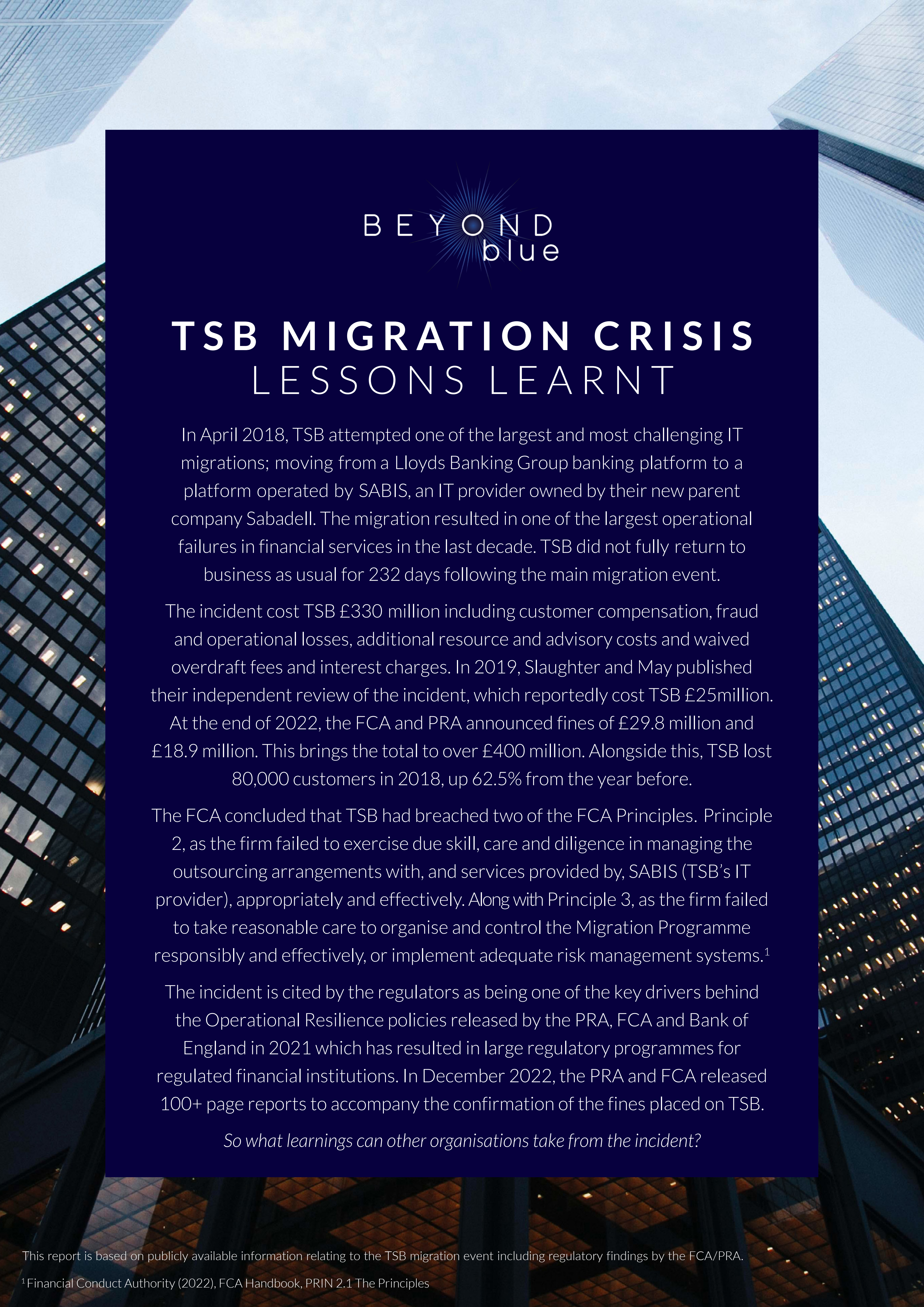


BEYOND blue

TSB MIGRATION CRISIS LESSONS LEARNT

In April 2018, TSB attempted one of the largest and most challenging IT migrations; moving from a Lloyds Banking Group banking platform to a platform operated by SABIS, an IT provider owned by their new parent company Sabadell. The migration resulted in one of the largest operational failures in financial services in the last decade. TSB did not fully return to business as usual for 232 days following the main migration event.

The incident cost TSB £330 million including customer compensation, fraud and operational losses, additional resource and advisory costs and waived overdraft fees and interest charges. In 2019, Slaughter and May published their independent review of the incident, which reportedly cost TSB £25million. At the end of 2022, the FCA and PRA announced fines of £29.8 million and £18.9 million. This brings the total to over £400 million. Alongside this, TSB lost 80,000 customers in 2018, up 62.5% from the year before.

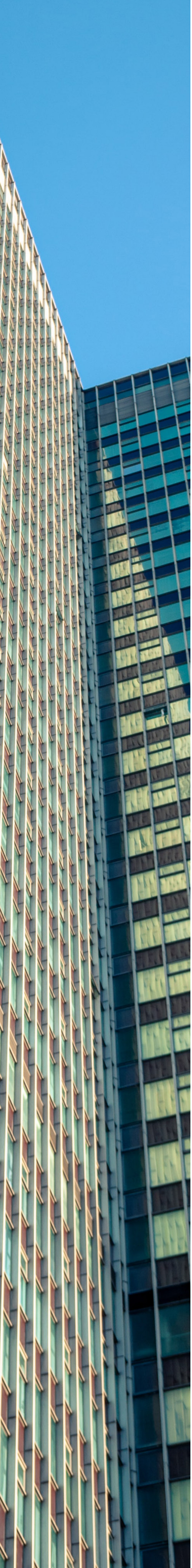
The FCA concluded that TSB had breached two of the FCA Principles. Principle 2, as the firm failed to exercise due skill, care and diligence in managing the outsourcing arrangements with, and services provided by, SABIS (TSB's IT provider), appropriately and effectively. Along with Principle 3, as the firm failed to take reasonable care to organise and control the Migration Programme responsibly and effectively, or implement adequate risk management systems.[1]

The incident is cited by the regulators as being one of the key drivers behind the Operational Resilience policies released by the PRA, FCA and Bank of England in 2021 which has resulted in large regulatory programmes for regulated financial institutions. In December 2022, the PRA and FCA released 100+ page reports to accompany the confirmation of the fines placed on TSB.

So what learnings can other organisations take from the incident?

This report is based on publicly available information relating to the TSB migration event including regulatory findings by the FCA/PRA.

[1] Financial Conduct Authority (2022), FCA Handbook, PRIN 2.1 The Principles



OVERVIEW FOR EXECUTIVES & BOARDS

The TSB Board and Bank Executive Committee (BEC) members had the structures and processes to conduct their governance oversight monitoring and assurance duties. However, there were several overlapping and compounding failures of governance and culture which jointly contributed to the main migration event (MME) failure. These are summarised below and examined further in the next section:

PRE MIGRATION

- **DISCUSSION AND CHALLENGE.** There appears to have been insufficient discussion and challenge from the Board and BEC about the risks and dependencies associated with an ambitious data and technology migration to a new platform.
- **PRESSURE ON TIMINGS AND ANNOUNCEMENTS.** In September 2017, it was decided to delay and re-plan the migration, but 9 days later, before the re-planning was complete, it was announced the migration would be in Q1 2018. This may have added implicit pressure to deliver to the new timescale, despite the Board's previously expressed view that they would only migrate when ready.
- **THIRD-PARTY ASSURANCE.** The insufficiency of the Board's challenge and discussion were exacerbated by a lack of adequate risk management and assurance of critical 3rd (SABIS) and 4th parties' capability, capacity, and readiness to deliver the technology migration. Certain limited or qualified assurances were not drawn to the attention of the TSB Board.
- **TESTING LESSONS IDENTIFIED NOT LEARNED.** There were several lessons identified following the initial migration programme setbacks, which led to the definition of 15 Guiding Principles to guide and test the re-plan. However, these were not implemented in full, with decision-making for this divergence not being escalated to a suitable governance level.
- **TEST ACTIVITIES – ARBITRARY VS. PLANNED ACTIVITY.** Test plans were based on a sequential set of activities that should have resulted in layered understanding of any technological issues. However, since the Integrated Master Plan (IMP) and the Defender Plan fell behind schedule, the test approach (including critical aspects of non-functional testing) were arbitrarily modified. Moreover, several test activities were run in parallel to suit the impending timelines with fundamental changes being made to its scope and timing. A lack of rigour also arose from such decisions being made outside of formal governance forums which introduced key risks relating to 'Active-Active configuration' in data centres.
- **RISK AND PROGRAMME MANAGEMENT INADEQUACIES.** The IMP consistently fell behind the schedule and failed to acknowledge the underlying reasons and risks for delays through to the point of re-plan (known as the 'Defender Plan'). It led to decisions that moved away from the key guiding principles of the programme. This also ties in with Governance and Culture aspects at the Board level where lack of sufficient challenge once again resulted in no in-depth understanding of risks or rationales for such delays or if these proposed plans were realistically achievable targets.

POST MIGRATION

- **INCIDENT MANAGEMENT.** Whilst an incident management model was in place between TSB and SABIS, there was no joint testing of incident management at a BEC level. In preparation for the MME, the BEC completed 3 incident management exercises, but these only simulated a 48-hour disruption and did not offer the opportunity to explore the challenges of mitigating the impact of a multi-week incident.
- **REMEDIATION VS. TREATMENT.** Initial focus was on identifying and remediating technical issues, rather than the treatment of customer impacts. It took four days following migration to set up a customer war room and overhaul the customer communications strategy.
- **CAPACITY OF WORKAROUNDS.** The planned workarounds and additional capacity for telephony and complaints was supposed to come from other teams within TSB. The aggregate impact of a 'multiple organ' failure scenario had not been considered, with these teams being the 'plan B' for multiple teams and services. This significantly reduced the overall capacity of the organisation to respond effectively.
- **VULNERABLE CUSTOMERS.** There was a failure to identify and categorise vulnerable customers as part of business as usual or to develop dedicated customer treatment strategies for these customers to invoke during an incident. These efforts would have helped to reduce the number of tabloid front page headlines focused on severe impacts to the minority of the customer base.

PRE MIGRATION TIMELINE OF EVENTS

TSB planned for the most rapid and largest IT migrations attempted by an organisation. In the 2 and a half years leading up the April 2018, issues relating to Supply Chain assurance, Testing, Governance & Culture and Risk Oversight & Audit, contributed to the incident that unfolded.

KEY

- ● Supply Chain Assurance
- ● Testing
- ● Governance & Culture
- ● Risk Oversight & Internal Audit
- ★ Milestone

2015

JULY

Sabadell acquired TSB.

NOVEMBER

Sabadell publicly stated that TSB would complete migration by the end of 2017. TSB Board's position was that it would not migrate until it was ready.

16 DECEMBER

At the TSB Board meeting, the outsourcing risk was identified in a memo, but there was no discussion about SABIS's capabilities to build and operate the platform and integrate systems or how that would be assessed.

DECEMBER

TSB Board decided to proceed with SABIS as the IT platform provider.

DECEMBER

In the TSB deep dives, non-functional testing was noted as a specific mitigation for the risk that the Proteo platform was not proven in the UK.

DECEMBER

3 deep dives with TSB Board to discuss a carve out approach vs. full migration. The plan was being designed right to left to hit the 2017 deadline.

DECEMBER

Functional requirements and the service model between TSB and SABIS or any third parties had not been defined at the point the decision was made to procced with SABIS. Following definition of these, no formal assurance process of SABIS was undertaken.

2016

MARCH

Target date of 5 November 2017 approved by TSB Board, despite being 3 months behind schedule. TSB Board remarked that the timescales were *"challenging, with little contingency,"*[1] and requested that TSB develop a fall-back plan should migration not be possible.

OCTOBER

Testing timelines had been replanned. Supply chain dependencies were increasing parallelisation of the plan (this breached Guiding Principle 3).

DECEMBER

Between November 2015 and December 2016, 22 programme risks were raised. They did not develop as the Migration Programme progressed.

2017

MAY

First phase of user acceptance testing (UAT) delayed by 3 months from end of April to end of August.

10 AUGUST

Internal Audit raised that the IT function did not have documentation outlining the architectural design of the IT platform to allow them to *"confirm that it is delivered as designed,"*[2] which they were accountable for. Internal Audit noted this could lead them to a breach of FCA Principle 3.

10 AUGUST

Internal Audit noted that not using a pre-production environment for non functional testing could result in instability and potential vulnerabilities in the production environment.

19 SEPTEMBER

An external consultancy firm projected that it would take 33 weeks to pass all 100% of in-scope test cases (i.e. into May 2018).

20 SEPTEMBER

Migration to be replanned with the report stating *"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."*[3]

29 SEPTEMBER

TSB publicly announced intent to migrate in Q1 2018.

OCTOBER

Risk Oversight raised that TSB did not understand full risk exposure of SABIS IT service provision. SABIS acknowledge TSB may not have sufficient visibility over fourth party risk.

OCTOBER

A report found that Governed Transition Events (GTEs) had several issues including build defects not identified in testing, configuration issues, delayed recovery, and performance and availability of services.

24 OCTOBER

Both Risk Oversight and Internal Audit provided opinions that the re-plan process (including assumptions and considerations of previous recommendations) was reasonable and satisfactory, noting the very limited scope of their reviews and subsequent opinions. These and underlying assumptions were not challenged by the TSB Board.

24 OCTOBER

The re-plan ("Defender Plan") presented to TSB Board during a deep dive session with 15 Guiding Principles to act as risk mitigants. The FCA assessed that the Board did not provide sufficient challenge to this plan. The plan did not clearly set out how far behind schedule the Programme was, the reasons for the delays, and their impact on future timings. TSB reduced the testing scope and the Defender Plan projected completion of testing by the end of 2017, based on a set of ambitious and unrealistic assumptions.

31 OCTOBER

In replacement of architectural design documentation, SABIS were asked to maintain a Configuration Management Database (CMDB) detailing all infrastructure. These documents could not be used to verify they had been built to the original design.

21 NOVEMBER

Testing was reported to be *"marginally behind plan"*[4] and it was unrealistic that they would complete before the end of the year.

2018

JANUARY

TSB accepted deviation from 3 of the 15 Guiding Principles.

JANUARY

External Consultant (on behalf of Risk Oversight) noted TSB would not be obtaining a pre-production environment before MME (it would be established post Go Live).

FEBRUARY

Internal Audit closed requirement for SABIS to maintain the CMDB as it was thought that infrastructure documents had finally been produced which provided the IT business function suitable visibility. This was not the case. Senior members of the IBS business function believed this had been closed prematurely: "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."

FEBRUARY

SABIS acknowledge a gap in its control environment relating to its supplier management model due to being unable to recruit someone for the role.

FEBRUARY

At the BEC Design Executive meeting a decision was taken for the IT business function to attest which non-functional requirements had been tested and which had not, instead of BEC members. This attestation was captured in the final NFT report.

23 FEBRUARY

Sabadell announced publicly at an investor event in London that MME would occur on 21 April 2018.

28 FEBRUARY

In the Migration Testing Forum a proposal was considered to only use one data centre for performance testing so as to not impact live services already running in the other data centre. This was in contrast to the initial decision to test in Active-Active configuration across two data centres. The final decision to do this was taken outside of the Migration Testing forum and was not escalated to the BEC Design Executive or TSB Board before migration. This was not in accordance with TSB' governance structure or procedures. This was based on the assumption that both centres were identically configured.

MARCH

An external adviser (on behalf of Risk Oversight) produced a report identifying the limited unfractured design documentation. It gave an action to define roles and responsbilities between TSB and SABIS, including those responsible for maintaining design documentation.

APRIL

Functional testing finished as testing of parts of the new systems were deferred and descoped until after MME. No specific regression testing took place (which breached Guiding Principle 10).

5 APRIL

Letter from SABIS confirmed non-functional readiness for migration, despite written confirmation not being received from one critical fourth party. This was received on 10 April. This letter and fourth party confirmations were forward looking statements of good intention or expectations rather than statements of fact about the completeness of readiness activities already undertaken.

8 APRIL

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. Risk Oversight agreed to make observations past this date. No observations were recorded.

10 APRIL

TSB Board approved for a Definitive Notice of Migration to be served to LBG on 12 April, thereby terminating the carve-out option and committing TSB to migration. At the same meeting, it was noted that TSB was not in a position to recommend proceeding with migration (this was expected by the next Board meeting on 18 April).

17 APRIL

Risk Oversight risk tolerated the action to define roles and responsbilities between SABIS and TSB until after MME, based on a satisfactory minimum level of compliance. TSB Executive and Board relied on the IT business functions attestation of SABID readiness. Only a SABIS employee would be able to attest to their ability to perform contractual obligations.

17 APRIL

The final NFT report was published stating that *"live production performance is expected to be better than under test conditions"*[5] (in relation to testing on only one data centre). The risk of only testing in one data centre was not identified as a risk, therefore no potential mitigants were considered and the BEC were unaware.

17 APRIL

Risk Oversight provided opinion, the scope of which did not cover non-functional testing, regression testing and end-to-end production proving. The scope was not challenged by the TSB Board.

18 APRIL

TSB Board meeting to provide GO/ NO GO decision. There were still eight outstanding areas of *"must-have functionality that either needed to pass testing or be mitigated"*[6]. The second and third line opinions provided confidence to the Board of appropriate consideration of the risks.

19 APRIL

TSB Board confirmed a GO decision for MME on weekend of 21/22 April.

[1] Financial Conduct Authority (2022), FINAL NOTICE 2022: TSB Bank plc, 39
[2] Financial Conduct Authority (2022), FINAL NOTICE 2022: TSB Bank plc, 74
[3] Financial Conduct Authority (2022), FINAL NOTICE 2022: TSB Bank plc, 41
[4] Financial Conduct Authority (2022), FINAL NOTICE 2022: TSB Bank plc, 46
[5] Financial Conduct Authority (2022), FINAL NOTICE 2022: TSB Bank plc, 66
[6] Financial Conduct Authority (2022), FINAL NOTICE 2022: TSB Bank plc, 52

PRE-MIGRATION

GOVERNANCE & CULTURE

- **DISCUSSION AND CHALLENGE.** There appears to have been insufficient discussion and challenge from the Board and BEC about the risks and dependencies associated with an ambitious data and technology migration to a new platform. The key observation from the TSB migration is that there was a systems design overreach (i.e., when designers build systems without anticipating the potential consequences of disruption). The lack of challenge and discussion that has been identified by the regulators indicates a culture which resulted in a failure to recognise this and dedicate time and effort to apply independent judgement, due care and diligence.
- **PRESSURE ON TIMINGS AND ANNOUNCEMENTS.** In September 2017, it was decided to delay and re-plan the migration. However, 9 days later, before the re-planning was complete, it was announced that the migration would be in Q1 2018. This may have added implicit pressure to deliver to the new timescale. This created perverse incentives to deliver to an artificial timeline, despite TSB Board's stated intent that it would not migrate until it was ready. This possibly fed into all the issues identified above.

SUPPLY CHAIN ASSURANCE

- **THIRD-PARTY ASSURANCE.** The insufficiency of the Board's challenge and discussion were exacerbated by a lack of adequate risk management and assurance of critical 3rd (SABIS) and 4th parties' capabilities, capacities, and readiness to deliver the technology migration. Whilst some limited or qualified assurances were made, they were not drawn to the attention of the TSB Board. These inadequate risk management efforts appear to have been a consequence of both 1) the inability of lower-level personnel to assure and challenge SABIS, and 2) governance bodies being overly accepting of what was being presented and not challenging gaps in reasoning used for the third-party assessments.
- **INTRA-GROUP ARRANGEMENTS.** Any explicit risks regarding SABIS, the most critical supplier, were not identified and TSB did not undertake any explicit assessment of the risk of inadequate performance. Given that SABIS was a subsidiary of Sabadell (the Spanish Bank that acquired TSB), the provision of their services relating to the build and design of the platform was treated much like an intra-group arrangement and was not robustly assessed for risks as an external third-party supplier. There was no formal due diligence to verify that SABIS had the capability to deliver the required platform (Proteo4UK). An Internal Audit report noted that this may have resulted in a breach of FCA (Financial Conduct Authority) Principle 3. However, no further action was taken on the back of Audit's observations. SABIS relied on 85 of their own third parties. By February 2018 (over 2 years into the project), TSB had not verified if SABIS's supplier management model complied with the TSB Group Outsourcing policy.

TESTING

- **TESTING LESSONS IDENTIFIED WERE NOT LEARNED.** There were several lessons identified following the initial migration programme setbacks. This led to 15 Guiding Principles to drive and test the re-plan. However, these were not implemented in full, with decision-making for this error not being escalated to a suitable governance level. In every major transformation and strategy that is implemented, there is always pressure of time, cost and quality in delivery. This often leads to technical debt and aspects of capability being traded out. But, in doing so, vulnerabilities in the final capability can be created. When lessons have been identified of the importance of specific forms of testing, then any divergence from this must be based upon clear reasoning and appropriate challenge within governance structures.
- **TEST ACTIVITIES.** Several assumptions were made about the UAT and the length of time it would take to complete this. However, the testing team did not undertake any validation of these assumptions and were also coupled with external consultants providing assessment of expected delays based on historical testing performance. Additionally, previous FCA enforcement action made reference to poorly planned and executed IT change management policies which were highlighted by an Internal Audit. However, these issues were risk-accepted on the basis that an approval would be sought prior to migration which never occurred. Migration also required two data centres to be configured to support the new platform by SABIS. The testing, however, only successfully tested one data centre. This eventually led to cross configuration errors across the two data centres and customer detriment.

RISK MANAGEMENT

- **INADEQUATE 2ND LINE CHALLENGE.** Senior executives at TSB recognised in the early phases of the project that there were inadequate capabilities in their 2nd line risk oversight function to challenge the project team on the risks associated with undertaking one of the most complex and ambitious IT system migration projects in the UK. This highlights the risk of not having an adequate level of risk management challenge capabilities within the organisation. Additionally, in the final week before going live, TSB executives were responsible for providing attestations on readiness components that they were responsible for. Despite the attestations remaining incomplete at such a late stage, there was a lack of due rigour and challenge from the Board. This is a key example of TSB bypassing key risk mitigation activities that were structured to ensure smooth delivery of the migration project.
- **GENERIC HIGH-LEVEL RISK .** The project team had also identified 22 risks associated with the project. However, the risks were defined in a very generic way such as "Excessive complexity", "Resilience", "Management stretch", "Cost increases", "Use of 3rd parties", etc. It could be argued that a complex IT migration project of such a large scale had risks which can only be adequately captured at such a generic level. However, this makes assigning risk owners and assessing such generic risks difficult. This in turn results in ineffective control mitigation. In the final week before the planned 'go live', none of the executives responsible had provided attestations on readiness that they were responsible for. The Board did not challenge, at this late stage, whether it was reasonable that none had been completed.

POST MIGRATION TIMELINE OF EVENTS

TSB took 232 days following the MME to fully return to Business as Usual. There were significant issues across all Channels (Digital, Telephony and Branch) for the 2 weeks following the MME with the media and social media filling the void of information and communications initially left by TSB.

KEY

Reaction

Recovery

Customer Treatment

Service Disruption

Milestone

2018

22 APRIL
MME WEEKEND

13:00 - GO LIVE Decision.

18:00 - Telephony & Internet Banking LIVE.

18:45 - Mobile App LIVE.

19:00 – Digital Channels taken offline to investigate root cause of data breaches and failed payments until 02:00 the next day .

23 APRIL

Digital channels – log-ons restricted due to limited capacity. 10% of internet banking log-ons and 65-85% of mobile app log-ons successful. 48% of payments on the mobile app and 59% of payments on internet banking failed.

Telephony - 25% capacity available whilst demanded quadrupled. Call wait times were on average 90 minutes with a 70% abandon rate.

Branches - failure of Chip and Pin, Voucher Readers (used to process cheques), Teller Cash Recyclers (used to manage cash), Immediate Deposit Machines (used by customers to deposit cash and cheques) and no ability to print.

24 APRIL

Telephony – average wait time was 1 hour 20 mins.

10:00 - Digital channels - taken down to apply fixes (expected to take 1 hour).

24 APRIL

Public commitment to *"no one will be left out of pocket as a result of these service issues."*[1]

25 APRIL

03:00 - Digital channels resumed.

25 APRIL

Third parties engaged to identify and resolve performance issues.

26 APRIL

Digital channels- *"unstable and almost unusable"*[2] until this point.

Complaints - 900% more complaints were logged than anticipated.

29 APRIL

Telephony - Average wait time was 46 minutes.

FIRST WEEK...

20-30% of retail and business customers could not make any online payments.

MAY

Putting Things Right Programme established.

2 MAY

Technical issue caused 70% of customers to drop out of Telephony queues before reaching the IVR system.

2 MAY

CEO & Chairman appeared in front of the Treasury Select Committee.

3 MAY

For a short period, colleagues unable to service any customers via Telephony.

4 MAY

1 hour of disruption with the Interactive Voice Response (IVR) due to legacy infrastructure issues .

6 MAY

Digital channel services issues continued until this date.

FIRST 2 WEEKS...

- 600,00 customers experienced delays in credits/ debits being charged.
- 600 customers were able to see other customers data or had incorrect access to accounts.
- Large proportion of business customers could not make payments to new beneficiaries.
- Customers had duplicate payments, incorrect account information or no access to their accounts (credit, debit, mortgage).

31 MAY

2,200 customers had experienced fraudulent attempts to access their accounts and 1300 suffered financial loss.

JUNE

All Mobile app defects remediated.

6 JUNE

CEO and Chairman in front of the Treasury Select Committee with the regulators.

MID-JUNE

Telephony wait times and abandonment rates back to BAU levels.

4 SEPTEMBER

CEO steps down.

10 DECEMBER

TSB fully returns to Business as Usual.

22 APRIL 2018 –
7 APRIL 2019

225,492 customer complaints (c.4.3% of its customer base at the point of migration).

£32,705,762 of customer redress paid.

[1] Financial Conduct Authority (2022), FINAL NOTICE 2022: TSB Bank plc, 9
[2] Financial Conduct Authority (2022), FINAL NOTICE 2022: TSB Bank plc, 17

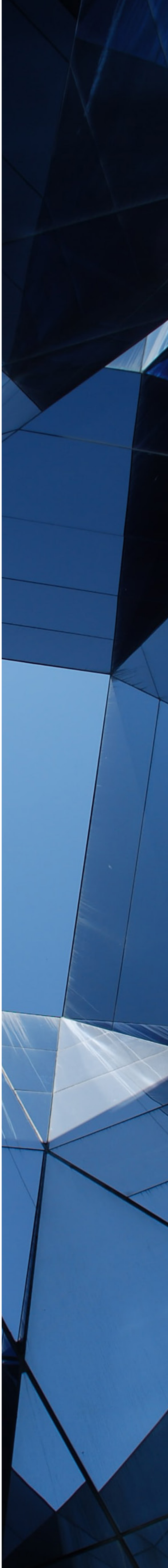
POST MIGRATION

INCIDENT MANAGEMENT

- **No joint testing** - A dedicated incident management model called "Post Go Live Support (PGLS)" was put in place between TSB and SABIS to manage incidents following MME. Despite this, there was no dedicated joint testing of incident management between TSB and SABIS at a BEC level, despite this being previously planned.
- **Lack of imagination** - In preparation for the MME, the BEC completed 3 incident management exercises, assisted by a third party. The scenarios and supporting playbooks only simulated 48-hour disruptions, in contrast to the 232 days it took TSB to return to Business as Usual. TSB did not plan for a crisis as complex or extended as transpired. The reason for this is that, if it had deemed that such a crisis plausible in the lead up to the migration, they would likely not have gone ahead with MME.
- **Insufficient testing of entire crisis management structure** - Incident management preparation focused on exercising BEC members who made up the "Gold" team and not the lower tiers of the crisis management structure, who were ultimately responsible for coordinating the complex and lengthy crisis that followed.
- **No Plan B** - Despite MME being the quickest planned IT migration of its kind in financial services, there was no ability to "roll back" to the LBG IT platforms. It also resulted in TSB's complete reliance on an outsourced IT service. The level of incident management and business continuity preparation was not commensurate with the risk posed to operational continuity.

CUSTOMER TREATMENT

- **Lack of ownership** - The delayed focus on customers and vulnerable customers is attributed to there being no first line owner who could coordinate the response across the organisation. The Policy for Customer Treatment was owned by the second line.
- **Focus on resolving the issue rather than addressing the impacts** - TSB's initial focus was on identifying and remediating the root cause of the incident, rather than the treatment of customer impacts. It took four days following migration to set up a customer war room and overhaul the customer communications strategy. The pre-planned customer communications for use in a post migration incident were *"not reflective of the genuine customer experience."*[1]
- **Insufficient telephony capacity** - Customers were unable to contact TSB due to insufficient capacity to answer an unprecedented volume of calls. It is estimated that seven times the number of staff would have been needed to deal with the number of calls received, but TSB only planned for an uplift of 70% (i.e., the uplift was one-tenth of the size required). Delays were further increased by the slow vetting processes required to get external resources onboarded.
- **Delayed complaint resolution** - Resolving all the migration related complaints took 12 months, due to a lack of resource available to process these. The vetting and onboarding process took 6 weeks, with further time required for training on systems before being "useful" resource.
- **Aggregation of impact** - The planned workarounds and additional capacity for telephony and complaints was supposed to come from other teams within TSB. What had not been considered is that those teams may in fact be busy dealing with their own issues or dealing with other areas of concern in the "multiple organ" failure scenario TSB were faced with. This concentration on specific teams to provide additional capacity may have been identified if a test had simulated that all business continuity plans would be activated at the same time.
- **Vulnerable customers** - TSB were aware that they had limited capability to identify and categorise vulnerable customers ahead of the MME. This hampered their ability to identify and treat these customers, unnecessarily increasing the stress and harm experienced. It was not until 26 April that a dedicated team within the Customer war room reviewed the response to vulnerable customers.
- **Customer compensation** - TSB committed that *"no one will be left out of pocket as a result of these service issues."*[2] Customers were able to claim £150 compensation without being required to provide proof of loss. Customers claimed for consequential loss, extensive distress, inconvenience payments and TSB remediated impacts on credit files. TSB provided temporary overdrafts for all accounts and waived fees, charges and interest on overdrafts and credit cards from March – May 2018 and proactively increased the interest rate on one account type. These actions were looked on favourably by the FCA and were considered a mitigating factor when settling on the regulatory action.



[1] Financial Conduct Authority (2022), FINAL NOTICE 2022: TSB Bank plc, 90
[2] Financial Conduct Authority (2022), FINAL NOTICE 2022: TSB Bank plc, 9

LESSONS LEARNT

SO, WHAT CAN ORGANISATIONS LEARN FROM THE INCIDENT?

1. Whilst there will always be an inherent tension between budgets, operations, security and resilience, organisations should **foster a culture of transparency and collaboration, where employees are encouraged to raise concerns and protected from the consequences of doing so.** Put the customer at the centre of your strategy and encourage employees to challenge each other when decisions, both tactical and strategic, cannot be traced back to a customer benefit.
2. Implement the governance structures to facilitate robust challenge. Diversifying Boards by recruiting Non-Executive Directors that align to your strategy, fill experience gaps, and can ask the challenging questions. **Identify the right Resilience metrics that drive the right behaviours and do not allow for risk to be lost or censored as it is summarised for senior audiences.** This is central to due care, skill and diligence expected of company directors and officers.
3. In line with the sentiment of the Operational Resilience Policies, organisations should **expect and anticipate that incidents will happen;** it is not a case of if, but when. This requires organisations to shift their mindset to consider not just risk but also resilience. Rather than focusing on reducing the likelihood of incidents and disruption, they should also invest in being able to respond and recovery quickly.
4. A failure of imagination when identifying the worst-case scenarios for your organisation may be costly. Many firms when developing scenarios do not assume operational outages longer than 24-48 hours, as they do not have an example of an internal incident that has exceeded this period. **Look outside your organisation to your competitors and to other sectors for inspiration.** Cyber-attacks that grind organisations to a halt for weeks, even months, do happen and are no longer unthinkable. The effects of climate change and heightened temperatures have caused data centre outages even for global Cloud providers. The lasting impact of COVID-19 lockdowns continues to cause significant supply chain challenges for all sectors. Economic headwinds have put many small independent organisations out of business when coupled with the impacts of Brexit and the Pandemic.
5. Many organisations' tend to focus on technical recovery during incidents ultimately aiming to identify and rectify the root cause. Whilst this is a critical part of responding to the incident, organisations should also have colleagues **focused on mitigating the customer impact of the incident** with an eye to impact tolerances and intolerable harm, especially in those incidents that are complex and likely to cause extended disruption. This requires organisations to proactively identify the key data they would use to determine customer impact and make this data readily available in an incident. Proactive communications and treatment strategies are key to managing customer sentiment and reaction.
6. **Collaborative testing with critical suppliers** provides a safe space to understand roles and responsibilities, reduce the number of assumptions made by both parties and identify gaps in response and recovery strategies. The traditional supplier assurance processes focused on Business Continuity and Disaster Recovery tests that do not provide sufficient confidence in supplier's resilience, especially when those suppliers supply multiple services to different parts of your organisation.
7. Understanding critical assets should not stop at those critical for business as usual. **Identify your third parties, technology and people critical to response and recovery.** If they are not involved in the day to day running of your operations, ensure that precious time isn't wasted during an incident getting individuals vetted, remote access for third parties established (and tested) and contracts including roles and responsibilities in place.
8. **Embed scenario testing into existing Change processes and lifecycles.** Functional, non-functional and user acceptance testing are critical and arguably the only way to validate performance, resilience, and capability. Whilst test environments can be both complex and costly, relying solely on a compliance-based approach focused on control testing in place of end-to-end testing will leave you exposed to unanticipated disruptions.