FINANCIAL CONDUCT AUTHORITY

12 Endeavour Square
London
E20 1JN

Tel: +44 (0)20 7066 1000
Fax: +44 (0)20 7066 1099
www.fca.org.uk

FINAL NOTICE

To: TSB Bank plc

Reference Number: 191240

Address: 20 Gresham Street, London EC2V 7JE

Date: 20 December 2022

1. ACTION

1.1 For the reasons given in this Final Notice, the Authority hereby imposes on TSB Bank plc ("TSB") a financial penalty of £29.75 million pursuant to section 206 of the Act.

1.2 TSB agreed to resolve this matter and qualified for a 30% (stage 1) discount under the Authority's executive settlement procedures. Were it not for this discount, the Authority would have imposed a financial penalty of £42.50 million on TSB.

2. SUMMARY OF REASONS

The Migration Programme

2.1 TSB was created by a divestment from Lloyds Banking Group ("LBG") in June 2014. Following the divestment, TSB continued to receive its core IT services from LBG, using 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 via a carve-out (creating a copy of the platform to be operated by a third party) or migrating to an entirely new platform.

2.2 In July 2015, TSB was acquired by Sabadell, a bank registered at the Registry of the Bank of Spain, which had a history of migrating banks on to its IT banking platform, Proteo. The strategic rationale for the takeover included the expected financial returns from a full migration of TSB's IT services on to Sabadell's Proteo technology platform. The aim was to achieve migration by the end of 2017.

2.3 The scale of the migration project was unprecedented - it was also ambitious for migration to a new build platform in the UK to occur in under three years. Sabadell had limited experience in the UK banking market. While it did have significant experience in delivering a larger and more complex platform in Spain (Proteo (Spain)), the migration would require the creation of a newly built version of the Proteo platform which was not yet proven (albeit created largely from the existing proven Proteo (Spain) platform), tailored for the UK banking market, requiring significant customisation and a large number of external suppliers. This new version of Proteo was known as Proteo4UK.

2.4 Between 2015 and 2018, TSB undertook 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 (the "Migration Programme"). TSB engaged Sabadell's subsidiary, SABIS Spain, to design, build and test the Proteo4UK Platform and migrate TSB's data to it. SABIS would also operate the platform following migration.

The Migration Incident

2.5 Over the weekend of 20 - 22 April 2018, TSB undertook the Main Migration Event ("MME"), during which it migrated the majority of the operations 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, TSB encountered serious issues which significantly impacted the ability of some customers to access and use their account in the first few days after MME. These included certain data breaches, failures with digital (internet and mobile) banking services, failures in telephone banking, branch technology failures, and consequential issues with payment and debit card transactions.

2.6 Failures in digital services caused a cascade effect, resulting in customers attempting telephone banking instead, but many customers faced increased wait times, and abandoned calls as a result, due to other IT issues in telephony and the overloading of the system under the weight of unprecedented levels of customer calls. With some digital customers facing issues accessing digital banking, and some customers unable to access telephone banking, long queues of customers built up in busy branches, in which services were running slowly due to numerous IT failures affecting the branches. These, although less serious, contributed to the issues experienced by those customers using branches due to the increased demand.

2.7 Certain customer services were disrupted on an extensive basis during the first week after the migration, with problems continuing in the following days and weeks. Overall, TSB did not return to a BAU position until 10 December 2018.

2.8 The scale of the Migration Incident was such that it attracted extensive media coverage, regulatory involvement and parliamentary interest. Some customers suffered significant detriment. Between 22 April 2018 and 7 April 2019, TSB received 225,492 complaints from customers (c.4.3% of its customer base as at MME) as a result of the Migration Incident, and paid a total of £32,705,762 in redress during that period.

Migration Programme Failings

2.9 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 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 adequately prepared for the events that took place post-MME, which had serious negative consequences for some of TSB's customers.

Migration Programme Planning

2.10 The aim was to achieve migration by the end of 2017, an ambition which was known publicly, however TSB remained of the view throughout that it would not migrate until it was ready. TSB adopted this ambitious timeframe in its March 2016 Integrated Master Plan ("IMP") despite running several months behind in the programme by that date.

2.11 The IMP, which set out the sequential design, build and testing phases, was planned on an insufficiently 'left-to-right' basis. The Migration Programme experienced delays from the outset and fell behind the IMP timings. While progress had been made, on 20 September 2017 the firm decided that the Migration Programme would have to be re-planned. However, nine days after it had resolved to re-plan, and before it had concluded its re-planning exercise, TSB publicly announced it would now migrate in Q1 2018.

2.12 The re-plan, known as the 'Defender Plan', was also planned on an insufficiently 'left-to-right' basis, with inadequate interrogation of the reasons why the programme had not been able to keep to the timelines in the IMP. Once again, the Migration Programme quickly fell behind schedule, certain plans and guiding principles (the "Guiding Principles") put in place for the running of the Migration Programme were departed from, and the date for MME was ultimately met following the deferral of certain pieces of banking functionality to after MME, or putting in place manual workarounds. Certain matters were not sufficiently discussed with or challenged by the TSB Board, including the overly ambitious timetable for migration, the reasons why the programme fell behind, or whether the Defender Plan was realistically achievable at the outset.

Testing

2.13 Testing phases during the Migration Programme did not always keep up with either the IMP or the Defender Plan timelines. The various types of testing were intended to run largely sequentially but, with testing phases running late, in order to meet the timelines types of testing ended up running in parallel, or being changed in scope. Testing only concluded the day before the decision to migrate was taken.

2.14 Non-functional testing (testing of TSB's non-functional requirements as to how the platform was supposed to operate at load/volume, for example how many customers could log in to the mobile banking app at any one time) was an important mitigant for certain risks in the programme. A decision was taken outside of the appropriate governance forum around the end of February 2018 which reduced the scope of a particular type of non-functional testing on the digital channels (known as testing in "Active-Active configuration") on TSB's data centres. Had this testing been conducted, it is likely that a problem in the configuration of certain components in the data centres, which caused unavailability to customers of internet and mobile banking for periods following MME, would have been found. TSB only considered the risks to disruption of services which were already live which would be caused by testing in Active-Active. TSB considered the matter to be a purely technical decision. The risks of not conducting testing in Active-Active were not identified or reported, and therefore potential mitigants were not considered.

2.15 Additionally, the decision to go ahead with the migration was taken following consideration of certain governance documentation and procedures which were put in place to analyse and assess the evidence that the relevant tests had been met. It was originally the responsibility of the Bank Executive Committee ("BEC") member business functions ("BEC business functions") to attest to their non-functional requirements having been met by the testing. In February 2018, TSB decided that the BEC member functions would sign-off on the non-functional requirements in their attestations while the IT business function would attest as to which non-functional requirements had been tested through non-functional testing. This was a change in responsibility that does not appear to have been explicitly drawn to the attention of the TSB Board or TSB Board sub-committees when taking decisions to go ahead with migration. Consequently they were unable to consider whether the fact that the IT business function was attesting to the completion of the centrally run non-functional testing (while the BEC member functions remained responsible for signing off their non-functional requirements) had introduced any additional risks into the programme.

Risk management

2.16 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. 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.

2.17 Additionally, some migration-related reviews 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 or challenged by the TSB Board at certain crucial junctures.

Outsourcing

2.18 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. Those services were therefore critical to the performance of TSB's regulated activities, and TSB was required by the regulatory regime to take reasonable care to avoid undue additional operational risk.

2.19 However, TSB did not at the outset when deciding to proceed with the migration programme utilising the Proteo4UK Platform conduct a formal comprehensive due diligence exercise to understand SABIS's capability to deliver and operate the Proteo4UK Platform, despite identifying that "*Ensuring the combined resources of TSB, Sabadell and LBG are capable of delivering the migration is key"*. Sabadell's resources included its subsidiaries. This issue was brought to the attention of the TSB Board, but it did not consider how that capability would be assessed. TSB did later carry out a number of due diligence exercises, but it remained the case that TSB did not sufficiently understand SABIS's capability to operate the platform.

2.20 In addition, TSB did not formally identify certain risks in relation to SABIS's capability, such as the possibility that SABIS may not be capable of delivering the platform within a two year time period, and so were not assessed by TSB. The operational risk of the outsourcing arrangement was unduly increased because TSB did not know in the form of a formal assessment whether SABIS would be able to deliver the outsourced services adequately.

2.21 Proteo4UK was being newly built by SABIS and was new to the UK banking market (albeit it was created largely from the existing Proteo (Spain) platform). It was therefore critical for TSB to understand how the 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 However, instead of requiring the production of design documentation, TSB alternatively agreed that SABIS would instead provide configuration documents (which in themselves could not be used to verify that the infrastructure had been built to the original design). In February 2018 TSB then decided not to require the full population of configuration documents. This was because TSB considered that there would be sufficient documents and service descriptions recently provided to go ahead with MME. 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, TSB worked throughout the programme without sufficient documentation. This placed extra importance on testing as a mitigant, whilst it also risked hampering the effectiveness of TSB's incident management response.

2.22 SABIS relied extensively on 85 third parties (TSB's fourth parties) to deliver the systems required for the migration and the operation of the platform, which required it to act as a service aggregator. By February 2018, TSB had still not ensured that SABIS's supplier management model (including its service risk assessment methodology and framework) was fully developed and complied with TSB Group Outsourcing policy. Supplier risk issues were not fully resolved prior to MME, however TSB deemed SABIS to be ready in respect of supplier procurement, subject to further steps being taken after MME. 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.

2.23 TSB also did not re-assess SABIS's capability to deliver the migration following issues encountered with the limited services that had already gone live on the platform ahead of MME. In addition, TSB undertook an audit on services that had already gone live but did not clearly identify the limitation that the live services were not as technically complex and had a more limited supply chain complexity compared to the services that would go live at MME.

2.24 Finally, SABIS provided a letter which it considered confirmed non-functional readiness to TSB, in respect of (i) the testing undertaken to prove the resilience and performance of the platform, and (ii) confirmations of readiness from three of SABIS's four 'critical' third party suppliers. A confirmation from the fourth third

party supplier was obtained prior to MME. These were referenced in (but not appended to) the letter from SABIS.

2.25 The letter from SABIS and the fourth party confirmations were to some extent forward looking statements of good intention or expectation rather than statements of fact about the completeness of readiness activities undertaken. All but one was caveated with a number of outstanding tasks or tests which had not yet been completed. 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 before MME to confirm that they were ready, nor did TSB request an updated confirmation of readiness from SABIS to support an attestation given to the TSB Board on this point.

Business Continuity Planning

2.26 Following MME, TSB quickly found itself in a crisis situation for which it was not prepared. Whilst TSB undertook a large programme of work in relation to business continuity planning ahead of MME, and had been prepared to deal with "*bumps in the road*", there were gaps in its oversight of the preparations of SABIS. In TSB's view, it would not have decided to proceed with the migration had it considered that an incident of the scale of the issues that arose post-migration might occur. Consequently, TSB's business continuity preparations were inadequate for the scale of the incident which ultimately took place.

2.27 TSB should have taken greater preparations in case of such an eventuality, when the context was that it was undergoing a large-scale change programme, leading to a go-live launch following which, if a major incident occurred, TSB would be unable to roll back on to the LBG Platform and would be reliant on SABIS as its outsourced IT service provider to fix multiple technical incidents which could have a major impact on customers.

2.28 TSB did not prepare nor oversee the preparation of sufficient plans to deal with a multiple incident scenario of the severity of the one that emerged post MME, and testing of incident management ahead of MME was limited due to there being few live services and incidents. TSB's internal assurance reviews identified deficiencies in incident management processes between April and November 2017, but the issue was considered low impact and audit actions were closed ahead of MME, apparently without considering what impact this might have in the scenario of multiple IT incidents occurring post-MME of the severity of those which arose. TSB also did not directly assess SABIS's readiness for incident response.

2.29 There were also other specific deficiencies in TSB's preparations. TSB utilised a Bronze, Silver, and Gold incident response structure, with a Gold incident being the most significant, and planned to operate MME as a Gold incident to mitigate the risk of unforeseen issues and provide additional assurance that TSB was adequately prepared for incidents. However, its practice Gold events were limited as they assumed resolution of incidents within a few days, whereas many post-MME events took weeks to resolve. They were also designed to be exercises for BEC members solely, without giving proper consideration as to whether this would be sufficient preparation for a multi organ IT crisis.

2.30 In addition, TSB's other preparations, such as its Incident Management Playbooks, were only designed to support the first 48 hours after an incident. Insufficient consideration was given to a customer communications strategy, how to significantly upscale resourcing at short notice to deal with a massive increase in complaints, and how to suitably deal with vulnerable customers in the case of a major and long-term incident.

2.31 TSB's failures in planning impacted customers post-MME. TSB's "pre written playbook responses and high level generic responses prior to MME did not address…customer queries and issues" and "were not reflective of the genuine customer experience". Customers were frustrated by the inability to contact TSB by telephone due to the unprecedented volume of calls which then exceeded the planned capacity and staffing of telephone banking. TSB was overwhelmed by the volume of complaints it received, having limited contingency plans to bring in external complaint resource, and took almost 12 months to deal with the complaints regarding the migration. Finally, with known pre-existing limitations on the categories of vulnerable customers captured in the systems in use prior to MME, insufficient preparations to identify vulnerable customers in the case of such an incident resulted in extra stress for some of those customers.

Remediation programme

2.32 In May 2018, TSB put in place its Putting Things Right Programme to deal with the problems, having previously published messages on 24 April 2018 assuring customers that "*no one will be left out of pocket as a result of these service issues"*. TSB put in place additional resource (including engaging third parties) to deal with the 225,492 complaints that it received. TSB paid a total of £32,705,762 in redress, including distress and inconvenience payments, customer expenses, and putting the customer back in the right position.

Principle breaches

2.33 In light of the above, the Authority considers that TSB failed to conduct its business with due skill, care and diligence, in breach of Principle 2. TSB also failed to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems, in breach of Principle 3.

2.34 TSB breached Principle 2 because it failed to exercise due skill, care and diligence in managing the outsourcing arrangements with, and services provided by, SABIS, appropriately and effectively. In particular:

a) TSB did not at the outset conduct a formal and comprehensive assessment of whether SABIS had the ability and capacity to perform the services under the MSA or OSA reliably and professionally, specifically: whether SABIS could deliver the Proteo4UK Platform in the timeframe adopted, or whether SABIS was sufficiently ready to safely operate the platform;

b) During the Migration Programme testing departed from plans and Guiding Principles. TSB also did not adequately (i) formally reassess SABIS's ability and capacity on an ongoing basis, (ii) have a sufficient grasp of whether SABIS's infrastructure designs reflected TSB's requirements, and the consequences of that, (iii) obtain sufficient assurance about SABIS's management of fourth parties, and (iv) obtain sufficient assurance about SABIS's readiness or that of critical fourth parties in the form of statements of proven fact about the completeness of readiness activities already undertaken; and

c) TSB also did not adequately assess the performance and service issues encountered with services that had already gone live, or sufficiently interrogate its readiness for MME.

2.35 Additionally, TSB failed to properly identify and evaluate the risks of not conducting testing of the digital channels in Active-Active configuration, only identifying the risks to disruption of services which were already online which would be caused by testing in Active-Active. TSB as such did not consider any potential mitigants for the risks of not testing in Active-Active. Further, TSB failed to take the decision within the relevant governance structure for such decisions and risk reporting escalation.

2.36 TSB breached Principle 3 because it failed to take reasonable care to organise and control the Migration Programme responsibly and effectively, or implement adequate risk management systems. In particular:

a) TSB did not take reasonable care in the planning and re-planning of the Migration Programme, and it failed to adequately mitigate operational risk. TSB adopted an overly right-to-left approach, setting an excessively ambitious timetable, publicly committing to a re-planned MME date before the completion or approval of re-planning, and not adequately investigating the cause of delays or their impact on the realistic time required to complete remaining tasks before migration;

b) TSB's governance of the Migration Programme was insufficiently robust. It does not appear certain matters were sufficiently discussed with or challenged by the TSB Board, such as the timetable for the migration, deviations from certain aspects of approved migration plans and Guiding Principles and the implications for the risk profile of the programme, and the readiness of the Proteo4UK Platform and SABIS;

c) TSB's risk management function did not adequately identify and report on certain risks during the Migration Programme. In particular, TSB did not explicitly identify the risks of SABIS's non-performance, or inadequate performance of its obligations to deliver a stable platform (although aspects of the impact of the non-performance were considered as part of the other programme risks). In addition, some assurances were limited or qualified in ways which do not appear to have been drawn to the TSB Board's attention or challenged by them; and

d) In the context of a large-scale change programme leading to a go-live launch following which, if a major incident occurred, TSB would be unable to roll back on to the LBG Platform and would be reliant on SABIS as an outsourced IT service provider to fix multiple incidents, TSB's incident management arrangements and business plans were insufficiently robust and ineffective.

2.37 The Authority has taken into account the comprehensive customer remediation programme conducted by TSB which, although it encountered delays both due to the unprecedented number of complaints received and some of the issues in business continuity planning described in this Notice, the steps taken were extensive. While TSB had some commercial interest in taking some of these steps

in the circumstances that transpired post-MME, the Authority considers that some of the measures (such as providing compensation up to £150 without requiring proof of loss, and providing redress for intangible harm) could be considered to be generous. The Authority has also taken into account TSB's voluntary provision to the Authority of technical reviews commissioned in the immediate aftermath of the migration, as well as its commission of a comprehensive independent review into many of the matters referred to in this Notice, which it committed to make public. Although ultimately TSB did not accept the findings of the independent review in a number of key respects, TSB agreed to provide the Authority with notes of interviews conducted as part of the review with relevant individuals. The Authority overall made some, but limited, use of the reviews.

2.38 For the reasons given in this Final Notice, the Authority hereby imposes on TSB Bank plc ("TSB") a financial penalty of £29.75 million pursuant to section 206 of the Act.

2.39 TSB agreed to resolve this matter and qualified for a 30% (stage 1) discount under the Authority's executive settlement procedures. Were it not for this discount, the Authority would have imposed a financial penalty of £42.50 million on TSB.

3. DEFINITIONS

3.1 The definitions below are used in this Notice:

"the Act" means the Financial Services and Markets Act 2000

"ATM" means Automated Teller Machine

"Incident Management Playbooks" mean reference documents containing practical actions to aid the restoration of operational capabilities during an incident

"the LBG IT Platform" means the IT platform used by LBG, which was also used by TSB until its migration on to the Proteo4UK Platform

"the PRA" means the Prudential Regulation Authority

"Principle" means the Authority's Principles for Businesses

"the Proteo4UK Platform" means a new version of the Proteo platform adapted for TSB and the UK market

"the Relevant Period" means 16 December 2015 to 10 December 2018

"Sabadell" means Banco de Sabadell S.A.

"SABIS" means SABIS Spain and SABIS UK

"SABIS Spain" means Sabadell Information Systems S.A.

"SABIS UK" means Sabadell Information Systems Limited

"the Tribunal" means the Upper Tribunal (Tax and Chancery Chamber)

"the TSB Board" means the Boards of TSB and TSBBG

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

4. FACTS AND MATTERS

4.1 The facts and matters set out below are organised by Sections, as follows:

a) Sections A – B describe TSB, the Migration Incident and the impact on customers;

b) Sections C – J describe the Migration Programme in chronological terms, with some individual Sections explaining particular features of the Programme; and

c) Sections K – N deal in a thematic manner with particular issues encountered during the Migration Programme.

SECTION A: BACKGROUND

TSB

4.2 TSB is a retail bank which was created by a divestment from 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.

4.3 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.

4.4 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').

SECTION B: THE MIGRATION INCIDENT

Sunday 22 April – Monday 23 April 2018

Digital channels

4.5 MME was authorised to go ahead at around 1pm on 22 April 2018. Telephony and internet banking were both live by 6pm. TSB encountered difficulties with getting the mobile app to go live, but it ultimately went live at 6.45pm. Problems became immediately apparent. TSB was aware of customers experiencing an intermittent service with digital banking, and initially sought to maintain the service by limiting the number of customers who could access it. As well as degraded performance, digital channels were also experiencing unsuccessful logins and issues with functionality such as unsuccessful payments.

4.6 TSB also became aware of further problems from approximately 40 customers who reported that when they logged in to their internet banking accounts, they were seeing details of other parties' finances, typically their relatives. In response to this issue, digital banking was taken down entirely at 7pm, in order to assess the root cause.

4.7 Following investigation, it was identified that some closely linked retail customers, (such as a customer who holds a power of attorney, or is a nominee, for another customer), could see data from both customers online when they would normally

only have access in branches. It was subsequently confirmed that 440 customers experienced this issue.

4.8 Following the implementation of fixes to resolve this issue, at 2am on Monday 23 April 2018, internet banking and the mobile app were brought back online. However, access to the digital channels remained limited. Part of the new IT platform was consuming extremely large amounts of memory affecting internet banking and mobile app services. TSB therefore restricted new logins to internet banking in order to protect the mobile app service.

4.9 More generally, login problems remained. Of the approximately 900,000 attempted logins that day, only approximately 10% of internet banking logins were successful, while mobile app logins moved from about 65% to 80% throughout the course of the day. For some of those customers able to log in, problems with degraded performance and functionality, such as unsuccessful payments, continued. Over the course of Monday 23 April 2018, 48% of attempted payments on the mobile app and 59% of attempted payments using internet banking were unsuccessful.

Telephony

4.10 On Monday 23 April 2018, the telephony channel received an extremely high volume of calls due to the issues with the digital channel and associated media coverage. 69,000 calls had already been received by 2pm that day. Despite an increase in telephony resource that had been planned in order to cope with an increase of up to 50% in call traffic, TSB lacked sufficient capacity to deal with the unprecedented volume of calls and its service was further hampered by a number of technical issues.

4.11 The technical issues affected matters such as customers' ability to interact with the computer-operated telephone system (Interactive Voice Recognition or "IVR"), and the ability of agents to transfer calls between them. Digital problems also impacted a telephony tool used to serve customers (Web on Behalf Of), and a connectivity issue between third parties caused some customer calls not to progress. In addition, configuration problems on the IVR lines meant that only c.25% of the telephone line capacity that TSB was due to have was available.

4.12 As a result there were significant problems for customers in connecting with contact centres, lengthy call wait times, and high rates of customers abandoning calls. During the day, a substantial proportion of calls did not even reach the IVR.

For those that did, customer call wait times were approximately 90 minutes with a 70% abandon rate. The average call time was also longer than normal, roughly quadrupling telephony demand.

Branches

4.13 The problems with the digital channels and in telephony resulted in more customers visiting branches. However, technical issues in branches (including the Proteo4UK branch application crashing) became apparent early on Monday 23 April 2018, primarily impacting key counter transactions. The key issues were caused by the unavailability of:

a) Chip and pin, used to identify and verify customers with debit cards to withdraw cash over the counter;

b) Voucher readers, used to read paper payment documents, typically cheques;

c) Ability to print, impacting the printing of withdrawal slips and passbook balances;

d) Teller Cash Recycler, used to authenticate incoming bank notes and securely store, issue and manage cash in an internal vault; and

e) Immediate Deposit Machines, where customers can deposit cash and cheques themselves (albeit this issue was not caused by a technical issue at migration).

4.14 Workarounds were slow, and these issues together with the problems with the digital channels and in telephony resulted in long queues in busy branches.

Continuing problems in the days and weeks following MME

4.15 Customer service disruption continued during the first week after migration, with certain problems continuing in the following days and weeks. On Wednesday 25 April 2018 a decision was made to bring in third parties to help identify and resolve performance issues.

Digital channels

4.16 Digital channels were taken down again at 10am on Tuesday 24 April 2018 for fixes, with the expectation that they would be made available again an hour later.

However, TSB was not able to reopen them until 3am on Wednesday 25 April 2018, and problems with access and functionality remained.

4.17 The digital channels remained "*unstable and almost unusable*" until Thursday 26 April 2018. Further fixes deployed overnight resulted in access and performance rates significantly improving during that day.

4.18 However, some very high impact functional issues remained at the end of the first week after MME. Some digital channel service issues continued in the second week after MME (Monday 30 April to Sunday 6 May 2018) stabilising by the end of that week, although certain issues arose again with access to the mobile app towards the end of May 2018, and specific defects continued into June 2018.

Telephony

4.19 On Tuesday 24 April 2018 the average customer telephone wait time was 1 hour 20 minutes (queue length 820 customers), compared to a BAU target wait time of 1 minute (queue length 80 customers). By the end of the week on Sunday 29 April 2018 average customer telephone wait time was 46 minutes.

4.20 Technical problems with telephony continued during the second week after MME, consisting both of a mix of issues that had become apparent during the first week, and new issues such as:

a) A third party multi-client issue occurred on Wednesday 2 May 2018 which caused 70% of customers to drop out of calls before reaching the IVR;

b) Three high impacting periods of degradation with Citrix (remote desktop infrastructure), also occurred on Wednesday 2 May 2018, during which 115 telephony partners had to log off and reboot;

c) Telephony agents were unable to service calls for a short period on Thursday 3 May 2018 due to further issues with Citrix which meant agents were unable to access the Proteo4UK Platform; and

d) A latency infrastructure issue occurred for an hour on Saturday 4 May 2018 which caused further issues with IVR.

4.21 Significant call wait times and high rates of customers abandoning calls continued into early June 2018, resolving by the middle of that month.

Branches

4.22 Similar issues as initially identified continued with branches through the first and into the second week following MME. Certain issues continued into June 2018.

Return to business as usual

4.23 Overall, TSB did not return to a BAU position until 10 December 2018.

Impact on customers

4.24 In the first few days following MME certain of TSB's customers experienced significant inconvenience and difficulties in accessing accounts, and contacting and transacting with TSB across digital, telephony and branch channels. In addition to the general problems described above, additional specific issues were encountered during, or at points during, the first two weeks following MME. These included:

a) Approximately 600 customers experienced issues relating to their data. As well as the nominee account issue, there was an issue with 138 business banking delegates having access to all the accounts of the business in internet banking rather than just the accounts they had access rights to. There was also an issue relating to 26 customers seeing other customers' statements or communications through the "inbox" on the internet banking screen;

b) A significant proportion of business banking customers could not make payments to new beneficiaries online as they had not yet set up the new Authenticator App;

c) During the first week 20 – 30% of retail and business customers could not make any payments online, due to password errors and an inability to reset their credentials. There was some improvement during the second week but the issues continued;

d) Approximately 60,000 customers experienced delays in credits or debits being applied to their accounts, for example due to waiting for manual branch transactions to be processed (such as cheques or withdrawals), or temporarily missing debit entries from successful Faster Payment Service outbound payments. Problems with visibility of standing order payments,

with internal accounts transfers, and with CASS, BACS, CHAPS, Faster Payments and Cheque Clearing occurred;

e) Some customers received incorrect or confusing information due to error messages or missing information in their accounts. For example, duplicated payments made because of error messages received following successful payments made in the digital channel; some customers were unable to see their mortgage account in digital banking or their savings accounts in the mobile app; some customers were provided with incorrect historical rolling balances for current accounts in digital banking, missing transactions in digital banking, and missing and incorrect information on credit cards in internet banking; some customers saw incorrect information on internet banking for their credit cards including minimum payment and payment dates, and confusing display of transactions; some customers did not receive text alerts or received alerts that were incorrect. Further, detailed information from migrated debit card transactions of business customers was not available in any channel; and

f) Customers also did not receive sufficiently timely, consistent and clear communications regarding the issues. However, this improved during the course of the first week with the development of a customer communications strategy and the establishment of a customer communications focus area reporting to Gold BEC reporting to the Executive Gold Team (described in paragraph 4.60).

Customer complaints

4.25 The volume of customer complaints quickly exceeded TSB's forecasting and planning. On Tuesday 24 April 2018 TSB published messages assuring customers that "*no one will be left out of pocket as a result of these service issues*". By Thursday 26 April 2018, only four days after migration, there was a bank-wide variance of 900% of complaints logged as compared to expected complaints logged (10,315, rather than the 1,146 complaints anticipated). The four most complained about topics at this stage related to (i) accessing internet, telephony and mobile banking; (ii) UK Payments Out; (iii) UK Payments In; and (iv) internal transfers, all of which showed a variance of over 2,500%.

4.26 In total, TSB received 225,492 complaints (from c.4.3% of its customer base as at MME) from 22 April 2018 to 7 April 2019, with a total of £32,705,762 redress paid out during that period. The most common amount paid to customers for a

complaint was £150 (49,910 instances), reflecting the low impact in those particular cases. Distress and inconvenience payments to customers totalled £22.7m, customer expenses totalled £5.8m, and putting the customer back in the right position totalled £1.2m. 308 customers fell within the "exceptional" remediation category and received payments of between £1,100 to £2,000, whilst 22 customers fell within the "extreme" category receiving payments above £2,100.

Migration Programme Failings

4.27 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 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 adequately prepared for the events that took place post-MME, which had serious negative consequences for some of TSB's customers.

SECTION C: MIGRATION PROGRAMME BACKGROUND

TSB's IT services and initial exit options

4.28 Following its divestment from LBG, TSB continued to receive its core IT services from LBG, using 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 creation 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.

4.29 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 (internet) and mobile).

4.30 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.

4.31 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

4.32 In March 2015, TSB received a takeover bid from Sabadell, a bank registered at the Registry of the Bank of Spain. At the time of the offer, Sabadell had previously migrated seven banks on to 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."*

4.33 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.

4.34 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 proven 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.

SECTION D: INITIAL PROJECT PLANNING JULY TO DECEMBER 2015 AND THE DECISION TO PURSUE THE PROTEO MIGRATION OPTION

TSB's IT services and initial exit options

4.35 In 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 Board in either late 2015 or early 2016 for discussion and, if appropriate, approval.

4.36 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 described in Section G), as well as work on the governance and risk management framework (see Section F).

4.37 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.

4.38 In November and December 2015, TSB held three 'deep dives' with the TSB Board to examine the approach and process to create 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.

4.39 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.

4.40 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.

4.41 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.

4.42 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.

SECTION E: KEY FEATURES OF THE MIGRATION PROGRAMME

4.43 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

4.44 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.

4.45 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.

4.46 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.

4.47 4.47. 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

4.48 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.

4.49 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

4.50 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.

4.51 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 IT 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 IT Platform instead of Proteo4UK.

4.52 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

4.53 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, SABIS UK, 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.

4.54 The relevant contracts were:

a) 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

b) 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

4.55 The Migration Programme was a "*complex and ambitious plan*" which contained significant operational risk. Migrating customers off a third party platform via a predominantly single event migration, newly built platform (albeit created largely from the existing Proteo (Spain) platform), with new data centres was unprecedented in the UK. 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 IT 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.

4.56 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.

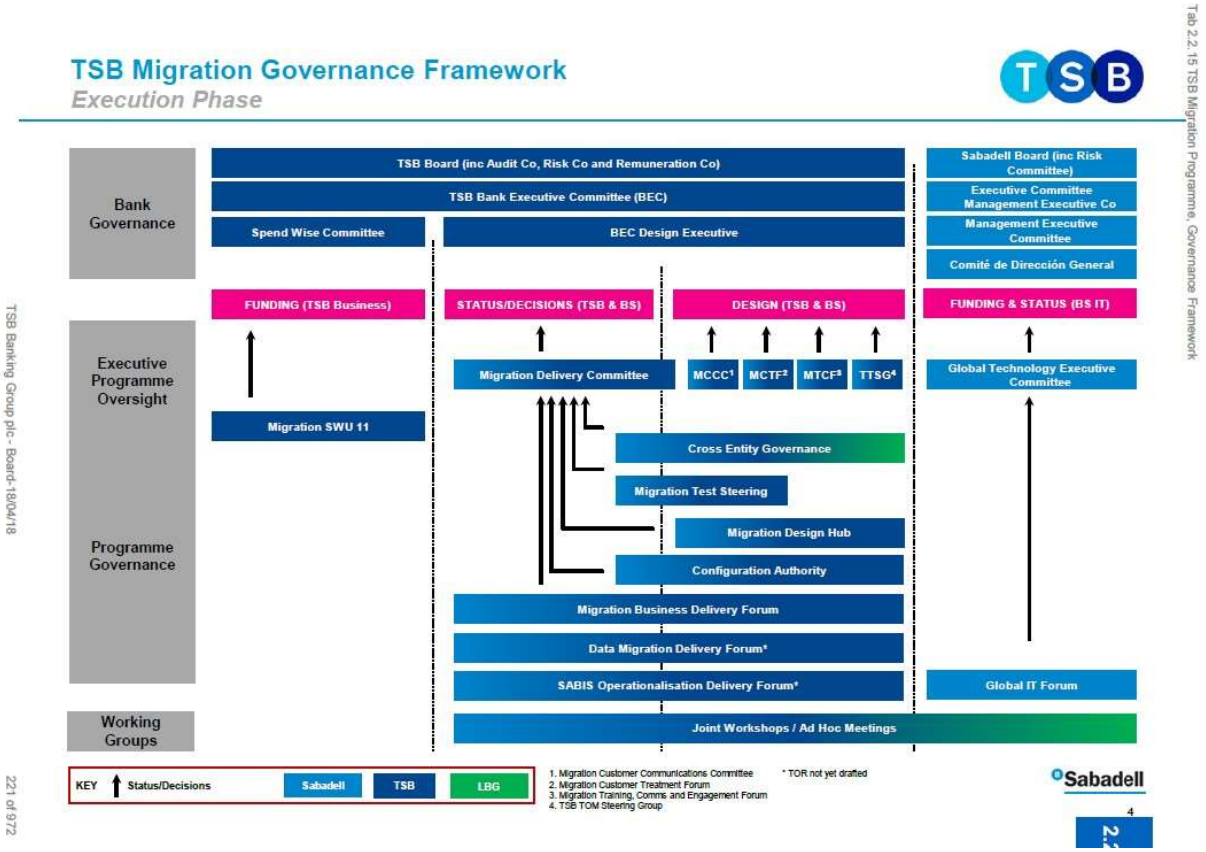
SECTION F: MIGRATION PROGRAMME GOVERNANCE AND RISK MANAGEMENT FRAMEWORKS

4.57 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

4.58 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 TSB Board Committees

TSB Board

4.59 The TSB Board had ultimate oversight of the Migration Programme, as well as of key development 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).

4.60 Ultimately the TSB Board delegated authority in April 2018 to a sub-committee to grant approval to an Executive 'Gold Team' to initiate MME.

4.61 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

4.62 The Board Audit Committee 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 TSB 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.

4.63 The Board Risk Committee oversaw the management of the programme risks as they may have affected TSB's BAU activities. It also reported to the TSB Board.

Executive Committees

The BEC

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

BEC Design Executive

4.65 The BEC Design Executive was established in early 2015 and was the main executive level forum through which TSB ran the Migration Programme. It reported to the BEC. The BEC Design Executive 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 the design principles, and the ownership and governance of the migration plan to align and deliver the strategic objectives.

4.66 Key programme-related decisions were made by the BEC members at the BEC Design Executive. 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 Design Executive.

Other key committees

4.67 A number of other migration programme-specific committees and working groups operated below the BEC and BEC Design Executive. The two below were the most significant.

Migration Delivery Committee ("MDC")

4.68 The MDC was established under the MSA. It reported to the BEC Design Executive. It was the over-arching governance and decision-making forum for the design and effective implementation of the migration. It delivered the migration plan to the BEC Design Executive 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)

4.69 The Migration Testing Forum reported to the MDC. It was accountable for providing the 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

4.70 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

4.71 The first line of defence was the business areas ("Business Areas") (also known as the BEC business functions), which were headed by the 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 TSB Board.

4.72 An external consultancy firm initially operated in TSB's first line, and provided a number of reviews of TSB's programme planning, management and controls, and governance.

Second Line of Defence

4.73 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.

4.74 From August 2017, the external consultancy firm operating in the Business Areas moved to assist 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

4.75 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 TSB 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 fair, balanced and reasonable;

reviewing the design and effectiveness of the key programme controls; and challenging executive management to improve risk management, governance and control.

4.76 A number of external consultancy firms provided co-source resources for a number of migration-related internal audits throughout the migration programme.

SECTION G: PROJECT PLANNING DECEMBER 2015 TO MARCH 2016 AND THE ADOPTION OF THE IMP

4.77 Following the decision at the December 2015 TSB Board meeting that TSB was minded to consider migration to Proteo4UK as the preferred solution, programme planning continued until March 2016. The planning work that took place between July 2015 and March 2016 culminated in the creation of the IMP.

Design Phase

4.78 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

4.79 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 that should be migrated at a different point to MME, and would therefore be exceptions 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.

4.80 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.

4.81 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.

4.82 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.

4.83 Nonetheless, TSB intended to present a consolidated programme plan to the TSB 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*" third party solutions already localised in the UK market.

4.84 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

4.85 On 15 March 2016, the IMP was presented to the TSB Board as the overall plan for the migration programme. As with the "*aspirational*" plan presented to the TSB Board in a deep dive session in November 2015, the IMP planned for MME to take place late in 2017, on 5 November 2017. This two year timeframe would also be agreed to in the MSA in due course.

4.86 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*".

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

a) Design Phase – to be completed in June 2016;

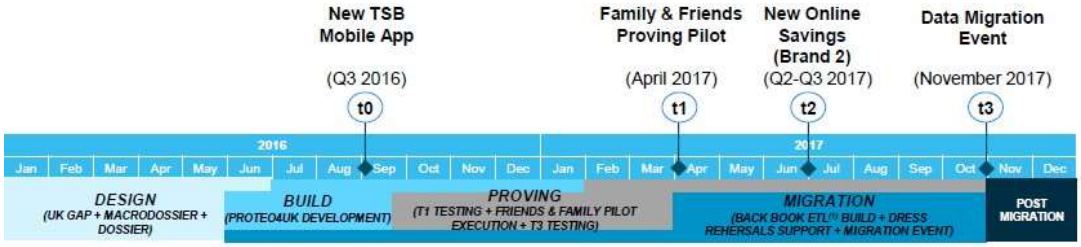
b) Build Phase – from May 2016 to January 2017;

c) Proving Phase – from September 2016 to November 2017;

d) Migration – from May 2016 to November 2017; and

e) Post Migration – after MME.

Figure 2:



4.88 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 Mortgages Governed Transition Event); and

d) t3 – the MME itself.

4.89 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

Phase	Expected completion
Migrated data testing ("MDT")	August 2017
Non-functional testing	
Non-functional testing (various types)[237]	End of July 2017
Testing of data migration	
Migration acceptance cycles ("MACs")	August 2017
Dress rehearsals	End of September 2017

Testing under the IMP

4.90 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).

4.91 Testing following the build phase would consist of functional testing, non-functional testing, and testing of data migration.

Functional Testing

4.92 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.

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

a) UAT involved testing the 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;

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.

Non-functional Testing

4.94 Non-functional testing 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.

4.95 Non-functional testing 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.

4.96 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

4.97 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

4.98 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.

SECTION H: MIGRATION PROGRAMME DELAYS AND THE SEPTEMBER 2017 DECISION TO RE-PLAN

Programme Delays

4.99 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 workstreams already, including infrastructure delays due to engagement issues with third parties, and UAT delays in a number of areas.

4.100 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.

4.101 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*". (See Section K for discussion of the problems associated with parallelisation). The third party consultant advised in an update that the phasing and extending activities were increasing pressure on resources and they advised that careful management was required to reduce inefficiencies due to duplication and re-work.

4.102 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 provided to the TSB 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.

4.103 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 now been delayed by three months from the end of April to the end of August 2017.

The decision to re-plan

4.104 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 the cleanliness of the data in different MACs, and (3) the difficulty in completing UAT.

4.105 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, TSB 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 announcement

4.106 However, 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.

SECTION I: OCTOBER 2017 DEFENDER PLAN AND SUBSEQUENT FURTHER PROGRAMME DELAYS

The Defender Plan

4.107 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.

4.108 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.

4.109 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 4.112 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 "*ready to migrate "as soon as possible"* currently envisaged to be Thursday 15 March 2018, "*and then to "land" the migration weekend in one of the agreed slots*".

4.110 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	End of December 2017
MDT	August 2017	End of December 2017
Regression testing	N/A	End of January 2018
Non-functional testing		
Non-functional testing (various types)	End of July 2017	End of November 2017 (with additional non-functional testing for extra-assurance by March 2018)
Testing of data migration		
MACs	August 2017	End of January 2018

Phase	Expected completion under the IMP	Expected completion under the Defender Plan
Dress rehearsals	End of September 2017	Early March 2018

4.111 These stages reflected the two workstreams 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.

4.112 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 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); and

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).

4.113 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 a number of incidents for services already in live production.

4.114 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 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*".

4.115 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 that 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 Q1 2018 MME.

4.116 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. It was acknowledged at the Board Audit Committee the day before 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 Board Audit Committee 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.

4.117 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 tests 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.

4.118 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 Area first line. 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.

4.119 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

4.120 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 Board Audit Committee meeting the day before, concern had been expressed over the degree of parallelisation of workstreams, 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.

4.121 By mid-December 2017, although UAT was 85% complete, it was clear that more UAT completion would now slip into January 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.

4.122 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.

4.123 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*". 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 as risk mitigants in the Defender Plan if TSB wished to migrate in April.

4.124 At a migration deep dive meeting of the Board Audit Committee 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.

4.125 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.

4.126 Also in January 2018, completion of the migration to the Defender Plan timetable took on additional significance. 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*", in proceeding with the MME in April 2018.

4.127 On 23 February 2018, Sabadell announced publicly at an investor event in London that 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.

4.128 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.

4.129 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.

SECTION J: THE APRIL 2018 DECISION TO GO LIVE

4.130 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).

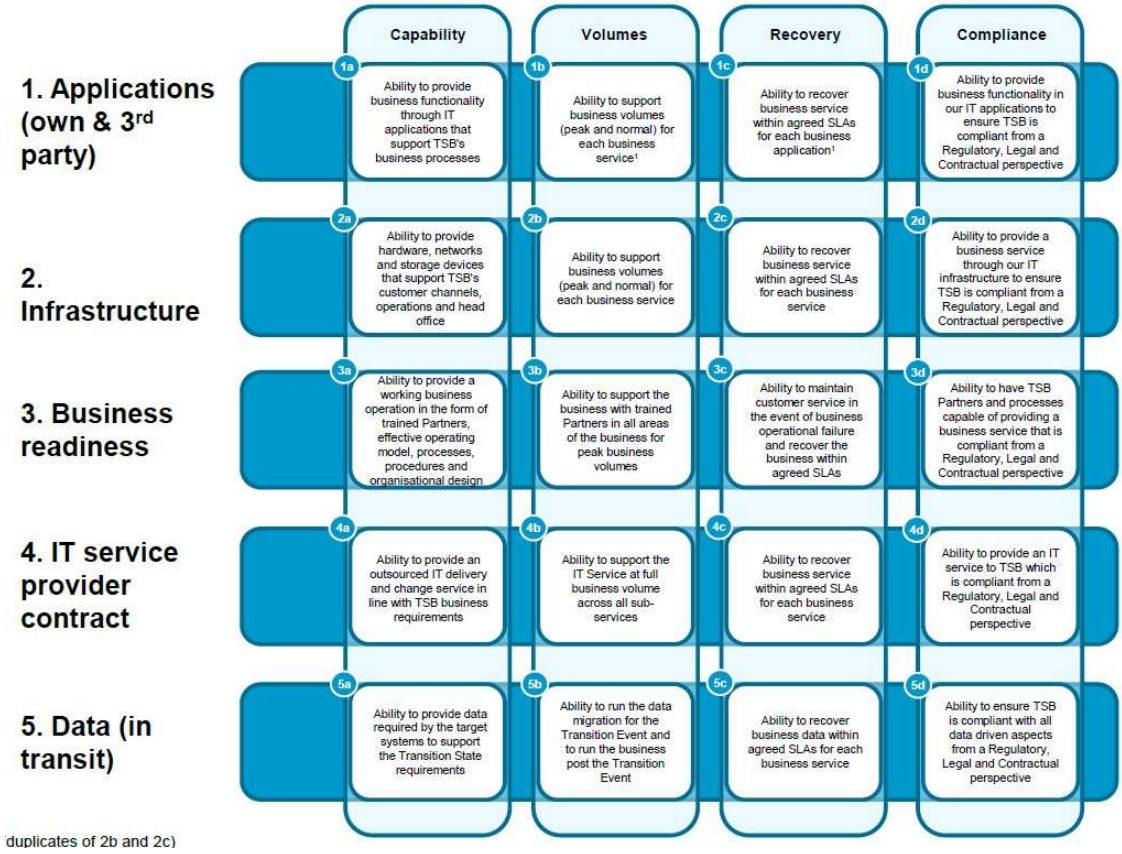
4.131 The ultimate decision to Go Live was taken following consideration of a number of assurance tools designed to draw together the assessments of the Business Areas, Risk Oversight and Internal Audit as to whether to proceed with the MME, i.e. migration of TSB's data from its existing location on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

4.132 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

4.133 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:



4.134 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.

4.135 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.

4.136 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 about SABIS readiness.

The T3 Memo

4.137 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 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 the Attestations testifying to the readiness of BEC business functions, 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 decision to Go Live

10 April 2018 TSB Board meeting

4.138 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.

4.139 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.

4.140 The 10 April 2018 TSB Board meeting was the last board meeting before the meeting on 18 April 2018 to consider the recommendation to progress 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.

4.141 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.

4.142 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.

4.143 BEC members also 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 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.

4.144 The paper noted that, contrary to Guiding Principle 3, a degree of parallel working remained (and that non-functional testing 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. Further, contrary to Guiding Principle 10, an explicit regression test phase 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.

4.145 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 away from certain of the Guiding Principles). Instead it stated 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.

18 April 2018 TSB Board meeting

4.146 On 18 April 2018, the TSB Board met to consider the recommendation to proceed with MME by delegating authority to the MME 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 as to readiness to proceed with migration, subject to addressing a limited number of further issues.

4.147 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 changes, 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.

4.148 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 non-functional testing in telephony had run up until 16 April 2018, albeit that testing had been passed.

4.149 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 non-functional testing ran in parallel into April 2018 in order to meet the deadline, contrary to Guiding Principle 3. Non-functional testing 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.

4.150 At the meeting the TSB Board discussed, 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 confidence that the platform had been tested to the point that it was ready for migration, confirmation of the readiness of SABIS, 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.

4.151 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

4.152 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.

Inadequacies in the Migration Programme as at Go Live

4.153 The Migration Programme did not run according to the IMP or the Defender Plan. As noted above, aspects of the testing programme it 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 been 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 Section B 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.

4.154 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.

SECTION K: TESTING

4.155 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

4.156 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 in Sections H, I and J, testing ran behind schedule during the Migration

Programme, with consequential impacts. Further detail of these issues is set out below.

Types of testing

4.157 Sections G and H described the types of testing that took place during the Migration Programme.

4.158 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;

b) Non-functional testing: this included security testing, performance testing, infrastructure testing, and disaster recovery testing; and

c) Testing of data migration: this included MACs, and dress rehearsals.

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

Functional Testing

4.160 As set out in Section G, 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.

4.161 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 non-functional testing and live proving and, under the Defender Plan, regression testing.

4.162 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 in one form of testing may invalidate part of the other type of testing already done on another component. However, 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*".

4.163 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.

4.164 As regards the intended final part of functional testing – 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 successful test phases, to ensure that the functionality still performed as intended despite interaction with new code subsequently deployed into the Proteo4UK Platform. However, a specific regression test phase did not occur as it had been effected through other elements of the plan due to time constraints in meeting the April 2018 date for MME.

4.165 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 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.

Non-functional testing

4.166 As described in Section G, non-functional testing 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.

4.167 Non-functional testing 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 non-functional testing would be required to mitigate this issue.

4.168 Non-functional testing 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 non-functional testing to identify potential issues.

4.169 Following delays in functional testing, TSB chose to start non-functional testing before the functional testing had completed. This came with the risks of parallelisation as described above. Additionally, the time available for non-functional testing was compressed. Having not proved the functionality of the Proteo4UK Platform before non-functional testing commenced, 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 non-functional testing.

4.170 A further reason for the compression of the time available for non-functional testing 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

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

4.172 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 are being delivered. In the case of the Migration Programme, this included services that had already gone live during the GTE, and would also be the environment in which live services would be provided following MME. During the Migration Programme, the production environment was used for most of the non-functional testing; and

c) GOS environment: this is a test environment built to be a simplified version of the production environment. During the Migration Programme, it was

used for some functional testing (MDT), some non-functional testing, and for all the testing of data migration.

4.173 TSB and SABIS decided to conduct the majority of non-functional testing (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 non-functional testing.

4.174 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 non-functional testing 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.

4.175 Internal Audit also noted previous FCA enforcement action in which there had been a lack of an appropriate testing platform and strategy with weaknesses in IT risk management and IT controls, as well the strategic priorities and concerns of the FCA in its 2017/2018 Business Plan regarding firms not being able to demonstrate effective oversight and governance of technological innovation due to poorly planned and executed IT change management plans, leading to more susceptibility to disruptions.

4.176 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 non-functional testing 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 non-functional testing. 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.

4.177 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 non-functional testing conducted. An example of this is the fact that NFT was not conducted in the 'Active-Active' configuration.

The Active-Active Configuration Issue

Background

4.178 Sabadell's infrastructure for Proteo in Spain used 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.

4.179 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

4.180 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.

4.181 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

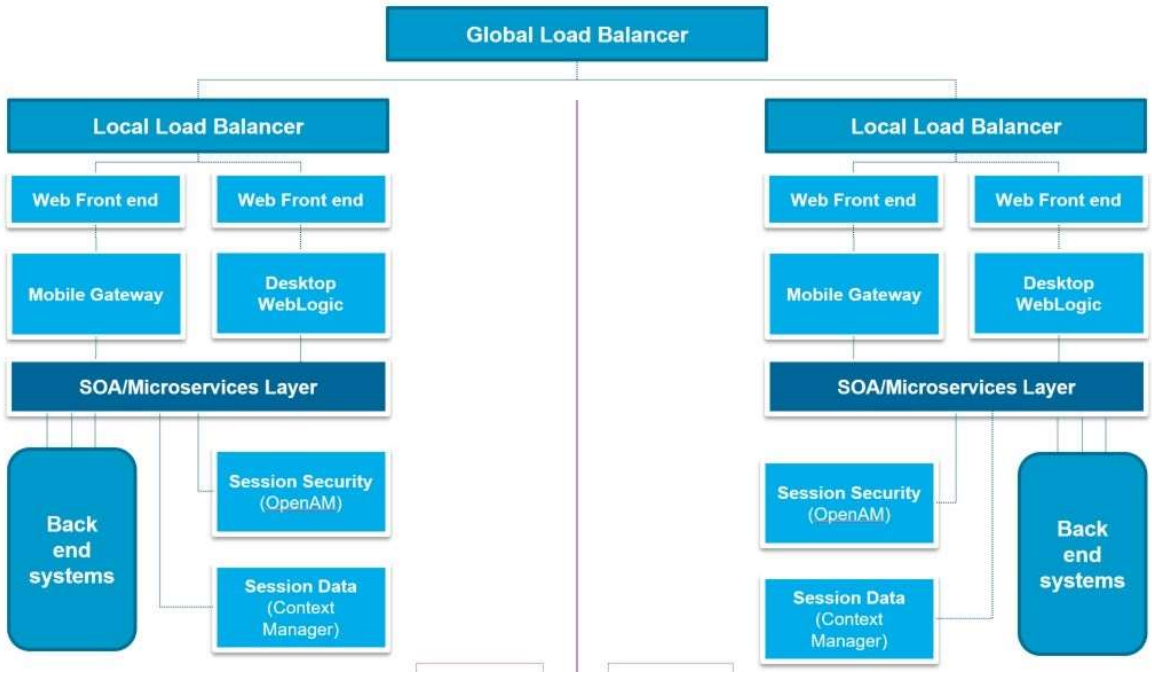
Load Balancer is a network box that receives all digital requests and decides, based on a set of rules, which one of the two data centres the request should be forwarded to. In the event of the failure of one data centre, the customer sessions running on that data centre would be automatically re-directed (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 on customers in the event of an IT incident affecting one of the data centres.

How Active-Active data centre configuration was designed to work

4.182 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 query.

4.183 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:

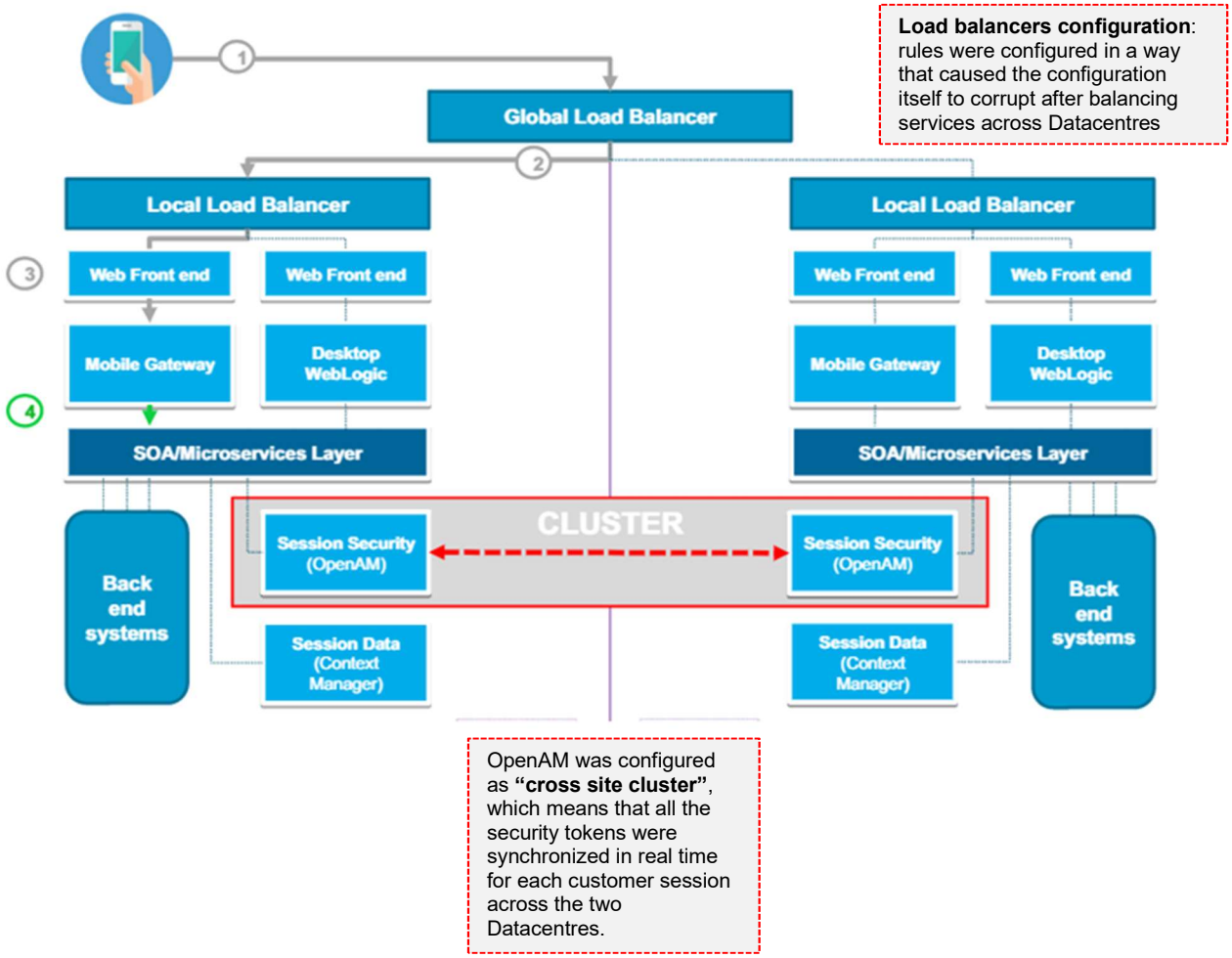


How Active-Active operated post-MME

4.184 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 (the platform responsible for customer authentication) were not directed to the 'local load balancer' in the relevant data centre, but had instead gone to the Global Load Balancer which at times sent them to the 'wrong' data centre. Further, the OpenAM component was configured in error as a cross-site cluster, which exacerbated the issues with session persistence.

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

Figure 5:



4.186 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

4.187 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 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.

4.188 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.

4.189 However, further non-functional testing, as planned for in TSB's T3 Non Functional Testing Strategy ("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

4.190 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.

4.191 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). But 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.

4.192 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.

4.193 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 Security Session (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.

4.194 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 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. If digital performance testing in Active-Active configuration had been carried out, it is likely that this issue would have been identified, and the consequences of the issue for customers avoided.

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

4.195 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 Design Executive.

4.196 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.

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

4.198 The Chair of BEC Design Executive 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 Design Executive, and the decision should have been formally recorded.

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

4.199 As described in Section J, 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.

4.200 Each BEC business function was required to review the evidence in respect of each 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.

4.201 However, as a result of the delays in conducting non-functional testing, at the 9 February 2018 BEC Design Executive meeting, the issue of the length of time that non-functional testing discussions had been taking was discussed. It was proposed instead that BEC business functions sign off their respective 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 Design Executive 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 non-functional testing, 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 non-functional testing report (the "NFT Report").

4.202 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 non-functional testing-related questions for their Business Areas.

4.203 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 than 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.

4.204 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 the sole responsibility for confirming that non-functional testing 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 non-functional testing met the non-functional requirements from BEC business functions to the IT business function.

4.205 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 non-functional testing (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.

SECTION L: RISK MANAGEMENT

4.206 As described in Section F, 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.

4.207 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

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

4.209 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).

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

4.211 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; and

c) MRR 41: complexity, or poor control in the delivery, or migration leads to unplanned costs or delays in implementation.

4.212 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.

4.213 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.

4.214 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

4.215 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 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.

<u>The Re-plan</u>

4.216 In relation to the re-planning exercise, the Board and Executive held a deep dive meeting 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*".

4.217 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 the plans for the 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.

4.218 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.

4.219 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).

4.220 Whilst the 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 or challenged by the TSB Board on 24 October 2017. This was despite their importance to the achievability of the re-plan and the mitigation of risk.

Recommendation to Go Live

4.221 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 non-functional testing, regression testing and end-to-end production proving.

4.222 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.

4.223 As regards non-functional testing, Internal Audit conducted a limited reconciliation review of the final non-functional testing 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

4.224 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 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.

4.225 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.

SECTION M: ASSESSMENT AND OVERSIGHT OF THE OUTSOURCING ARRANGEMENT WITH SABIS

4.226 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 agreement performance thresholds or service level agreements.

4.227 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.

4.228 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

4.229 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.

4.230 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"*.

4.231 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 it providing the ability to deliver TSB's desired range of functionality.

4.232 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.

4.233 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 TSB 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.

4.234 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 therefore undertake a definitive assessment of SABIS's capability at that point to deliver the Proteo4UK build or to operate Proteo4UK after migration, and would need to formally reassess SABIS's capability once TSB's requirements and service model became clearer.

4.235 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

4.236 As discussed in Section L, the 22 Programme Risks did not explicitly identify or 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.

Architectural designs of IT systems infrastructure

4.237 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.

4.238 Design documents were required under the MSA, but a different approach was agreed in 2017 following a review by Internal Audit. Internal Audit's report on 10 August 2017 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 it warned might 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.

4.239 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, leading to a breach of FCA Principle 3, increased regulatory scrutiny and a potential fine.

4.240 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.

4.241 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.

4.242 In the event, however, in February 2018, 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 instead 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.

4.243 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*."

4.244 Risks were again raised in relation to the limited infrastructure documentation in March 2018 by an external adviser which produced a report prepared 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 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 data centre 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.)

4.245 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 the *"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.

4.246 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

4.247 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). Although TSB did not have a contractual relationship with TSB's fourth parties, it retained responsibility for its obligations under the regulatory system when outsourcing critical or important operational functions or any relevant services and activities. 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.

4.248 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.

4.249 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] *completed 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

4.250 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.

4.251 The 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.

4.252 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.

4.253 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

4.254 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

4.255 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") which it considered confirmed 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.

4.256 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 from conversations on the subject.'

4.257 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.

4.258 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

4.259 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

4.260 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."

4.261 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.

SECTION N: EFFECTIVENESS OF PRE-MME BUSINESS CONTINUITY PLANNING AHEAD OF MME

4.262 Following MME, and as described in Section B, 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.

4.263 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.

4.264 A crisis situation caused by multiple IT incidents happening simultaneously with TSB struggling to fix them quickly enough was a residual risk identified ahead of Go Live, but not one for which TSB was adequately prepared at the scale at which the event actually arose. In TSB's view, it would not have decided to proceed with the migration had it considered that an incident of the scale of the issues that arose post migration might occur. Consequently, TSB's business continuity preparations were inadequate for the incident which ultimately took place.

4.265 This Section describes TSB's approach to business continuity planning ahead of MME, and in particular its:

a) Incident management and business continuity preparations for the fixing of IT defects should incidents arise following Go Live; and

b) TSB's operational preparations for dealing with the impact on customers as a result of such IT incidents occurring.

TSB's approach to business continuity planning

4.266 During the Migration Programme TSB, recognising that they were about to go into a major transformation and that their current business continuity plans would not be sufficient, undertook a programme of work to update their plans ahead of MME. As described below this included considering its disaster recovery requirements, reviewing the business continuity plans of SABIS, putting in place a Post Go Live Support ("PGLS") model for incident management, setting up war rooms, and testing business continuity through TSB Beta and through incidents in services already gone live. It also included engaging a third party adviser to prepare TSB and its executive team to be skilled enough in incident management and business continuity to go through MME, assisting TSB in reviewing their own plans and playbooks and running training scenarios to test the readiness of the executive team. TSB also prepared for customer impacts, taking into account previous migrations.

4.267 However, whilst TSB was prepared to deal with "*bumps in the road*", it was not prepared to deal with "*a massive failure in the configuration leading to an erratic digital service*". This was in the context of TSB undergoing a large-scale change programme leading to a go-live launch following which, if a major incident occurred, TSB would be unable to roll back on to the LBG Platform and would be reliant on SABIS as its outsourced IT service provider to fix multiple technical incidents which could have a major impact on customers.

4.268 The Attestations accompanying the T3 Memo did identify risks assessed to be residual, such as:

a) "*The operating model for running the services struggles to cope with multiple major incidents and multiple emergency changes happening simultaneously in the period immediately post go live*", with the impact if the risk crystallised identified to include prolonged downtime of critical

services, poor customer experience, reputational damage and, in extremis, regulatory sanction; and

b) "*Inability to successfully triage and fix incidents quickly enough post go live due to the number and nature of issues being experienced*" with the impact if the risk crystallised identified as possible loss of critical functionality for a period of time leading to poor customer experience and risk of reputational damage, in extremis regulatory sanction.

4.269 In both cases the key mitigants to these residual risks were the business continuity and incident management preparations that had been put in place. However, the severity of what they saw post-MME, with the problems with the digital bank, telephony and branches, "*was nothing they had planned for*". TSB acknowledged that when the crisis struck following MME, "*[r]*ather *than implementing the organisational plan that had been defined for Post Migration business-as-usual operation, crisis management governance was implemented…preparations were not in place for a contingency situation, and a thorough resilience plan for a crisis of this scale had not been prepared*".

4.270 TSB did not plan for such a crisis because, in its view, if it had considered there was a plausible risk of such problems occurring, it would not have gone ahead with MME. Consequently, whilst TSB undertook a large programme of work in relation to business continuity planning ahead of MME, in respect of each issue that is explained below, that planning was not sufficient to deal with the major incident that occurred post-MME. TSB did not adequately plan for how it would deal with an incident of the scale which transpired as it did not expect such a scenario to unfold following MME. Additionally, there were also gaps in the oversight of the preparations of SABIS.

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

4.271 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.

4.272 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.

4.273 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.

4.274 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

4.274. 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

4.275 TSB undertook internal assurance activity on both SABIS's operationalisation ahead of MME, and on 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.

4.276 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 and reviewed the process they had followed, to determine if they were ready to enter MME.

4.277 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".

4.278 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

4.279 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.

4.280 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

4.281 TSB needed to put in place suitable planning on its side to deal with any 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

4.282 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.

4.283 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

4.284 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.

4.285 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*".

4.286 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.

4.287 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.

4.288 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.

4.289 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.

Incident Management Playbooks

4.290 Following the second Gold practice event, the need to improve the quality of the Incident Management Playbooks being used by various Business Areas to support the management of incidents was identified. The Incident Management Playbooks were reference documents containing practical actions to aid the restoration of operational capabilities during an incident. Each of the Business Areas prepared one or more playbooks detailing how they would respond to incidents across eight

different scenarios: payments instability; penetration of TSB systems; loss of IT systems; loss, theft or denial of data; TSB / market instability; denial of people; denial of premises; and loss of critical supplier. The playbooks were signed-off by members of the BEC, underwent an internal QA analysis by the business continuity team and three of them were subject to a deep-dive review by a third-party expert consultancy firm. Additionally, this firm ran desktop exercises focussing on five of the eight different scenarios, to ensure that the playbooks were joined up in their approach to each.

4.291 The Incident Management Playbooks, were designed to support the first 48 hours after an incident. TSB expected that most issues could be resolved within 48 hours, following advice from their third party. However, consideration as to how to be prepared to deal with an incident, initially supported by the playbooks, but becoming large scale and lasting beyond a short period, was insufficient, as follows.

Customer communications

4.292 TSB's communications strategy was set out in its Corporate Affairs Playbook which set out the action plan for six scenarios for timeframes up to "48 hrs+". None of the examples included an IT incident as serious as the one experienced at MME. The communications plans include plans for a 48-hour timeframe, but these were drafted as resolution messages, as if the expected incidents had already been resolved within that period. However, the Migration Incident extended well beyond 48 hours. In the event, a Customer War Room was created on 26 April 2018 (4 days after MME) to manage customer communications.

Customer complaints

4.293 The Customer Relations Playbook envisaged resolving customer positions within 24 hours of an incident. It did include a plan of up to a 100% increase in complaints resourcing, but just over half of this (56%) this relied on bringing internal resource from other areas of the bank and that was not possible given the bank-wide disruption experienced at MME. It also noted the contact details for an external supplier of complaints handlers for a short term solution, but contained no plan for large-scale resourcing sufficient for the scale of the incident that occurred.

Vulnerable customers

4.294 None of TSB's playbooks relating to customer services, customer relations or corporate affairs made any specific provision for vulnerable customers in the event of a business continuity incident. It was not until the Customer War Room was created on 26 April 2018 (4 days after MME) that TSB started to develop an approach to proactively identify and reach out to vulnerable customers.

Customer impact of inadequate contingency planning

4.295 Some of TSB's customers were significantly impacted by shortcomings in TSB's contingency planning in relation to its customer communications strategy, complaints handling capacity and its ability to identify vulnerable customers.

Customer Communications Strategy

4.296 TSB did not prepare an adequate communications strategy for customers in the event of serious or longer-term issues arising at MME. This had impacts on customers following MME in terms of the messaging they received from the bank, and their ability to communicate with the bank.

4.297 As regards customer messaging, ahead of MME TSB prepared a customer communication strategy that included pre-prepared communications for the migration programme and weekend discussed in its Migration Customer Communications Committee, a communications playbook, (contained in its Corporate Affairs Playbook) and engaging with staff, media and government stakeholders to "*manage/mitigate reputational risk, and proactively position migration as a positive, transformative moment in TSB's history – which will change banking for consumers for good*."

4.298 The focus of TSB's customer communications was on the lead up to the migration and migration weekend. There was limited focus on contingency customer communications in the event of post MME incidents. A line by line plan and pre-approved contingency communications responsive to six scenarios lasting up to 48 hours were set out the Corporate Affairs Playbook. Additionally, pre-prepared messages for a positive migration outcome were several and varied, but the media and social media messages prepared for problems and defects characterised them as only snags and TSB did not prepare a communications plan for serious or sustained issues. It had only prepared for scenarios in which only minor problems occurred. The two media and social media responses were:

"Media Response:

- *We're really sorry that some of our customers are experiencing issues [with detail issue / defect]. This weekend we've been moving our 1.3 transformation programme of this size, we're experiencing a few snags.*

- *We're working around the clock to correct the snags as quickly as possible and will update customers as soon as we can. Customers are still able to [detail what customers are able to i.e. access ATMs, online / mobile banking etc] and if they have any questions or need more information they can give us a call on [insert phone number].*

Social Media Response:

- *Hi [XX], we're really sorry that you're experiencing issues [with detail issue / defect]. You can still [detail what customers are able to i.e access ATMs, online / mobile banking etc].*

- *This weekend we've been upgrading our systems and because of this we're experiencing a few snags. We're working around the clock to correct the snags as quickly as possible and will update you as soon as we can."*

4.299 The day after the migration, TSB moved to adopt a more proactive media approach in response to criticism.

4.300 In the days that followed the migration, TSB found the "responses covered by the pre written playbook responses and high level generic responses prior to MME did not address these customer queries and issues" and "were not reflective of the genuine customer experience".

4.301 It was not until four days after the migration that TSB overhauled its communication strategy and created a Customer War Room to manage customer communications.

4.302 In terms of customers' ability to communicate with the bank, customers were frustrated by the inability to contact TSB by telephone because of a lack of telephone capacity. Telephony requirements had been modelled ahead of MME

and compared to those required for previous migrations. However, in evidence given after the migration had occurred, one senior executive considered that TSB would have needed seven times the number of telephony staff at MME to be able to deal with the number of calls that were actually received.

4.303 TSB had plans in place for up to 70% additional resource in the event of an incident, which relied largely on internal resource levers but was insufficient to deal with the volume of calls which arose in practice following MME. TSB's ability to quickly bring in external resources to support Telephony was hampered by slow vetting processes. TSB did not consider in advance how to obtain sufficient resource in the event of a major incident.

Complaints

4.304 TSB expected to receive 2,000 complaints in the first week following MME, but it received approximately 37,000. TSB took steps to inform customers of their right to complain, but the volume of complaints overwhelmed TSB, senior staff were unprepared to deal with it and TSB was unable to respond to complaints within regulatory time limits.

4.305 TSB's contingency plans allowed for up to a 100% increase in complaints resourcing. This was insufficient in the circumstances that arose post-MME. As with telephony, the plan relied heavily on bringing internal resource from other areas of the bank and that was not possible given the bank-wide disruption experienced at MME.

4.306 TSB had limited contingency plans in place to bring in external complaint handling resource which required a six week onboarding and vetting process. TSB did not consider in advance how to address the effects of a lengthy onboarding process on its ability to bring in that resource quickly (other than to request contractors that had previously supported the department) in the event that a major incident occurred. TSB experienced significant problems bringing onboard effective external complaint handlers. For example, it agreed to bring in a third party to assist with complaints under the PTR Programme in May 2018, but the third party's effectiveness was considered by TSB to be limited. Further, they were only able to start on 16 July 2018, consequently TSB only began training them on its systems and to reach overall competence from that date, which contributed to delays in customer complaints being resolved.

4.307 TSB took almost 12 months to deal with complaints regarding migration.

Vulnerable customers

4.308 Prior to the Relevant Period, in February 2015, the Authority defined a vulnerable consumer as someone who, due to their personal circumstances, is especially susceptible to detriment, particularly when a firm is not acting with appropriate levels of care. Consumers in vulnerable circumstances may be more likely to suffer harm than other customers.

4.309 Prior to MME, TSB recognised the need to develop its vulnerable customer framework but it took a decision to delay key parts of its implementation until after MME, for example first-line ownership of this vulnerable customer framework. In addition, the introduction of a vulnerable customers flag on the systems and associated MI was scheduled to take place at MME. Information on vulnerability was not flagged on the front page customer profile prior to MME because it was not supported on the existing platform, but would be flagged going forward on the new Proteo4UK Platform.

4.310 After MME, TSB recognised that it needed to prioritise vulnerable customers and the Customer War Room (which had not been planned before MME, and was set up on 25 April 2018) established a vulnerable customer workstream.

4.311 On 26 April 2018, TSB established a focus group to review its response to vulnerable customers. However, TSB was hampered by its lack of management information. The lack of a dedicated vulnerable customer first line executive owner also added to TSB's slow identification of vulnerable customers, as there was no BEC member to drive forward TSB's work on potentially vulnerable customers.

4.312 The migration problems had the effect of making some vulnerable customers feeling particularly stressed and anxious. For example, a retail customer was frustrated at not being able check his account balance online. The customer felt that accessing telephony and branch services was extremely stressful due to his debilitating health condition. A further retail customer was unable to access TSB services online, and was unable to make payments to third parties (credit card, direct debit or standing order). The customer suffered from diagnosed anxiety and accessing branch and telephony services was extremely stressful.

4.313 Whilst a number of steps were taken post-MME during the Putting Things Right Programme to deal with issues being experienced in identifying and dealing with

vulnerable customers following the Migration Incident, the lack of focus in planning pre-MME was summarised by a senior TSB executive:

> *"[…] prior to the migration, […] second and third line had identified a lack of first line ownership of vulnerable customer strategy, customer treatment strategy. The policy for customer treatment is still held by the second line. It lacks a first line to own it and coordinate across the business. That same thematic gap in the first line management structure, org design, because it's a very functional org. design, it's part of the reason why we didn't think of the customer war room and customer perspective, until after we'd started to see the problems created by its absence."*

5. FAILINGS

5.1 The regulatory provisions relevant to this Notice are referred to in Annex A.

Principle 2: A firm must conduct its business with due skill, care and diligence

5.2 TSB breached Principle 2 because it failed to exercise due skill, care and diligence in managing the outsourcing arrangements with, and services provided by, SABIS, and the risks arising from this, including operational risk, appropriately and effectively.

5.3 In particular:

a) At the point of deciding to pursue the migration option and entering into the arrangement for services and outsourcing to SABIS, TSB did not conduct a formal and comprehensive assessment of whether SABIS had the ability and capacity to perform the services under the MSA or OSA reliably and professionally, specifically: whether SABIS could deliver the Proteo4UK Platform in the timeframe adopted, or whether SABIS was sufficiently ready to provide safely the ongoing outsourced services required to operate the Proteo4UK Platform;

b) TSB did not exercise due skill, care and diligence in managing the arrangement for services and outsourcing to SABIS:

i. Testing departed from certain aspects of TSB's plans and Guiding Principles, increasing operational risk;

ii. TSB did not formally and adequately reassess SABIS's ability and capacity on an ongoing basis;

iii. TSB failed to have a sufficient grasp of whether SABIS's infrastructure designs reflected TSB's requirements or whether the infrastructure had been built in accordance with the designs or, in some cases, how SABIS had carried out infrastructure testing;

iv. TSB did not obtain sufficient assurance about SABIS's management of fourth parties;

v. TSB did not obtain sufficient assurance about SABIS's readiness or that of critical fourth parties in the form of statements of proven fact about the completeness of readiness activities already undertaken, and

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

5.4 Further, TSB failed to exercise due skill, care and diligence in deciding not to conduct non-functional performance testing of the digital channels in Active-Active configuration in both data centres, resulting in the testing and production environments being distinctly different. TSB only considered the risks to disruption of services which were already online which would be caused by testing in Active-Active. As such TSB failed to properly identify and evaluate the risks of not conducting the testing in Active-Active configuration, nor consider any potential mitigants for the risks.

5.5 TSB also failed to take this decision in the Migration Testing Forum, and therefore within the governance structure in place for such decisions. The decision, and any risks that should have been identified in relation to the decision, were therefore not escalated within the governance structure. Neither were the risks identified in the Final NFT Report.

Principle 3: A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems

5.6 TSB breached Principle 3 because it failed to take reasonable care to organise and control the Migration Programme responsibly and effectively, or implement adequate risk management systems. In particular:

a) TSB did not take reasonable care in the planning and re-planning of the Migration Programme, and it failed to adequately mitigate operational risk:

i. Given the scale and complexity of the Migration Programme, the approach to planning in respect of the IMP adopted an overly right-to-left approach and as a result set an excessively ambitious timetable for migration;

ii. Re-planning of the Migration Programme in September and October 2017 to produce the Defender Plan again adopted an overly right-to-left approach (although TSB was of the view that it would not migrate until it was ready). TSB 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 TSB Board. In addition, TSB did not adequately investigate the technical causes of delays, or adequately assess their impact on the likely and realistic time required to complete the remaining tasks before migration; and

b) TSB's governance of the Migration Programme was insufficiently robust. It does not appear certain matters were sufficiently discussed with or challenged by the TSB Board. In particular the overly ambitious timetable for migration, deviations from certain aspects of the approved 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) TSB's risk management function did not adequately identify and report on risks during the Migration Programme. Specifically:

i. TSB did not explicitly identify 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, although aspects of the impact of the non-performance were considered as part of other programme risks;

ii. Some of the assurances provided by Risk Oversight and Internal Audit which supported the recommendation to proceed with Go Live were limited or qualified in ways which do not appear to have been drawn to the TSB Board's attention or challenged by them;

d) TSB's incident management arrangements and business continuity planning was undertaken in the context of TSB undergoing a large-scale change programme leading to a go-live launch following which, if a major incident occurred, TSB would be unable to roll back on to the LBG Platform and would be reliant on SABIS as its outsourced IT service provider to fix multiple technical incidents which could have a major impact on customers. In that context, TSB's incident management arrangements and business continuity plans were insufficiently robust and ineffective:

i. TSB 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. TSB did not ensure that it had sufficient oversight and assurance of SABIS's incident management capabilities;

iii. TSB did not undertake planning designed to deal with a major incident that lasted longer than a few hours or days, in particular in relation to its practice Gold events, playbooks, customer communications, and complaints handling, and its planning in relation to vulnerable customers was inadequate.

6. SANCTION

6.1 The Authority's policy for imposing a financial penalty is set out in Chapter 6 of DEPP. In respect of conduct occurring on or after 6 March 2010, the Authority applies a five-step framework to determine the appropriate level of financial penalty. DEPP 6.5A sets out the details of the five-step framework that applies in respect of financial penalties imposed on firms.

Step 1 – Disgorgement

6.2 Pursuant to DEPP 6.5A.1G, at Step 1 the Authority seeks to deprive a firm of the financial benefit derived directly from the breach where it is practicable to quantify this.

6.3 The Authority has not identified any financial benefit that TSB derived directly from its breaches.

6.4 Step 1 is therefore £0.

Step 2 – seriousness of the breach

6.5 Pursuant to DEPP 6.5A.2G, at Step 2 the Authority determines a figure that reflects the seriousness of the breach. Where the amount of revenue generated by a firm from a particular product line or business area is indicative of the harm or potential harm that its breach may cause, that figure will be based on a percentage of the firm's revenue from the relevant products or business area.

6.6 The Authority considers that the revenue generated by TSB is not an appropriate indicator of the harm or potential harm caused by its breaches. Whilst a wide range of TSB's product lines and business areas were at risk of and / or suffered serious disruption, the breaches did not in themselves relate to particular product lines or business areas. In any event, the revenue generated during the Relevant Period by the relevant product lines and business areas at risk of and / or which suffered serious disruption was approximately £3.3 billion. The Authority considers that a financial penalty based on revenue (if appropriate) of approximately £3.3 billion would be disproportionate to the harm caused by the breaches.

6.7 The Authority has not identified an alternative indicator of harm or potential harm appropriate to the breaches and so, pursuant to DEPP 6.5A.2G (13), has determined the appropriate Step 2 amount by taking into account relevant factors. In assessing the seriousness level for the purpose of penalty, the Authority takes into account various factors which reflect the impact and nature of the breach, and whether it was committed deliberately or recklessly.

Impact of the breach

6.8 The Migration Programme was the most important project being undertaken by TSB at the time, and had significant potential to negatively impact customers. The

Migration Incident resulted in a disruption to the continuity of certain aspects of TSB's provision of core banking functions (including branch, telephone, online and mobile banking). The issues with digital channels impacted its branches and the customers seeking to access the digital platform. A number of other specific technical issues impacted proportions of the customer base, 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 disruptions impacted all of TSB's 550 branches, and a significant proportion of its customers including a proportion of those on the digital platform.

6.9 The Migration Incident caused distress and inconvenience to some of the individual and business customers of TSB, and also to vulnerable customers.

6.10 It resulted in 225,492 complaints between 22 April 2018 to 7 April 2019, and caused TSB to pay TSB paid £32,705,762 to customers under the redress programme.

Nature of the breach

6.11 The breaches revealed serious weaknesses in elements of TSB's controls, governance and oversight (including in relation to third party parties), risk management and business continuity capabilities. Although some of the issues with the digital channels were significantly improved during 26 April 2018, disruption continued in all channels. TSB had the opportunity to identify and correct these failures ahead of the Migration Incident. The breaches occurred at points between 16 December 2015 and 10 December 2018.

Level of seriousness

6.12 DEPP 6.5A.2G(11) lists factors likely to be considered 'level 4 or 5 factors'. Of these, the Authority considers the following factors to be relevant:

a) The breaches caused a significant loss or risk of loss to individual consumers, with TSB ultimately paying £32,705,762 to customers under its redress programme;

b) The breaches revealed serious or systemic weaknesses in the firm's controls, governance and oversight (including in relation to third parties), risk management and business continuity capabilities over a period of time which TSB had the opportunity to identify and correct but did not.

6.13 DEPP 6.5A.2G(12) sets out the factors which are likely to be considered 'level 1 factors', 'level 2 factors' or 'level 3 factors'. Of these, the Authority considers the following factors to be relevant:

a) Little, or no, profits were made or losses avoided as a result of the breaches;

b) The breaches were committed negligently.

6.14 The Authority has not found that TSB acted deliberately or recklessly.

6.15 Taking all of these factors into account, the level of seriousness is 4 and the Step 2 figure is £50 million.

Step 3: aggravating and mitigating circumstances

6.16 Pursuant to DEPP 6.5A.3G, at Step 3 the Authority may increase or decrease the amount of the financial penalty arrived at after Step 2, but not including any amount to be disgorged as set out in Step 1, to take into account factors which aggravate or mitigate the breach.

6.17 The Authority considers that there are no aggravating factors and that the following factors mitigate the breach:

a) TSB has undertaken a comprehensive customer remediation exercise, putting in place additional resource (including engaging third parties) to deal with the 225,492 complaints that it received. The Authority considers that the remediation exercise encountered delays due to both the unprecedented number of complaints received and some of the issues in business continuity planning described in this Notice. However, the steps taken were extensive and include compensating customers for actual financial loss (including only requiring customers to provide evidence of financial loss where it was greater than £150), consequential loss, extensive distress and inconvenience payments, and dealing with non-financial loss such as impacts on credit files. The steps also include TSB putting in place temporary overdrafts (with no fees and charges) to all accounts, regardless of whether the customer had experienced issues following MME, as well as waiving fees, charges and interest on current account overdrafts and credit cards for March, April and May 2018, and increasing the interest rate on one particular account type. The Authority considers that while TSB had some commercial interest in the

circumstances that transpired post-MME in taking some of these steps, some of the measures (such as providing compensation up to £150 without requiring proof of loss, and providing redress for intangible harm) could be considered to be generous.

b) TSB also commissioned a number of technical reviews in the immediate aftermath of the migration, which it subsequently provided to the Authority. 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 independent review in a number of key respects, TSB agreed to provide the Authority with notes of interviews conducted as part of the review with relevant individuals. The Authority overall made some, but limited, use of the reviews.

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

6.18. Having taken into account these mitigating factors, the Authority considers that the Step 2 figure should be decreased by 15%.

6.19 Step 3 is therefore £42.50 million.

Step 4: Adjustment for deterrence

6.20 Pursuant to DEPP 6.5A.4G, if the Authority considers the figure arrived at after Step 3 is insufficient to deter the firm who committed the breach, or others, from committing further or similar breaches, then the Authority may increase the penalty.

6.21 The Authority considers that the Step 3 figure of £42.50 million represents a sufficient deterrent to TSB and others and so has not increased the penalty at Step 4.

6.22 Step 4 is therefore £42.50 million.

Step 5: Settlement discount

6.23 Pursuant to DEPP 6.5A.5G, if the Authority and the firm on whom a penalty is to be imposed agree the amount of the financial penalty and other terms, DEPP 6.7

provides that the amount of the financial penalty which might otherwise have been payable will be reduced to reflect the stage at which the Authority and the firm reached agreement.

6.24 The Authority and TSB reached agreement at Stage 1 and so a 30% discount applies to the Step 5 figure.

6.25 Step 5 is therefore £29.75 million.

Penalty

6.26 The Authority hereby imposes a total financial penalty of £29.75 million on TSB for breaching Principles 2 and 3.

7. PROCEDURAL MATTERS

7.1 This Notice is given to TSB under section 206 and in accordance with the section 390 of the Act.

7.2 The following statutory rights are important.

Decision maker

7.3 The decision which gave rise to the obligation to give this Notice was made by the Settlement Decision Makers.

Manner and time for payment

7.4 The financial penalty must be paid in full by TSB to the Authority no later than 4 January 2023.

If the financial penalty is not paid

7.5 If all or any of the financial penalty is outstanding on 5 January 2023, the Authority may recover the outstanding amount as a debt owed by TSB and due to the Authority.

Publicity

7.6 Sections 391(4), 391(6) and 391(7) of the Act apply to the publication of information about the matter to which this notice relates. Under those provisions, the Authority must publish such information about the matter to which this notice

relates as the Authority considers appropriate. The information may be published in such manner as the Authority considers appropriate. However, the Authority may not publish information if such publication would, in the opinion of the Authority, be unfair to you or prejudicial to the interests of consumers or detrimental to the stability of the UK financial system.

7.7 The Authority intends to publish such information about the matter to which this Final Notice relates as it considers appropriate.

Authority contacts

7.8 For more information concerning this matter generally, contact Rory Neary at the Authority (direct line: 020 7066 7972/email: rory.neary@fca.org.uk).

Kerralie Wallbridge

Head of Department
Financial Conduct Authority, Enforcement and Market Oversight Division

ANNEX A

RELEVANT STATUTORY AND REGULATORY PROVISIONS AND GUIDANCE

1. RELEVANT STATUTORY PROVISIONS

Financial Services and Markets Act 2000

1.1 The Authority's statutory objectives, set out in section 1B(3) of the Act, include the consumer protection objective (section 1C FSMA) and the integrity objective (section 1D FSMA).

1.2 Section 206(1) of the Act provides:

> "If the Authority considers that an authorised person has contravened a requirement imposed on him by or under this Act… 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.

2. RELEVANT REGULATORY PROVISIONS AND GUIDANCE

Relevant Regulatory Provisions

2.1 In exercising its powers to impose a financial penalty, the Authority has had regard to the relevant regulatory provisions published in the Authority's handbook. The main provisions that the Authority considers relevant are set out below.

Principles for Businesses

2.2 The Principles are a general statement of the fundamental obligations of firms under the regulatory system and are set out in the Authority's Handbook. They derive their authority from the Authority's rule-making powers set out in the Act.

The relevant Principles are as follows:

a) Principle 2 provides that a firm must conduct its business with due skill, care and diligence;

b) Principle 3 provides that a firm take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

Relevant Rules

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

Rules	**Derive from (prior to 3 January 2018)**	**Derive from or directly applicable (from 3 January 2018)**
Outsourcing (relevant general outsourcing requirements in SYSC)	• Article 13(5) of MiFID • Articles 13 and 14 of the MiFID implementing Directive	• Article 16(5) MiFID II • Articles 30 and 31 Outsourcing Requirements of the MiFID Org Regulation
Risk Control (SYSC 7.1.2R)	• Article 13(5) of MiFID • Article 7(1)(a) of the MiFID implementing Directive	• Article 23(1)(a) of the MiFID implementing Directive
General requirements (SYSC 4.1.6R business continuity)	• Article 13(4) of MiFID	• Article 16(4) of MiFID II
General requirements (SYSC 4.1.7R business continuity)	• Article 5(3) MiFID implementing Directive • Article 85(2) of the CRD	• Article 21(3) of the MiFID Org Regulation • Article 85(2) of the CRD

Outsourcing

Senior Management Arrangements, Systems and Controls (SYSC)

2.4 The general outsourcing requirements in SYSC applicable between 16 December 2015 to 2 January 2018 provided as follows:

SYSC 8.1.1R

"A common platform firm must:

1. when relying on a third party for the performance of operational functions which are critical for the performance of regulated activities, listed activities or ancillary services (in this chapter "relevant services and activities") on a continuous and satisfactory basis, ensure that it takes reasonable steps to avoid undue 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 appropriate regulator 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."

SYSC 8.1.4R

"For the purposes of this chapter 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 common platform 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."

SYSC 8.1.5R

"Without prejudice to the status of any other function, the following functions will not be considered as critical or important for the purposes of this chapter:

1. the provision to the firm of advisory services, and other services which do not form part of the relevant services and activities 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;

2. the purchase of standardised services, including market information services and the provision of price feeds;

3. the recording and retention of relevant telephone conversations or electronic communications subject to COBS 11.8."

SYSC 8.1.6R

"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."

SYSC 8.1.7R

"A common platform firm must 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 or of any relevant services and activities."

SYSC 8.1.8R

"A common platform 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 appropriate regulator and any other relevant competent authority in connection with the outsourced activities;

9. The firm, its auditors, the appropriate regulator 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 appropriate regulator 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."

SYSC 8.1.9R

"A common platform 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."

SYSC 8.1.10R

"If a common platform firm and the service provider are members of the same group, the firm may, for the purpose of complying with SYSC 8.1.7R to SYSC 8.1.11R and SYSC 8.2 and SYSC 8.3, take into account the extent to which the common platform firm controls the service provider or has the ability to influence its actions."

2.5 TSB Bank plc is a common platform firm for the purposes of SYSC.

2.6 From 3 January 2018, the general outsourcing requirements in SYSC apply to common platform firms as follows.

SYSC 8.1.1R

"A common platform firm must:

1. When relying on a third party for the performance of operational functions which are critical for the performance of regulated activities, listed activities or ancillary services (in this chapter "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 FCA 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."

2.7 In addition, a number of articles of the Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 (the "MiFID Org Regulation"), including Articles 30 and 31, are directly applicable to common platform firms since 3 January 2018 (see SYSC 8.1-2G and SYSC 1 Annex 1 3.2G(2)).

MiFID Org Regulation

2.8 The Outsourcing Requirements in Articles 30 and 31 of the MiFID Org Regulation (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/E, 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 manages 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."

Risk Control

SYSC

2.9 The relevant risk control requirements in SYSC applicable between 16 December 2015 to 2 January 2018 provided as follows:

SYSC 7.1.2R

"A common platform firm must establish, implement and maintain adequate risk management policies and procedures, including effective procedures for risk assessment, which identify the risks relating to the firm's activities, processes and systems, and where appropriate, set the level of risk tolerated by the firm."

MiFID Org Regulation

2.10 From 3 January 2018, Article 23 of the MiFID Org Regulation has been directly applicable to common platform firms (see SYSC 1 Annex 1 3.2G(2)). Article 23(1)(a) provides:

Article 23

Risk management

1. "Investment firms shall take the following actions relating to risk management:

    a) Establish, implement and maintain adequate risk management policies and procedures which identify the risks relating to the firm's activities, processes and systems, and where appropriate, set the level of risk tolerated by the firm"

General Requirements

SYSC

2.11 The relevant general requirements in SYSC applicable between 16 December 2015 to 2 January 2018 provided as follows:

SYSC 4.1.6R

"A common platform firm must take reasonable steps to ensure continuity and regularity in the performance of its regulated activities. To this end the common platform firm must employ appropriate and proportionate systems, resources and procedures."

SYSC 4.1.7R

"A common platform 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."

2.12 From 3 January 2018, SYSC 4.1.7R states:

SYSC 4.1.7R

"A CRR 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."

2.13 For the purposes of SYSC, a CRR firm includes a UK bank.

MiFID Org Regulation

2.14 From 3 January 2018, Article 21 of the MiFID Org Regulation has also been directly applicable to common platform firms (see SYSC 1 Annex 1 3.2G(2)). Article 21(3) provides:

Article 21(3)

"Investment firms shall establish, implement and maintain an adequate business continuity policy aimed at ensuring, in the case of an interruption to their systems and procedures, the preservation of essential data and functions, and the maintenance of investment services and activities, or, where that is not possible, the timely recovery of such data and functions and the timely resumption of their investment services and activities."

Relevant Guidance

Decision Procedures and Penalties Manual (DEPP)

2.15 Chapter 6 of DEPP, which forms part of the Authority's Handbook, sets out the Authority's statement of policy with respect to the imposition and amount of financial penalties under the Act.

The Enforcement Guide

2.16 The Enforcement Guide sets out the Authority's approach to exercising its main enforcement powers under the Act.

2.17 Chapter 7 of the Enforcement Guide sets out the Authority's approach to exercising its power to impose a financial a penalty.