery testing, we noted several weaknesses. The development phase lacks the definition and implementation of a consistent approach and process for the design of fail-over and recovery tests. Specifically noted, a baseline for the development of adequate and effective test scenarios is missing. Due to a missing pre-defined scenario catalogue, a complex and heterogeneous set of legacy-grown scenarios exists. Within the execution phase, we noted that the majority of tests focus on component tests, which are aimed at static and generic scenarios and approaches. The evaluation phase

misses appropriate and holistic reporting structures for fail-over and recovery testing, as well as a structured process for continuous improvement based on the results derived from the fail-over and recovery testing.

89 Based on the observed failures regarding the incident on 11 August 2020 and further review activities, we noted that the primary and secondary sites [REDACTED] are not identical in their functionality, making a site fail-over due to critical events impossible to execute in a timely manner. Also, there is no defined timeframe after which a site fail-over or regional fail-over should be triggered in case of an incident or crisis. Additionally, no BIA was performed to evaluate the availability requirements for critical IT components.

90 Regarding fail-over testing, we noted that only the T2S inter-regional recovery test was executed, while the fail-over tests for TARGET2 were not performed between the rotations 2019 and 2020.

4.3.4 Recommendations

91 For fail-over and recovery testing, we conclude that an overarching umbrella document should be created that defines the hierarchy and interaction between the various approaches and scenarios for fail-over and recovery testing. Current documentation should be reviewed regarding consistency of references, as well as completeness and consistency of terms and definitions. Next to this, roles and responsibilities of the different involved parties should be reviewed and where necessary revised to ensure proper segregation of responsibilities. With regard to the development, execution, and reporting of fail-over and recovery testing, we recommend implementing a consistent approach to develop adequate and effective test scenarios based on a pre-defined scenario catalogue, executing fail-over and recovery tests based on more specific and holistic scenarios, as well as improving the reporting of test results in combination with the development of an appropriate lessons learned process.

92 We recommend implementing functionally identical primary and secondary sites, including the configuration, to make a site fail-over in the case of severe incidents or a crisis possible in a timely manner. The functionally identical structure of the sites (to enable a site fail-over) should be monitored independently on a regular basis by implementing sufficient controls. We further recommend defining the criticality of the IT components. For the most business critical IT components, a time period should be determined after which a site fail-over shall be considered in case of an incident or crisis. This should include performing BIAs.

4.4 Communication protocols

4.4.1 Review procedures performed and review criteria applied

93 Regarding the area of communication protocols, we have performed review activities to ascertain the suitability of structures, principles, and procedures used to communicate during the occurrence of incidents. This includes the dimensions of communications concerning the sender, recipient, channel, time, content, and documentation. Communication is essential in ensuring timely, correct and consistent reactions of the various stakeholders.

In our review, we have focused on the appropriateness of information sharing, and the efficiency of the established and used communication processes during the incidents.

94 These review procedures included, amongst others, the following:

- Inquiries of employees responsible for communication processes during incidents at the ECB and 3CB/4CB
- Inspection of internal policies, processes, and procedures related to communication during incidents
- Review of the relevant communication reports, like incident or post-incident reports created during and after the respective incidents

95 Our evaluation of the underlying subject matter is based on the general criteria as described, and on specific criteria suitable for assessment of communication processes:

- Principles for financial market infrastructures, Bank for International Settlements and International Organisation of Securities Commissions, 2012.
- Application of the Principles for financial infrastructures to central bank FMIs, Bank for International Settlements and International Organisation of Securities Commissions, 2015.
- Assessment methodology for the oversight expectations applicable to critical service providers, Bank for International Settlements and International Organisation of Securities Commissions, 2014.

4.4.2 Process description

96 Communication in relation to incidents is laid out and defined in different processes. Within the incident management process, different communication subprocesses have been defined, including the identification of an incident, its communication to the service desk, the incident analysis, escalation, resolution, and reporting. These mandatory processes are defined for the communication of incidents between the ECB and the 4CB on all six dimensions of communication. The incident management process is set out to be updated regularly based on lessons learned to ensure continuous improvement.

97 Similarly, the crisis management process is laid out to negate the impact of incidents and events that exceed the pre-defined severity threshold. The crisis management process also considers events outside the system domain that have the potential to impact the services of the 4CB. The communication subprocesses between the ECB and the 4CB associated to the management of crises, have also been defined on all six dimensions of communication.

4.4.3 Findings

- 98 During our review of the communication protocols involved in both the TARGET2 and T2S services, we noted several weaknesses that can be categorised into three superordinate findings. These superordinate findings comprise the approach to external communications, the implementation of lessons learned, and the consistency and completeness of documented procedures.
- 99 The finding regarding the external communications approach is related to the information shared via the ECB website during incident resolution, effectiveness of alternative communication channels provided by ECB, and the provision of information regarding the incident resolution by NCBs. Market participants expressed that not enough information had been shared on the ECB website throughout the resolution of certain incidents, specifically the incidents on 16 March 2020 and 11 August 2020. We noted that market participants expressed uncertainty regarding the frequency of updates on the evolution of the incidents, as well as the roles and responsibilities to be assumed by each party following the communication of the incidents. Specifically, recommended contingency and mitigating actions were not included within the published messages. Subsequently, market participants lacked the support required in assessing their next steps. To some extent, the uncertainty was triggered by inaccessibility to the information being released by the ECB. Only participants who subscribed to the really simple syndication (RSS) feed and push notifications, which are not mandatory, received messages informing them about communications being released. As a consequence, not all market users had knowledge about communications available on the ECB website. Furthermore, the usability of ECB's website regarding the access to information related to ongoing incidents is perceived as not user-friendly. Additionally, we noted that different NCBs publish divergent messages informing about the same TARGET2 technical incident on their websites. Communications released by NCBs did not always contain the same detailed information as officially published by ECB, as they translated, summarised, or reworded the ECB approved message. Furthermore, the timing of the publication was not always aligned to the ECB release timeline.
- 100 Areas for improvements are documented in ECB internal post-incident reports which are created when the associated incident caused temporary unavailability of TARGET2, the incident required the involvement of crisis managers, deficiencies of a procedural nature were observed, and/or when the communication flows were considered insufficient or unclear. However, since there is no formal lessons learned process in place, formalised completion deadlines are not contemplated for the execution of such improvements. This issue not only affects the specific implementation regarding market communications, but any set of enhancements identified post-incident.
- 101 Our finding related to the consistency and completeness of documentation concerns the communication-related aspects, especially in incident and crisis management related procedures. In some communication processes, all communication elements (sender, recipient, channel, time, content and documentation) are addressed, and in other cases, there are elements, such as the channel, which are not mentioned.

4.4.4 Recommendations

102 We noted that internal communication operated effectively during the incidents in scope. However, we conclude that external communication could be improved by enhancing the usability of the ECB website, designing communication in a more bidirectional way, pushing market participants to subscribe to RSS feeds and push notifications, as well as streamlining communication of ECB and NCBs. Regarding internal communication, we recommend implementing a formal lesson learned process in order to improve existing IT management processes. Next to this, we recommend reviewing the current processes regarding communication, and addressing all communication elements to improve communication both internally and externally.

4.5 Governance

4.5.1 Review procedures performed and review criteria applied

103 Regarding the area of governance, we have performed review activities to ascertain the suitability of structures, principles, and procedures used to direct, control, and evaluate the TARGET Services. This includes good governance principles such as transparency, coherence, efficiency, accountability, and effectiveness. As requested, in our review we have focused on the appropriateness of information sharing, the efficiency of decision-making processes, effective operational control, and risk management.

104 These review procedures included, amongst others, the following:

- Inquiries of management and staff at the ECB and the service-providing national central banks responsible for governance, organisational structures, risk management, three lines of defence structures, and legal basis of the TARGET system;
- Inquiries of employees responsible for decision-making processes and administration of organisational structures, such as committees and working groups;
- Inquiries of employees responsible for maintaining and updating policies, process documentation, and legal documents;
- Inquiries of employees on continuous improvement, remediation of review findings, and oversight;
- Inspection of public and internal policies and processes in relation to governance;
- Inspection of regulations and contracts that form the legal basis of the TARGET system;
- Inspection of mandates and membership lists of committees and working groups;
- Inspection of disclosure reports against the principles for financial market infrastructures;
- Inspection of information published by the European system of national central banks on the governance of the TARGET system;
- Inspection of oversight and internal audit reports.

105 Our evaluation of the underlying subject matter is based on the general criteria as described, and on specific criteria suitable for assessment of governance:

- ECB Regulation on oversight requirements for systemically important payment systems (SIPS Regulation)
- CPMI-IOSCO Principles for financial market infrastructures (CPMI Papers No. 101)
- Application of the "Principles for financial market infrastructures" to central bank FMIs (CPMI Papers No. 130)
- Principles for financial market infrastructures: Assessment methodology for the oversight expectations applicable to critical service providers (CPMI Papers No. 123)
- Principles for financial market infrastructures: disclosure framework and assessment methodology (CPMI Papers No. 106)
- Eurosystem oversight policy framework

4.5.2 Process description

106 The governance of the TARGET Services is split up into three distinct levels, according to European Central Bank guidelines. Level 1, which consists of the Governing Council of the European Central Bank, is responsible for the direction, management, and control of the TARGET Services. Level 2 is responsible for certain technical and operational management tasks and consists of the Market Infrastructure Board (MIB) and substructures, as well as the CSD Steering Group (CSG) for the T2S services. Level 2 is made up of the European System of Central Banks. Level 3 provides the TARGET Services platforms and consists of the service-providing national central banks.

4.5.3 Findings

107 Within the above-mentioned structures, decision-making power is situated at high levels in the organisational structure, limiting responsiveness, as well as making updates to policies and procedures a time-consuming, multi-stage process.

108 The governance structure relies heavily on a large number of committees and working groups for decision-making, with each of the three levels having its own hierarchy of committees, including coexisting structures for TARGET2, T2S, and TIPS, both at the level of the service-providing national central banks and the ECB. We therefore noted that the governance and organisational structures of the TARGET Services are overly complex. Additionally, membership for some working groups and committees is not fixed, as members join on an ad-hoc basis without being formally nominated or assigned to the group.

109 In our review of documents, we noted that for the organisational structures, governance documentation is incomplete and inconsistently updated. Past, present, and future structures are not clearly marked and co-exist in documentation, which leads to a lack of transparency concerning the current setup. The legal structure consists of a complex mix of guidelines and contracts between the involved parties.

110 A second LoD, covering inter alia risk management and internal control has not yet been fully implemented. Current activities are mainly focused on information security and cyber resilience. A new, comprehensive risk management framework is expected to be implemented in the summer of 2021. We also noted that the current

risk management function did not yet formulate clear criteria for the necessary transparency, information sharing, and participation in decision-making, which is especially relevant with regard to the organisational structure between the service-providing national central banks, the ECB (Level 2), and the service-providing national central banks (Level 3 or 3CB/4CB). In addition, there is uncertainty concerning membership of the Securities Managers Group regarding the 2nd LoD, and no process has been set up and approved to integrate continuous improvements into the TARGET Services, so no formalised feedback loop for continuous improvement (i.e. Plan Do Check Act (PDCA)/Deming cycle) exists.

- 111 Finally, we noted that closing time for infringements identified by ECB Payments Oversight is unduly long. For example, the report “Assessment of TARGET2 against the SIPS regulation” from April 2017 identified infringements in the risk management and risk framework. The first remediation actions were completed by end of 2020, with several expecting completion in Q4 of 2021.

4.5.4 Recommendations

- 112 The governance structures as implemented may lead to delayed or inefficient deliberations, insufficient information sharing, lack of understanding concerning governance and organisational structures, ineffective decision-making, uncertainty regarding areas of responsibility, and unclear accountability. We therefore recommend reducing the overall organisational and governance complexity by streamlining the structures, consolidating committees and working groups, while moving responsibilities to decision makers on an appropriate operational level. Also, changes to organisational structures should follow a formalised process in line with industry best practises, based on clear criteria, resulting in a centralised documentation of all structures.
- 113 An insufficient 2nd LoD impedes understanding of risks, development of risk management and internal controls processes, increases the risk of unidentified gaps in risk management and control, and hampers dissemination of unbiased information to senior management regarding significant risks as well as risk mitigation efforts. We recommend the implementation of a 2nd LoD in all appropriate areas, including sufficient staffing, and introduction of a continuous improvement process. The 2nd LoD should also be mandated to ensure that concrete criteria for the necessary transparency, information sharing, and decision-making participation are implemented.
- 114 Missing processes and documentation are indicative of low organisational maturity and can impact the effectiveness of operations, decision-making and risk mitigation procedures. We recommend implementing clear rules on documentation to address these risks.

4.6 Data centre and IT operations

4.6.1 Review procedures performed and review criteria applied

- 115 In the area of data centre and IT operations, we have performed review activities to ascertain the suitability of structures, principles, and procedures regarding its suitability of the design and operating effectiveness of the IT-

related processes and controls to address the incidents. The focus of the review within data centre & IT operations of the TARGET Services related, among other things, to the adequacy of the monitoring processes and underlying Technical Monitoring Tool (TM), the completeness of the asset inventory and CMDB, the assignment of asset ownership defined in the asset inventory, the management of risks associated with third-party providers, as well as the measures relating to users or groups and their authorisations to avoid segregation of duties conflicts. To perform our procedures, we reviewed provided documents and collected additional information in meetings and in-depth interviews. The main contact persons were employees from the NCBs (Bdl and BBk).

116 The focus of our review with regard to provider management included measures defined in the rules and principles concerning management of risks associated with third-party providers. For this purpose, we reviewed relevant procedures, including the process documentation and written rules for service provider management, and collected additional information in meetings and in-depth inquiries with the responsible persons from 3CB and 4CB. During this, we also assessed measures regarding change and test management associated with changes conducted by third-party providers.

117 These review procedures included, amongst others, the following:

- Inquiry: Interviewed appropriate personnel about the timing, performance, and review of relevant IT-related processes and controls.
- Observation: Observed how specific processes and controls were conducted by the responsible parties via MS Teams.
- Review of documentation: Inspected documents and reports indicating the process and control design, as well as performance of the process and control by the responsible parties.

118 Our evaluation of the underlying subject matter is based on the general criteria as described, and on specific criteria suitable for assessment of communication processes:

- IT Infrastructure Library version 3 published by Central Computing and Telecommunications Agency (CCTA)
- ISO/IEC 20000 Service Management published by the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC).

4.6.2 Process description

IT Monitoring – Technical Monitoring Tool

119 [REDACTED]

Configuration Management Database & Asset Ownership

- 120 3CB and 4CB manage information about the IT infrastructure required for the provisioning of IT services by means of configuration items (CIs) in separate asset inventories for TARGET2 and T2S. There are defined mandatory fields that must be provided and maintained by asset owners when CIs are created and changed. The creation and maintenance of CIs are partly decentralised, for example the data-centre-related CIs are managed by BBk and Bdl. The management of hardware and software assets is defined in the asset inventory guideline. The formally defined process by 3CB and 4CB for asset management specifies that it is mandatory for each asset to have an assigned asset owner. There are procedures at 3CB and 4CB level that ensure correct assignment of asset ownership. Ownership is assigned when assets are created or transferred.

Third-Party Providers

- 121 There are guidelines in place that define the rules and principles concerning management of risks associated with third-party providers. This includes guidance on how to set up requirements when establishing contracts with third parties, and what security controls need to be applied respectively by the 3CB, 4CB, and the third party. Furthermore, 3CB and 4CB stated that vendor contracts are the result of a public tender process based on the "European Rules for Procurement".

Access Management – No definition of conflicts in Segregation of Duties

- 122 Segregation of duties (SoDs) is, for example, implemented at 3CB and 4CB between system development, testing, and implementation into production (strict segregation between the operations team and development team). The access to business data is provided on a need-to-know principle, which is formally described in the T2S Role Handbook, which is subject to regular reviews. In cases where strict SoD is not feasible (e.g., due to organisational or technical reasons or a crisis), specific monitoring and ex-post checks are – according to the information provided by 3CB and 4CB - in place along with management supervision activities. Additionally, user access is – according to the Access Control Guide - periodically reviewed. The user review process verifies the appropriateness of assigned access rights and SoD.

4.6.3 Findings

- 123 Regarding monitoring, we noted that there is no document describing the monitoring performed within the TM Tool. Alerts in the TM Tool are configured to identify malfunctions that can have multiple root causes. We could only understand the process regarding the control execution after in-depth explanations by the respective control owners. Furthermore, we noted that dedicated checklists to resolve an event were solely defined in the TM for a "small subset" of critical alerts related to T2S. This checklist is not available e.g. for network alerts or interface-related alerts. For a "small subset" of alerts related to TARGET2, the technical team created an unofficial document to ease the handling of alerts. This document is the outcome of tracking different alerts that have been created over time (repository of alerts).
- 124 Concerning the asset inventory, we identified that an established and formally defined process for the identification and maintenance of all TARGET2 and T2S related assets is in place at the 3CB and 4CB levels. Relevant

assets are recorded in a high-level asset inventory per system (TARGET2 and T2S), which is subject to periodic reviews. However, we noted that there is no sufficient CMDB according to ITIL from which the TM is derived.

125 Consequently, the risk is that information about changed, newly created, or transferred assets is not identified, and thus not included or adjusted in the TM. If all assets are not accurately maintained in the TM, there is the risk that errors or alerts are not (appropriately) identified, and their impact on other IT components and services may not be resolved in a timely manner, resulting in issues in the business operations of the TARGET Services.

126 The procedures regarding asset ownership as defined in the asset inventory at the 3CB and 4CB levels ensure the correct assignment of asset ownership. However, we noted that the asset owners defined in the asset inventory could not always be clearly identified. Not having a clear asset ownership bears the risk that the assets are not properly protected and managed.

127 As a result of our review of the provider management, we noted relevant weaknesses concerning the management of providers, especially with respect to the outdated 3CB and 4CB Third-Party Management Security Guideline. The Guideline does not reflect the current organisational structure and needs, resulting in inadequate internal control, as well as the insufficient review of vendor release notes, which contributed to the incident on 23 October 2020 when network connectivity between two switches was lost, triggering a cascade of further failures.

128 For the network, we noted that there is no functional test environment for changes in place. Thus, changes are implemented directly in the production environment. This could have a negative impact on the layers that depend on the network, e.g. the operating system and the application. Furthermore, we noted that critical network changes on the secondary site were conducted without testing the change on the primary site first. Deploying changes before a specific observation time or before conducting specific tests bears an increased risk on the business operations, as a site fail-over may not be possible anymore.

129 [REDACTED]

4.6.4 Recommendations

130 Taking a holistic view of the findings identified in our review for data centre and IT operations, we conclude that key operational and organisational aspects of the TARGET Services, such as the technical monitoring process, the monitoring of external service providers, as well as the IT operations setup, are not sufficiently designed and implemented. As described above, we have identified relevant weaknesses in these areas that affect the internal control system of the TARGET Services. An insufficient technical monitoring and overview of critical IT components may have a negative impact on the overall ability to respond appropriately and in a timely manner to alerts,

which favours the emergence of incidents. The current IT processes and controls within the TARGET Services need to be improved.

131 First, we recommend standardising and increasing the transparency of the monitoring for the TARGET2 and T2S systems across all layers (infrastructure, platform, and application). Critical alerts related to TARGET2 and T2S should be mapped to measures to ensure that they are resolved accurately and in a timely manner. We further recommend elaborating and defining process definitions and harmonising the monitoring process and handling of alerts across TARGET2 and T2S to achieve a uniform, traceable, understandable, and verifiable process across the various IT components, systems, and responsible parties.

132 We also recommend the service-providing national central banks capture all inventories relevant for the TARGET Services, including CIs, in a central asset inventory database. The CIs should be assigned to services to recognise the dependencies between the services, the CIs, and their impact on the TARGET Services in a timely manner in case of an incident.

133 Further, all critical IT components that make up the TARGET Services should be assigned to a clearly identifiable asset owner (person or role) to have a clear and overarching definition of authority and attribution of accountability.

134 Additionally, we recommend establishing a clearly defined testing strategy for network related changes and robust documentation of the process, including the outcome of the control execution. In particular, this strategy should prescribe that changes on the primary site should be tested before implementing them in the secondary site to enable a site fail-over. Release upgrades should always be reviewed and their impact on the internal control system should be evaluated before deploying the upgrade in the production environment.

135 [REDACTED]

5 Practitioner's conclusion

- 136 We issue the above report on the review of the backgrounds and causes of the incidents on 16 March 2020, 25 May 2020, 11 August 2020, 23 October 2020, and 13 November 2020 in relation to the TARGET Services in accordance with the external review assignment dated 21 December 2020.
- 137 A summary of our results is given in section 2 of this report.
- 138 We would like to point out that the addressees of this report are the executive management of the European Central Bank. This report has been prepared solely for the purpose of documenting the external review conducted in respect of ECB and not for the purposes of any third party to whom we are not liable.

Frankfurt am Main, 1 June 2021

Deloitte GmbH
Wirtschaftsprüfungsgesellschaft



Signed: Christian Haas
Wirtschaftsprüfer
(German Public Auditor)



Signed: Daniel Hellmann
Certified Information Systems Auditor

Appendix A: List of abbreviations

3CB	Service-providing national central banks (Deutsche Bundesbank, Banque de France, and Banca d'Italia)
4CB	Service-providing national central banks (Deutsche Bundesbank, and Banco de España, Banque de France, Banca d'Italia)
4CBNet	Network of the service-providing national central banks (Deutsche Bundesbank, Banco de España, Banque de France, Banca d'Italia)
BACM	Business Area Continuity Management
BBk	Deutsche Bundesbank (part of the 4CB)
BCM	Business Continuity Management
BCP	Business Continuity Plan
BdE	Banco de España
BdF	Banque de France
BIA	Business Impact Analysis
BS WP/vBP	Professional Code of Conduct for German Public Auditors and Sworn Auditors
CB	Central Bank
CCP	Central Clearing Counterparties
CCTA	Central Computing and Telecommunications Agency
CI	Configuration Items
CMDB	Configuration Management Database
CPA	Currency Participation Agreement
CPMI-IOSCO	Principles for financial market infrastructures
CRM	Change and Release Management
CROE	Cyber resilience oversight expectations for financial market infrastructures
CSD	Central Security Depositories
CSG	CSD Steering Group
DCPs	Directly Connected Parties
DKK	Danish Krone
EBA	European Banking Authority
ECB	European Central Bank
ESCB	European System of Central Banks
FA	Framework Agreement
GB	Gigabyte
ICS	Internal Control System
ICT	Information and Communication Technology
IDVP	Intraday Delivery versus Payment
IDW	Institut der Wirtschaftsprüfer (Institute of Public Auditors in Germany, Incorporated Association)
ISAE	International Standard on Assurance Engagements
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSCM	IT Service Continuity Management
ITSCP	IT Service Continuity Plan

LAU	Local Authentication
LoD	Line-of-Defence
MIB	Market Infrastructure Board
MOM	Mathematical Optimisation Module
NCB	National Central Bank
NTS	Night-Time-Settlement
PAPSS	Payment and Accounting Processing Services Systems
PDCA	Plan Do Check Act
PROD	Production IT Environment
RPO	Recovery Point Objective
RSS	Really Simple Syndication
RTGS	Real-Time Gross Settlement
RTO	Recovery Time Objective
SIPS	Systemically Important Payment Systems
SSP	Single Shared Platform
SWIFT	Society for Worldwide Interbank Financial Telecommunication
T2S	TARGET2-Securities
TARGET	Trans-European Automated Real-time Gross Settlement Express Transfer system
TIPS	TARGET Instant Payment Settlement
TM	Technical Monitoring
TT	Technical Team
U2A	User-to-Application
UoR	Use of Restrictions
WAS	Web Application Server
WPO	German Public Auditor Act