NHSBT Board Meeting
30 May 2019

ICT Update

1. Status – Official

2. Executive Summary

This paper provides an update on ICT, setting out:

- the position in January 2019, specifically NHSBT's key technology risks
- progress made, and actions taken since then
- a forward plan of the work required to mitigate these risks, and the 'anticipated' implementation timetable
- the delivery approach, including where support will be needed and how we will manage risks.

NHSBT is currently sitting on several major technology risks which have become clear since beginning my interim role in January 2019:

- significant technology skills and capability have been lost over recent years;
- critical infrastructure has received insufficient investment, resulting in poor performance, and ultimately poor user experience in key areas (e.g. workspace, G Drive);
- non-delivery of CSM has exacerbated an already fragmented solutions architecture and increased the total cost of systems ownership;
- there are several cyber security gaps, and risk has not been reduced to an acceptable level;
- the operating model is confused, with significant overlaps and gaps, and increasing year on year ICT costs.

These risks and the initial position are described further below.

Good early progress has been in made, both in terms of addressing several pressing issues, and in terms of understanding and building consensus on how to mitigate the significant risks outlined above.

Notwithstanding the good initial progress that has been made, the most significant work to be done to address the risks outlined remains. This is not just about fixing the basics – a major change programme is needed within ICT over the next 18-24 months, which will require significant investment in:

- infrastructure;
- cyber security;

- third-party support (Solution Strategy, Data Centre, Application Migration);
- re-structuring costs.

However, this investment is essential in building the capability, infrastructure and solutions that we will need to support NHSBT's ambitions moving forwards.

Key elements of this forward plan are described below - a high level 'anticipated' timetable is appended

3. Action Requested

The Board is asked to review and feedback on:

- **the initial position;**
- **progress made to date;**
- **the 'anticipated' forward plan for the work that has been agreed with the Executive;**
- **the proposed delivery approach.**

4. Initial Position

NHSBT is currently sitting on several major technology risks which have become clear since beginning my interim role in January 2019:

- significant technology skills and capability have been lost over recent years;
- critical infrastructure has received insufficient investment, resulting in poor performance, and ultimately poor user experience in key areas (e.g. workspace, G Drive);
- non-delivery of CSM has exacerbated an already fragmented solutions architecture and increased the total cost of systems ownership;
- there are several cyber security gaps, and risk has not been reduced to an acceptable level;
- the operating model is confused, with significant overlaps and gaps, and increasing year on year ICT costs.

These risks and the initial position are described further below.

People

People risk was at the top of the initial agenda; key resources, skills and capabilities had been lost through the life of the CSM programme, and the Chief Digital Officer and one of the most senior members of the ICT Senior Management Team (SMT) left the business at the end of 2018. Consequently, three out of six members of the initial SMT were on secondment/'acting up'.

Alongside this, ICT had also been largely unable to build the skills and capabilities envisaged in the original Platform Strategy, with much of the work done under CSM and ODT Hub being delivered by contractors or third parties.

Communication and engagement with the ICT SMT and wider ICT team was poor with considerable uncertainty and low morale evident. Resource constraints and key person risks were also evident.

Infrastructure
Progress on, and ultimately the halting of, the CSM programme exposed several key infrastructure risks, primarily insufficient focus, planning and investment in:

- hardware for key legacy applications;
- upgrades in local infrastructure;
- data centre facilities.

This has resulted in poor performance, and ultimately poor user experience in key areas (e.g. workspace, G Drive). Though these risks became clearer when CSM was halted, mitigating actions for these risks should have been considered before this.

Solutions
The halting of CSM left several residual solution issues:

- the technology portfolio has become more fragmented, and costly to support and maintain, as further applications had been added without any legacy decommissioning;
- the way forward, and future use of Pulse, CRM and other key applications was unclear;
- demand for change remains high, to deliver on requirements that were due to be met by CSM, and on the backlog of requirements that could not be met as all organisational focus was on CSM.
- Several relatively 'basic' business requirements remain unmet.

Cyber Security
NHSBT operates complex digital environments spread over numerous platforms, systems, user-bases, vendors, suppliers and locales. NHSBT currently implements protection using a range of mature and immature capabilities and resources. There has been limited single-point investment in cyber security – partly as cyber risk identification and organisational thinking has been immature. Developments in GDPR and DSPT also require NHSBT to evidence continual and higher levels of understanding and control of NHSBT's complex portfolio. Many gaps persist due to a lack of pro-active resource and supporting tooling to identify and eliminate/reduce threats to acceptable levels.

Operating Model
Several weaknesses and risks in the operating model were evident:

- a complicated organisation structure, with significant gaps, temporary moves/arrangements and overlaps
- fragmentation of technology decisions, accountability and supplier management
- point-based sourcing decisions, rather than any clear build/buy strategy

- significant differences in deliver methodology, processes, route to live and support models across the technology estate
- increasing resources and costs, without a clear understanding of, or choices, regarding the total cost of systems ownership.

5. Progress

Good early progress has been in made, both in terms of addressing several pressing issues, and in terms of understanding and building consensus on how to mitigate the significant risks outlined above.

People
This has been a key focus over the last few months, with extensive Senior Management Team and wider ICT team engagement and communication. Significant time has been spent on F2F and Skype sessions mixed with regular open and transparent team notes and Yammer posts. There have been no further senior resignations/losses since arrival. The team appear re-focused, and anecdotal, direct and 360 feedback from the SMT and the wider team suggest good levels of engagement and positive feedback on leadership approach and agenda. Work is also progressing in terms of performance and development conversations with some key members of the team. An induction plan has also been created for any new contractor/third party supplier/agency personnel coming onboard.

One of the three interim roles have now been filled. The other two remain on secondment, though we have started the recruitment process for one of the others, the AD IT Service and Operations.

Reducing key person risk and addressing resource constraints has also been a focus. Key person risk has not been significantly reduced (aside from stabilisation and engagement) as we have made limited recruitment and/or structural changes in the short term. We are taking steps to address resource constraints, but they have a significant lead time due to the lead time needed to recruit or procure external support.

Infrastructure
This has been a key focus over the first quarter, with significant emphasis on:
- the workspace remediation programme, where additional hardware is being introduced to improve workspace and pulse performance prior to the data centre move;
- incepting the local infrastructure programme covering a range of upgrades and improvements to telephony, site servers, key machines, the Filton LAN and the development of a partner portal (a secure platform for connectivity of 3rd party equipment across 10 key sites);
- shaping the case for the Data Centre programme – the outline business case is currently being developed.

Solutions

The initial focus here has been on safeguarding our critical legacy applications, particularly Pulse. Significant effort has been expended on re-building relationships with Savant. In addition, as mentioned above, a key focus of the workspace remediation project is on safeguarding Pulse performance.

Contract extensions (final year of current contract) have also been put in place with Savant for Pulse and Hematos.

Focus here has also been on framing the approach and proposal for the Technology (Solutions) Strategy work for Blood. A Statement of Requirement for support was issued in April. Similar work is also being done with ODT, focused on the affordability and total cost of ownership of the ODT solution set.

Cyber Security
A clear view of the cyber risks has now been established and a phased, risk-based approach to addressing the cyber challenge has been developed; this was approved by the Executive and the GAC in March.

The first steps that were approved are underway:

- securing an external contract to ensure that the GBEST Threat Intelligence information is constantly refreshed ensuring that new threats are identified and that NHSBT's external footprint is constantly reducing;
- appointment of a new Information Security Manager to improve the pace of response on outstanding GDPR & DSPT gaps and analyse priority risks, and potential solutions;

though these are subject to procurement and recruitment lead times.

Operating Model
This area has not been a major focus over the last few months, though some initial work has been done to:

- Understand the current operating model – gaps, overlaps, issues and risks
- Understand the cost base
- Frame the work that is needed to develop a new operating model.

6. Forward Plan

Notwithstanding the good initial progress that has been made, the most significant work to be done to address the risks outlined remains.

This is not just about fixing the basics – a major change programme is needed within ICT over the next two years, which will require significant investment, particularly in terms of:

- infrastructure;
- cyber security;
- third-party support (Solution Strategy, Data Centre, Application Migration);
- re-structuring costs.

However, this investment is essential in building the capability, infrastructure and solutions that we will need to support NHSBT's ambitions moving forwards.

Key elements of this forward plan are described below, broken down across the five key areas. A high level 'anticipated' timetable is appended. Where possible, recruitment and/or procurement lead times have been reflected in the timetable.

People
There will be a continued focus on communication and engagement with the SMT and wider ICT team. Recruitment is also being progressed in key areas, most notably the recruitment of the AD for IT Operations mentioned above which will help strengthen the SMT.

We are also taking steps to source additional capability and capacity where required, this includes:

- putting in place preferred supplier arrangements for contract resources – sourcing contractors currently is not straightforward and is largely dependent on arrangements that were only put in place for CSM;
- appointing a resource augmentation partner for Technology Services resources – a Statement of Requirement has been issued and we expect a partner to be on board by June.

Infrastructure
Driving the delivery of workspace remediation and the local infrastructure programme (encompassing telephony upgrades, partner portal, site server and key machines) are key elements of the forward plan, and both will help mitigate current risks.

However, the data centre programme is critical to reducing infrastructure risk to an acceptable level – until this programme is delivered, ageing infrastructure that supports our legacy applications will continue to pose significant risk to the organisation.

We are currently in the middle of a tender process to engage client-side support for the data centre programme to:

- review and confirm the data centre strategy and outline business case;
- develop the detailed hardware specifications and requirements to support the procurement of new equipment, migration support and ongoing data centre management services;
- to work with us to formulate the detailed business case, which will need to be approved before contracts can be awarded.

We have decided to seek this support to supplement internal capability and capacity - without this, much of our technology services resource would have to be fully assigned to the Data Centre programme. We expect to award the contract for this client-side support in May.

In terms of Board engagement, we are aiming to bring:

- high-level approach to Board in July;

- full OBC to Board in September;
- full DBC (and proposed contract awards) to Board in May 2020.

Solutions
The inception of a technology strategy project was agreed at the March Board encompassing:

- confirmation of broad Blood business requirements (current and emerging);
- assessment of current Blood applications/solutions and their capability to meet these requirements – as previously proposed, this assessment will look at whether we could and/or should re-use any of the code developed within CSM;
- assessment of alternative Blood applications/solutions;
- confirmation of recommended solutions architecture (middleware and integration approach);
- confirmation of infrastructure/hosting strategy (cloud, on-prem, hybrid);
- consideration of broader Office365 business implementation and ways of working
- consideration of the operational support needed and the total cost of ownership of solutions

A Statement of Requirement for this work has been developed, and was issued in April. We expect the contract to be awarded and work to begin on 5th July, with work to be completed by the end of October. The detailed technology roadmap and resulting projects to migrate to target solutions will be developed after this.

Later this year we will also go out to tender for support to Pulse and Hematos, where current contracts are in their final year. New contracts need to be in place by March 2020, and will be required (though proposed contract term may change) regardless of the outcome of the technology strategy.

Cyber Security
A rolling programme of cyber improvements is currently being developed. For each element of the rolling programme, its' options, costs and benefit, will be developed for review by the Executive and the GAC a bi-monthly basis. Regardless of the options that are chosen, we anticipate that significant investment will be required in cyber security over the next 18 months.

Operating Model
An operating model review is currently being shaped; the review is expected to encompass:

- ICT remit
- Structure, roles and responsibilities/accountabilities
- Service capabilities and maturity
- Resource and process gaps (e.g. Service Design, Digital, Data)
- Relationship management/Business Partnering
- Opportunities for improvement

In addition, the review will also need to consider ICT's role in the broader change process (portfolio management and prioritisation) as some

rationalisation is needed across current BTS (project) Quality and ICT transition processes. We have not fully scoped and sized this project, so do not have a considered view of anticipated costs but would expect some re-structuring costs to be incurred.

7. Delivery Approach

Key elements of the delivery approach for this work are:

- putting in place arrangements for resource augmentation in key areas to allow these ICT changes to be progressed alongside a significant delivery portfolio for the organisation;
- securing third party support in key areas (data centre, solutions strategy and operating model);
- active engagement with internal audit, in framing, and measuring progress, against the agreed agenda.

We are also investigating options for independent QA and delivery assurance.

In all cases, we are trying to ensure that key CSM lessons are learned, particularly ensuring that we have the skills and capabilities (Accountable Executive, Subject Matter Experts, Project/Programme Management) needed to be confident of delivering each piece of work, before we start it.

8. NED Scrutiny

Helen Fridell, Jeremy Monroe

9. Appendices

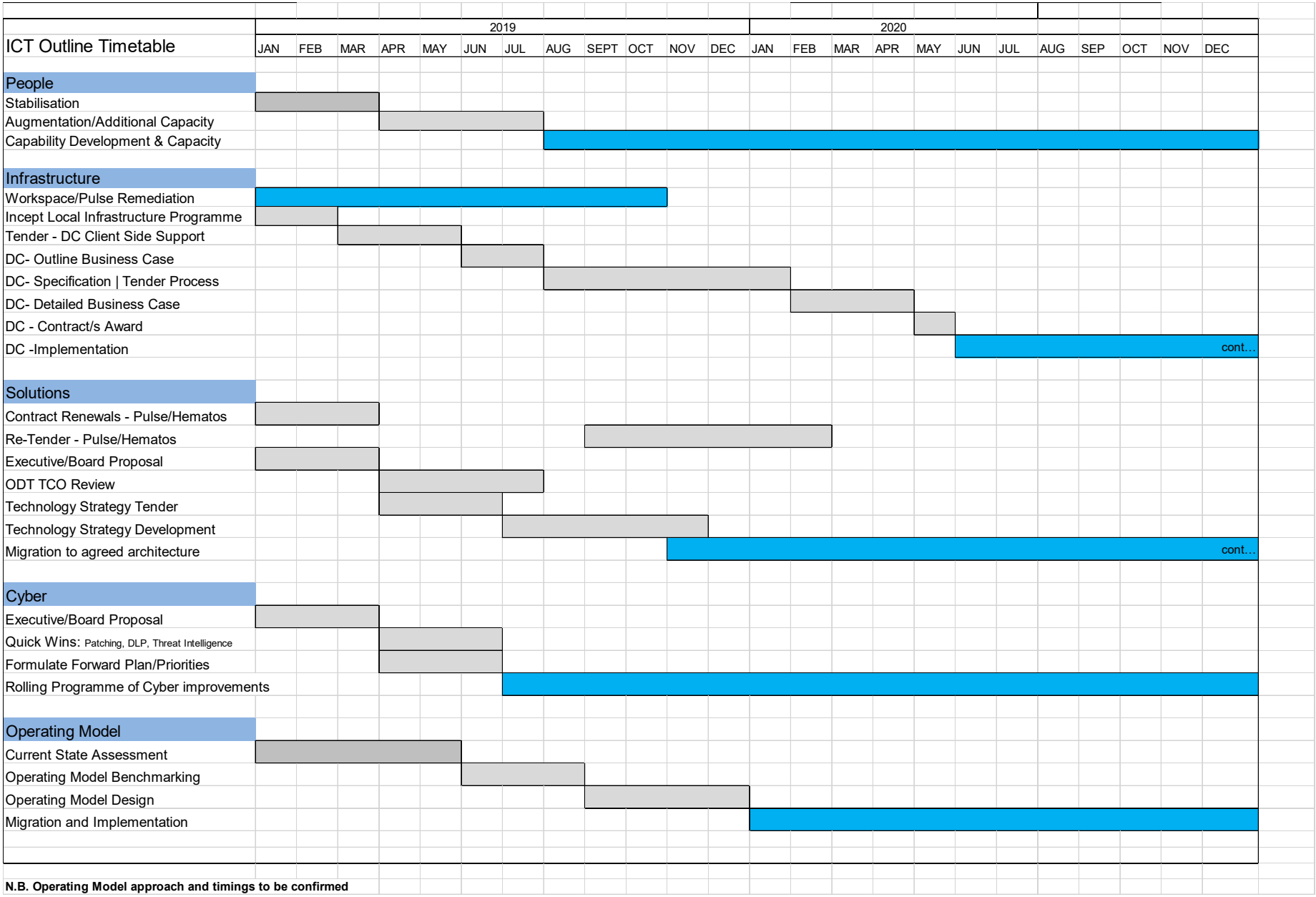
ICT ‘Anticipated’ Timeline.

Author

Brian Henry, Interim Technology Director

Responsible Director

Brian Henry, Interim Technology Director



N.B. Operating Model approach and timings to be confirmed