

Audit Committee

Monday 30 January 2023



Report of: Tim Borrett, Director: Policy, Strategy and Digital

Title: Digital Transformation change and governance update

Ward: Citywide

Member Presenting Report: N/A

Recommendation

Note the report and steps being taken to address the root causes of low and limited assurance for IT governance.

Summary

In recent years the council has undertaken major digital transformation activity to modernise, improve and secure its IT estate and operations. Whilst much progress has been made, seven internal audits of transformation and associated IT issues have provided only Limited Assurance, highlighting gaps in several areas. These audits and issues have been published and discussed previously. This report summarises activity undertaken since new leadership arrangements took effect in April 2022, plus in-flight work and future plans to address the root causes of this limited assurance.

The significant issues in the report are:

- The root causes of assurance issues most often relate to the themes of Governance; Project Planning and Management; Policies and Procedures; Technical Security Controls; Decentralised IT Functions.
- These are all well-known and recognised by management, with much improvement work already undertaken and more planned over the coming 12-18 months.
- Major changes and in-flight improvements since the focus of previous audits include: new Digital Strategy; updated Digital Transformation Programme with full Programme Management support and embedded Internal Audit assurance; procuring a single Digital Strategic Partner; new approved projects to make further improvements in the digital estate and its security; a centralisation of IT, applications and digital support activity; a pending root-and-branch restructure of the Digital Transformation service.

Background and Context

1. Since April 2021, Internal Audit has undertaken seven IT internal audits and three follow up reviews. Six of these (85%) were assigned a ‘low’ or ‘limited’ level of assurance rating. This has led to a retrospective independent analysis of the reviews to identify root causes of the issues raised, in support of existing work and planning of further activity to enhance the control environment and improve performance.
2. Across seven IT internal audit (ITIA) reports previously presented to this Committee, there were 36 findings which have been classified into 15 risk areas. Analysis has examined the number of times these risk areas appeared in the seven ITIA reports. These 15 risk areas are then grouped into five common themes: Governance; Project Planning and Management; Policies and Procedures; Technical Security Controls; Decentralised IT Functions.
3. The seven audits were:

Review Title	Date	Assurance Rating
Cyber Security (BCC)	May 2021	Limited
IT Transformation Programme Review (ITTP)	May 2021	Limited
Cyber Security BCC Group Companies (controls relevant to BCC arrangements)	October 2021	Limited
IT Resilience	October 2021	Limited
Digital Transformation Programme Governance (Tranche 1)	April 2022	Reasonable
IT Governance Review	May 2022	Limited
Cloud Control Review	August 2022	Limited

Across the five common themes:

- 7 of 7 audits identified risks and issues relating to Governance
- 7 of 7 audits identified risks and issues relating to Project Planning and Management
- 5 of 7 audits identified risks and issues relating to Policies and Procedures
- 4 of 7 audits identified risks and issues relating to Technical Security Controls
- 3 of 7 audits identified risks and issues relating to Decentralised IT Functions

Root Causes

4. Across the five themes, the following root causes have been identified:

Theme	Description of key issue(s)	Root Cause
Governance	There was a lack of consistent oversight from the various committees and groups on IT-related processes.	An ineffective governance structure and lack of awareness of roles and responsibilities.
Project Planning and Management	Projects were not appropriately managed from planning stage to post-completion.	Lack of project management capability and capacity issues.
Policies and Procedures	Fit for purpose documentation was not available or not sufficiently updated to assist staff managing and operating the process.	Lack of monitoring controls and ownership and resourcing / capacity issues
Technical Security Controls	There were insufficient technical security controls in place to identify and prevent compromise of sensitive information and computer systems.	Lack of technical and cyber capability within the Council and a lack of collaboration between governance forums.
Decentralised IT Functions	There was a lack of a centralised approach to IT functions, impacting IT change management and IT resiliency.	Lack of governance oversight.

5. Whilst the themes are recognised and the majority of findings were accepted by management with remedial actions agreed, there are some important points of context to the findings and work to follow:
 - i. Much of the audit activity focused on activity during and shortly following major, complex change to the IT environment following a prolonged period of disinvestment in IT and technology.
 - ii. Many lessons were learned from this, including via Internal Audit activity, and have already been remediated. For example, full professional Project Management support from the council's Project Management Office was sought. It is notable that the only audit providing Reasonable Assurance was Digital Transformation Programme Governance (Tranche 1), which examined activity which followed this change.
 - iii. There have been some differences of professional view on the proportionality of some IA findings and suggested actions; for example, about whether it is proportional for an organisation of the council's size, with its increasingly limited resources, to invest in a fully fledged Security Operations Centre and meet other 'gold standards' for security, governance and assurance which would require substantial permanent investment.
 - iv. During the time of the audits and since, there have been no major IT outages or security incidents, and key corporate and line of business systems have all met targets relating to their availability.
 - v. Following the departure of the previous Director: Digital Transformation and with a need to reduce senior management cost, the former Chief Executive combined two Director roles to create Director: Policy, Strategy and Digital; with new leadership coming in to effect from April 2022.

Actions since April 2022

6. As new leadership took effect, many of the themes and issues raised in the Internal Audits were recognised and the former Chief Executive had formed a Digital Transformation Programme Board, chaired by the Cabinet Member and executive-chaired by the Chief Executive. This Board includes embedded Internal Audit assurance and representation from senior business users, Finance, Information Governance, Change Services, IT, Citizen Services, Procurement, and Internal Communications. It continues to operate to lead what is now the council's single Digital Transformation Programme (DTP), which was approved by Cabinet in July 2022. The Board is now chaired by the Director: Policy, Strategy and Digital.
7. A complete refresh of the council's Digital Strategy was undertaken, providing a high-level strategy and action plan which was developed alongside external experts and with co-production alongside a range of council services and clients. This represents the top of the council's policy and strategy hierarchy for IT and Digital, and it was approved by Cabinet in June 2022.
8. A Full Business Case (FBC) was developed for the single Digital Transformation Programme, consolidating legacy projects under DTP Board governance and establishing a new set of projects required to progress digital transformation efforts, remediate known issues, undertake 'must do' work to maintain and modernise the IT environment. This FBC included inter-project dependency mapping, completing a previous audit recommendation. The Programme includes £18m of investment over three years and was approved by Cabinet in July 2022. All DTP projects produce monthly highlight reports which are reviewed by DTP Board, consolidated (with all Change Services project highlight reports) and provided to Executive Director Meetings and Corporate Leadership Board.
9. A project within the Digital Transformation Programme sought to procure a single Digital Strategic Partner for the council, establishing a five-year contract with a major IT and digital supplier to provide ongoing strategic advice, support and challenge; proactive input to IT and digital policy and strategy; and a full range of IT and digital professional skills which can be drawn upon to support the council's limited capacity and its range of IT and digital change projects. This project has proceeded on-course and a supplier is anticipated to be appointed in February 2023.
10. As part of the council's Common Activities Programme, staff roles across the organisation have been

assessed and 35.6FTE decentralised IT-related roles have been centralised. These predominantly related to Applications Support for major line of business IT systems operated in Housing, Finance and Social Care services.

11. A restructure of third tier management arrangements for Policy, Strategy and Digital has been undertaken, reshaping leadership of the division and establishing a new role of Head of Digital Strategy and Transformation. This role is currently being recruited, with a job description which aligns closely to the common themes identified in the audits:
 - i. To lead development, delivery and evaluation of the council’s Digital Strategy and any associated transformation programmes, projects or activity hosted within the Digital Transformation service.
 - ii. To develop, maintain and ensure council-wide implementation of a coherent, well governed IT policy framework, including the provision of reasonable assurance and evidence of its efficacy.
 - iii. To act as principal contract manager and lead officer for the council’s Digital Strategic Partnering arrangement, ensuring it is highly effective, offers best value and realises benefits in delivering demonstrable digital transformation.
 - iv. To provide subject matter expertise in regard to all facets of digital transformation and IT, including the technical, governance and cultural aspects of providing a modern digital transformation function.
 - v. To provide inclusive, collaborative leadership in managing complex relationships across the breadth of services being delivered by Bristol City Council, including via a formal IT Business Relationship Partnering service. Within this, ensure the systematic and effective enacting of digital and IT policy, strategy and standards across diverse business areas outside of the post-holder’s direct hierarchal control. Support all areas of the organisation in relation to annual service planning, identifying ongoing or future requirements for digital and/or IT products and services which are compatible and compliant with the council’s Digital Strategy and related policies.
 - vi. To lead significant improvement in the council’s governance surrounding IT, including compliance in contracting and procurement, management of risk, and approach to Line of Business System management. This includes accountability for exercising significant, effective influence across the council including areas outside of the post-holder’s direct hierarchal control.
 - vii. To work in close partnership with the Head of IT Operations to ensure a seamless, one-team approach to operationalising IT and digital strategy and policy, and to provide visibly joined-up leadership and management across the Digital Transformation service.

12. A full restructure of the Digital Transformation service is currently in development and will establish the Head of Digital Strategy and Transformation’s department, including investment in roles relating to the root causes of low and limited assurance. This will be consulted upon with staff and Trade Unions imminently, and subject to consultation feedback and onward processes to appoint staff, will take effect by the end of Q1 2023/24. It should be noted that due to the council’s significant financial challenges this restructure does not represent overall investment in the service, in fact it will aim to make major financial savings up to circa £1m which will inevitably require challenging decisions about which elements of the service are reduced, removed or otherwise changed to enable it to function within its new budget envelope. In this context, our continued Digital Transformation Programme is critical, as it will remove the need to service a ‘hybrid’ IT environment which has some modernised, cloud-based infrastructure whilst still maintaining traditional on-premises hardware. If the financial savings target is not possible to safely achieve, it will require substitution and work is already underway to scope contingency options including further reviews of third-party spending in addition to one

already undertaken within the Digital Transformation Programme.

13. In addition to the largely strategic work noted above, several operational changes have been made to improve governance, encourage a ‘one council’ culture and mitigate risks. These include:

- i. Re-instating regular senior and operational meetings with the Procurement & Contract Management Service to review procurement needs and contract planning.
- ii. Senior IT representation at Information Governance Board.
- iii. Ensuring major IT change projects run outside the Digital Transformation service are overseen by Digital Transformation Board, e.g. Housing Major Systems replacement.
- iv. Re-instating links to the Connected Bristol service to ensure awareness and alignment of internal IT and digital work with outward-facing work related to the council’s BNET network, CCTV, Operations Centre etc.
- v. Surveying Heads of Service across the council about Business Continuity and IT Resilience, drafting a wider-reaching ICT Response and Recovery Plan.
- vi. Reviewing IT contract register details and working with the Procurement & Contract Management Service to strengthen this.
- vii. Newly established regular Divisional Management Team oversight of key IT operational decisions and minor works.

Proposals

Looking ahead, much work will continue to strengthen the control environment for Digital Transformation over the coming 12 – 18 months, with much of the work due to be complete and starting to realise benefits sooner. This includes:

- i. Completing, launching and embedding the new Digital Transformation service structure; potentially providing improved capacity and skills relating to the key risk areas identified by IA.
- ii. Appointing the Digital Strategic Partner and reviewing the IT and digital policy and strategy framework alongside them.
- iii. Continuing the Digital Transformation Programme, increasing security and resilience with further transition to the Cloud and optimisation of this environment, including actions to address the findings of the Cloud Security audit. Other work in the programme related to the root causes will help the council achieve National Cyber Security Centre ‘Better’ standards for cyber security, and improve project management capabilities with a Project Portfolio Management Tool.
- iv. A review of the IT and digital governance framework to ensure appropriate Boards, group membership, terms of reference and onward reporting within the council’s governance hierarchy are in place and working effectively. This will be complemented by the work on policy refreshes and testing, ensuring that where the council is making mindful risk-based decisions relating to issues like security and resilience, these are recorded in policy, properly assessed and approved with the reasoning explained; rather than relying on custom-and-practice or uncodified policy.
- v. Working alongside Information Security colleagues and a Microsoft partner to improve certain elements of our cyber security. This will start imminently, with a Microsoft partner providing an analysis of our Security Event and Incident Monitoring toolset, to be followed by work to implement any recommendations arising.

In addition (or in some cases as part of) these actions, there will be continued delivery of actions already agreed in response to audits and the following actions will also be added:

Theme	Actions
Governance	<ol style="list-style-type: none"> 1. Per above, revisit the Terms of References of governance committees and groups to confirm the coverage of each group. Review attendance of the groups to ensure they have required

	<p>capability and capacity to provide necessary challenge and oversight.</p> <ol style="list-style-type: none"> 2. Following this, identify dependencies between the governance groups in the Terms of References and subsequently the roles and responsibilities needed to deliver requirements. 3. Ensure appropriate training is provided, where required, to members of the governance groups. 4. Sign off the refreshed Terms of References at the appropriate level.
Project Planning and Management	<ol style="list-style-type: none"> 1. Continue to ensure projects have sufficient resource and project leads and support staff have the required project management skills to deliver large scale, complex IT projects. This will include drawing upon Digital Strategic Partner resource. Any absence of sufficient resource and skills will continue to be escalated to the appropriate Project Board and, where required, Programme Board, to be recorded in the risk register and considered. 2. Management will consider the use of programme assurance partners for the largest projects to help to minimise delivery failure. This will be case-by-case given existing plans for a DTP Benefits and Assurance role; and the support and challenge available from both the Digital Strategic Partner and the council's internal project management governance framework; which has already been found to provide Reasonable Assurance. Within this, all DTP projects go through a process of internal assurance at project gateways, whereby business cases are peer-reviewed by professional project managers who are independent from the Programme, with assurance ratings reported to the Board to aid decision-making.
Policies and Procedures	<ol style="list-style-type: none"> 1. As part of the previous described review of the policy and strategy framework, a mapping exercise will be undertaken to clearly understand and define which policies should be reviewed and approved by which committees / groups, which will then be agreed by the governance committees and groups. 2. Policies will be added to the council's overarching policy library and framework, ensuring they are tracked and benefit from appropriately scheduled review and approvals. 3. Any capacity (insufficient staffing) issues faced by IT Services and IG team will be escalated to the appropriate governance group via management reporting and/or risk register. The impact of this should be clearly identified and reported to the governance groups. 4. If more roles are required, clear business cases will be generated to demonstrate the need, urgency and cost benefit analysis of the roles required; and consideration given to utilising temporary or project-based reach-back capacity from the Digital Strategic Partner.
Technical Security Controls	<ol style="list-style-type: none"> 1. Security will be the first area to be reviewed within the policy and strategy framework, and any gaps addressed with appropriate creation or updates of Information Governance and/or Cyber Security policy or strategy; with these providing priorities for specific focus.

	<ol style="list-style-type: none"> 2. We will review past work to risk assess with relevant members of IT and across the council key technical security risks, ensuring this is up-to-date and provides a clear picture of risk and priorities. 3. This will inform evaluation of our security controls and the design of the controls, complementing work within the DTP End User Compute project to achieve the NCSC Better State standard of security. 4. Regular checks will be established to assess the operating effectiveness and continued relevance of the controls. The regularity of this needs to be considered once risk levels are reviewed, with the response and resourcing be proportionate to the risk. 5. Workforce planning activity in Digital Transformation and Information Governance services will consider the need for new or improved capabilities or growth; including building the required skills for newer and evolving areas of the council’s IT and digital estate, such as Cloud. Any need for growth needs to be carefully considered and contextualised within the council’s wider budget pressures and need to provide critical life-and-limb services.
Decentralised IT Functions	<ol style="list-style-type: none"> 1. As part of the previously noted review of governance arrangements, we will consider if and how oversight is needed and/or available of all IT and digital systems and processes, including those dispersed around the council. 2. We will build on recent operational improvements and review and establish (where necessary) processes for regular collaboration between the central IT and divisional IT-related functions. (Noting most IT-specific functions are now already centralised). 3. We will review arrangements to ensure service areas and decentralised functions have clear ownership and understanding of their roles and responsibilities for any IT or digital systems or contracts they own. 4. We will consider with our Digital Strategic Partner whether our strategy, service plans and risks require further consideration of fuller centralisation of IT and digital activity; noting this may come with significant change cost and growth, as much activity in the business is undertaken as opportunity cost by managers.

Timescales for the above actions cannot be confirmed until we have certainty about:

- Successfully appointing our Digital Strategic Partner
- Successfully appointing a Head of Digital Strategy and Transformation
- Consulting upon and successfully implementing (including any recruitment to) the revised Digital Transformation service structure

It is not anticipated that the full scope of actions could realistically be completed in less than 18 months from April 2023, however some would move more quickly, and incremental improvements are anticipated throughout the improvement journey.

Consultation

1. Internal

- SIRO (Senior Information Risk Owner) [Director: Legal and Democratic Services]
- Director: Workforce and Change
- Head of Information Governance
- Head of IT Operations
- Digital Transformation Programme Manager
- Resources EDM
- Chief Executive
- Cabinet Member - Finance, Governance, Property and Culture

2. External

Not applicable

Appendices:

None

LOCAL GOVERNMENT (ACCESS TO INFORMATION) ACT 1985

Background Papers:

None