Bank of England

Prudential Regulation Authority

FINAL NOTICE

To: **TSB Bank plc (FRN 191240)**

Date: **20 December 2022**

1. Action

1.1. For the reasons given in this Notice, the PRA imposes a financial penalty on TSB Bank plc ('TSB' or the 'Firm') of £27,000,000 for the Firm's breaches of PRA Fundamental Rules 2 and 6 between 16 December 2015 and 10 December 2018 (the 'Relevant Period') or parts thereof.

1.2. The Firm agreed to settle during the Discount Stage of the PRA's investigation and therefore qualified for a 30% settlement discount pursuant to the PRA Settlement Policy, under which the financial penalty was reduced to £18,900,000.

2. Summary of Reasons for Action

TSB, the Sabadell acquisition and the Proteo platform

2.1. The Firm is a UK retail bank created by a divestment from Lloyds Banking Group ('LBG') in June 2014. It provides various services to its customers including personal current accounts; business banking; savings accounts; mortgages; insurance; loans; and credit cards. During the Relevant Period, it had approximately 5.2 million customers. TSB's customers accessed services through digital channels (both through internet-banking and through its mobile app), telephone banking and by visiting branches.

2.2. TSB is regulated by the PRA for prudential purposes and by the FCA for conduct matters.

2.3. TSB started trading under its own brand in 2013, while still part of LBG. Following its divestment from LBG in June 2014, the Firm continued to receive its core IT services from LBG, utilising the LBG IT platform. Under its contract with LBG, TSB had the option to continue to use the LBG IT platform for a period of up to 10 years (until 2024), or it could exit the arrangement through two

options, either: (1) via migration; or (2) a carve-out (where a copy of the LBG IT platform would be created and then operated by a new third party service provider).

2.4. There were benefits to TSB in using the LBG IT platform, including access to a stable, resilient and scalable platform, through which it had the capability to offer the full product range of a major UK retail bank through multiple channels (branch, telephony, desktop and mobile). However, there were also significant strategic factors in favour of exiting the arrangement, due to the limited duration of the agreement with LBG – detracting from the benefits of its scalability, anticipated cost savings and a desire for greater strategic flexibility in terms of changes to the platform within TSB's preferred costs and timescales. TSB therefore started considering possible options for exiting the LBG arrangement soon after the arrangement had commenced.

2.5. In March 2015, the Firm received a takeover bid from Banco de Sabadell, S.A. ('Sabadell'), a Spanish bank with a history of acquiring banks in Spain and integrating them onto its IT banking platform ('Proteo'). A key strategic aim of the proposed acquisition was a full migration of the Firm's IT services onto the Proteo platform. Sabadell put together a timeline which aimed for migration to be achieved by the end of 2017.

SABIS and the Proteo4UK Platform

2.6. In December 2015, the Firm committed to deploying resources towards migrating its IT services from the LBG IT platform to a new purpose-built version of Sabadell's Proteo platform (the 'Migration Programme'), whilst retaining the carve-out option. Proteo was proven in Spain, but the Firm recognised it would need to be adapted for the Firm, and the UK market, with upgraded digital capacity. The Firm also recognised that the new version of Proteo ('Proteo4UK Platform') would need to be '*proven at scale'*. TSB began working with Sabadell on the design of the platform in December 2015 and on the build from April 2016. It was understood that Sabadell (via IT service subsidiaries) would design, build and operate the Proteo4UK Platform and migrate TSB's data to it. The two IT service subsidiaries would be Sabadell Information Systems, S.A. ('SABIS Spain') and Sabadell Information Systems Limited ('SABIS UK') (together, 'SABIS').

2.7. TSB and SABIS subsequently entered into two contracts intended to govern the relationship: (1) the Migration Services Agreement ('MSA') which governed the design, build and testing of the Proteo4UK Platform, and the migration of TSB's data to it, by SABIS; and (2) the Outsourced Services Agreement ('OSA') which governed the operation of the Proteo4UK Platform by SABIS. As with many IT projects, the arrangements provided for SABIS to engage third party service providers (external vendors to SABIS) to deliver systems and services required for the Proteo4UK Platform and the migration.

Operational Risk

2.8. TSB was the first major bank in the UK to undertake a Migration Programme of this scale and complexity, seeking to migrate customers off a third party platform via a predominantly single migration event to a newly built platform (which was created largely from the existing Proteo (Spain) platform) with new datacentres, to be delivered and operated by an IT service provider with no experience of managing service delivery from UK subcontractors. Achieving the migration would involve cooperation not only with SABIS and its external suppliers, but also with LBG, who owned the source platform from which the data would be migrated. The Proteo4UK Platform was an unproven version of the existing Proteo (Spain) platform and required significant customisation to meet TSB's requirements. Migration off the LBG platform onto Proteo4UK was irreversible, creating risk if any major issues arose. It was also ambitious for migration to a new build platform in the UK to occur in under three years. All of these factors presented significant operational risk to the Firm.

2.9. TSB's migration to the Proteo4UK Platform and the provision of IT services and infrastructure via contractual arrangements with SABIS were critical to TSB's safety and soundness, and its ability to provide continuity of Critical Functions. TSB considered SABIS and LBG to be suppliers for critical outsourced banking functions ('Critical Third Party Suppliers'), noting (amongst other things) that SABIS's and LBG's services were vital for delivering TSB's core services, and could not be interrupted for more than 24 hours without material business impact. At the outset of the Migration Programme, the PRA notified TSB that, while the impact of any operational failure on TSB's brand was unknown because of the lack of other examples to date, it had a concern that the result could potentially be more severe for TSB's recently established brand as a challenger bank if customers felt that it impacted their confidence in TSB's safety and soundness.

2.10. The intragroup nature of the relationship between TSB and SABIS did not necessarily mean that the outsourcing arrangement between TSB and SABIS did not share some of the same risks as a comparable arrangement with an unrelated service provider, albeit the PRA acknowledges the commercial interests of TSB and its service provider were substantially aligned. Nevertheless, the PRA expected the Firm to comply with PRA rules, including outsourcing rules. It also expected the Firm to organise and control the Migration Programme responsibly and effectively, with prudent and effective planning, governance, and business continuity arrangements, sufficient to minimise the operational risk of disruption to the continuity of TSB's Critical Functions.

Migration Programme Governance and Risk Management Frameworks

2.11. The Firm put in place an extensive governance framework for the Migration Programme. The TSB Board had ultimate oversight of the Migration Programme as well as of key developmental aspects of the assurance framework. The Board Audit Committee ('BAC') was responsible for oversight of the management of Migration Programme risks as they affected delivery of the programme and its objectives. The Bank Executive Committee ('BEC') provided collective support in developing and implementing TSB's strategy, and monitoring business performance. The BEC Design Executive ('BEC DE') was responsible for the ownership and governance of the migration plan to align and deliver strategic objectives.

2.12. The Firm operated its risk management through a '*three lines of defence*' model incorporating the Business Areas (first line), Risk Oversight (second line) and Internal Audit (third line). The Business Areas was responsible for identifying, assessing, managing and mitigating risks relevant to their areas within the Board's risk appetite parameters. Risk Oversight was responsible for providing independent oversight and challenge and TSB-wide risk reporting. Internal Audit provided independent and objective assurance over the Business Areas' management of risk and control, and Risk Oversight's supervision of TSB's risks. Each of the three lines of defence were also assisted to some degree with additional resource and expertise from external consultants.

Migration Programme planning, re-planning and delays

2.13. The Firm adopted a Migration Programme plan in March 2016 (the 'Integrated Master Plan' or 'IMP') with a main migration event ('MME') set for 5 November 2017. The IMP was described as '*aspirational*' and reflected a top-down and '*right-to-left*' approach to planning to meet the target migration date. A '*left-to-right*' plan was subsequently developed and was reviewed by a third party firm. That firm noted that the plan covered the major activities that would be seen for comparable programmes, and made some recommendations, which were actioned.

2.14. The Migration Programme experienced delays from the outset and, while significant progress had been made, on 20 September 2017 the Firm decided that the Migration Programme would have to be re-planned. In doing so, the Firm acknowledged that the November 2017 target date had been set two and half years previously and was '*deliberately ambitious*', had acted as a '*forcing mechanism*' to ensure that the business and suppliers worked '*at pace*' but had been '*based on very little information*'. The Firm announced to the public nine days later, on 29 September 2017, that MME would be re-planned '*into Q1 2018*'. This announcement was almost a month before the re-planning exercise was completed and approved by the TSB Board on 24 October 2017 (the 'Defender Plan'). The Defender Plan was premised on TSB being '*migration ready*' as soon as possible in 2018, with the earliest possible MME date being 15 March 2018 (later determined to be 22 April 2018). However, the PRA acknowledges that TSB remained of

the view throughout the Migration Programme that it would not migrate until it was ready to do so.

2.15. The Defender Plan had a significant focus on testing, and incorporated guiding principles designed to minimise operational risk. The Migration Programme quickly fell behind the Defender Plan schedule, with the result that critical testing plans and principles had to be deviated from to keep on track for MME. It does not appear that deviations from the Defender Plan were sufficiently challenged by the Firm, and the Firm failed to assess what these deviations meant for the overall risk profile of the Migration Programme and the readiness of SABIS to operate the Proteo4UK Platform. The Firm did not sufficiently reflect on the process and programme delays under the IMP.

2.16. The PRA expected the Firm to organise and control the Migration Programme responsibly and effectively with prudent and effective planning and robust governance. This required realistic planning from the outset based on a '*left-to-right*' or *'bottom-up'* approach and a dynamic assessment of risk such as robustly challenging what deviations from testing principles and plans mean for the overall risk profile of the migration and the readiness of Proteo4UK and SABIS to operate those platforms effectively.

Assessing the readiness to go live

2.17. TSB developed the Assurance Matrix as a framework for the First Line to give a comprehensive overview of all the assurance parameters required for First Line validation of the Migration Programme deliverables. BEC business functions were responsible for completing the Assurance Matrix (by answering the relevant questions with supporting evidence) before giving attestations as to the readiness of their functions to Go Live.

2.18. Along with the Assurance Matrix, the T3 Memo was a key tool used by TSB to assess the readiness to Go Live. The T3 Memo consisted of 972 pages and included a recommendation to proceed with the Main Migration Event ('MME'), attestations testifying to the readiness of BEC business functions, and opinions from Risk Oversight and Internal Audit on the Business Areas' interpretation of the facts, the risks to the business of proceeding with the MME and the effectiveness of the mitigating actions.

2.19. The governance for the final steps leading up to the migration from the LBG platform to the Proteo4UK Platform involved several decisions. On 10 April 2018, the Board approved the service of a Definitive Notice of Migration on LBG, meaning that TSB was committed to exiting from the LBG platform via migration to a new platform. On 18 April 2018, the Board considered the T3 Memo and approved the constitution of a sub-committee with authority to grant approval to an Executive Gold Team to initiate the data migration. On 19 April 2018, the Board sub-committee gave that authorisation. On 20 April 2018, the Executive Gold Team decided to initiate

the migration. On 22 April 2018, the Board sub-committee authorised the Executive Gold Team to complete the migration.

Non-Functional Testing

2.20. As reflected in the Defender Plan, testing was critical to ensure the readiness of the new Proteo4UK Platform. Testing consisted of functional testing, which was intended to determine if the systems behaved as required (encompassing user acceptance testing or 'UAT', migrated data testing or 'MDT' and regression testing), and non-functional testing ('NFT'), which was intended to assess whether the tested product would provide a good and reliable user experience at volume (encompassing security testing, performance testing, infrastructure testing and disaster recovery testing). NFT was an important mitigant in relation to operational risk (alongside SIT and UAT) because of the manner in which TSB had executed the Migration Programme (including the absence of detailed design and testing documentation for the newly built data centre infrastructure).

2.21. Satisfactory completion of testing was a key component of the Assurance Matrix. In February 2018, TSB's IT Business Function decided that they, rather than BEC business functions, would attest as to which non-functional requirements had been tested through NFT, albeit BEC members would sign-off on the actual non-functional requirements in their attestations.

2.22. The new Proteo4UK Platform's infrastructure involved duplicate data centres using solutions in Active-Active configuration, which was intended to prevent outages for key systems even if one data centre failed, thereby ensuring operational continuity. The Firm had originally planned to conduct NFT in both data centres in Active-Active configuration in the production environment. However, TSB accepted a '*counter-proposal*' by SABIS in the weeks leading up to MME to conduct testing on only one data centre. Not conducting this testing was not identified to be a risk by TSB, and consequently potential mitigants were not considered. This meant that testing was conducted in an environment which was distinctly different from the production environment. The decision was taken informally, outside of TSB's governance structure or procedures, was not documented, and was not escalated.

2.23. Owing to delays in testing, NFT ran right until the day before the MME decision with a final report ('NFT Final Report') provided in the afternoon of 17 April 2018 (the day before the Board met to approve the final governance steps required to authorise MME). The NFT Memo did not explicitly flag that testing had not been conducted in both data centres in Active-Active configuration, although this was noted in relation to the digital NFT in the NFT Final Report.

2.24. The PRA expected the Firm to take all reasonable steps to decrease operational risk, and critical decisions such as those related to critical aspects of NFT, to be escalated and risk

assessed. However, TSB's IT business function did not at the time consider that their decision represented a risk and therefore it was not escalated.

2.25. Post-MME, Active-Active configuration errors in the two data centres resulted in failed customer sessions on digital access systems, i.e. mobile app and internet banking. By not conducting NFT in both data centres in Active-Active configuration, an opportunity to potentially identify some of the configuration issues experienced post MME was lost.

Approach to Risk Management

2.26. Between November 2015 and December 2016, the Firm identified 22 risks in relation to the Migration Programme, classified into programme execution risks and risks to the TSB business from migration. In addition, the Firm recorded three migration-related Material Risks (i.e., risks deserving prominence at Board and BEC level), the two most relevant being:

a. MRR 39: risk that migration causes operational instability or a degradation in resilience and poor customer outcomes;
b. MRR 41: complexity, or poor control in the delivery, of migration leads to unplanned costs or delays in implementation.

2.27. Although there was monitoring and reporting of the 22 programme risks in the course of the programme, the effectiveness of this was limited in three respects:

a. first, TSB's identification of programme risks did not explicitly address risks arising from its outsourcing arrangements with SABIS, a service provider with no experience of managing service delivery from a large number of UK subcontractors, nor did it explicitly address risks from TSB's limited experience of supplier oversight in an IT change management project of this scale and complexity. While a number of TSB's programme risks considered the risks that arose from SABIS's central role in the programme, there was no explicit assessment by TSB of the risk of non-performance, or inadequate performance, by SABIS of its obligations to deliver and operate Proteo4UK in a manner which met TSB's requirements.

b. second, while the Programme Risks were reviewed at the monthly Migration Delivery Committee, and TSB considered whether all relevant risks had been captured and considered new risks to the Programme on an ongoing basis, the list of the 22 Programme Risks remained unchanged for the duration of the programme. Consequently, any initial shortcomings in risk identification prior to December 2016 (such as SABIS's lack of experience managing service delivery from a large number of UK subcontractors, and TSB's limited experience of supplier oversight in an IT change

management project of this scale and complexity) remained for the rest of the programme.

c. third, although Risk Oversight and Internal Audit carried out a large number of migration-related reviews and audits, some of these were limited in scope or were expressly stated to be '*point-in-time'* reviews which might have been overtaken or were otherwise qualified. However, these limitations and/or qualifications do not appear to have been specifically discussed with the TSB Board at certain crucial junctures which could have led to challenge. This meant that the assurance provided by Risk Oversight and Internal Audit which supported the recommendation to proceed with Go Live was inadequate and inappropriate for the scale, complexity and level of operational risk arising from the Migration Programme.

Oversight of SABIS's Readiness

2.28. The supply chain of service providers delivering services to TSB (i.e., through SABIS and its third parties) exposed TSB to operational risk. TSB sought to mitigate this, including by obtaining formal assurance in the two weeks leading up to MME as to the readiness of SABIS (confirmation that SABIS was ready to operate Proteo4UK). This included:

a) a letter from SABIS dated 5 April 2018 (the 'SABIS Confirmation') stating confidence as to the migration readiness of the platform, providing an early report on NFT results (noting that some tests were still to be completed) and referring to confirmations of readiness received or anticipated from parties whom SABIS considered to be critical third parties ('Critical Fourth Parties'); and

b) a paragraph in the IT business function attestation that formed part of the T3 Memo, which asserted that SABIS was ready for MME and that TSB's IT business function were satisfied that the SABIS Confirmation could be relied upon.

2.29. However, the SABIS Confirmation and the fourth party confirmations referred to were, to some extent, forward looking statements of good intention or expectations, rather than statements of fact about the completeness of readiness activities undertaken. The further tests referred to in the SABIS Confirmation were completed on 17 April 2018, and the underlying statements made by the Firm's Critical Fourth Parties included caveats. While TSB continued to have ongoing dialogue in the run-up to MME with SABIS and the fourth parties, TSB relied on the fact that fourth party confirmations had been given to SABIS without verifying whether SABIS had critically assessed these.

2.30. Whilst TSB had identified, from an early stage of the programme, the need for strong supply chain management to mitigate risks arising from the dependence on fourth parties in the ongoing

provision of services after MME, the PRA also expected it to have controls in place to ensure that it had the necessary visibility of supply chain risks during the build of the platform. However, as late as February 2018, TSB was aware that SABIS's supplier management model (including its service risk assessment methodology and framework) was not fully developed and did not comply with TSB Group Outsourcing policy. Whilst TSB and SABIS agreed a number of steps to address this, and TSB had worked closely with SABIS throughout the programme, the fact that this was a concern at this late stage of the programme meant that TSB could not have been confident that SABIS was overseeing fourth party service delivery in a way that was commensurate to the criticality of the service or the overall complexity and scale of the migration programme.

Incident Management

2.31. Given the scale, level of complexity and risk of the Migration Programme and, in particular, the fact that it would be largely impossible to roll back to the LBG platform once the data migration had completed, the PRA expected the Firm to be proactive in ensuring its Critical Third Party Supplier had adequate systems and controls in place for IT incident management. Most importantly, TSB had to satisfy itself that SABIS not only had a framework in place, but that it could use it effectively. Service failures during earlier stages of the Migration Programme, particularly in relation to the phased transition of functionality to the new platform ('Governed Transition Events' or 'GTEs'), gave TSB an opportunity to observe TSB's incident management capabilities. However, these were relatively confined and did not reflect the multi-channel failures that occurred post-MME.

2.32. The post-MME incidents revealed a number of deficiencies in incident management. The fact that processes were not embedded within SABIS, between TSB and SABIS, or between SABIS and fourth parties upon whom incident management responses relied, could have been identified by TSB involving all of these parties in rehearsals. The failure to test SABIS's incident response processes in a more robust way meant that the Firm was not prepared to handle the crisis that unfolded post MME.

Migration Incident

2.33. MME took place over the weekend of 20 to 22 April 2018, and almost immediately the Firm encountered serious and well publicised issues, including failures with online, telephone and mobile banking services, branch technology failures, and consequential issues with payment and debit card transactions (albeit the underlying payment systems were themselves functional) (together, the 'Migration Incident'). Whilst the data migration itself was successful, the Migration Incident resulted in significant disruption to the continuity of TSB's provision of core banking functions (including branch, telephone, online and mobile banking) immediately post migration,

with some more limited issues persisting for a sustained period of months. All 550 of its branches and a significant proportion of its customers (including a proportion of those customers on the digital platform) were impacted. The initial issues with digital channels, some of which were significantly improved within three days, impacted its branches and the customers seeking to access the digital platform at that time. Parts of the customer base continued to be affected by technical issues, and the disruption to channels and the ensuing concern among customers led to higher levels of traffic than some of TSB's channels had been scoped to handle, leading to further customer inconvenience. The Migration Incident followed a combination of failings relating to planning, testing, governance, risk management, third party oversight (including lack of design documentation), lack of visibility and management of fourth party risks, and poor preparation for incident management.

2.34. As a challenger bank, TSB was potentially more vulnerable to brand damage arising from operational failures and therefore at risk of loss of confidence in the event of significant operational disruption, leading to potential depositor outflows. Depositor outflows can pose a risk to safety and soundness of a firm and could also impact confidence in challenger banks more broadly, and therefore potentially have a negative impact on financial stability.

2.35. As a result of the Migration Incident and the potential impact on the safety and soundness of the Firm and financial stability, the PRA decided to investigate whether the Firm's planning of the migration, governance, risk management and oversight arrangements and approach to operational risk complied with the relevant requirements in the PRA Rulebook.

3. Breaches and Failings

3.1 The PRA's investigation identified that during the Relevant Period the Firm breached Fundamental Rules 2 and 6 of the PRA Rulebook.

Fundamental Rule 2

3.2 In breach of Fundamental Rule 2, the Firm failed to manage appropriately and effectively its services and outsourcing arrangements with SABIS and the risks, including operational risk, arising from the arrangements. In particular, the Firm failed to exercise due skill, care and diligence:

a. when entering into the arrangement for services and outsourcing to SABIS. The Firm did not formally and comprehensively assess whether SABIS had the ability, capacity, resources and appropriate organisational structure to deliver the Proteo4UK Platform in the timeframe adopted, and were ready to provide the ongoing outsourced services required to operate the Proteo4UK Platform reliably and professionally;

b. when managing the arrangement for services and outsourcing to SABIS. Testing for the Migration Programme was executed in a manner which departed from the Firm's stated plans and guiding principles, increasing operational risk. The Firm did not formally and adequately reassess SABIS's ability and capacity on an ongoing basis, including in light of service level breaches encountered with the GTEs. It did not receive formal assurance from SABIS in the form of statements of fact about completeness of readiness activities already undertaken by it, or the Firm's Critical Fourth Parties, nor about SABIS's management of the Firm's Critical Fourth Parties, including whether SABIS had robust testing, monitoring and control over the Firm's Critical Fourth Parties; and

c. in not adequately assessing the performance and service issues encountered with some of the GTEs, which had in some instances led to slow recovery from incidents and breaches of service level agreements. The Firm did not at this stage interrogate sufficiently its readiness for MME in light of these issues but instead took comfort from the fact that the Proteo4UK Platform would have matured by the time of MME, with these issues manifesting as expected dips in service.

3.3 Further, the Firm failed to exercise due skill, care and diligence when TSB decided not to conduct NFT of the digital channels in Active-Active configuration in both data centres. This resulted in the testing and production environments being distinctly different, which meant that an opportunity to potentially identify some of the configuration issues experienced post MME was lost. This meant that, while TSB did consider that there were risks in conducting Active-Active performance testing in the live environment, TSB failed to identify and evaluate the risks of not conducting the testing in Active-Active configuration, nor did it consider any potential mitigants for the risks.

3.4 The Firm also failed to take a critical decision regarding NFT in the Migration Testing Forum, which was the governance structure in place for such decisions. The risks were not identified in the NFT Final Report. Therefore, the decision was not escalated or sufficiently explained to the appropriate committees and/or decision makers, because this was viewed as purely technical and not presenting a risk to TSB.

Fundamental Rule 6

3.5 In breach of Fundamental Rule 6, the Firm failed to organise and control the Migration Programme responsibly and effectively. In particular:

a. the Firm's planning and re-planning of the Migration Programme was, insufficiently robust and failed to adequately mitigate operational risk:

i. the initial planning for the Migration Programme adopted a right-to-left approach and as a result set an overly ambitious timetable for migration, given its scale and complexity, and the degree of operational risk;

ii. re-planning of the Migration Programme in September/October 2017 did not adequately investigate the technical causes of delays, or adequately assess the performance and service issues with the Governed Transition Events which had in, in some instances, resulted in outages and/or breaches of service level agreements which should have caused the Firm to question SABIS's readiness. When re-planning during this period, the Firm produced the Defender Plan, which also adopted an overly right-to-left approach, albeit the PRA acknowledges that TSB was of the view that it would not migrate until it was ready to do so. The Firm missed an opportunity to properly assess the extent of the delays to the Migration Programme, to learn critical lessons from that assessment, and to realistically assess the volume of work that needed to be achieved before it was '*migration ready'*; and

iii. the Firm publicly committed to a re-planned MME date into Q1 2018 before the re-planning of the Migration Programme had been completed or approved by the Board.

b. the Firm's governance of the Migration Programme was insufficiently robust. It does not appear that certain matters were sufficiently discussed with the TSB Board, which could have led to challenge, in particular the overly ambitious timetable for migration, deviations from certain aspects of the migration plans and certain guiding principles and what they meant for the overall risk profile of the programme, and the readiness of the Proteo4UK Platform and SABIS;

c. the Firm's risk management function did not adequately identify, assess and report on key risks, in particular operational risk related to the Migration Programme:

i. the Firm did not explicitly identify risks related to non-performance, or inadequate performance, of the firm's key supplier so that adequate consideration is given on an ongoing basis to the operational risks for the Firm arising from that relationship, and action taken accordingly to mitigate those risks, although aspects of the impact of the non-performance were considered as part of other programme risks;

ii. the scope of some of the assurances provided by Risk Oversight and/or Internal Audit were limited or qualified and, as a result, were inappropriate for the scale, complexity and level of operational risk arising from the Migration Programme. These limitations or qualifications do not appear to have been specifically drawn to the Board's attention and were therefore not scrutinised appropriately;

d. the Firm's incident management arrangements were insufficiently robust and ineffective.

i. the Firm did not undertake adequate exercises to test its and SABIS's ability, from an IT perspective, to recover from all aspects of an IT failure of the size of the one which manifested after MME;

ii. the Firm did not ensure that it had sufficient oversight and assurance of SABIS's incident management capabilities.

4. Reasons why the PRA has taken action

4.1 The PRA is responsible for the prudential regulation and supervision of banks, building societies, credit unions, insurers, and major investment firms. The PRA's role is to promote the safety and soundness of those firms. Adverse effects on the stability of the UK financial system, including through threats to customer confidence in individual firms, may result from disruption to the continuity of financial services. The way in which a firm manages operational resilience is an integral part of the PRA's assessment of a firm's safety and soundness. The PRA therefore places high priority on embedding operational resilience in its supervisory approach to mitigate the risk of such disruption.

4.2 The PRA also has a secondary competition objective. When discharging its general functions in a way that advances its objectives, the PRA must so far as is reasonably possible act in a way which facilitates effective competition in the markets for services provided by PRA-authorised persons. Challenger banks, such as TSB, facilitate effective competition in the UK banking market. Challenger banks can only facilitate effective competition if they instill confidence with depositors. A disruption to the performance of operational functions which are critical for the performance of regulated activities, listed activities or ancillary services ('Critical Functions') on a continuous and satisfactory basis risks eroding confidence in that bank and potentially also of challenger banks more broadly.

4.3 Effective, prudent management and governance is required for firms to ensure their own safety and soundness, and this relies on an effective board. The PRA expects a firm's board to run the business prudently, consistent with the firm's own safety and soundness and the continuing stability of the financial system. This requires firms to observe high standards of operational risk management and, as emphasised in recent policy initiatives, take appropriate measures to remain operationally resilient. Although the PRA's current, overarching operational resilience framework was introduced after the Relevant Period (specifically, in 2021), the PRA's requirements and expectations as regards managing operational resilience consolidate many long standing and well understood areas of prudential regulation that have formed part of the PRA Rulebook for several years, including during the Relevant Period.

4.4 In the context of a major strategic initiative such as an ambitious and complex IT change management programme carrying a high level of operational risk, effective, independent, well-informed oversight by the board is essential. In particular, the PRA expects boards to challenge executive management to test the robustness and prudence of their plans as appropriate; review and challenge the adequacy (including the level of detail and integrity) of any management information they receive relating to the plan and its execution, and active, regular consideration of whether implementation is consistent with prudent management and the firm's risk appetite (as approved by the board). This involves having clear escalation policies that are widely understood so that risks and crystallised issues can be managed and addressed at the appropriate level of seniority as soon as possible.

4.5 Firms should be particularly conscious of the risks of operational failure where IT services and the development of IT infrastructure upon which they rely for continuity of financial services are outsourced to third parties. They must therefore have robust outsourcing arrangements, with prudent governance and risk management and business continuity planning, commensurate with the complexity and size of the firm and the criticality, complexity and scale of the functions being outsourced. In the context of an ambitious and complex IT migration programme, this should include adopting an approach to: i) planning which sets an appropriate timetable for the migration; and ii) re-planning which ensures that the causes of issues are investigated adequately.

4.6 The PRA's rules on outsourcing apply whether a service provider is an independent third party or an intragroup provider. While certain limited aspects of firms' management of outsourcing arrangements can be adjusted in an intragroup situation (for instance, group policies on data protection if deemed fit for purpose), firms that enter into intragroup services and outsourcing arrangements must be prepared to comply with the outsourcing rules. The fact that a firm and its service provider are within the same group does not do away with the need for a careful assessment, by the firm, of whether the service provider has the ability, capacity, resources and appropriate organisational structure to support the performance of the outsourced functions, and for this assessment to be revisited where appropriate.

4.7 Firms should also assess the relevant risks of sub-outsourcing before entering into an outsourcing agreement. They must therefore have visibility of the supply chain and consider whether extensive outsourcing could compromise their ability to oversee and monitor an outsourcing arrangement. In addition, they must ensure that the service provider has the ability and capacity on an ongoing basis to appropriately oversee any material sub-outsourcing in line with the firms' relevant policy or policies. Where firms are reliant on an outsourced service provider to manage fourth parties to ensure that the firm's interests and needs are met, firms are expected to take a sufficiently *engaged and proactive* approach to oversight of the outsourced service provider.

4.8 However, firms must do more than negotiate outsourcing agreements intended to support their compliance with the PRA's outsourcing rules. Whilst the effort involved in negotiating such

agreements must be acknowledged, the firm's actual oversight of the outsourcing must also live up to the intent of the contract. Firms must be willing to take, and in fact take, prompt and appropriate action when it appears that the service provider may not be carrying out the outsourced functions effectively, including the exceptional audit of subcontractors if appropriate and necessary to address operational risk.

4.9 Key person risk can undermine the implementation of what may otherwise be a carefully designed assurance and governance framework for a complex change management project with a significant outsourcing component. This emphasises the importance of firms retaining the necessary expertise to manage the risks associated with the outsourcing, ensuring that such expertise is not concentrated in any single individual.

4.10 Firms must ensure their incident management arrangements, and those of their outsourced serviced providers, are sufficiently robust and effective. Firms must implement disaster recovery and incident management arrangements which ensure their service providers – and where relevant, their subcontractors – can effectively and promptly support the recovery of Critical Functions. The Bank/PRA's and FCA's recent policy on operational resilience (which was mostly developed and finalised after the TSB outage) strengthens and underscores firms' obligations in this area.

4.11 It is essential that Senior Management Functions ('SMFs') understand the importance of recognising the risks involved in decisions that they take. Where the decision relates to an area involving highly specialised technical expertise, which is not shared across the firm's executive and board, it is all the more important for the SMF to recognise whether the decision is his or her own to take, whether it should be escalated to a different governance forum, and the importance of explaining the risks involved in the decision to other SMFs and the board. Failing to do so means that the executive and board will make decisions in a manner that is not fully cognisant of significant risks. Such decisions must be recorded and documented to ensure the rationale for such decisions can be revisited at a later date if required.

4.12 The imposition of a financial penalty on the Firm supports the PRA's objectives. It emphasises the importance of firms' building greater operational resilience in order to mitigate the risk of disruption to the provision of Critical Functions. Improved operational resilience is a way for firms to reduce the number and impact of IT or operational incidents, and therefore reduce potential impact on financial stability. Whilst the PRA had not issued its policy on operational resilience during the Relevant Period, the PRA's 'operational resilience' framework relies on many long standing and well understood areas of prudential regulation (including rules on governance, operational risk management, business continuity planning, and the management of outsourced relationships). These rules that underpin the operational resilience framework were in place during the Relevant Period.

5. Sanction

5.1 Taking into account the facts and matters in Annex A and the relevant factors set out in the PRA Penalty Policy, the PRA concluded that the Firm's breaches of PRA Fundamental Rules 2 and 6 justified the imposition of a financial penalty of £27,000,000. That penalty was reduced by 30% to £18,900,000 because the Firm agreed to settle with the PRA during the Discount Stage.

6. Annexes/Appendices and Procedural Matters

6.1 The full particulars of the facts and matters relied on by the PRA in its decision-making process regarding the Firm can be found in **Annex A**. The Firm's breaches and failings are detailed in **Annex B** and the basis for the sanction the PRA proposes to impose is set out in **Annex C**. The procedural matters set out in **Annex D** are important. The definitions used in this Notice are set out in Appendix 1 and the relevant statutory, regulatory and policy provisions are set out in Appendix 2.

Oliver Dearie
Head of Legal, Enforcement and Litigation Division
for and on behalf of the PRA

Annex A – Facts and Matters Relied Upon

1. Background

TSB

1.1 TSB is a Category 2 UK retail bank (meaning it has the capacity to cause some disruption to the UK financial system if it were to fail) which was created by a divestment from Lloyds Banking Group ('LBG') in June 2014. TSB provides various services to its customers including personal current accounts, business banking, savings accounts, mortgages, insurance, loans and credit cards. During the Relevant Period, it had approximately 5.2 million customers. TSB's customers accessed services through digital channels (internet banking and mobile app), telephone banking and by visiting branches.

1.2 Between 2015 and 2018, TSB undertook a major IT change programme, involving the design, build and testing of a new core banking platform (the 'Proteo4UK Platform') and associated IT systems, followed by migration of TSB's corporate and customer services data on to the Proteo4UK platform. The IT change programme was developed and delivered by TSB senior executives, and governed through executive and board-level committees with TSB Board oversight.

Migration incident

1.3 TSB undertook the Main Migration Event ('MME') on 22 April 2018, during which it migrated the majority of the operation of its corporate systems, customer services and customer data to the new Proteo4UK Platform. From an early point after the system went live on 22 April 2018, whilst the data migration itself was successful, TSB encountered serious issues which significantly impacted the ability of some customers to access and use their accounts in the first few days post MME. These included certain data breaches, failures with digital banking services, telephone banking, branch technology failures, and consequential issues with payment and debit card transactions (together, the 'Migration Incident').

Migration Programme Failings

1.4 The direct causes of the technical problems experienced during the Migration Incident substantially related to issues with IT configuration, capacity and coding. However, there were also a number of failings at points during the Migration Programme and excessive operational risk ahead of the migration by the point of MME. These failings were present in planning, testing, risk management, and outsourcing. Risks were either unrecognised or not adequately dealt with,

and there were certain governance failures in escalation and challenge. Consequently, TSB went ahead with MME having not undertaken sufficient contingency planning, that would have made it sufficiently prepared for the events that took place post-MME.

Migration Programme background

1.5 Following its divestment from LBG, TSB continued to receive its core IT services from LBG, utilising the LBG IT platform (the 'LBG IT Platform'). The arrangements were governed by an outsourcing agreement with LBG, under which TSB had the option to continue to use the LBG IT Platform for a period of up to 10 years (until July 2024), or it could serve notice to exit the arrangement. The agreement provided for the following possible exit options:

a) carve-out: this option would involve the creating of a copy of the LBG IT Platform which would then be operated by a third party service provider for use by TSB independent of LBG; or

b) migration: this option would involve TSB either acquiring a third party bank and moving from the LBG IT Platform to the existing platform operated by that third party bank, or moving to a new build platform using customised applications from multiple vendors and the support of a specialist IT systems integrator.

1.6 There were benefits to TSB in continuing to use the LBG IT Platform. The benefits included access to a stable, resilient and scalable platform, through which they had the capability to offer the full product range of a major UK retail bank through multiple channels (branch, telephony, desktop and mobile).

1.7 However, there were also significant strategic factors in favour of exiting the LBG arrangement. These included the limited duration of the agreement with LBG - detracting from the benefits of its scalability, anticipated cost savings and a desire for greater strategic flexibility in terms of being able to bring about new functionality or other changes to the platform within TSB's preferred costs and timescales. In addition, TSB hoped that a successful migration would result in increased capital efficiency. The PRA had required TSB to hold additional capital against the risks associated with outsourcing to another major UK bank, and it was hoped that a successful migration would release it. TSB therefore started considering possible options for exiting the LBG arrangement soon after the divestment.

1.8 In December 2014, TSB obtained an external assessment of its different exit options from the LBG outsourcing agreement, which was considered by the TSB Board. The external assessment recommended that the preferred exit route should be a carve-out, rather than a migration to another bank's system or a new build platform using customised applications from multiple vendors. The recommendation at that point was based on there not currently being any

acquisition targets that would offer an attractive IT platform, and carve out having advantages over building a new platform where there was no '*bank in a box'* solution available that could meet TSB's needs. The plan that emerged, i.e. a European merger offering an existing IT platform (proven in Spain) which could be customised to the UK market, was not an option considered in the external assessment. The TSB Board agreed with the recommendation, but it was noted that it needed to be economically viable (In June 2015 the TSB Board confirmed carve-out as the preferred exit route following receipt of relevant financial analysis.)

Acquisition by Sabadell and the Proteo Option

1.9 In March 2015, TSB received a takeover bid from Sabadell, a bank registered at the Registry of the Bank of Spain with a history of acquiring banks in Spain and integrating them onto its IT banking platform, Proteo. At the time of the offer, Sabadell had previously migrated seven banks onto its IT banking platform, Proteo, following their acquisition, as well as conducted other integrations resulting from business acquisitions, portfolio acquisitions and carve-outs. The Proteo architecture had been developed in 2000 with Sabadell's acquisition strategy in mind. The Offer Document stated that:

> '*Sabadell estimates that it can deliver, through the application of Sabadell's skills and technology, efficiency cost savings in IT amounting to approximately £160 million per annum on a pre-tax basis, in the third full year after completion of the Offer. These expected savings derive from a full migration of the IT transitional services currently provided by Lloyds onto Sabadell's proprietary Proteo technology platform.*'

1.10 Full migration of TSB's IT services on to Sabadell's Proteo technology platform was described in the Offer Document as '*expected*'. Sabadell put together a timeline which aimed for that migration to be achieved by the end of 2017. The financial returns from the migration were part of Sabadell's strategic rationale for the takeover.

1.11 The scale of the migration project was unprecedented in the UK. Although Sabadell did have significant experience in delivering a larger and more complex platform (i.e., Proteo (Spain)), TSB's migration would be different to the migrations that Sabadell had previously undertaken in that Sabadell had not previously customised its platform to requirements in the UK. Sabadell had limited experience with the UK banking market. In addition, the version of Proteo that was in use by Sabadell at that time was Proteo (Spain). A new version of Proteo tailored for the UK banking market would be required for TSB (Proteo4UK), which was not yet proven, although it was to be created largely from the existing Proteo (Spain). By early July 2015, around the time that Sabadell acquired TSB, there was awareness within TSB of the potential challenges involved in re-platforming the entire bank successfully and on budget by the end of 2017.

TSB's IT services and initial exit options

1.12 TSB began to undertake an assessment of migration to Proteo. From July 2015, a project was established, run by a joint TSB / Sabadell team, to investigate the migration option (in terms of its feasibility, implications and attractiveness) and develop a migration plan / proposal which would be brought to the TSB Board in either late 2015 or early 2016 for discussion and, if appropriate, approval.

1.13 Sabadell had previously set out its integration methodology that it had developed on previous projects in a Change in Control application to the FCA and PRA in April 2015. The model envisaged four main phases to the project: Phase I Project Plan Design, Phase II Project Plan Execution, Phase III Migration, and Phase IV Post Integration. The work that was undertaken from July 2015 in investigating the Proteo migration option, and when a subsidiary of Sabadell began making preparations for the project in September 2015, included some of the work that was envisaged to take place early on in Sabadell's standard methodology. This included design work, as well as work on the governance and risk management framework.

1.14 By at least 14 October 2015, TSB was working on the basis of a November 2017 migration. In early November 2015, Sabadell publicly stated that TSB would complete the migration by the end of 2017, although the position of the TSB Board was that it would not migrate until it was ready.

1.15 In November and December 2015, TSB held three '*deep dives'* with the TSB Board to examine the process to create the overall plan for the migration plan, as well as the key components of the plan, concluding with consideration of the risks and benefits of carve out versus migration as the approach to exiting the arrangements with LBG.

1.16 The second deep dive regarding the proposed plan considered the complexity of the project. It was noted that the new platform would have to be proven to work prior to data migration, noting that previous bank IT migrations (including those undertaken by Sabadell in Spain) had involved either transferring data to an operational IT platform, or the creation of an IT platform, without material change to its functionality. In addition, the differentiating factors of this migration were stated to be (i) Sabadell's business operations and processes in Spain differed significantly from those of TSB in the UK; (ii) that a new IT platform was being created, a UK localised version of Proteo (Proteo4UK) with new components; and (iii) that this would be deployed in new UK data centres with a new local network.

1.17 The plan was described to have been '*designed back from the y/end 2017* deadline'. It was stated that '*The current plan is aspirational: it has been created to meet the deadlines for the Proteo build and the data migration in 2017. As such it has been created on a top-down and "right-to-left" basis*.' It was recognised that the plan would need to be verified and detailed '*left-to-right*'

plans created having regard to detailed requirements that were still to be identified. The third deep dive referred to 5 November 2017 as the intended migration date.

1.18 Following the deep dives, a TSB Board meeting was held on 16 December 2015, at which the migration option was discussed. The migration option was recommended in a memo to the TSB Board, which set out the strategic benefits of migration to the new platform, but acknowledged that migration carried a number of risks. The memo stated that '*Migrating the infrastructure for a bank of the size and complexity of TSB is an extremely challenging technical undertaking. Ensuring the combined resources of TSB, Sabadell [including its subsidiaries] and LBG are capable of delivering the migration is key*'. However, at the meeting the TSB Board did not discuss how that capability would be assessed, nor the ability and capability of Sabadell or other members of the Sabadell group of companies (the 'Sabadell Group') to meet the particular challenges of both the build and ongoing operation of the platform.

1.19 Nonetheless, the TSB Board agreed that they were minded to consider migration to Proteo4UK to be their preferred solution, but not to give up TSB's contractual right to the carve-out option at that stage. This was on the basis that further assurance was required to confirm that Proteo4UK was a stable, workable infrastructure for TSB.

Key features of the Migration Programme

1.20 By the time of the December 2015 TSB Board meeting, through a combination of Sabadell's standard methodology and the work done on assessing the Proteo Option for TSB, the key features of the Migration Programme were apparent.

Approach to migration

1.21 The papers for the first deep dive set out that there were two distinct pieces of work required for the Migration Programme: (i) the delivery of the Proteo4UK Platform, and (ii) the migration of TSB's data on to the platform.

1.22 The work for delivery of the Proteo4UK Platform would involve a standard set of project phases and testing:

a) programme planning and analysis. This would involve the gathering of the specific functional and technical requirements that TSB would have of the platform and verifying and approving those requirements;

b) design phase. This encompassed the initial platform design, and validation of the design against the agreed requirements;

c) build phase. This phase would involve detailed platform design and commencement of the build, validation of the detailed design and build with high level design and requirements, and component testing (validation of individual platform components);

d) testing. Various types of testing would be carried out to ensure the compatibility of individual components and validation against design, performance of the parts of the platform, testing of specific products as well as their integration, user acceptance of the products, and validation against original requirements; and

e) deployment of the platform, carrying out operational readiness testing.

1.23 The programme for migrating the data on to the Proteo4UK platform would typically involve a number of transition phases, each proved through a comprehensive assurance programme. These would be:

a) understanding all the primary data sources on the LBG systems;

b) mapping the LBG data sources across to the target Proteo4UK systems data model;

c) cleansing and de-duplicating the data in the LBG source systems to reduce the need for unwanted data and enable cleaner mappings;

d) building the scripts and logic to extract the data from the LBG source systems, transform it, and load it on to the Proteo4UK Platform;

e) testing to check that the data extract, transform and load processes would work;

f) Preparing for Go Live (dress rehearsals of the schedule, trial account migrations of small batches of dummy data, and live trials of live accounts); and

g) Go Live: a weekend over which the data would be migrated to the new Proteo4UK Platform.

1.24 The various stages above were more broadly encompassed in the four overall phases which, as noted above, were Sabadell's standard migration methodology as set out in its Change in Control application: Phase I Project Plan Design, Phase II Project Plan Execution, Phase III Migration, and Phase IV Post Integration. This methodology was broadly adopted by TSB.

Implementation model

1.25 Sabadell's existing methodology for IT migrations was to use a 'Big Bang' or single operation data migration approach, under which all data would be migrated in a single main migration event weekend. TSB opted for a predominantly single event data migration, although some functionality and data was migrated prior to the MME through Governed Transition Events (or 'GTEs') starting in 2017. These included the Faster Payments system, mobile app and ATMs.

1.26 TSB largely adopted Sabadell's methodology for the migration. This had three key features: (i) heavy reliance on outsourcing, with Sabadell Group IT service subsidiaries providing services related to the programme to TSB, some of those services being further outsourced to external suppliers, (ii) designing and planning the migration project by reference to gap analysis phases, and (iii) a 'Big Bang' (in the sense of a single event) data migration model where by all data would be migrated over a weekend with any exceptions to be determined through the gap analysis phases.

1.27 The reasons TSB adopted a predominantly single event data migration, phased by functionality were:

a) the challenges of attempting a staged migration, particularly those related to moving from a platform hosted and operated by one provider to another;

b) the costs of a staged migration;

c) its belief that LBG was resistant to a staged approach; and

d) its belief that there were advantages in doing so, including having the least impact on customers. For example, it would have been impossible for customers to retain a single view of their products, in the event that a migration was staged by product, or sort code.

Inability to revert to the LBG platform

1.28 A predominantly single operation creates certain risks. Given the entire customer base is being migrated at essentially the same time, if a significant problem is encountered when the new system goes live then it has the potential to cause serious customer harm. Sometimes, a firm will have a '*roll-back*' plan, where, in the face of major problems, it can revert to the previous system. A '*roll-back*' plan was not possible for TSB in these circumstances.

1.29 Under TSB's arrangements, it was contractually required to notify LBG of its intentions to exit the agreement via migration (and thereby waive its right to the carve-out option which it would

otherwise retain until 31 March 2019). Once it had done so, TSB would not be able to continue to use LBG's platform long term. In addition, following the data migration there would be a very short window to stop the LBG platform from being disabled. Consequently, after MME it was, technically speaking, essentially impossible to roll back from the changes made and revert to using the LBG platform instead of Proteo4UK.

1.30 There was awareness at TSB of this risk. The minutes for the December 2015 TSB Board meeting recorded that '*the Board could not be put in a position where they gave up the carve-out option, migration "stalled" or was found to be unworkable leaving the bank in a position without an IT infrastructure*.'

Outsourcing

1.31 TSB's Migration Programme was heavily reliant on outsourcing, with Sabadell Group IT service subsidiaries providing services related to the programme to TSB, and some of those services being further outsourced to external suppliers. TSB appointed Sabadell's IT service subsidiaries, SABIS Spain and a new UK subsidiary, Sabadell Information Systems Limited ('SABIS UK') (together 'SABIS') to provide the required services in relation to the Proteo4UK Platform, with SABIS retaining contractual responsibility for the work of any external suppliers which it appointed.

1.32 The relevant contracts were:

(i) the Migration Services Agreement ('MSA') between TSB and SABIS Spain (and from 18 May 2018, SABIS UK) which governed the design, build and testing of the Proteo4UK Platform, and which required SABIS Spain to implement a two year plan to build Proteo4UK and migrate TSB's data to it; and

(ii) the Outsourced Services Agreement ('OSA') between SABIS Spain, SABIS UK, and TSB, which governed the operation of the Proteo4UK Platform by SABIS following migration.

Operational Risk

1.33 The Migration Programme was a *'complex and ambitious plan'* which contained significant operational risk. Migrating customers off a third party platform via a predominately single event migration, to a newly built platform (albeit created largely from the existing Proteo (Spain) platform). The Proteo4UK Platform was an unproven version of the existing Proteo (Spain) platform and required significant customisation to meet TSB's requirements and the UK market. Migration off the LBG Platform to Proteo4UK was irreversible, creating risk if any major issues arose. The migration would also involve the cooperation of LBG, as the owner of the original platform on which the data was based, as well as SABIS and its numerous external suppliers. In

addition, TSB was trying to achieve the entirety of the Migration Programme in two years, when even simply building a new platform in the UK in under three years was unprecedented.

1.34 In order to mitigate the risks of the migration approach, TSB would need to ensure the Proteo4UK platform worked ahead of the migration date, as well as have reasonable plans in place to ensure minimal customer impact and detriment if the migration did not work as planned.

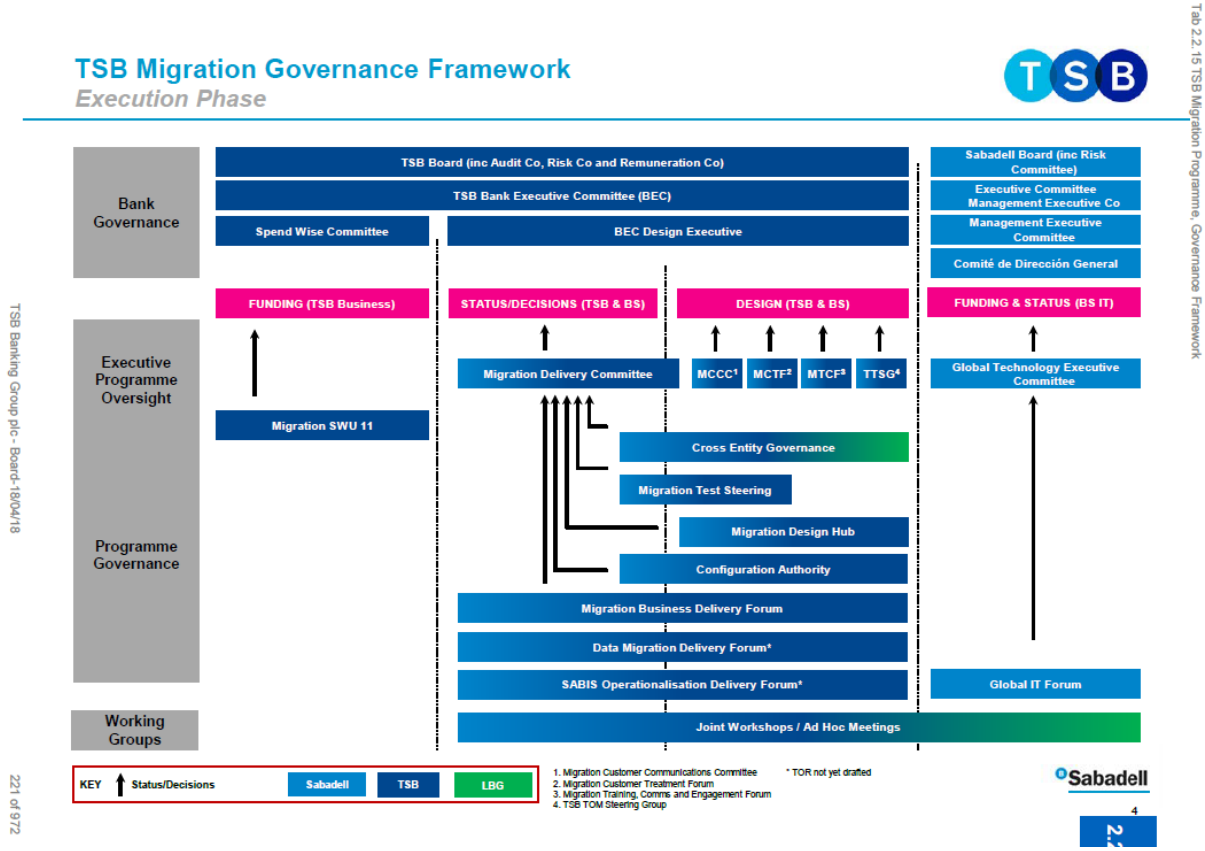
2. Migration Programme Governance and Risk Management Frameworks

2.1 The early planning stages also involved work on the Migration Programme governance and risk management frameworks. This section sets out what the developed frameworks for the Migration Programme would ultimately be.

Governance

2.2 TSB established an extensive governance framework to oversee the Migration Programme. Figure 1 below shows the governance framework as at MME. Whilst the governance framework underwent a series of revisions during the Migration Programme, these are not material to the key aspects of the framework as summarised below.

Figure 1:



TSB Board and Board Committees

TSB Board

2.3 The TSB Board had ultimate oversight of the Migration Programme, as well as of key developmental aspects of the assurance framework. The TSB Board was responsible for making key strategic decisions during the Migration Programme. These included:

a) approving the detailed Migration Programme plan;

b) approving the issuance of the exit notice in respect of TSB's contractual arrangements with LBG;

c) approving the migration test strategy;

d) approving various events ahead of MME such as the decision to enter into live trials, and entry into the faster payment scheme;

e) approving the strategy for the MME weekend, and business readiness and post Go-Live plans; and

f) approving the decision to go ahead with MME (which also required approval of the Sabadell Board).

2.4 Ultimately, the TSB Board delegated authority to a sub-committee to grant approval to an Executive Gold Team to initiate MME.

2.5 The TSB Board was assisted at times during the Migration Programme by independent advisers to help ensure that the TSB Board '*asked the right questions of the executives and enabled the TSB Board to discharge its oversight responsibilities effectively during the Migration Programme*'. The advisers were in place between April and November 2016, and from April 2017.

Board Committees

2.6 The Board Audit Committee ('BAC') was the primary Board level governance forum for oversight of the programme, receiving regular updates and scrutinising the progress of the programme. It reported to the Board. The Board Audit Committee provided oversight of the management of the Migration Programme risks as they affected the delivery of the programme and its objectives. It

also provided assurance on the internal controls and risk management system, of the Migration Programme in consideration of these risks.

2.7 The Board Risk Committee ('BRC') oversaw the management of the programme risks as they may have affected TSB's business as usual ('BAU') activities. It also reported to the Board.

Executive Committees

Bank Executive Committee ('BEC')

2.8 The BEC was TSB's principal executive committee. Its role was to provide collective support in developing and implementing the TSB's strategy, monitoring business performance and agreeing any actions required to manage issues affecting TSB.

BEC Design Executive ('BEC DE')

2.9 The BEC DE was established in early 2015 and was the main executive forum through which TSB ran the Migration Programme. It reported to the BEC. The BEC DE was accountable for the economic and competitive position of TSB through prioritisation of investment and the design of change. It was also responsible for the ownership and design of the target operating model of TSB and the end state of the IT Migration Programme through enforcement of design principles, and the ownership and governance of the migration plan to align and deliver the strategic objectives.

2.10 Key programme-related decisions were made by the BEC members at the BEC DE. For example, under the MSA key decisions relating to the design and effective implementation of the Migration Programme (such as the migration plan) were approved by the BEC DE.

Other key committees

2.11 A number of other Migration Programme-specific committees and working groups operated below the BEC and BEC DE. The two below were the most significant:

Migration Delivery Committee ('MDC')

2.12 The MDC was established under the MSA. It reported to the BEC DE. Its role was to provide an over-arching governance and decision making forum for the design and effective implementation of the migration. It delivered the migration plan to the BEC DE for approval and oversaw the

delivery of migration and the end-to-end progress of the build, testing, implementation and Go Live (i.e., going live with the Proteo4UK Platform).

Migration Test Steering (also known as the Migration Testing Forum)

2.13 The Migration Testing Forum reported to the MDC. It was accountable for providing over-arching governance and decision-making forum for the testing delivery domain of the Migration Programme, and for approving any test delivery domain decision through to the MDC. It was responsible for overseeing the effective delivery of testing, the end-to-end process of the critical path for all stages of the testing life cycle, it supported the testing teams managing risks and issues, and also supported the control of the deliverables and managing testing domain costs.

Risk Management

2.14 TSB used its Risk Management Framework to manage risk generally, using a '*three lines of defence*' model outlined in the framework.

First Line of Defence

2.15 The first line of defence was the business areas ('Business Areas') (also known as the BEC business functions), which were headed by BEC members and supported by business unit control functions. Business Areas had primary responsibility for risk decisions and actions as well as measuring, monitoring and controlling risks within their areas of accountability. They were responsible for identifying, assessing, managing and mitigating the risks relevant to their areas, and for establishing controls to ensure compliance with TSB's policies and the risk appetite parameters set out and approved by the Board.

Second Line of Defence

2.16 The second line of defence was TSB's risk oversight function ('Risk Oversight'). Risk Oversight was responsible for providing independent oversight and challenge, and TSB-wide risk reporting. It recommended risk strategy and TSB's risk appetite to the Board, as well as advised the business and facilitated design and embedding of policy and compliance. As part of the migration Risk Oversight was responsible for undertaking independent oversight of TSB elements of the Migration Programme, facilitating the creation of remedial activities to mitigate gaps, and monitoring, reporting and escalating as required.

2.17 From August 2017, the external consultancy firm operating in the Business Areas moved to assist the Risk Oversight in the run-up to Go Live, including making assessments of the risks associated with the migration and conducting deep dive reviews on migration build and test activities.

Third Line of Defence

2.18 TSB's third line of defence was its internal audit function ('Internal Audit'). It provided independent and objective assurance over the Business Areas' management of risk and control, and Risk Oversight's supervision of TSB's risks. It also reported on the effectiveness of TSB's risk management activities to the Board and senior management. For the Migration Programme, its focus was on whether the key risks were being adequately addressed and reported, and the information presented to decision-makers was fair, balanced and reasonable; reviewing the design and effectiveness of key programme controls, and challenging executive management to improve risk management, governance and control.

2.19 TSB also supplemented risk management resource with extensive support and involvement from external consultants, who initially operated in certain Business Areas. The external consultants also attended the Board and the BAC at key points throughout the programme. The consultants undertook a broad range of reviews, producing over 40 reports across planning, management controls and governance, solution design and code quality and target state for completeness, as well as to provide general observations on the Programme, as well as later support to Risk Oversight.

3. Programme Planning and Execution

Design phase

3.1 The Design Phase had been initiated during the initial project planning between July and December 2015. The Design Phase involved defining TSB's requirements. These were the functional requirements defining '*what a system is supposed to do' and the non-functional requirements defining 'how a system is supposed to be'* (the '*what*' and the '*how*' being a '*dossier*').

Gap analyses

3.2 To define TSB's requirements, three gap analyses were undertaken:

a. a UK gap analysis: this was an initial overview of country level gaps between the UK and Spanish banking market, identifying where Proteo would have to be customised so that it was suitable for UK products and the UK regulatory environment;

b. a Macro Dossier gap analysis: this involved identifying high level functional gaps between TSB and the current Proteo platform at the macro level. This would be used to inform a number of matters, including the architecture design and identifying functions to the 'Big Bang' (in the sense of a single event) data migration model; and

c. a Dossier Phase: this was intended to be a detailed gap analysis between TSB and the current Proteo platform at the micro level.

3.3 The UK gap analysis and the Macro Dossier gap analysis were completed ahead of the December 2015 TSB Board meeting. TSB had originally also intended to complete the Dossier Phase by December 2015, but were still working on it in March 2016 by which time they were three months behind schedule.

3.4 The plan to build the platform and migrate data by the end of 2017 (which had been presented to the TSB Board in November 2015), was intended to be verified through defining detailed requirements in the Dossier Phase. It was intended to achieve an understanding of TSB's detailed functionality requirements and identify all gaps, which would in turn inform several key inputs to the overall Proteo4UK design, such as target IT architecture, functional design and application requirements. There were approximately 150 '*dossiers*', which were '*like chapters of a book that describes how a bank works*' and which had to be signed off by a senior executive with responsibility for that dossier.

3.5 Difficulties occurred during the Dossier Phase due to lack of clarity about the level of detail and quality required in functional design documents that were intended to record these requirements. This resulted in regular requests to business leads to undertake additional work and to inconsistencies in functional design content. The resulting delays meant that the Dossier Phase did not fully complete until at least April 2016.

3.6 Nonetheless, TSB intended to present a consolidated programme plan to the Board in mid-March 2016. By that point, TSB had identified 115 country gaps, and 296 macro-dossier gaps (of which 46 were considered to be critical). Whilst the Dossier Phase was still ongoing, TSB had identified that 80% of the desired functionality would be covered by Proteo and existing third party applications, with the remaining 20% to be provided by '*best of breed*' 3rd party solutions already localised in the UK market.

3.7 This meant that customisation and integration would be needed to meet TSB's requirements and those of the UK market. (Ultimately, the Proteo4UK Platform required 221 applications and significant customisation: 69 already existed in Proteo, 81 were non-Proteo applications but

would be used for TSB, 13 were new Proteo applications designed for Proteo4UK, and 58 were new third-party applications to be implemented for TSB.)

March 2016 IMP

3.8 On 15 March 2016, the Integrated Master Plan ('IMP') was presented to the TSB Board as the overall plan for the Migration Programme. As with the '*aspirational*' plan presented to the Board in a deep dive session in November 2015, the IMP planned for MME to take place in late 2017, on 5 November 2017, however, TSB remained of the view throughout that it would not migrate until it was ready. This two year timeframe would also be agreed to in the MSA.

3.9 The target of late 2017 for migration was maintained despite TSB being three months behind schedule for completing the Design Phase. The fact that it had not yet completed meant that TSB prepared a plan in circumstances where it had not yet finished defining its requirements (what the system was supposed to do and how it was supposed to be). This ran the risk that the draft plan might not reflect the true amount of work required if, as dossiers were signed off, dependencies were identified which would make it necessary to revisit requirements and solutions for other dossiers or if assumptions underlying some of the dossiers (such as the use of a particular third party) did not hold true. Commencing work on the infrastructure before TSB's requirements had been finalised created a risk of having to revisit that work if the assumptions underlying it (for example, as to capacity) turned out to conflict with the eventual requirements. This risk was flagged to the TSB Board by Internal Audit. Specifically, Internal Audit noted that, '*although the level of detail and quality required had not always been clear at the outset of the phase…documentation was now becoming more consistent*' and concluded by confirming that they '*did not consider there to be any reason why the migration programme should not proceed to the next stage*'. In response, the TSB Executive acknowledged Internal Audit's report and noted that '*The risk exposure to TSB through the programme is understood and being managed*'.

3.10 The IMP was divided into five phases, four of which had some overlap, as follows:

a. design Phase – to be completed in June 2016;

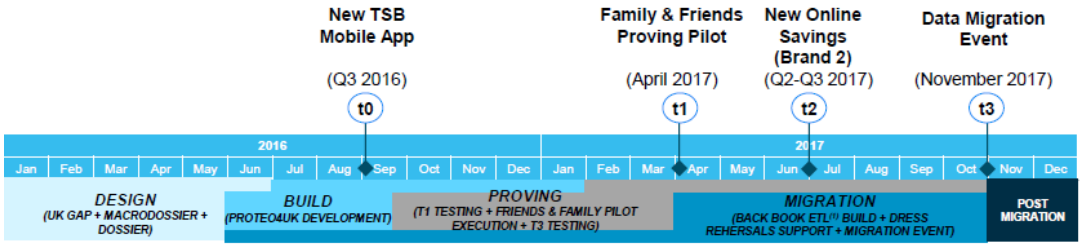
b. build Phase – from May 2016 to January 2017;

c. proving Phase – from September 2016 to November 2017

d. migration – from May 2016 to November 2017;

e. post Migration – after MME.

Figure 2:



3.11 The IMP intended that the Migration Programme would be delivered through four transition events (the first three of which would comprise some, but not all, of the GTEs):

a) t0 – launch of the new TSB mobile app;

b) t1 – execution of a Friends & Family proving pilot, involving operating a fully functional live version of the new platform for a pilot set of friends and family customers as a proving event for the platform;

c) t2 – launch of a new online savings product (although ultimately there would instead take place t2a, a mortgage sales and origination transition); and

d) t3 – the MME itself.

3.12 The key build and testing milestones set out in the IMP included:

Phase	**Expected completion**
Design phase	
Functional design of the Proteo4UK application software	March 2016
Technical design of the Proteo4UK application software	June 2016
Build Phase	
Build of the Proteo4UK application software and unit testing	End of September 2016
System integration testing ('SIT') of the Proteo4UK application software	End of January 2017
Functional testing	
User acceptance testing ('UAT')	End of March 2017
Migrated data testing ('MDT')	August 2017
Non-functional testing	
Non-functional testing ('NFT') (various types)	End of July 2017
Testing of data migration	
Migration acceptance cycles ('MACs')	August 2017

Phase	Expected completion
Design phase	
Dress rehearsals	End of September 2017

Testing under the IMP

3.13 The IMP envisaged that there would be a period of essentially sequential testing following the build of the Proteo4UK Platform. The build phase would include unit testing (testing each isolated unit of the application code) and then system integration testing. This stage included system testing (bringing together application components and subsystems to verify the system will operate in line with requirements), within the overall system integration testing (validating that the system will integrate technically and operate successfully with external systems and applications).

3.14 Testing following the build phase would consist of functional testing, non-functional testing ('NFT'), and testing of data migration.

Functional Testing

3.15 Functional testing was used to test the Proteo4UK Platform's functional requirements (i.e., that the functionality, which was delivered during the build phase, worked as it was meant to). An example would be whether customers could make payments via particular apps.

3.16 Functional testing under the IMP consisted of UAT and MDT:

a) UAT involved testing the Proteo4UK Platform to ensure that TSB's functional business requirements had been met and that the TSB business users were satisfied. This testing used synthetic data rather than data that was migrated across from the LBG IT Platform; and

b) MDT involved conducting UAT using real data that had been migrated across from the LBG IT Platform to ensure TSB's functional requirements had been satisfied.

NFT

3.17 NFT was used to test the Proteo4UK Platform's non-functional requirements (i.e., how the system was supposed to operate). An example would be its performance requirements, such as how many customers could log in to apps at any one time.

3.18 NFT consisted of infrastructure testing, performance testing, security testing, and disaster recovery testing:

a) infrastructure testing – used to verify that all the environments were stable, had sufficient capacity to perform volume tests, and that software had been deployed safely;

b) performance testing – used to validate that the application functionality satisfied the system non-functional requirements, for example transaction response times;

c) security testing – used to verify that security measures (such as firewalls, authentication servers, access control products, monitor and intruder detection, and so on) have been implemented to mitigate risks identified by the parties; and

d) disaster recovery testing – used to validate that the infrastructure built to serve as an alternative in case of a major failure in order to provide service continuity.

3.19 It would also ultimately include operational acceptance testing (which verifies the operational readiness of a product, software, application or service before it is released to production (i.e., into live).

Testing of data migration

3.20 Testing of data migration was used to validate that data could be transferred from the LBG IT Platform to the Proteo4UK Platform following the design and build of relevant data migration tool and processes. It involved:

a) MACs – these tested the migrated data during the extract, transform and load process to confirm such matters as the quality of the data and whether it could be migrated within certain timescales; and

b) dress rehearsals – these were essentially MACs carried out in the timeframe that would be required for MME.

Approval of the IMP

3.21 Aware that the IMP timescales were '*challenging, with little contingency*', the TSB Board decided to authorise the BEC to commit the required resources to develop the migration option. At the same meeting, the TSB Board requested that TSB develop a fall-back plan should migration not be possible, to avoid the risk of having no infrastructure on which to operate.

Migration Programme delays and the September 2017 decision to re-plan

Programme delays

3.22 Delays in the Migration Programme became apparent in the months following the approval of the IMP. A review of the IMP by an external consultant in April 2016 noted that the plan broadly covered the major activities typically seen in programmes of a comparable size, but made a number of recommendations for improvement, including that third party delivery milestones should be integrated into the plan and their commitment to deliver secured, otherwise this could significantly impact the timing of the critical path. But by May 2016, TSB had tracked the fact that there were delays in a number of work streams, including infrastructure delays caused by engagement issues with third parties, and UAT delays in a number of areas.

3.23 Thereafter functional testing, in particular UAT, fell behind schedule early on. A Migration Programme update provided to the TSB Board for its meeting on 19 October 2016 stated that the IMP which was '*high level*' had intended for '*the complete build of the whole bank moving as one complete entity through each of the different test phases*', with SIT completing by the end of September 2016, and UAT then following on immediately. However, while the same update noted that while the IMP '*anchor points*' had been held, SIT had been delayed due to issues with the stability of the test environment, and not all of the build had been completed by the end of September due to a combination of design complexity and fully integrating plans with third parties.

3.24 The update noted that to mitigate the delays and to maintain the critical path of the IMP to t1 (the planned '*Friends and Family*' launch which was itself to be conducted in a phased approach), the testing had been split into tranches so that as each tranche completed SIT, it would then enter into UAT (rather than fully completing SIT across all the tranches first). The update noted that there was no compromise to UAT scope, and the tests planned ensured that the end-to-end bank would still be completely tested as the phased approach completed. That month an external review of the Migration Programme noted that '*third-party dependencies present challenges, resulting in increased parallelisation of the plan*' and that while positive progress had been made in agreeing the plan interlocks with relevant third parties, '*there is felt to be a lack of clarity around IT delivery dates [which] could lead to challenges within multiple teams and workstreams when increasing plan granularity*'. This increased pressure on resources and they advised that careful management was required to reduce inefficiencies due to duplication and re-work. In December 2016, the PRA advised TSB that its approach to parallelisation involved a certain amount of risk, which needed to be transparent and visible to the key stakeholders, and that the PRA would expect TSB to have appropriate measures and actions in place to mitigate the risks involved with this approach.

3.25 A few months later it was noted in an update for the TSB Board meeting on 22 March 2017 that the planned deadline of the end of April 2017 (already extended from the end of March) for the first phase of UAT would not be met, and that this would need to be re-planned, with a further check on whether they were delivering on the revised plans in May. It was made clear there would be no reduction in UAT scope and that the number of defects captured per test continued to be lower than expected – with most of the failures associated with a lack of full functionality to test – with only 18% of failures relating to genuine user defects. The update to the Board stated that the delay was due to having less functionality available to test than planned, and that the IMP had not reflected with sufficient accuracy dependencies at a very detailed level on design decisions.

3.26 On 23 May 2017, a further Migration Programme update report for the TSB Board stated that, following the review of the UAT plan, completion of the first phase of UAT had been delayed by three months from the end of April to the end of August 2017.

3.27 In late July 2017, the PRA wrote to TSB, noting that successful delivery of this project was key to releasing future financial and operational benefits for TSB with only three months to go until the MME, there was still significant work to be done and that TSB continued to be reliant on third parties to deliver elements of the plan. It also noted that, due to rescheduling, some elements, such as UAT, were being delivered several months later than initially planned. The PRA accepted that while this might give more realistic timelines, it would also '*increase the volume of work to be delivered in the final months and could put pressure on TSB to cut corners'*. The letter referred to TSB having agreed a contingency migration date in early 2018, saying that the PRA took comfort from this *'as it is essential that TSB does not accept lower standards to deliver on time'*. TSB acknowledged the PRA's concerns and noted that the PRA did not raise any significant new risks or issues that TSB was not already aware of. TSB resolved to make the PRA aware of any issues that could delay the planned November migration date.

The decision to re-plan

3.28 By September 2017, it was apparent that there was little chance that TSB would be ready to migrate by November 2017, and work would therefore begin on a replan. At that point the reasons why TSB would not be ready to migrate were: (1) delays in the second data centre; (2) problems with cleanliness of data in different MACs; and (3) the difficulty to complete UAT.

3.29 It was reported to the TSB Board at a meeting on 20 September 2017 that TSB would not be in a position to complete the data migration in November 2017. In doing so, the Firm acknowledged that the November 2017 migration target date had been set two and a half years previously and was '*deliberately very ambitious*', had acted as a '*forcing mechanism*' to ensure that the business and suppliers worked '*at pace*' but had been '*based on very little information*'. The report stated '*When we forecast a new T3 migration date we will do so from a much more informed position.*

We want to re-plan the date for T3 once and with confidence. We will only do that one all "known unknowns" in the Programme have been identified…We expect to confirm a new date in early October'. The TSB Board resolved to '*ask the executive to start taking now the steps necessary to re-plan*' the migration for a possible MME taking place in either early/mid-February 2018 or on another date that was consistent with its safe and effective delivery.

Delay announcements

3.30 On 29 September 2017, nine days after resolving to commence the re-plan of the migration, and before completing the re-plan and determining a new date for MME, TSB issued a news release announcing that it would be delaying MME and re-planning it into Q1 2018. In publicly announcing that it was re-planning MME for Q1 2018 before having completed the re-plan, TSB needed to ensure the re-plan fitted that timeframe, and could have been exposed to operational risk if the migration did not occur within or close to that timeframe.

October 2017 Defender Plan and subsequent further programme delays

The Defender Plan

3.31 TSB's re-planning exercise resulted in the presentation of a new plan (the 'Defender Plan') at the TSB Board deep dive meeting on 24 October 2017. The Defender Plan was accompanied by a re-plan memo which set out the approach to the re-plan, a high level summary of the new plan with risks and recommendations.

3.32 The re-plan memo stated that the Defender Plan had been produced by the BEC with involvement from Risk Oversight and Internal Audit, refreshing '*from the bottom up*' the key activities needed to be completed to deliver MME and incorporating the experience developed over the last c.24 months in estimating the time required to complete each of the activities.

3.33 The re-plan memo explained that analysis of the re-plan had involved: (1) identifying the plan which would enable TSB to be *'migration ready'* at the soonest point possible in 2018 consistent with a '*safe*' migration and with the guiding principles (discussed in paragraph 3.36 below); and (2) identifying the steps necessary to agree with relevant industry participants a number of options for the MME weekend consistent with (1). The options for the MME weekend that had been identified were 16 – 18 March, 23 – 25 March and 20 – 22 April 2018. It was emphasised that this was a plan to be '*Migration Ready as soon as possible in 2018…currently envisaged to be Thursday 15 March 2018'*, and then *'to "land" the migration weekend in one of the agreed slots*'.

3.34 The key testing milestones set out in the Defender Plan (and as compared to the original milestones in the IMP) included:

Phase	**Expected completion under the IMP**	**Expected completion under the Defender Plan**
Functional testing		
UAT	End of March 2017	December 2017
MDT	August 2017	December 2017
Regression testing for UAT and MDT	N/A	End of December 2017 to end of January 2018
Non-functional testing		
NFT (various types)	End of July 2017	End of November 2017 (with additional NFT for extra-assurance by March 2018)
Testing of data migration		
MACs	August 2017	End of January 2018
Dress rehearsals	End of September 2017	End of February 2018

3.35 These stages reflected the two work streams in progress. The first, to deliver the core capability (the platform) by the end of 2017, and the second to prove the migration, extract, transform and load process through the MAC and MDT cycles.

3.36 The Defender Plan set out various assumptions, dependencies and risks for the plan, with the re-plan memo identifying the most significant risks. The Defender Plan also set out 15 guiding principles ('Guiding Principles') to guide and test the re-plan, based on the principles behind the migration work to date and supplemented with new principles developed from the learnings over the last 24 months. The Guiding Principles included:

a) reduced levels of parallel work streams (Guiding Principle 3);

b) the achievement of a clean MAC (i.e., events which were designed to test the migrated data at each stage of the extract, transform and load process, to confirm, for example, the quality of the migrated data and the ability to meet the required timescales) before the start of dress rehearsals (which were a version of MACs carried out in '*real time*' to confirm that the combination of software, people and processes could achieve the migration) (Guiding Principle 4);

c) an explicit regression test phase (re-execution of UAT and MDT tests following their original successful test phases, to ensure that the functionality still performed as intended despite interaction with new code that had been subsequently deployed) (Guiding Principle 10).

3.37 The Defender Plan also extended the period for production (i.e., live) proving until the platform was deemed to be migration-ready. It was intended to use the extended production proving to confirm the maturity of the target operating model between TSB and SABIS. In addition, the Programme would learn from the t2a (Mortgages Governed Transition Event) experience to '*more fully prove*' new capability in the production environment at volume. The initial part of the proving pilot, Friends & Family, had used a scripted set of activities. This part of the proving pilot, which was referred to as TSB Beta, would involve an unscripted set of activities carried out on a wider scope of products and channels, using up to 2,000 TSB staff customers to flush out configuration issues and operational issues. The longer period of production proving was also intended to mitigate the issue that the then relative immaturity of the operating model had resulted in incidents for services already in live production.

3.38 At the deep dive meeting in October 2017 the TSB Board did not provide sufficient challenge to the Defender Plan. Whilst some challenge was subsequently provided at the deep dive meeting in January 2018, the TSB Board had missed an opportunity to challenge whether or not the assumptions in the re-plan in October 2017 were reasonable and whether the proposed plan was realistic. The TSB Board approved the plan and *'requested the Executive to dedicate the time and effort to the Migration Programme required to ensure that TSB was, consistent with a safe migration and with the Guiding Principles in the deep-dive papers, Migration Ready as soon as possible in 2018. This was currently envisaged to be no earlier than Thursday 15th March 2018*'.

3.39 The re-plan was an opportunity for TSB properly to consider what was still required to be achieved before MME and ensure that a suitable and realistic plan was put in place. Whilst the re-plan memo stated this had been done, the Defender Plan put together by the BEC and considered by the TSB Board did not clearly set out how far behind schedule the Migration Programme was, the reasons for the delays, and their impact on future timings. The Board had, throughout the programme to date, been provided with regular updates on the status of the programme. However, insufficient consideration was given at the time of the re-plan to these issues and to the likely and realistic time needed to complete outstanding remaining tasks (such as testing, build and business continuity) for the Migration Programme to be ready, in circumstances where TSB had publicly committed to a Q1 2018 MME.

3.40 For example, in a report dated 19 September 2017 an external consultancy firm advising on Migration Programme assurance, a re-plan was required for the remaining UAT test cases and regression cycle, as the existing target could not be met. The day before, it was acknowledged at the BAC that action was needed to tackle the progress of UAT. Progress on UAT was being impaired by missing functionality. It was also impaired by environment instability and slow defect turnaround times (which were recognised in the prior BAC update). They noted that they could

not see evidence that the defect resolution rates would improve sufficiently to exit UAT on schedule for the original MME. The firm projected in September 2017 that at the current rate of passing UAT tests, based on evidence collected from the last five months, it would take 33 weeks to pass all 100% of in-scope test cases (i.e., into May 2018), or 23 weeks if TSB reduced the scope of the tests down to 38,848 test cases (i.e., until the end of February 2018). This was on the assumption that as functionality was complete, there would be a tipping point at which point tests would be able to run at a faster rate than had previously been the case.

3.41 However, the Defender Plan projected completion of UAT by the end of 2017, with the exception of ten dossiers projected to complete UAT by the end of January 2018, based on a reduced scope of 39,278 test cases (i.e., more than the reduced scope envisaged by the external consultancy firm and starting at a later date). The projected completion date was based on ambitious assumptions such as there being sufficient IT capacity to fix all high and urgent defects, change requests (defects identified in the design during testing) and regulatory changes in time to be tested by Christmas, that no new business defects would be identified by testing, and that the remaining outlying dossiers could increase the pace of delivery and close out UAT within the allotted time, as the remaining functionality was completed and ready to be tested .

3.42 The Defender Plan did not contain any analysis of why those assumptions and dependencies were considered to be reasonable. The accompanying Risk Oversight opinion stated that the re-plan assumptions were reasonable, that there was a rationale for every improvement expected, and the key risks were declared by the Business Areas. However, it also noted that due to the short timescales of the re-plan their opinion was based on observation of workshops and document review of the steps taken to develop the re-plan and a high level opinion on the Defender Plan itself, and that control based deep dives had not been completed. Internal Audit found the assumptions made to arrive at the re-planned MME date to be satisfactory overall, but noted that they had not tested the *'bottom-up'* details supporting the re-plan such as the capacity of SABIS (who were responsible for fixing defects and dealing with change requests) to deliver in line with the re-plan assumptions and as such this was identified as a risk, and remained subject to difficulties.

3.43 The Defender Plan noted that while the Guiding Principles reflected the experience of the Programme, and learnings to date, there were a number of key areas which required further detailed work to fully assure the plan. Eight such areas were identified, one of which was IT capacity to deliver the change requests and defect fixes to this plan. Consequently TSB was driving forward a plan to achieve a Q1 2018 MME in circumstances where it had not completed the detailed work to assure some of the ambitious assumptions it was based on, and which related to issues that had been occurring in the Migration Programme to date. As would become apparent shortly, the Migration Programme did not progress in accordance with the Defender Plan, and one of the areas which fell behind schedule was UAT, with defects and change requests continuing to arise and resolution rates not sufficiently improving.

Further programme delays

3.44 As had happened with the IMP, the Defender Plan also quickly fell behind schedule. By the time of the TSB Board meeting on 21 November 2017 (one month after approval of the Defender Plan), UAT was reported to be '*marginally behind plan*' and '*we have not seen the expected reduction in overall defect numbers and the current trajectory is not consistent with completing the majority of dossiers before Christmas*'. At the BAC meeting the day before, concern had been expressed over the degree of parallelisation of work streams, the volume of matters flagging red and amber, there being no contingency apart from the proposed landing slots, and whether a landing slot in March was possible.

3.45 By mid-December 2017, although UAT was 85% complete, it was clear that more UAT completion would now slip into January 2018 than originally envisioned. This was in part due to the need to resolve high severity infrastructure connectivity defects, issues with environment stability and dependency on other upstream testing or defect resolution.

3.46 At that point negotiations with LBG and other third parties were also continuing to agree suitable dates for MME. By 12 December 2017, TSB had agreed potential '*landing slots*' for MME in April 2018.

3.47 In the meantime, the programme continued to fall behind schedule. On 18 January 2018, as part of its monthly Risk Oversight review of Migration Programme risks, Risk Oversight opined to the BEC if MME were to be achieved in April 2018, '*it will be difficult to avoid increased levels of parallel activity, to achieve a clean MAC cycle before commencement of dress rehearsals, or to allow an explicit regression phase after completion of UAT and MDT*'. This meant that TSB was therefore aware, and had accepted, that there would be deviation from three of the Guiding Principles (Principles 3, 4 and 10) put in place to minimise operational risk arising from the pace of delivery required by the Defender Plan if TSB wished to migrate, as was then anticipated as being possible, in April.

3.48 At a migration deep dive meeting of the BAC on 22 January 2018, to which other members of the TSB Board were invited, a paper was presented on the glidepath to being migration ready at the end of Q1 2018, reviewing completed and outstanding tasks, and assessing how the programme had performed against the Guiding Principles.

3.49 Whereas under the Defender Plan it had been intended to complete the MAC cycles before starting the three dress rehearsals, and having an explicit regression testing phase once UAT and MDT were complete and stable, the new glidepath to MME included continuing to run downstream testing alongside the other activities of the plan including dress rehearsals, with regression activities now to be carried out following completion of the majority of UAT and MDT

rather than all of it. As noted above, this would comprise deviation from Guiding Principles 3, 4 and 10.

3.50 Also in January 2018, completion of the migration to the Defender Plan timetable took on additional significance. TSB became aware that maintaining its *'Internal Ratings Based'* approach to capital required TSB to migrate to the Proteo4UK Platform by June 2018. Risk Oversight flagged this as a key strategic financial risk which '*may be amplified by any further delays to migration*'. This pressure was described by Risk Oversight as '*a regulatory reputational risk'* and '*a public reputational risk*' with the MME in April 2018.

3.51 On 23 February 2018, Sabadell announced publicly at an investor event in London that the MME would occur on 21 April 2018. If TSB were to go live on that date it would need to ensure that it would indeed be ready by then to go live despite the delays and compromises introduced into the programme.

3.52 On 8 March 2018, the PRA emailed TSB noting that there was still a lot to complete before the end of April, but that the PRA had taken comfort from the fact that a back-up date had been agreed in May. The email conveyed the PRA's view that if those dates were not viable, migration would have to be deferred until at least August. The PRA noted the potential for increased opportunities for resilience and outage shocks should TSB migrate in April or May with a lesser scope of activity implemented' (i.e., if TSB decided to undertake a more phased migration than that which was then anticipated). In the same email the PRA also noted that pressure on staff could be an issue if migration continued to be delayed beyond April 2018. The PRA notified TSB of triggers that would increase its concerns, being '*(1) slippage with delivery; (2) UAT and/or the dress rehearsals fail or do not fully pass; and (3) further de-scoping of activity or extended plans'*.

3.53 By March 2018, with large numbers of defects remaining in the functionality still being tested, there was an increasingly urgent concentration on identifying '*must-have*' functionality required for MME to go ahead on the weekend of 20-22 April 2018, and on creating workarounds or deferring functionality where tests were not passed. The frequency of the meetings of the Migration Deferred Defects Forum, where such matters were discussed, was increased and the length of each session extended. Functional and non-functional testing was expected to continue until the end of March 2018.

3.54 Risk Oversight noted that due to delays in the completion of functionality and testing, there was limited capacity for regression testing or proving the edges of the solution, and that it was likely that some material defects would emerge post-Go Live, although it noted that the programme planned to retain capacity and expertise to resolve those defects quickly.

The April 2018 'go live' decision

3.55 A number of important governance meetings took place in the course of April 2018, which ultimately resulted in TSB deciding to proceed with MME (the decision to Go Live).

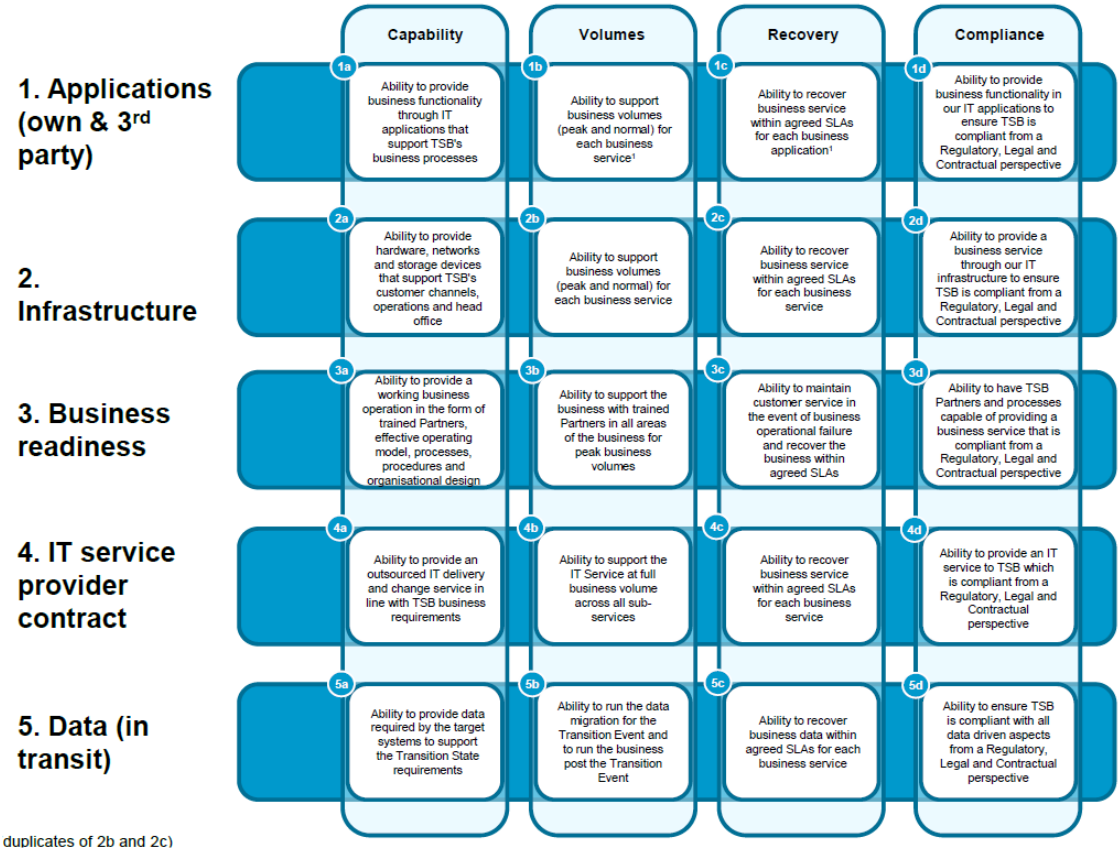
3.56 The ultimate decision to Go Live was taken following consideration of a number of assurance tools designed to draw together the assessments of the Business Areas, Risk Oversight and Internal Audit as to whether to proceed with the MME, i.e., migration of TSB's data from its existing location on the LBG IT Platform on to the Proteo4UK Platform, and putting the Proteo4UK Platform live to its customers.

3.57 The assurance tools used in assessing TSB's readiness to Go Live were (i) the Assurance Matrix and (ii) the T3 Memo.

The Assurance Matrix

3.58 TSB developed the Assurance Matrix in 2016 as a *'framework for the first line to give a comprehensive overview of all the assurance parameters required for first line validation of the Migration Programme deliverables'* and that it would be used for the GTEs and the MME *'to inform the go/no go decision to go live*'.

Figure 3:



3.59 The Assurance Matrix comprised a grid made up of five horizontal rows (the 'horizontals') and four vertical columns (the 'verticals'). The horizontals related to programme components (applications and infrastructure for platform build, business readiness, the IT service provider contract with SABIS, and the data which would populate the new system). The verticals related to the performance standards required of each programme component.

3.60 Underlying the intersections, or '*cells*', were assurance questions to ensure the collection and assessment of appropriate evidence. The evidence that was gathered and reviewed was stored in a virtual data room.

3.61 BEC business functions were responsible for completing the Assurance Matrix (that is, ensuring there were answers to the questions underlying each cell and that evidence supporting those answers was documented and providing a written attestation confirming the readiness of their business functions for the MME, along with residual risks). All the BEC business function attestations were identical apart from the IT business function attestation which contained an additional paragraph regarding SABIS readiness.

The T3 Memo

3.62 Along with the Assurance Matrix, the T3 memo was a key tool used by TSB to assess the readiness to Go Live with migration. The T3 memo dated 14 April 2018 consisted of 972 pages and set out in broad terms:

a. an overview of the governance, executive accountabilities and various committees/fora of the Migration Programme;

b. the recommendation to proceed with the MME;

c. copies of attestations testifying to the readiness of BEC business functions areas, including residual risks, as required by the Assurance Matrix;

d. Risk Oversight's opinion on the Business Areas' interpretation of the facts, the risks to the business of proceeding with the MME and the effectiveness of the mitigating actions; and

e. Internal Audit's opinion on the Business Areas' interpretation of the facts, the risks to the business of proceeding with the MME and the effectiveness of the mitigating actions.

Governance meetings leading to the decisions to Go Live

3.63 On 4 April 2018, the PRA again advised TSB of its concerns around TSB's readiness for migration on 20-22 April due to the fact there were a significant number of *'must-have'* functionalities that had not been delivered, that full capital impairment testing would not take place until after migration and that deferrals of related aspects of the migration could be of concern if significant defects were uncovered. TSB also noted that it may be difficult to source the staff to deal with a high number of defect workarounds. The PRA highlighted the need for TSB to provide it with comfort that they would be going into migration with a stable platform and asked whether TSB would stop the migration if there were still a high number of issues outstanding. A BEC member responded that the Firm had been rehearsing the executive team quite hard on whether they were genuinely ready, and that code would be frozen on 6 April to enable TSB to have a stable period on the platform in the run up to migration. The BEC member also explained, in particular in relation to the deferral of defects that TSB was aware of the identified defects and the fallback to each. The emphasis of the work was currently in identifying fixes, making improvements and noting that specific items had been deferred. It was expected that a substantial amount of the *'must-have'* defects would be completed in the coming days.

10 April 2018 TSB Board meeting

3.64 On 10 April 2018 a TSB Board meeting took place where the decision was taken to serve a Definitive Notice of Migration to LBG on 12 April 2018, thereby terminating the carve-out option and committing TSB to the migration option.

3.65 This was the first of three decisions which, when taken together, would enable TSB to proceed with the migration from the LBG Platform to the Proteo4UK Platform over the weekend of 21/22 April 2018. The other two decisions – the approval of a sub-committee with the authority to grant approval to an Executive Gold Team to initiate the data migration event consistent with a migration of the weekend of 21/22 April 2018, and the approval of an escalation approach to be used during MME with certain issues delegated to the Executive Gold Team – were to be taken at the TSB Board meeting on 18 April 2018.

3.66 The 10 April 2018 TSB Board meeting was the last board meeting before the meeting on 18 April 2018 to consider the recommendation to proceed with MME. It was noted that TSB was not currently in a position which would allow the recommendation to proceed with the migration, but it was expected that this would be possible by the TSB Board meeting on 18 April 2018.

3.67 At the meeting it was noted that there were some macro risks, one of which was that the Proteo4UK Platform did not function as expected post-MME, but it was considered that this had

been mitigated through the design and execution of the various test phases associated with the Migration Programme.

3.68 In addition, a '*high level summary of the status of the migration readiness process*' was provided. It was noted that fixing of defects had continued ahead of a code freeze on 8 April. Testing of defects was continuing, and it was intended to assess key areas of functionality that would not be fully delivered ahead of MME. Also, currently none of the attestations were complete, although it was expected (albeit with issues to resolve) they would be ready by the end of 17 April 2018 (the day before the TSB Board meeting to decide whether to initiate the data migration event). The TSB Board did not challenge the fact that at this late stage none of the attestations were complete and what this might mean for how the programme had progressed.

3.69 BEC members presented a short paper on how the programme had measured up against its Guiding Principles with a particular focus on the failure to perform a specific regression test phase (The failure to conduct regression testing in January 2018 had also been queried by the PRA). The paper had been prepared to reflect on a previous question from a board member as to whether the programme had remained true to its governing principles, and to address a question previously raised about the forms of regression testing undertaken.

3.70 The paper noted that, contrary to Guiding Principle 3, a degree of parallel working remained (and that NFT would be continuing up until MME). Contrary to Guiding Principle 4, a clean MAC cycle once UAT and MDT were complete and stable had not been held, but that regression activities had been effected across a number of elements of the plan, including through the GTEs, MACs, dress rehearsals, UAT and MDT.

3.71 In light of this, the TSB Board did not specifically challenge the lack of a regression test phase (or interrogate the programme deviations away from certain of the Guiding Principles), but noted in the minutes that: '*it was important for the Executive to provide an overall assessment that the amount of testing was appropriate and reasonable*'. In response, the TSB Board were told the position as to whether the amount of testing was appropriate and reasonable would not be confirmed until 18 April 2018, the day the TSB Board would make its decision whether to proceed with the migration.

3.72 On 13 April 2018, the PRA informed TSB that the PRA's focus was on financial stability and therefore wanted to ensure TSB had a stable platform which was secure and resilient. The PRA expressed concerns about the volume of '*must-have*' functionality still to be delivered and the risk that any workarounds might be put in place without adequate systems and controls. Noting a concern that '*not everything may be delivered, or adequate testing may not be possible*', the PRA advised that, should TSB decide to proceed, it expected '*a clear articulation of the risks which have been accepted and why*', as well as more detail on the current situation with '*must-have*' functionality.

18 April 2018 TSB Board meeting

3.73 On 18 April 2018, the TSB Board met to consider the recommendation to proceed with MME by delegating authority to the TSB Board sub- committee to initiate the MME over the weekend of 20-22 April 2018. The recommendation and supporting evidence were contained in the T3 memo. It included confirmations from the Business Areas (by way of the Assurance Matrix and the BEC business functions' attestations), and Risk Oversight and Internal Audit's to readiness to proceed with migration, subject to addressing a limited number of further issues.

3.74 The outstanding matters in the programme were noted. At the time of the TSB Board meeting that day, there were still eight outstanding areas of '*must-have*' functionality that either needed to pass testing or be mitigated. The functionality issues related to specific issues being encountered in the following areas: SMS text messaging, overdraft establishment charges, business banking authentication app, fraud operations, cards, transaction listing in digital, re-bonus of savings accounts, and crediting eSaver accounts. Consequently, eight attestations (and Assurance Matrices) had been completed and the remaining four, together with the final Risk Oversight and Internal Audit Opinions were expected to follow later that day upon resolution of these outstanding issues.

3.75 It was also noted that, in addition to the ongoing testing and mitigation of '*must-have*' functionality, other functional defects would have to be carried into MME for which TSB had designed mitigants - such as (i) the temporary withdrawal of products and services and their phased re-introduction by way of scheduled functionality releases in May, June and July as they would not be ready in time for MME (e.g. mortgage further advances, business bank account applications), (ii) deterioration of services (e.g. reduction of periods during which foreign currency payments would be available), and (iii) manual workarounds for which there had been recruitment of additional employees (e.g a telephony customer being required to speak to an operator rather than use an automated service). Further, in relation to performance issues, it was noted that NFT in telephony had run up until 16 April 2018, albeit that testing had been passed.

3.76 To summarise, by the time of the TSB Board meeting, the key deviations away from the Defender Plan had been as follows: UAT and MDT had been planned to complete at the end of January, but had not in fact completed until April, which meant that rather than achieving a stable environment first, other workstreams including NFT ran in parallel into April 2018 in order to meet the deadline, contrary to Guiding Principle 3. NFT also only completed around the time of the TSB Board meeting to decide whether to go ahead with the migration. There had been no clean MAC (contrary to Guiding Principle 4). The specific regression testing phase had not taken place due to running out of time (contrary to Guiding Principle 10), although regression activities had taken place in parallel with other workstreams. Certain functionality was being deferred or work arounds put in place due to timing. Additionally, and separately to the deviations from the Defender Plan, the late running of the testing meant the attestations were still not complete.

3.77 The TSB Board considered the concerns raised by the PRA in its email dated 13 April 2018 relating to the resolution of outstanding '*must-have*' functionality and the deferral of functionality. The Board was satisfied, based on the discussion at the meeting, that these had been addressed. That discussion had covered, amongst other things, the articulation of risks associated with the migration, the outstanding '*must-have*' functionality, the deferral of functionality so it would be delivered in scheduled releases post-MME, confirmation of the confidence that the platform had been tested to the point that it was ready for migration, and mitigation of the risk of unforeseen issues by the fact that the BEC would operate as a '*Gold incident'* (an incident of the highest severity) from Monday 23 April. The opinions provided by Risk Oversight and Internal Audit also provided comfort that the information provided to the TSB Board was fair, balanced and reasonable, that the key risks of MME had been appropriately identified, managed and reported, and that key issues raised by Risk Oversight and Internal Audit had been adequately documented and addressed and that all associated actions required to be closed pre-MME were complete.

3.78 The TSB Board resolved to approve the constitution of a sub-committee with authority to grant approval to initiate the MME over the weekend of 21/22 April 2018 (subject to resolving or identifying suitable solutions or alternatives to the issues outlined in the T3 memo). Later that day, a follow-up memo, which was presented to the TSB Board sub-committee on 19 April 2018, was produced on the progress in resolving functionality issues (confirming either that they had been resolved or a suitable alternative found) and completion of the remaining Assurance Matrices and attestations.

Decisions 19 to 22 April 2018

3.79 On 19 April 2018, the TSB Board sub-committee gave approval to the Executive Gold Team to initiate the MME over the weekend of 21/22 April 2018. On 20 April 2018, the Executive Gold Team decided to initiate the migration. On 22 April 2018, the TSB Board sub-committee authorised the Executive Gold Team to complete the migration and proceed to take the platform live.

3.80 The Migration Programme did not run according to the IMP or the Defender Plan. As noted above, aspects of the testing programme only completed just before MME with some deferrals of functionality and workarounds put in place, whilst three of the Guiding Principles in the Defender Plan had departed from, in order to be able to migrate on the weekend of 21/22 April 2018. It was decided to go ahead with MME that weekend, and whilst the data migrated successfully on to the Proteo4UK Platform, the Migration Incident (described in paragraphs 1.3 to 1.4 above) took place, resulting in some customers suffering problems accessing digital channels (internet banking and the mobile app), as well as widespread problems across telephony and in branches.

3.81 The Migration Incident occurred following inadequacies in the safeguards meant to identify problems and prevent TSB from going live with the new platform before it was ready. The Migration Programme had built in protections to reduce operational risk, such as testing, risk management measures, attestations from BEC business functions and confirmations of readiness from key suppliers, and business continuity planning. Inadequacies in these measures, some of which had been considered by the TSB Board but some of which were not known to them, meant that TSB went live with the Proteo4UK Platform before it was ready to do so.

4. Testing

4.1 A number of issues occurred during the testing phase of the Migration Programme which increased the risk in the programme and/or resulted in negative consequences for customers following MME. This section details these issues.

Testing delays: impact and risks

4.2 Testing was conducted on the Proteo4UK Platform largely following the build of its components. It was the third phase of the Migration Programme following the design and the build phase and would be followed by the migration itself. As set out above, testing ran behind schedule during the Migration Programme, with consequential impacts. Further detail of these issues is set out below.

Types of testing

4.3 Paragraphs 3.13 to 3.29 above described the types of testing that took place during the Migration Programme.

4.4 Unit testing and systems integration testing took place during the build phase. Testing following the build phase was planned to consist of:

a. functional testing: this included UAT, MDT, and regression testing;
NFT: this included security testing, performance testing, infrastructure testing, and disaster recovery testing; and

b. testing of data migration: this included MACs, and dress rehearsals.

4.5 These types of testing were to take place under the IMP and the Defender Plan, in accordance with the MSA.

Functional testing

4.6 As set out in paragraphs 3.15 to 3.16 above, functional testing was used to confirm that the Proteo4UK Platform's functionality worked as intended, for example the ability to make internet banking payments. Issues concerning functional testing during the Migration Programme fell into two categories: delays in the completion of the overall functional testing phase resulting in parallelisation of types of testing, and the omission of the planned regression testing part of the functional testing phase.

4.7 Functional testing was originally meant to be complete under the IMP by March 2017, and under the Defender Plan by January 2018. The intention under the plans was to finish the functional testing before conducting NFT and live proving and, under the Defender Plan, regression testing.

4.8 However, delays in functional testing resulted in it running parallel with other forms of testing which had meant to follow it. Parallelisation of testing runs the risk that changes in the components of one form of testing may invalidate part of the other type of testing already done on another component, although having no parallelisation means that it is not possible to close-down testing while the system is being built. Increasing parallelisation ran contrary to Guiding Principle 3 under the Defender Plan that '*The re-plan will have reduced levels of parallel work streams to decrease regression risk and resourcing schedule contention*'.

4.9 Notwithstanding its original completion targets of March 2017 under the IMP, and January 2018 under the Defender Plan, functional testing continued into April 2018 and was only brought to a close by TSB taking decisions to defer and de-scope completion of certain parts of the functionality of the new system until after the MME had taken place, with these functions only to be introduced later, after the relevant testing was completed.

4.10 As regards the intended final part of functional testing, i.e., regression testing, the Defender Plan included a specific regression test phase, in accordance with Guiding Principle 10. This testing would have involved the re-execution of UAT and MDT tests following their original test phases, to ensure that the functionality still performed as intended despite interacting with new code subsequently deployed into the Proteo4UK Platform. However, a specific regression test phase did not occur due to time constraints in meeting the April 2018 date for MME, although it had been effected through other elements of the plan.

4.11 The lack of a specific regression test phase formed part of the residual risks taken into MME. TSB acknowledged that this, alongside other factors, may result in a higher than expected volume of defects being found in the live environment for the first time which could have significant impacts on BAU teams and processes, although key mitigants were put in place to identify and resolve new defects arising in live before critical impacts accumulate.

NFT

4.12 As described in paragraphs 3.17 to 3.19 above, NFT was used to confirm the Proteo4UK Platform satisfied its non-functional requirements (how it was supposed to operate, as opposed to what it was supposed to do), for example how many customers could log in to apps at any one time.

4.13 NFT was an important mitigant for certain risks in the programme. In the papers for the third deep dive on 14 December 2015, and for the TSB Board meeting on 16 December 2015 at which the TSB Board agreed they were minded to consider migration to Proteo4UK to be their preferred solution, it was acknowledged that the Proteo platform was not proven in the UK (despite apparently comparable stability and resilience as the LBG IT platform), and that NFT would be required to mitigate this issue.

4.14 NFT was an important mitigant in relation to testing the infrastructure of the Proteo4UK platform (alongside other forms of testing such as UAT and SIT), particularly where limited infrastructure build and validation information, and very limited infrastructure testing documentation were available to TSB, meaning it was not clear whether the testing performed had covered all TSB's requirements. This placed more emphasis on NFT to identify potential issues.

4.15 Following delays in functional testing, TSB chose to start NFT before the functional testing had completed. This came with the risks of parallelisation as described above. Additionally, the time available for NFT was compressed. Having not proved the functionality of Proteo4UK Platform before NFT commenced, that there were incidences of non-functional tests failing as the functionality required to run the tests was incomplete. This meant that these tests had to be run again, leading to further reduction in the time available for completion of NFT.

4.16 A further reason for the compression of the time available for NFT was that there were difficulties in finding suitable slots in which to conduct elements of it, in part due to ongoing functional development.

Use of Testing Environments

4.17 The use, or omission of, particular testing environments introduced risks into the programme, as described below.

4.18 Various types of environments were used for testing during the Migration Programme, including:

a. UAT environment: this was used for conducting UAT;

b. production (or live) environment: this is an environment in which live services were being delivered. In the case of the Migration Programme, this included services that had gone live during the GTE, and would also be the environment in which live services would be provide following MME. During the Migration Programme, the production environment was used for most of the NFT; and

c. GOS environment: this is a test environment built by TSB to be a simplified version of the production environment. During the Migration Programme, it was used for some functional testing (e.g. MDT), some NFT, and for all the testing of data migration.

4.19 TSB and SABIS decided to conduct the majority of NFT (including performance testing) in the production environment. The MSA had envisaged the use of a pre-production environment during this stage. This would allow changes to be tested without impacting users of the production environment (for example having to interrupt the services that had already gone live). However, a pre-production environment was not available, and so TSB used mainly the production environment, and partly the GOS environment, in which to conduct NFT.

4.20 Although there were advantages in using the production environment to conduct testing, as it presented the opportunity to validate the systems in the environment in which services would go live, both Risk Oversight and Internal Audit raised concerns regarding not conducting NFT using a pre-production environment. In August 2017 Internal Audit noted that a controlled test platform replicating the live production platform, the need for which had been recognised in the MSA, could identify possible conflicts in code or component regression testing prior to promoting applications, functionality and infrastructure from the test environment into live. Not using a pre-production environment could result in instability and potential vulnerabilities in the production environment.

4.21 The issue was risk accepted but TSB committed to obtaining a pre-production test environment closer to MME. However, by January 2018, an external consultant acting on behalf of Risk Oversight observed that TSB would not be obtaining a pre-production environment before MME after all, and that the pre-production environment would be set up following Go Live, using and upgrading the GOS environment. TSB would use it to support NFT where required after MME instead. The reason for the delay was that following the re-plan, additional MAC cycles had been included for the testing of data migration, and the GOS environment was being used for that until the final MAC cycles had been completed. In the meantime, TSB would continue to use the production environment and, in some cases, the GOS environment for NFT. The external consultant noted that there were risks in using the GOS environment. Differences between the GOS and the production environments in which the functionality would be released could cause reduced system availability or non-functional issues in the production environment.

4.22 As regards using the production environment, consequential decisions made to protect services that had already gone live, and therefore currently using the production environment, constrained

some of the NFT conducted. An example of this is the fact that NFT was not conducted in Active-Active configuration.

The Active-Active configuration issue

Background

4.23 Sabadell's infrastructure for Proteo in Spain involved duplicate data centres, which were located in separate buildings with some kilometres' distance between them. Whenever the technology allowed, they used solutions in Active-Active mode, or configuration to minimise disruption of service in case of an incident. They also used duplicate network components to ensure continuity of service in case of failure.

4.24 During TSB's Macro Dossier gap analysis phase in October 2015, TSB proposed a *'target infrastructure model'* in the UK along the same lines as that of Sabadell in Spain, using twin data centres in different locations. The intention was that the target operating mode for critical live services (meaning customer-facing services) would be Active-Active mode.

Active-Active vs Active-Passive configuration

4.25 Active-Passive configuration means both data centres host applications, with customer sessions only being serviced by the Active data centre. In the event of a failure in the Active data centre, customer sessions are re-directed to the Passive data centre (which becomes Active), with some loss of service.

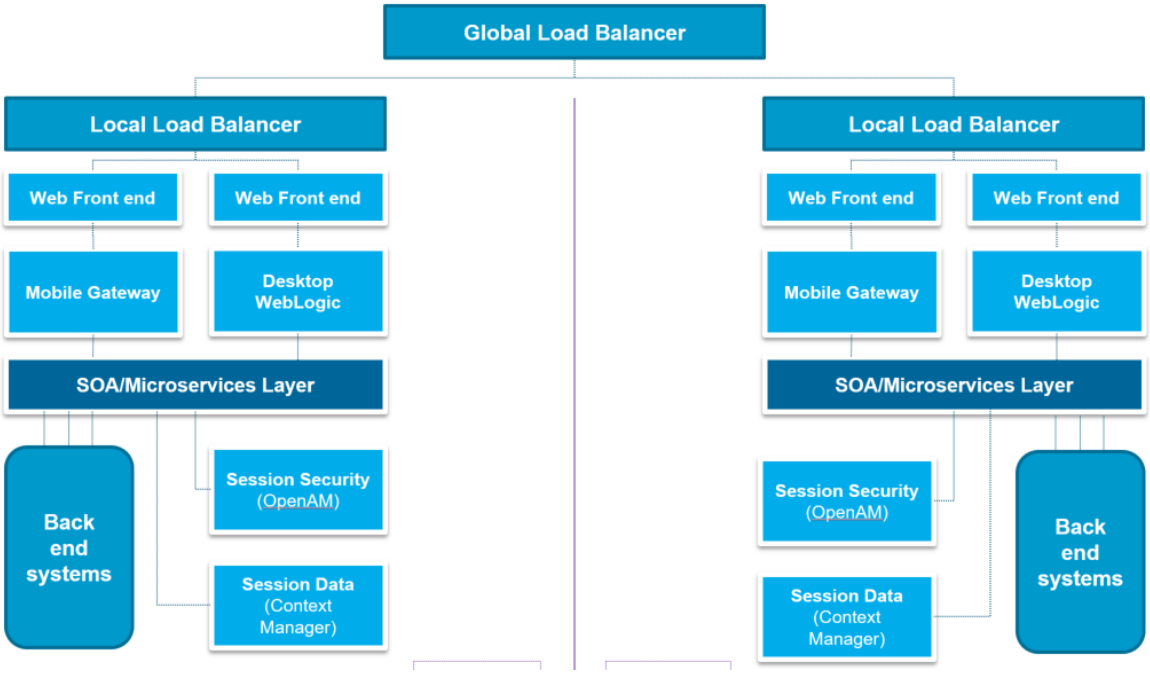
4.26 In contrast, in Active-Active configuration both data centres run at the same time, with the load of the customer sessions on the Proteo4UK Platform balanced between each data centre as required, using a Global Load Balancer. A Global Load Balancer is a network box that receives all digital requests and decides, based on a set of rules, which one of the two data centres the request should be forwarded to. In the event of the failure of one data centre, the sessions running on that data centre would be automatically re-directed (or failover) to the other data centre, which had the capacity to run the entirety of the customer sessions on its own. It was considered that using Active-Active configuration would provide better operational resilience and business continuity, minimising the impact in the event of an IT incident affecting one of the data centres.

How Active-Active data centre configuration was designed to work

4.27 The graphic at Figure 4 is a simplified demonstration of how the data centres were designed to work in Active-Active configuration for digital services. When a customer wanted to access TSB's services, such as mobile app banking, the Global Load Balancer would direct the customer to one of the two data centres. That data centre would, in isolation, then deal with the customer's request.

4.28 A *'local load balancer'* within that data centre would direct the request to one of multiple local instances of the applications within the data centre. The request would then be routed through the web front end layer (which is a gateway for web service endpoints, such as mobile, internet, telephony, and ATMs) to the mobile gateway. This would then interact with the middleware layer to provide the required customer session. Customer credentials would then be validated for security purposes through the *'Session Security (OpenAM)'* component (which validates customer credentials and returns a '*security token'* that is used to protect the customer session). Following this, the customer could then proceed with the session. Any transactions made by the customer would then be re-routed through the Global Load Balancer into the same data centre.

Figure 4:

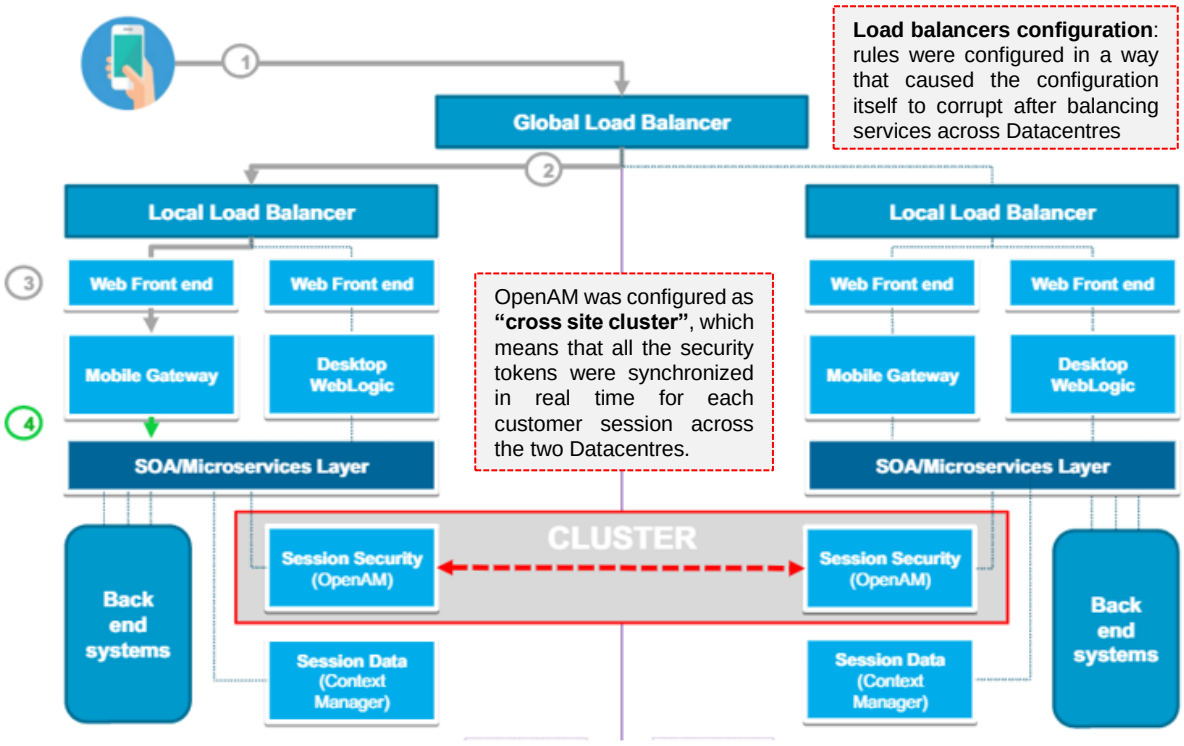


How Active-Active operated post-MME

4.29 Post-MME, an Active-Active configuration issue occurred within the two data centres, which meant that customer sessions on digital access systems, i.e., mobile app and internet banking, were not being kept on a single data centre. Whilst the login was served on one data centre, the next transaction for that customer would, at times, end up at the other data centre where the customer did not have a session meaning that there were problems with session persistence. This was because requests to OpenAM, when re-routed through the Global Load Balancer, were at times, not directed to the same data centre. Further, the OpenAM component was configured in error as a cross-site cluster, which exacerbated the issues with session persistence.

4.30 The graphic at Figure 5 shows how the data centres worked in practice, following Go Live.

Figure 5:



4.31 The issues with configuration resulted in customers receiving error messages such as '*your session has expired*' or '*your session is not valid'*. This, combined with knock-on issues, meant the ability of TSB customers to log in to their account and make payments was affected and many digital sessions failed. In the first week following MME, there were periods where digital channels were completely unavailable to customers. It also compromised the ability of each data centre to cope individually with digital business volumes in its entirety, and the ability to allow a complete failover in the event of one data centre failing.

Background to the Active-Active Performance Testing Decision

4.32 Due to the significant scale and cost of the task, as well as the low likelihood of identifying an error in a line of configuration in this way, TSB did not themselves check the specific configuration put in place by fourth party suppliers, nor conduct an audit of it. TSB used established and contracted fourth party suppliers, engaged under contracts conforming to the FCA's outsourcing rules, whilst engaging an external consultant to do a review of data centre infrastructure readiness, which they expected to be conducted on a sampling basis.

4.33 In addition, TSB relied on assurances that the Active-Active data centre componentry had been configured correctly and took confidence from the fact that certain services were already running in live both data centres. Infrastructure testing was conducted to ensure that the data centre infrastructure (including componentry) was working according to design.

4.34 However, further NFT, as planned for in TSB's T3 NFT strategy, was required to ensure that the channels would operate and perform end-to-end in accordance with TSB's non-functional requirements. Disaster recovery testing was performed to test the Active-Active failover functionality, but it was digital performance testing that aimed to ensure that the application / system as a whole could service the expected load with suitable response time. Whilst these tests were not designed to test componentry and/or the configuration of the data centres, they were intended to identify risks that the components making up TSB's business services, including critical customer-facing services, may not perform post-MME at volume. Although services may functionally work end-to-end with one user, they may not work end-to-end under the load of a large number of users.

The Active-Active Performance Testing decision

4.35 TSB did not have a pre-production environment on which to conduct testing which would stress the platform without affecting the live production environment, and so planned to conduct end-to-end performance testing in both data centres in Active-Active configuration in the production environment.

4.36 The matter was discussed at the Migration Testing Forum on 28 February 2018. A proposal was made to use only one of the data centres for performance testing purposes, leaving live services that had already migrated over to the Proteo4UK Platform (such as the public website, ATMs, and mortgages) to continue on the other data centre (i.e., the tests would not be performed in Active-Active configuration). TSB initially decided that the test should be conducted in Active-Active configuration to ensure that the conditions were the same as expected at MME.

4.37 However, subsequent to the Migration Testing Forum on 28 February 2018, TSB accepted a '*counter-proposal*' by SABIS to conduct the testing in only one data centre. This was due to concerns that the live services would otherwise be unavailable (for example ATMs would not have been available for a period of approximately three to four hours) and thereby impact customer services and cause customer disruption. It was assumed that the configuration in both data centres was symmetric following assurances received, the fact specialist third/fourth parties had been engaged and that a third party had reviewed the infrastructure and that passing the performance testing on a single data centre would be reassuring in respect of the bank being able to cope with volumes, as it would have twice as much capacity when running two data centres. In addition, TSB took further comfort from live services already migrated on to the Proteo4UK Platform under the GTEs, such as ATMS and the public website, as these were run from both data centres pre-MME.

4.38 Relying on the assumption that the data centres were identically configured, and taking comfort from the performance to date of the live services, TSB decided to prioritise continuing to run the live services, and conducting the testing only in one data centre, over risking customer disruption by taking the live services offline for a short period in order to conduct the end-to-end performance testing in Active-Active configuration. However, following MME it became apparent that both the Global Load Balancer and the OpenAM component of the data centres had not in fact been correctly configured, leading to the issues experienced by customers in trying to access the digital channels.

4.39 TSB did not perceive there to be a risk in not conducting digital performance testing in Active-Active configuration at the time (rather, they considered that there were risks in conducting Active-Active performance testing in the live environment). In particular, TSB did not perceive the risk that the testing as performed would not fulfil the purpose of ensuring that the application could service the expected load with suitable response time. This was because TSB considered volume testing on a single data centre to be an adequate test, as if it could pass with half the capacity, it would be able to easily pass using data centres. TSB did not consider that testing in a single data centre may fail to identify a risk that the components making up TSB's business services, including critical customer-facing services, may not perform post-MME. However, the testing environment in which testing was conducted prior to Go Live should have simulated the post-migration environment as closely as possible. In this case, a decision was taken which resulted in the testing and the production environments being distinctly different. As it was not identified as a risk, consequently potential mitigants were not considered. By not conducting this testing an opportunity to potentially identify some of the configuration issues experienced post MME was lost.

The decision was not taken or escalated in accordance with TSB's governance structure or procedures

4.40 The decision was taken informally, outside of TSB's governance structure or procedures, was not documented, and was not escalated. TSB did not believe this decision (amongst other technical decisions) represented a risk and considered it to be purely a matter of technical judgement. However, the decision should have been taken in the Migration Testing Forum, and the decision and risks that should have been identified from the decision reported to the MDC, where it may potentially have been escalated to the BEC DE.

4.41 The Migration Testing Forum was accountable for providing the over-arching governance and decision-making forum for testing delivery, and its purpose was to approve any test delivery domain decision through to the MDC. It was responsible for overseeing the effective delivery of testing, supporting the testing team in managing risks, and providing progress reports to the MDC on, amongst others, testing risks and key decisions.

4.42 The MDC was responsible for reporting, amongst others, risks and key decisions, including in relation to testing, to the BEC DE. The BEC DE received inputs from the MDC, and was responsible for the resolution of design risks and issues.

4.43 The Chair of BEC DE told the FCA and PRA in interview that where testing was completed in an environment that was materially different from the live environment, this had to be escalated, discussed and agreed on how it would be mitigated either within the Migration Testing Forum, or through to the BEC DE, and the decision should have been formally recorded.

NFT Memo and NFT Final Report: TSB and BEC business function attestations

4.44 As described in paragraphs 3.58 to 3.78 above, the Assurance Matrix was a framework for capturing the assurance parameters required for the validation by the Business Areas of the Migration Programme deliverables. TSB captured their assessment of the technical specifications of the Proteo4UK Platform infrastructure (the data centres and connections within TSB sites and the branch network) in the Infrastructure horizontal cells in the Assurance Matrix.

4.45 Each BEC business function was required to review the evidence in respect of the detailed questions set out in the Assurance Matrix for their Business Areas, and provide a written attestation, independently confirming that the questions had been addressed and that their Business Areas were ready to go live.

4.46 However, as a result of the delays in conducting NFT, at the 9 February 2018 BEC DE meeting, the issue of the length of time that NFT discussions had been taking was discussed. It was proposed instead that BEC business functions sign-off on their non-functional requirements in their attestations, whilst the IT business function would specify in their attestation which of the non-functional requirements had been included and tested, and which ones had not, and explain why they had not. The BEC DE agreed with this proposal. This meant that whilst each BEC business function would remain responsible and accountable for answering the questions in the Assurance Matrix for their Business Areas, in respect of questions relating to NFT, they would be doing so based on confirmation from the IT business function that the testing had been completed to the Business Areas' specifications. The evidence for the confirmation would be contained in a NFT report (the 'NFT Report').

4.47 The final version of the NFT Report (the 'NFT Final Report') summarising the NFT results was circulated in the afternoon of 17 April 2018. The NFT Final Report was 65 pages long. A two page memo (the 'NFT Memo') summarising the content of the NFT Final Report was also produced, which was circulated to BEC business functions at 17:19 on 17 April 2018. It was relied on by BEC business functions when completing the NFT-related questions for their Business Areas.

4.48 The NFT Final Report stated that performance testing had been conducted in the production environment, but that *'tests have been conducted on half the installed capacity (one data centre only), so live production performance is expected to be better under test conditions'*. It also stated (under the banner of Key Activities required to prove that the Target will perform at Volume) that one of the benefits of performance testing would be to prove that the production network and middleware components are all set up and configured correctly. However, neither the NFT Final Report nor the NFT Memo referred to any risks associated with conducting performance testing in only one data centre. Consequently, BEC business functions were unaware of any such risks when completing their attestations.

4.49 The T3 Memo relied, amongst other material, on the completed Assurance Matrix and BEC business function attestations to recommend that the TSB Board take the final steps towards proceeding to migration. The T3 Memo stated that the Assurance Matrix had been subject to review by an external consultant through which it had been refined and finalised. However, the review work conducted by the external consultant had taken place before the decision on 9 February 2018 (to give the IT business function responsibility for confirming that NFT had been completed to the Business Areas' specifications). Further, the external consultant's contribution to a Risk Oversight review of the evidence and quality control process for the Assurance Matrix in April 2018 did not refer to the change in responsibility for confirming the NFT met the non-functional requirements from BEC business functions to the IT business function.

4.50 This change does not appear to have been explicitly drawn to the attention of the TSB Board or board sub-committee when making decisions to proceed with migration on 10, 18 and 19 April

2018, based on the latest versions of the T3 Memo. The TSB Board was therefore unable to consider whether the fact that the IT business function was attesting to the completion of the centrally run NFT (while the BEC members remained responsible for signing off their non-functional requirements) had introduced risks into the Assurance Matrix, and whether this would have any effect on their decision-making.

5. Approach to Risk Management

5.1 As described in paragraphs 2.14 to 2.19 above, TSB used its three lines of defence – the Business Areas, Risk Oversight, and Internal Audit – to manage risk generally, as outlined in its Risk Management Framework. Each line undertook Migration Programme-related risk management tasks and responsibilities.

5.2 This section describes TSB's identification of risks in relation to the Migration Programme and the risk appetite framework, and then discusses specific issues relating to risk reporting and oversight.

Risk identification

5.3 Putting in place effective risk management required adequate identification and monitoring of the risks relating to the Migration Programme.

5.4 Between November 2015 and December 2016, the Business Areas identified and presented to the TSB Board 22 risks in relation to the Migration Programme (the '22 Programme Risks'), which were classified into programme execution risks (such as the Proteo build, data migration, milestone delivery and so on), and risks to the TSB business arising from migration (such as customer experience, and regulatory compliance).

5.5 The 22 Programme Risks included poor planning (defined as '*Lack of a complete plan, (eg left-to-right planning, test strategy) causes delays'*) and another to use of third parties ('*The programme may fail from lack of adequate expertise or failure to heed external advice*').

5.6 The 22 Programme Risks were mapped across to three of the risks on the Material Risk Register (risks deserving prominence at Board and BEC level). These were:

a. MMR 37: Risk of insufficient focus on BAU given additional Group focus and associated integration / migration activity;
b. MRR 39: risk that migration causes operational instability or a degradation in resilience and poor customer outcomes;
c. MRR 41: complexity, or poor control in the delivery, of migration leads to unplanned costs or delays in implementation.

5.7 The 22 Programme Risks were monitored and reported in the course of the programme by both the Business Areas and Risk Oversight. However, the effectiveness of this was limited because the 22 Programme Risks were not comprehensive, and because they did not develop as the Migration Programme progressed.

5.8 In relation to the first issue, TSB's identification of the programme risks did not explicitly address risks arising from its outsourcing arrangements with SABIS (a service provider with no experience of managing service delivery from a large number of UK subcontractors), nor did it explicitly address risks from TSB's limited experience of supplier oversight in an IT change management project of this scale and complexity. Therefore, there was no explicit assessment by TSB of the risk of non-performance, or inadequate performance, by SABIS of its obligations to deliver and operate Proteo4UK in a manner which met TSB's requirements.

5.9 While the Programme Risks were reviewed at the monthly Migration Delivery Committee, and TSB considered whether all relevant risks had been captured and considered new risks to the Programme on an ongoing basis, the list of the 22 Programme Risks remained unchanged for the duration of the programme. Consequently, any initial shortcomings in risk identification prior to December 2016 (such as SABIS's lack of experience managing service delivery from a large number of UK subcontractors, and TSB's limited supplier oversight in an IT change management project of this scale and complexity) remained for the rest of the programme.

Risk reporting

5.10 Although Risk Oversight and Internal Audit carried out a large number of migration-related reviews and audits, some of these were limited in scope, were expressly stated to be '*point-in-time'* reviews which might have been overtaken, or were otherwise expressly qualified. However, these limitations and/or qualifications do not appear to have been specifically discussed with the TSB Board at certain crucial junctures which could have led to challenge.

The Re-plan

5.11 In relation to the re-planning exercise, the Board and Executive held a deep dive meeting on the re-planning exercise on 24 October 2017. The papers for the deep dive and the discussion held during it concentrated more on the risks of the re-plan and the risks to programme delivery, while risks to BAU were discussed to a more limited extent. In the papers it was considered that the re-plan would have no impact on resilience risk (the risk to TSB's business if the target platform (and associated business processes) delivered a lower level of resilience than the current LBG arrangements). It was stated that '*The current relative immaturity of the operating model… has*

resulted in a number of incidents for services in live production. However, this is mitigated by the longer period of production proving'.

5.12 Risk Oversight's opinion, presented at the October 2017 re-plan deep dive meeting, was that overall, the revised plan assumptions were reasonable and that previous Risk Oversight recommendations had been adequately addressed. However, Risk Oversight noted that '*Due to the short timescales of the re-plan, Oversight have not completed control based deep dives, therefore our opinion is based on observation and document review to form an opinion based on "reasonableness" of the steps taken by the 1st line to develop the re-plan, and high level opinion on the plan itself*'. The opinion also noted that it did not cover plans for production proving from November, as these were not yet sufficiently mature to be reviewed. This gap in the opinion from Risk Oversight was important in circumstances in which TSB was relying on production proving to mitigate risk to resilience from the re-plan.

5.13 Internal Audit also presented its opinion of the reasonableness of the process followed and assumptions made to arrive at the re-planned MME date. Its view was that these were satisfactory overall. However, Internal Audit noted that it had not tested the *'bottom-up'* details supporting the re-plan, such as the interlocking with all relevant third parties, nor the capacity of BEC business functions or SABIS to deliver in line with the re-plan assumptions.

5.14 Both Risk Oversight and Internal Audit gave weight to the fact that the Business Areas had a rationale supporting their views in relation to (i) expected improvements in performance which would be required to execute the re-plan (Risk Oversight opinion), and (ii) assumptions deferring to the current track record or assumptions that had not been proven (Internal Audit opinion).

5.15 Whilst key points from the work by Risk Oversight and Internal Audit were explained to the Board it does not appear the expected improvements in performance, and the underlying assumptions were specifically discussed with the TSB Board on 24 October 2017, which could have led to challenge. This was despite their importance to the achievability of the re-plan and the mitigation of risk.

Recommendation to Go Live

5.16 Risk Oversight provided an opinion dated 17 April 2018 supporting the recommendation to proceed with the final steps required before MME, but noted that there were '*only a few gaps*' in their reviews of the effectiveness of testing where they had had '*limited coverage'* due to the design or timings of migration deliverables and these gaps included NFT, regression testing and end-to-end production proving.

5.17 As explained above, a longer period of production proving had been a stage explicitly identified in the re-plan that would mitigate resilience risk, albeit Risk Oversight had not been able to review

it at the re-plan stage as the plans were not sufficiently mature. Now Risk Oversight was noting that their coverage of production proving ahead of Go Live was limited.

5.18 As regards NFT, Internal Audit conducted a limited reconciliation review of the final NFT results which did not include a review of the underlying source data about the testing that had been performed. Despite the importance of testing (including performance testing) in production proving – itself a key mitigant against operational risk – it does not appear the implications from an operational risk perspective of the '*limited coverage*' in Risk Oversight's opinions were specifically discussed with or challenged by the TSB Board on 18 April 2018.

Conclusion of risk oversight activities before the end of the Migration Programme

5.19 Risk oversight of the Migration Programme came to an end before the end of the programme, leaving a gap in oversight in the run up to MME. The oversight of the Migration Programme by Risk Oversight ran until 8 April 2018, about two weeks before MME. At this point the BEC asked Risk Oversight to conclude its oversight activity so as not to distract from the effort to get ready for MME and to avoid new actions being raised in the weeks leading to the MME with no time to conclude them. It was also considered that the work was taking the Business Areas away from activity for MME and by that stage they were very time short to get sufficiently ready.

5.20 Risk Oversight was asked to conclude the activities they had inflight and to ensure the remaining actions got closed. In closing the remaining actions they distinguished between actions that were critical for migration which would not be able to proceed without them being closed (and ensured that they were closed), and actions which were important but not necessary for MME. Risk Oversight agreed to make observations but not raise any further actions prior to MME after the code freeze which took place on 8 April 2018. In the event, however, Risk Oversight do not appear to have made any observations after 8 April 2018.

6. Assessment and Oversight of SABIS's Readiness

SABIS's roles and responsibilities

6.1 SABIS was TSB's principal outsourced provider for the Migration Programme. The services that SABIS was providing to TSB were critical to the success of the migration and to the stability and operation of TSB's banking services on the Proteo4UK Platform. Under the MSA the services included the design, build and testing of the Proteo4UK Platform and data migration software, as well as being a systems integrator responsible for setting up two UK data centres, managing and coordinating the design and delivery of data centre components from vendors, and configuring

and integrating the components to work together. SABIS's responsibilities under the OSA were to operate the Proteo4UK Platform and meet agreed performance thresholds or service level agreements.

6.2 These services were critical to the performance of TSB's regulated activities and TSB was required by the regulatory regime to take reasonable steps to avoid undue additional operational risk.

6.3 This section describes issues in respect of certain aspects of TSB's assessment and oversight of its outsourcing arrangement with SABIS.

Assessing SABIS's capability

6.4 At the outset when deciding to proceed with the migration option utilising the Proteo4UK Platform, TSB did not conduct a formal comprehensive due diligence exercise to understand SABIS's capability to deliver and operate the Proteo4UK Platform. Subsequently once TSB had defined its requirements and service model more precisely, TSB did carry out a number of due diligence exercises. However, it remained the case that TSB did not sufficiently understand SABIS's capability to operate the Proteo4UK Platform.

6.5 In the lead up to the TSB Board's decision on 16 December 2015 on the migration plan, TSB considered Sabadell's previous experience with migrations and integrations, the capabilities of the Proteo platform itself and Sabadell Group IT service stability (measured by availability of services). TSB identified certain risks in relation to outsourcing. On a broad level, the memo to the TSB Board setting out the strategic benefits of migration to the Proteo4UK Platform acknowledged that '*Migrating the infrastructure for a bank of the size and complexity of TSB is an extremely challenging technical undertaking. Ensuring the combined resources of TSB, Sabadell and LBG are capable of delivering the migration is key'*.

6.6 TSB also identified specific outsourcing risks, namely the dependency on integrating third party suppliers with Proteo and potentially inadequate capabilities of either TSB or SABIS to control the timelines and quality of the required deliverables, albeit viewing reliance on third parties as favourable in terms of providing the ability to deliver TSB's desired range of functionality.

6.7 Nonetheless, despite identification of these broad and specific risks, TSB did not at the outset carry out a formal assessment of SABIS's capability (as a resource of Sabadell) in relation to them. There was no discussion at the 16 December 2015 TSB Board meeting about either SABIS's abilities in relation to systems integration, or SABIS's overall capability to deliver migration by building and operating the platform, or how that would be assessed, other than the operation of the migration programme itself.

6.8 In addition, certain risks in relation to SABIS's capability were not formally and explicitly identified. For example, the analysis recommending Proteo4UK as the preferred exit option compared the time to implementation for carve out (up to four years) and migration (two years), which was said to be on the basis of '*Group experience and current plan for a 2 year implementation period'*. However, the evidence for this statement was the plan itself and the fact that the two year timescale had been communicated to the market, as indicated in a document circulated to the TSB Board in February 2016, albeit the Board was aware of SABIS's previous experience in conducting migrations. TSB did not consider the risk of overruns and build in contingency to its plan accordingly.

6.9 In any event, at the time of its decision to proceed with SABIS in December 2015, TSB was still defining its functional requirements for the system, and it had not confirmed the service model between TSB, other members of the Sabadell Group and any third party suppliers. TSB could not undertake a definitive assessment of SABIS's capability at that point to deliver the Proteo4UK after migration, and would need to formally reassess SABIS's capability once TSB's requirements and service model became clearer.

6.10 However, even once its requirements and service model were defined, TSB did not conduct any formal assessment of SABIS's capability to deliver and operate the Proteo4UK Platform. This unduly increased the operational risk of the outsourcing arrangement because TSB did not know in the form of a formal assessment whether SABIS would be able to deliver the outsourced services adequately.

Identification of outsourcing risks

6.11 As discussed above, the 22 Programme Risks did not explicitly address risks arising from its outsourcing arrangements with SABIS, a service provider with no experience managing service delivery from a large number of UK subcontractors, nor did it explicitly address risks from TSB's limited experience of supplier oversight in an IT change management project of this scale and complexity. There was therefore no explicit assessment by TSB of the risk of non-performance, or inadequate performance, by SABIS of its obligations to deliver and operate Proteo4UK in a manner which met TSB's requirements.

Architectural designs of IT systems infrastructure

6.12 TSB knew that Proteo4UK was being newly built by SABIS and was new to the UK banking market (noting that it was created largely from the existing Proteo (Spain) platform). It was therefore critical for TSB to understand how the system infrastructure had been built, whether it reflected TSB's requirements, and how testing was being carried out. TSB also required designs to support effective disaster recovery.

6.13 Design documents were required under the MSA, but a different approach was agreed in 2017, following a review by Internal Audit. Internal Audit report raised concerns that the IT business function did not yet have *'a formal, complete and verified architectural design of the IT infrastructure and systems to support oversight and validation of the IT estate build'* which may result in the IT business function being unable to *'execute their architecture accountability and assurance role over the design and implementation of the IT infrastructure, identify ad-hoc changes between design and build and confirm that it is delivered as designed'*. One of the examples it noted was that the absence of an approved infrastructure design had limited TSB's ability to monitor the delivery of the dual data centres.

6.14 The Internal Audit report considered that the issue reflected the speed of delivery and the emerging third party relationship, and noted that risks included TSB not being able to demonstrate having adequate systems and controls in place to identify and manage their exposure to IT risks, increased regulatory scrutiny and a potential fine.

6.15 Instead of requiring the production of design documentation, the agreed management actions, to be completed by 31 October 2017, were for the IT business function to '*develop and maintain the high level architectural service views*' to be supported by a Configuration Management Database ('CMDB') detailing the supporting infrastructure, and for SABIS to provide evidence that it was populating and maintaining a fully documented, accurate and proven CMDB.

6.16 Configuration documents in a CMDB describe what has been built, as opposed to design documents which show what would be built, how and why. This meant they could not be used to verify that the infrastructure had been built to the original design. The intention was that ultimately TSB would potentially generate design documents after the event from the CMDB.

6.17 In the event, however, in February 2018, TSB's Internal Audit closed the requirement for SABIS to provide evidence that it was populating and maintaining a fully documented, accurate and proven CMDB. This was because it was then decided that evidence of the CMDB's accuracy was no longer necessary to address the IT business function's need for access to complete architectural designs to allow oversight and validation of infrastructure delivery for MME, and ongoing management of the estate through its lifecycle. It was thought that there were a number of infrastructure documents and service descriptions that had now finally been produced in the run up to migration that would be sufficient to demonstrate IT business function visibility of the systems, applications and infrastructure being delivered. Having initially agreed an alternative which could not be used to verify that the infrastructure had been built to the original design ahead of MME, and worked throughout the programme without sufficient documentation, TSB now risk accepted those pieces of documentation that had finally been produced.

6.18 However, senior members of the IT business function considered that Internal Audit may have prematurely closed this action because TSB was still not in possession of architectural

infrastructure designs for all the services, meaning TSB had neither full architectural infrastructure designs nor a fully populated CMDB. Internal emails in response to the closure of the audit action noted '*I'll stay quiet with audit but we must still push to have the right level of information to be able to support the business and satisfy regulation!*', the reply to which was: '*Audit have prematurely closed this action but we must do the best thing for TSB which is continue to push*.'

6.19 Risks were again raised in relation to the limited infrastructure documentation in March 2018 by an external adviser which produced a report for Risk Oversight (although the report status rating was yellow, meaning that some improvement was required, that poses no material threat to current or future risk outcomes). The report noted that limited up-to-date infrastructure design documentation had been observed, which could impact on the effectiveness of TSB's response to changes and incidents and could result in the IT business function being limited in its ability to assure the IT environment. It also noted that TSB had very limited infrastructure testing documentation from SABIS, in the absence of which it was not clear whether the testing performed had covered all TSB's requirements, placing greater emphasis on application NFT to identify potential issues.

6.20 The report gave as an action point that the IT business function/SABIS operating model should be defined in more detail to clarify roles and responsibilities, including in relation to maintenance of design documentation (presumably with a view to the design documentation then being kept up to date). However, on 17 April 2018, just ahead of MME, TSB's Operational Risk Oversight confirmed this action was being risk tolerated (and therefore had not been actioned) until after MME on the basis that they had *'a minimum level of compliance that we can work with'*, relying on the attestations, the architecture documentation that had been received, disaster recovery events proving data centre capability, and in flight OSA discussions.

6.21 Consequently, TSB continued to accept having a lack of comprehensive architectural infrastructure design documentation on a risk tolerance basis. Instead of having the infrastructure design documentation to verify that the infrastructure had been built to the original design, TSB used solution design documents, but these did not provide traceability back to all of the functional design requirements. Instead, BEC business functions had to decide if the solution design was aligned to their expectations and sign off the documents through their attestations as part of the Assurance Matrix.

TSB's oversight of SABIS's management of fourth parties

6.22 Under both the MSA and OSA, SABIS relied extensively on third parties (TSB's fourth parties) to deliver the systems and services required for the migration and its operation, which required it to act as a service aggregator. The MSA and OSA identified that TSB would obtain the services of 85 fourth parties through SABIS (11 of which were 'Material Subcontractors', i.e., suppliers of

critical or important functions under the regulatory outsourcing requirements). SABIS remained contractually responsible to TSB for the work of its subcontractors. As a result of SABIS's aggregator role, and TSB's lack of contractual relationships with the fourth parties delivering services under the MSA and OSA, TSB was exposed to significant operational and regulatory risk.

6.23 In October 2017, a concern was raised in the monthly CRO report to the TSB Board that TSB was still not able to understand the risk exposure of the full SABIS IT service provision (i.e., services to be provided under the OSA), including in relation to fourth parties. SABIS acknowledged that TSB might not have enough visibility over risks posed to it by fourth parties.

6.24 By February 2018, TSB had still not ensured that SABIS's supplier management model (including a service risk assessment methodology and framework) was fully developed and complied with TSB Group Outsourcing policy. SABIS acknowledged there was a gap in the control environment which was proving difficult to close due to its recruitment difficulties. SABIS requested the secondment of an experienced person from TSB, '*to get the basics* [of supplier risks] c*ompleted in time for MME'*. The issues were not fully resolved before MME, however TSB subsequently deemed SABIS to be migration ready (in the context of procurement oversight) on the basis of there having been '*sufficient tasks completed ahead of MME on a prioritised basis'*, subject to further steps being taken after migration. Nonetheless, TSB had not ensured the adequacy of SABIS's supplier management model over a considerable period of time in the lead up to MME, nor had TSB ensured that it had sufficient visibility over the risks associated with the fourth parties SABIS was sub-contracting to in relation to services provided under the OSA.

SABIS's operational readiness for MME

Issues with GTE live services

6.25 A report produced in October 2017 by BEC members found several issues in respect of GTEs– that is the limited number of services which had already gone live and were being run prior to MME. This report also found that where there were incidents, in some cases the root cause was a build defect that was not identified in testing, such as configuration issues, and recovery from those incidents was too slow.

6.26 Issues with the performance and availability of various GTE services (including faster payments, mobile banking, and ATMs) continued, albeit with some improvement during January and February 2018.

6.27 Despite the problems that it had experienced for each of the GTEs in the months leading up to MME, TSB did not re-assess SABIS's capability to deliver the migration in light of the service level breaches encountered with the GTEs.

Internal Audit's assessments of SABIS's operational readiness

6.28 TSB conducted audits of the project up to April 2018 and had received warning signs that further work was required to embed and document SABIS's IT control framework. Internal Audit's report on SABIS Operationalisation (Phase 2) assessed controls by taking samples from business services that had already gone live to determine if they were ready to enter MME. However, the live services were not as technically complex and had limited supply chain complexity compared to the services stood up at MME, which was a limitation on the assurance obtained. Internal Audit's report did not clearly identify the differences between the GTE live services and the services that would be operated post-MME, and the minutes of the 10 April 2018 and 18 April 2018 meetings of the TSB Board do not indicate any questions or discussion about the basis upon which the audits were conducted.

SABIS and fourth party confirmations

6.29 There were 85 fourth parties, of which 11 were Material Subcontractors. Four of the Material Subcontractors were SABIS's critical third party suppliers. On 5 April 2018, TSB received a letter from SABIS (the 'SABIS Confirmation') confirming non-functional readiness for migration, in response to a request for '*comfort regarding the ability of the new Platform to meet the Service Level Agreements between SABIS and TSB*'. The SABIS Confirmation covered two areas: (i) testing undertaken to prove resilience and performance and (ii) confirmations of readiness dated 4-5 April 2018 from three of SABIS's four '*critical*' third party suppliers (i.e., TSB's fourth party suppliers) that SABIS had requested on 4 April 2018. These fourth party confirmations of readiness were not directly passed to TSB at the time, but were referenced in the SABIS Confirmation.

6.30 The SABIS Confirmation stated that:

> *'In the few exceptions where there are further tests that need to be completed in the next week or so, because of different circumstances, we feel comfortable that we will not find any cause for concern towards being 'migration ready' by the 19th of April. Also, from the point of view of critical Third Parties ('fourth parties' in the case of TSB), I have received positive written confirmation from [three of SABIS's 'critical' third party suppliers] that they are confident that their infrastructure is fit for purpose and therefore that they are prepared for the expected volumes […]. I am awaiting written confirmation from [one "critical" third party supplier], but I do not expect any issue in receiving it from conversations on the subject.'*

6.31 The outstanding confirmation from SABIS's '*critical*' third party supplier was received on 10 April 2018, (the same day that the TSB Board was meeting to determine whether to serve the definitive notice of migration on LBG and thereby commit to TSB to the migration option and to forego the back-up LBG carve-out option.)

6.32 SABIS's Confirmation and the confirmations from fourth parties were, to some extent, forward looking statements of good intention or expectations, rather than statements of fact about the completeness of readiness activities already undertaken. Moreover, all but one were caveated with a number of outstanding tasks or tests which had not yet been completed. TSB was aware that there were outstanding tasks or tests at the point they were given. While TSB continued to have ongoing dialogue in the run-up to MME with SABIS and the third parties, TSB did not ask SABIS to obtain further formal comfort from the '*critical*' third party suppliers in the period from 4-5 or 10 April 2018 to the MME decision on 18 April 2018 to confirm that they were ready. Nor did TSB request an updated SABIS Confirmation of readiness to support the IT business function attestation given to the TSB Board.

TSB IT business function attestation

6.33 Although the SABIS Confirmation was uploaded to the virtual data room in which Assurance Matrix evidence was stored, it was not contained in the papers for TSB Board meetings prior to MME. Instead, the TSB executive and TSB Board relied upon the IT business function to attest to SABIS's readiness. This was covered in a single paragraph in the attestation dated 17 April 2018:

> *'Sabadell Information Systems S.A.U. (SABIS), as key supplier, is prepared for the T3 Event. SABIS has confirmed… that it will have performed its obligations as set out in the Master Services Agreement between TSB and SABIS (the MSA) and Contract Change Note no. 1 to the MSA dated 10 April 2018 (the CCN) (to the extent that these are required to be performed ahead of the T3 Event) and will be ready to perform its remaining obligations under the MSA and CCN as well as its obligations under the Outsourced Services Agreement between TSB, SABIS and Sabadell Information Systems Limited from the T3 Event. [The IT business function is] satisfied that this confirmation can be relied upon.'*

6.34 This paragraph of the attestation repeated SABIS's expectation that it will have performed its obligations under the MSA ahead of MME and that it will be ready to perform its obligations under the OSA from MME, but did not constitute an attestation as to any steps that had been taken by SABIS to perform its contractual obligations. Indeed, only a SABIS employee would be able to attest to those steps.

7. Effectiveness of pre-MME Business Continuity Planning ahead of MME

7.1 Following MME, and as described in paragraphs 1.3 to 1.4 above, TSB quickly found itself in a crisis situation, with IT incidents affecting its general operations intensely in the early stages and then intermittently over a number of months. Digital, telephony and branches were all affected, with IT incidents in the digital channels causing a chain reaction of events as customers affected by the incidents sought other means of conducting their banking, moving from digital to telephony to visiting branches.

7.2 As described below, TSB did not expect the scale and complexity of the IT incidents and had difficulties in dealing with them, as well as in providing timely, consistent and clear information to customers. TSB struggled to prioritise vulnerable customers, and quickly became overwhelmed with complaints. Ultimately TSB put in place its Putting Things Right Programme in May 2018 to try to deal with the problems.

Incident management and business continuity planning for the fixing of technical defects post-Go Live

7.3 TSB worked with SABIS ahead of Go Live on incident management and business continuity planning in respect of the fixing of technical defects that may occur following migration.

7.4 TSB required SABIS to comply with business continuity and disaster recovery obligations under the MSA in respect of the design, build and testing of the Proteo4UK Platform. However, its obligations both in respect of services that had gone live ahead of MME and services that went live at MME were governed by the OSA. These included:

a. provision of continuous incident management for all services for incidents (such as any unplanned interruptions or reduction in quality of a service) in accordance with the Incident Management Procedures Manual; and

b. provision of services in compliance with TSB's Business Continuity Policy and IT Disaster Recovery Policy and Standards, as well as maintain its own business continuity plans for business disruption events and IT events causing disruption to the services or Proteo4UK Platform, and procure or provide for business continuity plans of Material Subcontractors.

7.5 SABIS had business continuity plans in respect of each of the services being provided, and TSB conducted a desktop review of a sample of those plans. Required disaster recovery times were assessed by the Business Areas in their review of their business continuity plans.

7.6 TSB also worked with SABIS in creating the PGLS model, *'intended to create protocols for our partners to quickly report any snags or any problems without having to deal with complicated processes*'. It was a model that was mainly directed by TSB but supported by and agreed with SABIS. It included 24/7 staffing models, and TSB's plans to have '*war rooms*' for all its critical areas. SABIS confirmed that it had the equivalent '*war rooms*' available to support those of TSB, and also supplied TSB with specific people to call in its '*war rooms*'. It also replicated a Gold, Silver, Bronze support structure that was being run by TSB. However, because TSB had not envisaged that a multiple incident scenario of the scale that occurred would materialise, TSB did not prepare, and was aware that SABIS had not prepared, any particular contingency plans beyond those required to support the programme preparations.

Testing of incident management

7.7 Testing of incident management ahead of MME was limited due to there being few live services and incidents. Incident management was tested through some simulated incidents, as well as through real incidents in services already gone live and in the TSB Beta phase. Pre-MME incidents were low in volume and complexity due to the limited services live at the time, whilst TSB Beta was '*broad but thin*', as the breadth of real incidents that had to be fixed was limited by the number of participants (around 2,000 TSB staff) and their accounts.

TSB review of SABIS's operationalisation

7.8 TSB undertook internal assurance activity on both: (i) SABIS's operationalisation ahead of MME; and (ii) the IT business function's business readiness controls to monitor and oversee third party suppliers and support the business in being safe and compliant from migration go live.

7.9 In relation to SABIS's operationalisation, an Internal Audit report dated 3 April 2018 reviewed incident management controls (amongst others) by taking a sample of 25 incidents for live business services between April to November 2017. It also reviewed the process they had followed, to determine if they were ready to enter MME.

7.10 TSB was aware from the report that the incident management process had '*insufficient evidence of control mechanisms to support the incident prioritisation and root cause analysis decisions*', and that the '*documentation of evidence to demonstrate the execution of key controls is inadequate to provide assurance that the process is* effective'. The report noted that processes for the management and oversight of incidents were still being established as part of the Migration

Programme plan, and that the problems had not been fixed because '[d]*ue to the current stage of the Migration Programme, the team are currently focused on resolving incidents*'.

7.11 Subsequent to the review process improvements were made and additional members were recruited to the Incident Management team. Management actions from the audit included the identification of principles for assigning incident priority ratings and completing incident root causes. TSB considered the issue to be low impact and the audit actions were closed. It does not appear that TSB gave consideration to what impact this issue might have in the scenario of multiple IT incidents occurring post-MME, or that TSB conducted any further audit review directly of incident management controls following the work between April to November 2017. Internal Audit was satisfied that the actions critical for MME had been closed.

TSB review of TSB IT business function's business readiness controls

7.12 As regards the IT business function's business readiness controls for post-migration, TSB recognised in its Internal Audit Report dated 17 April 2018 that it was expected that '*a number of operational incidents will occur during and following the MME that may impact operational availability, business and customer processes. The ability to prioritise and manage the remediation of incidents and delivery of agreed releases and functionality is dependent on the [IT business] function and SABIS having the appropriate resources in place post MME*' [our emphasis]. For example, SABIS resources were intended to be integrated into the process and decision-making structures for identifying, triaging and resolving problems as part of the PGLS model. Different technical teams at SABIS, supporting the different dossiers, would be deployed to fix issues depending on whether they were functional or non-functional issues.

7.13 The internal audit conducted was focused on whether the IT business function had appropriate controls and processes in place to monitor and oversee third party suppliers and support the business to be safe and compliant from migration go live. TSB did not directly assess SABIS's readiness in relation to incident response, or whether it was prepared for a multiple incident scenario. The Internal Audit Report dated 17 April 2018 stated that '*we have assessed the readiness of the [IT business] function, and by extension Sabis'* [emphasis added]. It also noted that '*work continues to develop the governance and processes to manage and prioritise the aggregate of the post MME fix* activity'.

TSB's operational preparations to deal with incidents following MME

7.14 TSB needed to put in place suitable planning on its side to deal with incidents that might arise following MME, including in relation to unanticipated disruptions for its customers following IT incidents. TSB undertook a programme of work ahead of MME to prepare itself, as described below. The work undertaken did not, however, prepare TSB to deal with an incident of the size and scale that occurred following the migration, despite the particular circumstances of the large-scale IT change project it was undertaking, the inability to roll back to the LBG IT Platform should a large incident occur, and its reliance on its outsourced IT service provider to fix any IT incidents that might occur.

TSB's incident management policies and procedures at MME

7.15 TSB updated its business continuity plans ahead of MME. TSB's Business Continuity and Incident Management Policy (the 'BCIM Policy') required TSB to have continuity plans to recover operations and a structure to respond to incidents. The BCIM Policy identified roles to be in place across the bank to take responsibility within their area of the business, and required business units to plan how they would recover their business operations immediately following a disruption event. This included, on an at least annual basis:

a. undertaking and approving a business impact risk assessment, in which they were to identify all of their business activities and impact assess them against complete cessation to determine (i) level of criticality to TSB, and (ii) timescale of their recovery post incident (which was then mapped across to disaster recovery requirements and testing);

b. determining and documenting their strategy for recovering their critical activities, captured in their business continuity plans;

c. ensuring an annual schedule of business continuity and incident management testing and exercising were complete and reviewed at least annually to ensure they were on track and proved required response and recovery timescales; and

d. BEC business functions had to provide an attestation of readiness confirming that the incident response and business continuity planning was in a state of operational readiness.

7.16 The BCIM Policy also required TSB to have an incident management framework to lead and direct an initial response to an incident, managing through recovery and the return to BAU. The incident management framework as at the date of migration was set out in the Business Continuity Management Procedure, Incident Management document. It used a Bronze, Silver, and Gold incident response structure, with a Gold incident being the most significant.

Incident management structure: Gold Event

7.17 TSB planned to work as a Gold incident from 23 April 2018 (the first day post-MME) to mitigate the risk of unforeseen issues, and provide additional assurance that TSB was adequately prepared for incidents.

7.18 A Gold event had only ever been invoked once previously, in the early life of TSB. Consequently, TSB engaged an external consultant to assist its Gold incident team respond to and recover from potential crisis management scenarios. Three practice Gold events were undertaken with the external consultant during the Migration Programme, in May 2016, March 2017 and March 2018. The third and final exercise concerned a multi incident event arising post migration, involving a ransomware attack, along with performance issues in digital and telephony, an increase in calls from customers not able to access their accounts in digital, Proteo going down following the application of a patch to resolve some of the issues identified, and lack of branch capability. The scenario assumed SABIS was working on fixing the technical issues. This final Gold event was described as '*the equivalent of multiple organ failure*', and '*presenting a situation of a combined cyber-attack plus catastrophic failure of one of the data centres*'.

7.19 However, in the context of the scale of the changes being undertaken in the Migration Programme, and the potential for unforeseen incidents, the Gold events were limited in two respects. First, they assumed resolution of the incidents within a few days, whereas many post-MME events took weeks to resolve.

7.20 Second, the Gold events were designed to be exercises for BEC members solely, to test their ability to cope with a Gold incident, how to react, using playbooks, who to inform, and what to communicate internally and externally. The external consultant created the simulation for the IT incident that was intended to be the equivalent of a multiple organ failure. TSB did not require SABIS to participate (albeit the Managing Director of SABIS UK attended the second Gold event as an observer). It had originally been intended, and the TSB Board had been informed in May 2017, that the final Gold team exercise would include SABIS. However, TSB decided by the time of the final Gold team exercise that SABIS's time would be better spent working on the PGLS model.

7.21 Ultimately in the Gold meetings and calls that occurred during the real Migration Incident, SABIS was in fact required to attend. It was required that anyone who could help to fix the relevant

problems should attend, and getting SABIS's engagement in the Gold meetings was seen as vital.

7.22 In the scenario of a multi organ failure IT crisis, where the ability to address the incident would depend heavily on SABIS, and where such an incident following MME would have a major impact on customers, proper consideration needed to be given by TSB as to whether a traditional practice Gold event involving BEC members only would therefore be sufficient preparation for such a situation.

7.23 TSB did not undertake any exercise from an IT perspective to test the ability to recover from an IT failure. This was not unusual as there were real incidents to prove its incident management process. However, by March 2018 (when the last Gold exercise was run) and certainly by the MME weekend in late April 2018, TSB had information which – in aggregate – should have caused it to take more action to ensure the effectiveness of SABIS's incident management capabilities and processes.

Annex B – Breaches and Failings

1. Breaches

1.1 During the Relevant Period, as a result of the facts and matters set out at Annex A to this Notice, the Firm breached relevant requirements of the PRA's Rulebook – Fundamental Rules 2 and 6.

a. Fundamental Rule 2 requires that a firm must conduct its business with due care, skill and diligence; and

b. Fundamental Rule 6 requires that a firm must organise its affairs responsibly and effectively.

1.2 These rules are included at **Appendix 2**.

2. The PRA's expectations

2.1 The PRA's primary objective is to promote the safety and soundness of firms, and it advances that objective by seeking to ensure that the business of firms is carried on in a way which avoids any adverse effects on the stability of the UK financial system. Such adverse effects, including through threats to customer confidence in individual firms, may result from disruption to the continuity of financial services. Operational disruption can: i) impact financial stability; ii) threaten the viability of individual firms and financial market infrastructures; iii) cause harm to consumers, policyholders, and other parts of the financial system.

2.2 The PRA also has a secondary competition objective. When discharging its general functions in a way that advances its objectives, the PRA must so far as is reasonably possible act in a way which facilitates effective competition in the markets for services provided by PRA-authorised persons. Challenger banks, such as the Firm, facilitate effective competition in the UK banking market. Challenger banks can only facilitate effective competition if they instill confidence with depositors. A disruption to the performance of Critical Functions on a continuous and satisfactory basis risks eroding confidence in that bank and potentially also of challenger banks more broadly.

2.3 In pursuing these objectives, the PRA places a high priority on developing and embedding operational resilience in its supervisory approach in order to mitigate the risk of disruption to the provision of Critical Functions. Operational resilience is the ability to prevent, adapt and respond to, and recover and learn from operational incidents, including but not necessarily limited to those relating to cyber and technology. Managing operational resilience adequately is a way firms can reduce the number and impact of IT or operational incidents. The way in which a firm manages

operational resilience is an integral part of the PRA's assessment of a firm's safety and soundness.

2.4 Although the PRA's current, overarching operational resilience framework was introduced after the Relevant Period (specifically, in 2021), the PRA's requirements and expectations as regards managing operational resilience consolidate many long standing and well understood areas of prudential regulation that have formed part of the PRA Rulebook for several years, including during the Relevant Period. These areas include governance, operational risk management, business continuity planning and the management of outsourced relationships. These requirements and expectations are reflected in the underlying rules, including:

a. as regards outsourcing: (i) prior to 3 January 2018, PRA Outsourcing Rules 2.1, 2.2 and 2.4 to 2.8; (ii) from 3 January 2018, PRA Outsourcing Rules 2.1 and 2.1A; and (iii) the outsourcing requirements set out in Articles 30 and 31 of the MODR (which came into effect on 25 April 2016);

b. the PRA Risk Control Rule 3.4 (which came into effect on 2 April 2015);

c. the PRA General Organisational Requirements 2.5 and 2.6 (which came into effect on 2 April 2015), of which rule 2.6 was amended from 3 January 2018.

2.5 These rules, which are set out in detail at Appendix 2, underpin the PRA's operational resilience framework. For firms to be operationally resilient, the PRA expects firms to be able (so far as practicable) to prevent disruption from happening. However, the PRA's policy on operational resilience expects firms to assume that disruption is inevitable. Therefore, in addition to taking reasonable steps to prevent disruption, firms should adapt systems and processes to continue to provide services and functions in the event of an incident. We expect firms to return to normal running promptly when a disruption is over, and learn and evolve from incidents and near misses.

2.6 These rules are particularly pertinent in relation to migration programmes, if there is potential impact of operational failure arising from the migration: namely, the adverse effects on the stability of the UK financial system which may result from disruption to the continuity of financial services. To comply with these rules, the PRA expects firms to prudently manage the significant operational risks of undertaking the migration programme. That is all the more so in relation to a migration programme of this scale and complexity.

2.7 In summary, the PRA's expectations in this regard include that firms should:

Governance

(1) have in place robust governance arrangements that ensure adequate assessment of the readiness and delivery of the migration programme. This should include:

(a) prudent and effective planning and re-planning of the migration programme to ensure it can be organised and controlled responsibly and effectively. This should include adopting a robust approach to:

i) planning which sets an appropriate timetable for the migration commensurate with its scale, complexity and level of operational risk, including sufficient contingency; and

ii) re-planning which ensures that the reasons for any delays to the migration programme are investigated adequately, and appropriately addressed, so that the volume of work remaining can be realistically assessed;

(b) clear escalation policies that are widely understood so that emerging risks and crystallised issues can be managed and addressed at the appropriate governance forum as soon as possible. Such policies should enable SMFs to easily recognise the risks involved in the decisions that they take and whether such decisions are his or her own to take;

(c) recognising the importance of responsible SMFs explaining to the relevant governance forum, and the board as required, the risks involving in decisions they have taken, particularly where the decision relates to an area involving highly specialised technical expertise, which is not shared across the firm's executive and board;

(d) ensuring such decisions are recorded and documented to ensure the rationale for such decisions can be revisited at a later date; and

(e) effective and timely challenge including at board level. In particular, we expect the board to challenge executive management to test the robustness and prudence of their plans as appropriate; review and challenge the adequacy (including the level of detail and integrity) of any management information they receive relating to the plan and its execution, and active, regular consideration of whether implementation is consistent with prudent management and the firm's risk appetite (as approved by the board).

Risk management

(2) ensure that the firm's risk management function adequately identifies, assesses and reports on key risks, in particular operational risk, in relation to the migration programme. This should include:

(a) making provision for the business areas to explicitly identify risks related to the non-performance, or inadequate performance of the firm's third party supplier so that adequate consideration is given on an ongoing basis to the operational risks for the firm arising from that relationship, and action taken accordingly to mitigate those risks;

(b) ensuring that the scope of the assurances provided by risk oversight and/or internal audit are proportionate and appropriate to the scale, complexity and level of operational risk arising from the migration programme, and that any limitations or qualifications are specifically drawn to the board's attention and scrutinised appropriately.

Business continuity planning

(3) ensure that the firm's incident management arrangements, and those of its outsourced service providers, are sufficiently robust and effective. Firms must implement disaster recovery and incident management arrangements which ensure their service providers – and where relevant, their subcontractors – can effectively and promptly support the recovery of Critical Functions. The Bank/PRA's and FCA's recent policy on operational resilience (which was mostly developed and finalised after the TSB outage) underscores firms' obligations in this area.

Management of outsourced relationships

(4) be particularly conscious of the risks of operational failure where IT services and the development of IT infrastructure upon which they rely for continuity of financial services are outsourced to third parties. Firms must therefore have robust outsourcing arrangements with prudent governance and risk management, commensurate with the complexity and size of the firm and the criticality, complexity and scale of the functions being outsourced. This expectation also applies where the outsourcing arrangement is with an intragroup service provider even though some of the ways in which firms discharge this expectation may differ in practice in intragroup arrangements. This should include:

a) an assessment of the relevant risks of sub-outsourcing or supply chains before entering into an outsourcing agreement. Firms must pay particular attention to the potential impact of large, complex sub-outsourcing chains on their operational resilience. Firms must have visibility of the supply chain and consider whether extensive outsourcing could compromise their ability to oversee and monitor an outsourcing arrangement;

b) appropriate monitoring and oversight of the service provider, including procedures for the ongoing assessment of service providers' performance. A firm must take prompt and appropriate action when it appears that the service provider may not be carrying out the

outsourced functions effectively. This includes the exceptional audit of subcontractors if appropriate and necessary to address operational risk;

c) ensuring that the service provider has the ability and capacity on an ongoing basis to appropriately oversee any material sub-outsourcing in line with the firms' relevant policy or policies. Where firms are reliant on an outsourced service provider to manage fourth parties to ensure that the firm's interests and needs are met, firms are expected to take a sufficiently engaged and proactive approach to oversight of the outsourced service provider;

d) addressing key person risk, which can undermine the implementation of what may otherwise be a carefully designed assurance and governance framework for a complex change management project with a significant outsourcing component. This emphasises the importance of firms retaining the necessary expertise to manage the risks associated with the outsourcing, ensuring that such expertise is not concentrated in any single individual;

e) ensuring that boards and senior management, in particular individuals performing SMFs, do not outsource their responsibilities. Firms that enter into outsourcing arrangements remain fully accountable for complying with all their regulatory obligations. This is a key principle underlying all requirements and expectations regarding outsourcing and non-outsourcing third party arrangements, and applies equally to situations where a subsidiary relies on an intragroup service provider for a major change management initiative or for the provision of an important business service. In those scenarios, subsidiary boards should be suitably empowered and informed to discharge their responsibility to act in the best interests and safeguarding the safety and soundness of the firm for which they are responsible.

2.8 As set out above, the PRA's outsourcing rules during the Relevant Period applied specifically to the '*performance of operational functions which are critical for the performance of relevant services and activities'*. TSB's migration to the Proteo4UK Platform and the provision of IT services via services and outsourcing arrangements with SABIS were critical to the Firm's ability to provide continuity of services, and therefore to its safety and soundness. SABIS and LBG were contracted to provide Critical Functions on behalf of the Firm: they provided core banking platforms that were critical to the performance or ongoing continuity of the Firm and such services could not be interrupted for more than 24 hours without material business impact. The PRA therefore expected the Firm to manage all aspects of the Migration Programme, including SABIS's design and build of its new IT systems as well as SABIS's ongoing operation of those new systems, with the outsourcing rules and the Fundamental Rules in mind.

3. Failings

3.1 The PRA has concluded that during the Relevant Period, the Firm breached Fundamental Rules 2 and 6 of the PRA's Rulebook.

Fundamental Rule 2 (A firm must conduct its business with due skill, care and diligence)

3.2 The Firm breached Fundamental Rule 2 because it failed to exercise due skill, care and diligence in managing appropriately and effectively the outsourcing arrangements with, and services provided by, SABIS and the risks arising from this, including operational risk. The Firm's breach of Fundamental Rule 2 stemmed from an undue reliance on SABIS as an intragroup provider, which in turn led to a level of oversight that was not consistent with the importance and scale of the Migration Programme. In particular, the Firm failed to exercise due skill, care and diligence:

a. when entering into the arrangement for services and outsourcing to SABIS. The Firm did not formally and comprehensively assess whether SABIS had the ability, capacity, resources and appropriate organisational structure to deliver the Proteo4UK Platform in the timeframe adopted and were ready to provide the ongoing outsourced services required to operate the Proteo4UK Platform reliably and professionally. Owing to this failing, the Firm did not:

(i) adequately address risks arising from its outsourcing arrangements with SABIS, in particular, that SABIS was a service provider with no experience of managing service delivery from a large number of UK subcontractors and that TSB had limited experience of supplier oversight in an IT change management project of this scale and complexity;

(ii) adequately consider how the outsourcing risks needed to be mitigated in practice. If the Firm had done so, it may have been in a position to mitigate risks arising from the Firm:

- needing to appropriately manage and control SABIS in delivering both the transformation and an operational services capability;
- taking account of SABIS's learning curve in providing services in the UK market and complying with the UK regulatory environment having accountability for the design and robustness of the services being delivered and the need for SABIS to deliver the required level of service for the Firm; and

- needing to develop capabilities for oversight of fourth party supply chains.

(iii) have a sufficient grasp of whether SABIS's infrastructure designs reflected TSB's requirements or whether SABIS had built the infrastructure in accordance with the designs and how SABIS had carried out testing;

(iv) ensure there was an effective IT control framework commensurate to the significant operational risk involved in the Migration Programme and the switch to a new IT service provider.

b. when managing the arrangement for services and outsourcing to SABIS. Testing for the Migration Programme was executed in a manner which departed from the Firm's stated plans and guiding principles, increasing operational risk. The Firm did not formally and adequately reassess SABIS's ability and capacity on an ongoing basis including in light of service level breaches encountered with the GTEs. It did not receive formal assurance from SABIS in the form of statements of fact about the completeness of readiness activities already undertaken by it, or the Firm's Critical Fourth Parties, nor about SABIS's management of the Firm's Critical Fourth Parties, including whether SABIS had robust testing, monitoring and control over the Firm's Critical Fourth Parties. Owing to this failing, the Firm did not:

(i) have sufficient regard to the risks to which it was exposed through the supply chain. The Firm's approach to its oversight of SABIS was not sufficiently engaged and proactive given that the Firm was reliant on SABIS to manage fourth parties to ensure that the Firm's interests and needs were met. As the Firm did not have the necessary visibility of the supply chain risks, the Firm could not have been confident that SABIS was overseeing fourth party service delivery in a way that was commensurate to the criticality of the service or overall complexity and scale of the Migration Programme;

(ii) engage adequately with the indications in late 2017 that SABIS was not fully ready to operate the platform after migration. This included failing between October 2017 and January 2018, to re-assess SABIS's capabilities in light of the problems that the Firm had experienced for each of the GTEs (which in some cases had led to slow recovery from incidents), or take a holistic view of the risks associated with its outsourcing arrangement by considering SABIS's capabilities with respect to the remaining services to be delivered;

(iii) ensure that SABIS's supplier management model (including a service risk assessment methodology and framework) was fully developed and complied with TSB Group Outsourcing policy, or consider whether a formal re-

assessment was required to have a full picture of the operational risks presented by the Migration Programme; and

(iv) give sufficient consideration to the appropriateness of relying on the SABIS Confirmation which was, to some extent, a forward looking statement of good intention or expectations, rather than a statement of fact about the completeness of readiness activities already undertaken.

3.3 Further, the Firm failed to exercise due skill, care and diligence when TSB decided not to conduct NFT of the digital channels in Active-Active configuration in both data centres. This resulted in the testing and production environments being distinctly different which meant that an opportunity to potentially identify some of the configuration issues experienced post MME was lost. This meant that, while TSB did consider that there were risks in conducting Active-Active performance testing in the live environment, TSB failed to identify and evaluate the risks of not conducting the testing in Active-Active configuration, nor did it consider any potential mitigants for the risks.

3.4 The Firm also failed to take a critical decision regarding NFT in the Migration Testing Forum, which was the governance structure in place for such decisions. This decision was not escalated or sufficiently explained to the appropriate committees and/or decision makers, because this was viewed as purely technical and not presenting a risk to TSB. Neither were the risks identified in the Final NFT Report. This was a significant failing. NFT was itself an important risk mitigant in relation to testing the infrastructure of the Proteo4UK platform (alongside other forms of testing such as UAT and SIT) particularly where limited infrastructure build and validation information, and very limited infrastructure testing documentation were available to TSB.

Fundamental Rule 6 (A firm must organise and control its affairs responsibly and effectively)

3.5 The Firm breached Fundamental Rule 6 because it failed to organise and control the Migration Programme responsibly and effectively. In particular:

a. The Firm's planning and re-planning of the Migration Programme was insufficiently robust and failed to adequately mitigate operational risk. Expanding on this:

i. The initial planning for the Migration Programme adopted a '*right-to-left*' approach and as a result set an overly ambitious timetable for migration, given its scale and complexity, and the degree of operational risk. This inevitably gave rise to greater operational risk than if the Firm had adopted a '*left-to-right*' approach, as it forced the Firm into a position where it needed to re-plan;

ii. re-planning of the Migration Programme in September and October 2017 did not adequately investigate the technical causes of delays, or adequately assess the performance and service issues with the Governed Transition Events which had, in some instances, resulted in outages and/or breaches of service level agreements which should have caused the Firm to question SABIS's readiness. When re-planning during this period, the Firm's Defender Plan also adopted an overly right-to-left approach (although TSB was of the view that it would not migrate until it was ready). The Firm missed an opportunity to properly assess the extent of the delays to the Migration Programme, to learn critical lessons from that assessment, and to realistically assess the volume of work that needed to be achieved before it was '*migration ready*'. As a result, the Firm did not have an adequate understanding of what the delays meant for the overall risk profile of the Migration Programme, or how they impacted its understanding of the platform's readiness and of SABIS to operate it; and

iii. the Firm publicly committed to a re-planned MME date in Q1 2018 before the re-planning of the Migration Programme had been completed or approved by the Board. This was premature. Further, the public commitment exposed the Firm to greater reputational risk if the migration did not occur within or close to this timeframe. The TSB Board should have considered whether this public commitment might increase pressure to complete the programme, thereby increasing exposure to operational risk if compromises were taken to meet the announced timeframe. Certain compromises were taken, for example, in relation to key risk mitigants set out in the Defender Plan. In addition, the Firm did not adequately investigate the technical causes of delays, or adequately investigate their impact on the likely and realistic time required to complete the remaining tasks before migration;

b. the Firm's governance of the Migration Programme was insufficiently robust. It does not appear certain matters were sufficiently discussed with the TSB Board, which could have led to challenge. In particular, the overly ambitious timetable for migration, deviations from certain aspects of the migration plans and Guiding Principles and what they meant for the overall risk profile of the programme, and the readiness of the Proteo4UK Platform and SABIS;

c. the Firm's risk management function did not adequately identify, assess and report on key risks, in particular operational risk, related to the Migration Programme. Specifically:

i. the Firm did not explicitly identify risks related to the non-performance, or inadequate performance of the Firm's key supplier so that adequate

consideration was given on an ongoing basis to the operational risks for the Firm arising from that relationship, and action taken accordingly to mitigate those risks, (although aspects of the impact of the non-performance were considered as part of other programme risks). As a result, the Business Areas failed to explicitly assess the risk of non-performance, or inadequate performance, by SABIS of its obligations to deliver a stable platform that met TSB's requirements and to operate that platform;

ii. although Risk Oversight and Internal Audit carried out a large number of migration-related reviews and audits, some of these were limited in scope, were expressly stated to be '*point-in-time*' reviews which might have been overtaken or were otherwise expressly qualified. However, these limitations and/or qualifications do not appear to have been specifically discussed with the TSB Board at certain crucial junctures which could have led to challenge. This meant that the assurance provided by Risk Oversight and Internal Audit which supported the recommendation to proceed with Go Live was inadequate and inappropriate for the scale, complexity and level of operational risk arising from the Migration Programme.

d. The Firm's incident management arrangements were ineffective and insufficiently robust. The Firm's failures in this regard meant that the Firm was not prepared to handle the crisis that unfolded post MME. Specifically:

i. the Firm did not undertake adequate exercises to test its and SABIS's ability, from an IT perspective, to recover from all aspects of an IT failure of the size of the one which manifested after MME. In particular, the exercises intended to prepare for '*multiple organ failure*' were limited without more comprehensive participation, particularly from SABIS. This failure was compounded by the Firm's assessment that it was realistic to anticipate some operational incidents following MME (although they did not anticipate the scale of the incidents that eventuated), and that the Firm's ability to address these incidents would involve heavy reliance on SABIS;

ii. the Firm did not ensure that it had sufficient oversight and assurance of SABIS's incident management capabilities. In light of the Firm's awareness that SABIS would be relying on a large number of third parties to provide a fully functioning bank after migration, exposing the Firm to operational and other risks which were not fully visible to it, the Firm should have taken further steps to embed the controls relevant to effective incident response. Such steps would have included insisting upon clear and comprehensive process definition and documentation, and more rigorous business continuity exercises specifically testing areas of greater dependence on SABIS and fourth party suppliers.

Conclusion on failings

3.6 Taken together, the Firm's failings in relation to governance, risk management, third party oversight, lack of visibility and management of fourth party risks, and limitations in preparation for incident management each involved breaches of the rules underpinning those constituent parts of the PRA's operational resilience framework that were in effect during the Relevant Period. These breaches resulted either from a failure to exercise due skill, care and diligence or a failure to organise and control its affairs responsibly and effectively. The way in which a firm manages operational resilience is an integral part of the PRA's assessment of a firm's safety and soundness. Adverse effects on the stability of the UK financial system, including through threats to customer confidence in individual firms, may result from disruption to the continuity of financial services. This is why the PRA places such a high priority on embedding operational resilience in its supervisory approach to mitigate the risk of such disruption.

3.7 These failings are particularly significant given: a) the scale, complexity, and unprecedented nature of this Migration Programme, which inherently heightened operational risk; and b) as a challenger bank, the Firm was potentially more vulnerable to brand damage arising from operational failures and therefore at risk of loss of confidence in the event of significant operational disruption, leading to potential depositor outflows (in this case, we note that this risk did not in fact materialise). Depositor outflows can pose a risk to safety and soundness of a firm, and could also impact confidence in challenger banks more broadly, and therefore potentially have a negative impact on financial stability. The Migration Incident resulted in significant disruption to the continuity of the Firm's provision of core banking functions (including branch, telephone, online and mobile banking) immediately post migration, with some more limited issues persisting for a sustained period of months. All 550 of its branches and a significant proportion of its customers (including a proportion of those customers on the digital platform) were impacted.

3.8 These breaches therefore had the potential to impact adversely on the Firm's safety and soundness. The Firm fell short of the PRA's expectations.

3.9 As a result of these failings, the Firm breached Fundamental Rules 2 and 6 of the PRA's Rulebook during the Relevant Period.

Annex C: Penalty Analysis

1. Financial Penalty

1.1. The PRA Penalty Policy for imposing a financial penalty is set out in *'The PRA's approach to enforcement: statutory statements of policy and procedure' (September 2021)*', in particular in the '*Statement of the PRA's policy on the imposition and amount of financial penalties under the Act'* (the 'PRA Penalty Policy'). Pursuant to paragraphs 12 to 36 of the PRA Penalty Policy, the PRA applies a five-step framework to determine the appropriate level of financial penalty.

1.2. The PRA considered whether to calculate separate penalties in respect of the Firm's breaches of Fundamental Rules 2 and 6. However, as the systems and controls failings underpinning the misconduct in relation to these regulatory breaches are linked, the PRA concluded that a single penalty calculation is appropriate.

Step 1: Disgorgement

1.3. Pursuant to paragraph 17 of the PRA Penalty Policy, at Step 1 the PRA seeks to deprive a person of any economic benefits derived from, or attributable to, the breach of its requirements, where it is practicable to ascertain and quantify them.

1.4. The PRA has no evidence that the Firm derived any economic benefit from the breaches, including profit made or loss avoided. The PRA therefore does not require the disgorgement of any sum from the Firm.

1.5. The Step 1 figure therefore is **£0**.

Step 2: The seriousness of the breach

1.6. Pursuant to paragraph 18 of the PRA Penalty Policy, at Step 2 the PRA determines a starting point figure for a financial penalty having regard to the seriousness of the breach by the firm, including any threat it posed, or continues to pose, to the advancement of the PRA's statutory objectives, and the size and financial position of the firm.

1.7. Paragraph 19(a) of the PRA Penalty Policy sets out that a suitable indicator of the size and financial position of the firm may include, but is not limited to, the firm's total revenue in respect of one or more areas of its business. Further, paragraph 19(c) sets out that the PRA will apply an appropriate percentage rate to the firm's relevant revenue to produce a figure at Step 2 that properly reflects the nature, extent, scale and gravity of breaches.

1.8. The Firm's total business revenue for the financial year ending 31 December 2017 (being the financial year preceding the date when the breaches ended) is £1,099,800,000. The Firm uses a calendar year as its financial year. Taking into account the seriousness, scale and effect of the Firm's breaches, the PRA considers that a financial penalty based on the application of a seriousness percentage to the Firm's total revenue would be disproportionate.

1.9. To arrive at a penalty, pursuant to paragraph 21 of the PRA Penalty Policy, the PRA has instead taken the following factors into account (alongside the size and financial position of the firm) to produce a figure at Step 2 that properly reflects the nature, extent, scale, gravity and overall seriousness and significance of the breaches:

(1) firms' operational resilience is fundamental to the PRA's ability to advance its general objective of promoting the safety and soundness of the firms it regulates. This is made explicit by section 2B(3)(a) of the Act which provides that the PRA's general objective is to be advanced by seeking to ensure that the business of the PRA-authorised firms is carried on in a way which avoids any adverse effect on the stability of the UK financial system. Further, section 2B(4) of the Act defines such adverse effect as including those that may result from the disruption of the continuity of financial services. Therefore, the PRA's priorities since 2016 have included a strong focus on operational resilience.

The Firm was, and remains, a retail bank with a relatively simple business model, but as at MME, it had more than 5 million customers. Its size, interconnectedness and business type gave the Firm the capacity to cause some disruption to the UK financial system (and through that, economic activity more widely) if it carried on its business in an unsafe manner. It also had a significant role to play in the UK financial system as a relatively new challenger bank (notwithstanding TSB's customer base was far more akin to the large, established banks), which had explicitly been created to increase competition in the UK retail banking sector.

(2) TSB encountered serious issues which significantly impacted the ability of some customers to access and use their accounts in the first few days post MME. These included certain data breaches, failures with digital banking services, telephone banking, branch technology failures, and consequential issues with payment and debit card transactions). Whilst the data migration itself was successful, the Migration Incident resulted in significant disruption to the continuity of TSB's provision of core banking functions (including branch, telephone, online and mobile banking) immediately post migration, with some more limited issues persisting for a sustained period of months. All 550 of its branches and a significant proportion of its customers (including a proportion of those customers on the digital platform) were impacted. Residual issues remained and overall, TSB did not return to a BAU position until 10 December 2018.

(3) the breaches revealed serious weaknesses in elements of the Firm's governance and

oversight (including in relation to third parties), risk management and business continuity capabilities.

(4) these breaches occurred at points between 16 December 2015 (when the planning and execution of the Migration Programme commenced), continued through the Migration Incident (during and after MME) and until 10 December 2018 (when BAC downgraded the priority/severity of the migration-related issues in its term of reference).

(5) the Firm's breaches were neither deliberate nor reckless.

1.10. The PRA has also had regard to the matters set out at Annexes A and B to this Notice.

1.11. Taking all of these factors into account, the PRA considers the failings in this case were significant and determined that the appropriate Step 2 figure is **£30,000,000**.

Step 3: Adjustment for any aggravating, mitigating or other relevant factors

1.12. Pursuant to paragraph 24 of the PRA Penalty Policy, the PRA may increase or decrease the Step 2 figure to take account of any factors which may aggravate or mitigate the breaches. The factors that may aggravate or mitigate the breach include those set out at paragraphs 25 and 26 of the PRA Penalty Policy. Any such adjustments will normally be made by way of a percentage adjustment to the figure determined at Step 2.

1.13. In deciding whether any adjustment for aggravating or mitigating factors is warranted, the PRA has considered the following factors:

(1) the Firm has cooperated with the PRA's investigation. TSB commissioned a number of technical reviews in the immediate aftermath of MME, which it subsequently provided to the PRA. In addition, TSB voluntarily commissioned a comprehensive independent review into many of the matters referred to in this Notice, and committed to make the final review public. Although, ultimately, TSB did not accept the findings of the review in a number of key respects, TSB agreed to provide the PRA with notes of interviews conducted as part of the review with relevant individuals.

(2) the Firm does not have any previous disciplinary history.

(3) the Firm has undertaken a comprehensive remediation programme and restructured its IT operations in the aftermath of the Migration Programme. In the circumstances of the significant disruption to the continuity of TSB's provision of core banking functions that transpired for some

customers immediately post-MME, the PRA considers that TSB had some commercial interest in taking remedial steps. However, the PRA acknowledges that some of the remedial steps could be considered to be generous.

1.14. The PRA has also considered and already taken into account the action proposed by the FCA to impose a financial penalty on the Firm arising from the same events and substantially the same facts and matters.

1.15. The PRA considers that the mitigating factors at paragraph 1.13, when considered together, warrant an adjustment to the Step 2 figure. Accordingly, the PRA has concluded that the Step 2 figure should be decreased by 10%

1.16. The Step 3 figure is therefore **£27,000,000.**

Step 4: Adjustment for deterrence

1.17. Pursuant to paragraph 27 of the PRA Penalty Policy, if the PRA considers the figure arrived at after Step 3 is insufficient to effectively deter the firm that committed the breach, or others, from committing further or similar breaches, then the PRA may increase the penalty at Step 4 by making an appropriate adjustment to it.

1.18. Taking into account all the circumstances, the PRA does not consider an adjustment for deterrence is necessary in this matter.

1.19. The Step 4 figure is therefore **£27,000,000.**

Step 5: Application of any applicable reductions for early settlement or serious financial hardship

1.20. Pursuant to paragraph 29 of the PRA Penalty Policy, if the PRA and the firm upon which a financial penalty is to be imposed agree the amount of the financial penalty and any other appropriate settlement terms, the PRA Settlement Policy provides that the amount of the penalty which would otherwise have been payable may be reduced.

1.21. The PRA and the Firm reached an agreement to settle during the Discount Stage, therefore a 30% settlement discount applies to the Step 4 figure.

1.22. The Step 5 figure is therefore **£18,900,000**.

Conclusion

1.23. The PRA has therefore imposed on the Firm a financial penalty of **£18,900,000** for its breaches of the PRA Fundamental Rules 2 and 6.

Annex D: Procedural Matters

Decision maker

1. The settlement decision makers made the decision which gave rise to the obligation to give this Notice.

2. This Notice is given under and in accordance with section 390 of the Act.

Manner and Time for Payment

3. TSB must pay the financial penalty in full to the PRA by no later than 10 January 2023. If all or any of the financial penalty is outstanding on 11 January 2023, the day after the due date for payment, the PRA may recover the outstanding amount as a debt owed by TSB and due to the PRA.

Publicity

4. Sections 391(4), 391(6A) and 391(7) of the Act apply to the publication of information about the matter to which this Notice relates. Under those provisions, the PRA must publish such information about the matter to which this Notice relates as the PRA considers appropriate. However, the PRA may not publish information if such publication would, in the opinion of the PRA, be unfair to the persons with respect to whom the action was taken or prejudicial to the safety and soundness of PRA-authorised persons or prejudicial to securing an appropriate degree of protection to policyholders.

PRA contacts

5. For more information concerning this matter generally, contact Press Office (press@bankofengland.co.uk).

Appendix 1: Definitions

The definitions below are used in this Notice:

1. the 'Act' means the Financial Services and Markets Act 2000 (as amended);

2. 'Active-Active configuration' means configuration of both data centres of the Proteo4UK Platform which enables their simultaneous operation for the purpose of balancing the load of customer sessions between each data centre using a Global Load Balancer;

3. 'Active-Passive configuration' means configuration of both data centres of the Proteo4UK Platform such that they both host applications, while customer sessions are being serviced only by the Active data centre;

4. 'Assurance Matrix' means a risk assessment tool used by TSB to assess its readiness for going ahead with the migration of data from the LBG IT Platform to the Proteo4UK Platform;

5. 'BAC' means the Board Audit Committee;

6. 'BAU' means business as usual;

7. 'BCIM Policy' means TSB's Business Continuity and Incident Management Policy;

8. 'BEC' means TSBBG's Board Executive Committee;

9. 'BEC DE' means TSBBG's BEC Design Executive;

10. 'Big Bang' means the data migration model in which data is migrated from one IT platform to another through a single event;

11. The Boards of TSB and TSBBG, also referred to as 'the Board';

12. 'TSBBG' means TSB Banking Group plc, which is the holding company of TSB, noting that the boards of both entities have the same composition.

13. 'BRC' means TSBBG's Board Risk Committee;

14. 'Bronze incident' means a low severity incident simulated in a test environment;

15. 'Business Areas' or 'BEC business functions' means the first line of defence, responsible for risk

decisions and actions as well as measuring, monitoring and controlling risks within their areas of accountability;

16. ‘CMDB’ means Configuration Management Database consisting of documents related to the migration infrastructure;

17. ‘Critical Functions’ means operational functions which are critical for the performance of regulated activities, listed activities or ancillary services;

18. ‘Critical Fourth Parties’ means the parties whom SABIS considered to be critical third parties as set out in the SABIS Confirmation;

19. ‘Critical Third Party Suppliers’ means SABIS and LBG, which TSB considered to be suppliers for critical outsourced banking functions;

20. ‘Defender Plan’ means a memo presented to the TSB Board on 24 October 2017 which sets out the Firm’s decision to postpone the IT migration from 5 November 2017 to Q1 2018;

21. ‘Definitive Notice of Migration’ means a notice TSB served to LBG on 12 April 2018 which terminated the carve-out option and committed TSB to the migration option;

22. ‘Design Phase’ means the phase during which TSB defined its migration platform requirements;

23. ‘Discount Stage’ means, as provided for in the PRA Penalty Policy and PRA Settlement Policy, the early period of an investigation during which the subject of an investigation will qualify for a 30% discount to the proposed financial penalty if they enter into a settlement agreement with the PRA;

24. ‘Dossier Phase’ means the phase during which a detailed gap analysis of the Proteo4UK Platform at a micro level was undertaken;

25. ‘Executive Gold Team’ means a group of TSB senior executives who took part in testing rehearsals before MME;

26. ‘Failover’ means a scenario whereby one data centre automatically transfers control to the other when it detects a fault or failure;

27. ‘FCA’ means the Financial Conduct Authority;

28. ‘Firm’ or ‘TSB’ mean TSB Bank plc;

29. ‘Global Load Balancer’ means a network box that receives all digital requests and decides, based

on a set of rules, which one of the two data centres the request should be forwarded to;

30. ‘Gold incident’ means an incident of the highest severity simulated in a test environment;

31. ‘Go live’ means a weekend over which data would be migrated from the LBG IT Platform to the Proteo4UK Platform;

32. ‘Go-No Go Decision’ means BEC’s decision on whether to proceed with the data migration;

33. ‘GOS environment’ means a test environment built by TSB as a simplified version of the production environment;

34. ‘Governed Transition Events’ or ‘GTEs’ mean phased transition of functionality to the Proteo4UK Platform;

35. ‘Guiding Principles’ mean 15 Guiding Principles relating to testing which had been designed to minimise operational risks and were a key feature and risk mitigant of the Defender Plan;

36. ‘IMP’ means Integrated Master Plan which sets out the overall migration plan presented to the TSB Board on 15 March 2016;

37. ‘Internal Audit’ means the third line of defence, responsible for independent and objective assurance over the Business Areas’ management of risk and control, and Risk Oversight’s supervision of TSB’s risks;

38. ‘LBG’ means Lloyds Banking Group;

39. ‘LBG IT Platform’ means the IT platform used by LBG, which was also used by TSB until its migration on to the Proteo4UK Platform;

40. ‘MACs’ means Migration Acceptance Cycles which tested the migrated data during the extract, transform and load process;

41. ‘Macro Dossier gap analysis’ means a detailed gap analysis of the Proteo4UK Platform at a macro level;

42. ‘Material Risk Register’ means a register recording all material risks which deserve prominence at Board and BEC level;

43. ‘Material Subcontractors’ mean suppliers of critical or important functions under the regulatory outsourcing requirements;

44. ‘MDC’ means TSB’s Migration Delivery Committee;

45. ‘MDT’ means Migrated Data Testing;

46. ‘Migration Deferred Defects Forum’ means a TSB forum which assessed the outcome of functional and non-functional testing to determine whether TSB had the required functionality to proceed with the migration;

47. ‘Migration Incident’ mean serious and well publicised issues, which took place immediately after the MME, that resulted in a significant disruption to the continuity of TSB’s provision of core banking to some customers in the first few days post MME including certain data breaches, failures with online, telephone and mobile banking services, branch technology failures and issues with payment and debit card transactions;

48. ‘Migration Programme’ means a major IT change programme, involving the design, build and testing of the new Proteo4UK Platform and associated IT systems, followed by migration of TSB’s corporate and customer services on to the new platform;

49. ‘Migration Testing Forum’ means a TSB forum which was accountable for providing the over-arching governance and decision-making for testing and for providing reports to the MDC;

50. ‘MME’ means Main Migration Event at which TSB migrated its corporate systems, customer services and customer data from the LBG IT Platform to the Proteo4UK Platform over the weekend of 20 to 22 April 2018;

51. ‘MSA’ means the Migration Services Agreement entered into between TSB and SABIS which governed the design, build and testing of the Proteo4UK Platform, and the migration of TSB’s data to it, by SABIS;

52. ‘NFRs’ mean non-functional requirements;

53. ‘NFT’ means Non-Functional Testing which consists of infrastructure testing, performance testing, security testing, and disaster recovery testing;

54. ‘NFT Final Report’ means the final report on Non-Functional Testing dated 17 April 2018;

55. ‘NFT Memo’ means the confirmation that NFT had been completed according to the requisite specifications;

56. ‘Notice’ means this Final Notice, together with its Annexes and Appendices;

57. ‘OSA’ means the Outsourced Services Agreement entered into between TSB and SABIS which

governed the operation of the Proteo4UK Platform by SABIS;

58. ‘PGLS model’ means Post Go Live Support model which was a post-MME contingency plan that consisted of a process flow from identifying a problem through to delivery of an IT solution;

59. ‘PRA’ means the Prudential Regulation Authority;

60. ‘PRA Rulebook’ means a rulebook which contains provisions made by the PRA that apply to PRA-authorised firms;

61. ‘PRA Penalty Policy’ means ‘*The Prudential Regulation Authority’s approach to enforcement: statutory statements of policy and procedure (effective from September 2021), Appendix 2 – Statement of the PRA’s policy on the imposition and amount of financial penalties under the Act*’;

62. ‘PRA Settlement Policy’ means ‘*The Prudential Regulation Authority’s approach to enforcement: statutory statements of policy and procedure (effective from September 2021), Appendix 4 - Statement of the PRA’s settlement decision-making procedure and policy for the determination of the amount of penalties and the period of suspensions or restrictions in settled cases*’;

63. ‘Pre-production environment’ means a mirror copy of the production environment which allows changes to be tested without impacting users of the production environment;

64. ‘Production environment’ means an environment in which live services were being delivered;

65. ‘Proteo’ means Sabadell IT banking platform;

66. ‘Proteo4UK Platform’ means a new version of Proteo platform adopted for TSB and the UK market;

67. ‘Relevant Period’ means the period between 16 December 2015 to 10 December 2018;

68. ‘Risk Oversight’ means the second line of defence, responsible for independent oversight and challenge and TSB-wide risk reporting;

69. ‘Sabadell’ means Banco de Sabadell, S.A;

70. ‘Sabadell Group’ means the Sabadell group of companies;

71. ‘SABIS’ means both SABIS Spain and SABIS UK;

72. ‘SABIS Confirmation’ means a letter from SABIS, dated 5 April 2018, stating confidence as to the migration readiness of the platform, providing an early report on NFT results (noting that some tests

were still to be completed) and referring to confirmations of readiness received or anticipated from Critical Fourth Parties;

73. ‘SABIS Spain’ means Sabadell Information Systems, S.A;

74. ‘SABIS UK’ means Sabadell Information Systems Limited;

75. ‘Service Level Agreements’ mean agreed performance thresholds between TSB and SABIS;

76. ‘Silver incident’ means a medium severity incident simulated in a test environment;

77. ‘SIT’ means System Integration Testing of the Proteo4UK application software;

78. ‘SMF’ means Senior Management Function specified by the PRA or FCA for employees performing a certification function and directors of authorised persons;

79. ‘T3 memo’ means the memorandum to the TSB Banking Group dated 14 April 2018 which included a recommendation to proceed with MME, attestations testifying to the readiness of BEC business functions and opinions from Risk Oversight and Internal Audit on the Business Areas’ interpretations of the facts, the risks to the business of proceeding with the MME and the effectiveness of the mitigating actions;

80. ‘Three lines of defence’ means the risk management framework that incorporates the Business Areas (first line), Risk Oversight (second line) and Internal Audit (third line);

81. ‘Tribunal’ means the Upper Tribunal (Tax and Chancery Chamber);

82. ‘UAT’ means User Acceptance Testing; and

83. ‘UAT environment’ means an environment used for conducting UAT.

Appendix 2: Relevant Statutory and Regulatory Provisions

1. Relevant Statutory Provisions

1.1. The PRA has a general objective, set out in section 2B of the Act, to promote the safety and soundness of PRA-authorised persons. The PRA seeks to advance this objective by seeking to ensure that the business of PRA-authorised firms is carried on in a way which avoids any adverse effect on the stability of the UK financial system.

1.2. Section 206 of the Act provides that: '*If the appropriate regulator considers that an authorised person has contravened a relevant requirement imposed on the person, it may impose on him a penalty, in respect of the contravention, of such amount as it considers appropriate*.'

1.3. TSB Bank plc is an authorised person for the purposes of section 206 of the Act. Relevant requirements imposed on an authorised person include rules made under the PRA Rulebook, including the PRA's Fundamental Rules, the Branch Return Rule and the Notifications Rules.

2. Relevant Regulatory Provisions

2.1. In addition to its Threshold Conditions, the PRA has a number of Fundamental Rules which apply to all PRA-authorised firms. These are high-level rules which collectively act as an expression of the PRA's general objective of promoting the safety and soundness of regulated firms.

2.2. Fundamental Rule 2 states that: *'A firm must conduct its business with due skill, care and diligence.'*

2.3. Fundamental Rule 5 states that: *'A firm must have effective risk strategies and risk management systems.'*

2.4. Fundamental Rule 6 states that: *'A firm must organise and control its affairs responsibly and effectively.'*

2.5. The following table shows the changes to the relevant rules concerning outsourcing, risk control, business continuity and general organisational requirements prior to and from 3 January 2018 when MiFID II came into effect. However, the relevant rules in place from 3 January 2018 are not substantively different to the old rules.

Rules	Prior to 3 January 2018	From 3 January 2018
Outsourcing	• Article 13(5) of MiFID • Articles 13 and 14 of the MiFID implementing Directive (**Old Outsourcing Rules**)	• Article 16(5) of MiFID II • Articles 30 and 31 (Outsourcing Requirements) of the MODR (**New Outsourcing Rules**)
Risk Control 3.4	• Article 76(5) of the CRD	• Article 76(5) of the CRD
GOR 2.5 (business continuity)	• Article 13(4) of MiFID	• Article 16(4) of MiFID II
GOR 2.6 (business continuity)	• Article 5(3) MiFID implementing Directive • Article 85(2) of the CRD	• Article 85(2) of the CRD

2.6. Prior to 3 January 2018, PRA Outsourcing Rules 2.1, 2.2, 2.4 to 2.8 (which came into effect on 2 April 2015) state:

Rule 2.1: *'A firm must:*

(1) when relying on a third party for the performance of operational functions which are critical for the performance of relevant services and activities on a continuous and satisfactory basis, ensure that it takes reasonable steps to avoid undue additional operational risk;

(2) not undertake the outsourcing of important operational functions in such a way as to impair materially:

(a) the quality of its internal control; and

(b) the ability of the PRA to monitor the firm's compliance with all obligations under the regulatory system and, if different, of a competent authority to monitor the firm's compliance with all obligations under MiFID.'

Rule 2.2: *'For the purposes of this Part an operational function is regarded as critical or important if a defect or failure in its performance would materially impair the continuing compliance of a firm with the conditions and obligations of its authorisation or its other obligations under the regulatory system, or its financial performance, or the soundness or the continuity of its relevant services and activities.'*

Rule 2.4: *'If a firm outsources critical or important operational functions or any relevant services and activities, it remains fully responsible for discharging all of its obligations under the regulatory system and must comply, in particular, with the following conditions:*

(1) the outsourcing must not result in the delegation by senior personnel of their responsibility;

(2) the relationship and obligations of the firm towards its clients under the regulatory system must not be altered;

(3) the conditions with which the firm must comply in order to be authorised, and to remain so, must not be undermined;

(4) none of the other conditions subject to which the firm's authorisation was granted must be removed or modified.'

Rule 2.5: *'A firm must exercise due skill and care and diligence when entering into, managing or terminating any arrangement for the outsourcing to a service provider of critical or important operational functions or of any relevant services and activities.'*

Rule 2.6: *'A firm must in particular take the necessary steps to ensure that the following conditions are satisfied:*

(1) the service provider must have the ability, capacity, and any authorisation required by law to perform the outsourced functions, services or activities reliably and professionally;

(2) the service provider must carry out the outsourced services effectively, and to this end the firm must establish methods for assessing the standard of performance of the service provider;

(3) the service provider must properly supervise the carrying out of the outsourced functions, and adequately manage the risks associated with the outsourcing;

(4) appropriate action must be taken if it appears that the service provider may not be carrying out the functions effectively and in compliance with applicable laws and regulatory requirements;

(5) the firm must retain the necessary expertise to supervise the outsourced functions effectively and to manage the risks associated with the outsourcing, and must supervise those functions and manage those risks;

(6) the service provider must disclose to the firm any development that may have a material impact on its ability to carry out the outsourced functions effectively and in compliance with applicable laws and regulatory requirements;

(7) the firm must be able to terminate the arrangement for the outsourcing where necessary without detriment to the continuity and quality of its provision of services to clients;

(8) the service provider must co-operate with the PRA and any other relevant competent authority in connection with the outsourced activities;

(9) the firm, its auditors, the PRA and any other relevant competent authority must have effective access to data related to the outsourced activities, as well as to the business premises of the service provider; and the PRA and any other relevant competent authority must be able to exercise those rights of access;

(10) the service provider must protect any confidential information relating to the firm and its clients;

(11) the firm and the service provider must establish, implement and maintain a contingency plan for disaster recovery and periodic testing of backup facilities where that is necessary having regard to the function, service or activity that has been outsourced.'

Rule 2.7: *'A firm must ensure that the respective rights and obligations of the firm and of the service provider are clearly allocated and set out in a written agreement.'*

Rule 2.8: *'If a firm and the service provider are members of the same group, the firm may, for the purpose of complying with 2.5 to 2.9, take into account the extent to which the firm controls the service provider or has the ability to influence its actions.'*

2.7. From 3 January 2018, PRA Outsourcing Rules 2.1 and 2.1A state:

Rule 2.1: *'A firm must:*

(1) when relying on a third party for the performance of operational functions which are critical for the performance of relevant services and activities on a continuous and satisfactory basis, ensure that it takes reasonable steps to avoid undue additional operational risk; and

(2) not undertake the outsourcing of important operational functions in such a way as to impair materially:

(a) the quality of its internal control; and

(b) *the ability of the PRA to monitor the firm's compliance with all obligations under the regulatory system and, if different, of a competent authority to monitor the firm's compliance with all obligations under MiFID II.'*

Rule 2.1A: *'A MiFID investment firm must extend the arrangements and meet the requirements of the Articles 30, 31 Outsourcing Requirements, so they apply with respect to other matters on the following basis:*

(1) references to 'authorisation' under MiFID II are references to authorisation under section 31(2) of the Act;

(2) references to 'obligations under MiFID II are references to a firm's obligations under the regulatory system;

(3) references to 'investment services and activities' are references to relevant services and activities;

(4) references to 'client' includes anyone who is a client; and

(5) references to 'competent authority' are references to the PRA or the FCA acting other than in the capacity of a competent authority for the purposes of MiFID II or CRR.'

2.8. The Outsourcing Requirements in Articles 30 and 31 of the MODR (which came into effect on 25 April 2016) state:

*'**Article 30***
Scope of critical and important operational functions

1. For the purposes of the first subparagraph of Article 16(5) of Directive 2014/65/EU, an operational function shall be regarded as critical or important where a defect or failure in its performance would materially impair the continuing compliance of an investment firm with the conditions and obligations of its authorisation or its other obligations under Directive 2014/65/EU, or its financial performance, or the soundness or the continuity of its investment services and activities.

2. Without prejudice to the status of any other function, the following functions shall not be considered as critical or important for the purposes of paragraph 1:

(a) the provision to the firm of advisory services, and other services which do not form part of the investment business of the firm, including the provision of legal advice to the firm, the training of personnel of the firm, billing services and the security of the

firm's premises and personnel;

(b) the purchase of standardised services, including market information services and the provision of price feeds.

Article 31
Outsourcing critical or important operational functions

1. Investment firms outsourcing critical or important operational functions shall remain fully responsible for discharging all of their obligations under Directive 2014/65/EU and shall comply with the following conditions:

(a) the outsourcing does not result in the delegation by senior management of its responsibility;

(b) the relationship and obligations of the investment firm towards its clients under the terms of Directive 2014/65/EU is not altered;

(c) the conditions with which the investment firm must comply in order to be authorised in accordance with Article 5 of Directive 2014/65/EU, and to remain so, are not undermined;

(d) none of the other conditions subject to which the firm's authorisation was granted is removed or modified.

2. Investment firms shall exercise due skill, care and diligence when entering into, managing or terminating any arrangement for the outsourcing to a service provider of critical or important operational functions and shall take the necessary steps to ensure that the following conditions are satisfied:

(a) the service provider has the ability, capacity, sufficient resources, appropriate organisational structure supporting the performance of the outsourced functions, and any authorisation required by law to perform the outsourced functions, reliably and professionally;

(b) the service provider carries out the outsourced services effectively and in compliance with applicable law and regulatory requirements, and to this end the firm has established methods and procedures for assessing the standard of performance of the service provider and for reviewing on an ongoing basis the services provided by the service provider;

(c) the service provider properly supervises the carrying out of the outsourced

functions, and adequately manage the risks associated with the outsourcing;

(d) appropriate action is taken where it appears that the service provider may not be carrying out the functions effectively or in compliance with applicable laws and regulatory requirements;

(e) the investment firm effectively supervises the outsourced functions or services and manage the risks associated with the outsourcing and to this end the firm retains the necessary expertise and resources to supervise the outsourced functions effectively and manage those risks;

(f) the service provider has disclosed to the investment firm any development that may have a material impact on its ability to carry out the outsourced functions effectively and in compliance with applicable laws and regulatory requirements;

(g) the investment firm is able to terminate the arrangement for outsourcing where necessary, with immediate effect when this is in the interests of its clients, without detriment to the continuity and quality of its provision of services to clients;

(h) the service provider cooperates with the competent authorities of the investment firm in connection with the outsourced functions;

(i) the investment firm, its auditors and the relevant competent authorities have effective access to data related to the outsourced functions, as well as to the relevant business premises of the service provider, where necessary for the purpose of effective oversight in accordance with this article, and the competent authorities are able to exercise those rights of access;

(j) the service provider protects any confidential information relating to the investment firm and its clients;

(k) the investment firm and the service provider have established, implemented and maintained a contingency plan for disaster recovery and periodic testing of backup facilities, where that is necessary having regard to the function, service or activity that has been outsourced;

(l) the investment firm has ensured that the continuity and quality of the outsourced functions or services are maintained also in the event of termination of the outsourcing either by transferring the outsourced functions or services to another third party or by performing them itself.

3. The respective rights and obligations of the investment firms and of the service provider

shall be clearly allocated and set out in a written agreement. In particular, the investment firm shall keep its instruction and termination rights, its rights of information, and its right to inspections and access to books and premises. The agreement shall ensure that outsourcing by the service provider only takes place with the consent, in writing, of the investment firm.

4. *Where the investment firm and the service provider are members of the same group, the investment firm may, for the purposes of complying with this Article and Article 32, take into account the extent to which the firm controls the service provider or has the ability to influence its actions.*

5. *Investment firms shall make available on request to the competent authority all information necessary to enable the authority to supervise the compliance of the performance of the outsourced functions with the requirements of Directive 2014/65/EU and its implementing measures.'*

2.9. PRA Risk Control Rule 3.4 which came into effect on 2 April 2015 states: *'A firm must ensure the following:*

(1) the risk management function is independent from the operational functions and has sufficient authority, stature, resources and access to the management body;

(2) the risk management function ensures that all material risks are identified, measured and properly reported, is actively involved in elaborating the firm's risk strategy and in all material risk management decisions and is able to deliver a complete view of the whole range of risks of the firm; and

(3) the risk management function is able to report directly to the management body in its supervisory function, independent from senior management and that it can raise concerns and warn the management body, where appropriate, where specific risk developments affect or may affect the firm, without prejudice to the responsibilities of the management body in its supervisory and/or managerial functions pursuant to the CRD and the CRR.'

2.10. PRA General Organisational Requirements 2.5 and 2.6 which came into effect on 2 April 2015 state:

Rule 2.5: *'A firm must take reasonable steps to ensure continuity and regularity in the performance of its regulated activities. To this end the firm must employ appropriate and proportionate systems, resources and procedures.'*

Rule 2.6: *'A firm must establish, implement and maintain an adequate business continuity*

policy aimed at ensuring, in the case of an interruption to its systems and procedures, that any losses are limited, the preservation of essential data and functions, and the maintenance of its regulated activities, or, where that is not possible, the timely recovery of such data and functions and the timely resumption of those activities.'

2.11. From 3 January 2018, PRA General Organisational Requirements 2.6 states: '*A firm must establish, implement and maintain contingency and business continuity plans to ensure the firm's ability to operate on an ongoing basis and limit losses on the event of severe business disruption.'*

3. Relevant Statutory Policy

Approach to the supervision of banks

3.1. *The Prudential Regulatory Authority's Approach to Banking Supervision, June 2014* (as updated in October 2018) sets out how the PRA carries out its role in respect of deposit-takers and designated investment firms. One of the purposes of the document is to communicate to regulated firms what the PRA expects of them, and what they can expect from the PRA in the course of supervision.

Approach to enforcement

3.2. *The Prudential Regulation Authority's approach to enforcement: statutory statements of policy and procedure*, *April* 2013 (as updated in September 2021) sets out the PRA's approach to exercising its main enforcement powers under the Act.

3.3. In particular, The PRA's approach to the imposition of penalties is outlined at Annex 2 *Statement of the PRA's policy on the imposition and amount of financial penalties under the Act*; and the PRA's approach to settlement is outlined at Annex 4 - *Statement of* the *PRA's settlement decision-making procedure and policy for the determination of the amount of penalties and the period of suspensions or restrictions in settled cases*.