AGENDA FOR

AUDIT COMMITTEE

Contact:: Andrea Tomlinson
Direct Line: 0161 253 5399
E-mail: a.j.tomlinson@bury.gov.uk
Web Site: www.bury.gov.uk

To: All Members of Audit Committee

Councillors : S Butler, U Farooq, I Gartside, M Hayes, B Mortenson, J Rydeheard, M Smith, M Whitby (Chair) and S Wright

Dear Member/Colleague

Audit Committee

You are invited to attend a meeting of the Audit Committee which will be held as follows:-

Date:	Thursday, 30 September 2021
Place:	Town Hall
Time:	7.00 pm
Briefing Facilities:	If Opposition Members and Co-opted Members require briefing on any particular item on the Agenda, the appropriate Director/Senior Officer originating the related report should be contacted.
Notes:	

AGENDA

1 APOLOGIES FOR ABSENCE

2 DECLARATIONS OF INTEREST

Members of the Audit Committee are asked to consider whether they have an interest in any of the matters on the agenda and, if so, to formally declare that interest.

3 MINUTES OF THE LAST MEETING *(Pages 5 - 14)*

The Minutes of the last meeting of the Audit Committee held on 21st July 2021 are attached.

4 MATTERS ARISING

5 INFORMATION GOVERNANCE PROGRESS REPORT *(Pages 15 - 82)*

A report from the Deputy Chief Executive is attached.

6 MAZARS AUDIT STRATEGY MEMORANDUM *(Pages 83 - 118)*

Report attached.

a REDMOND REVIEW

The Chair will provide a verbal update.

7 RISK REGISTER UPDATE *(Pages 119 - 138)*

A report from the Councils Section 151 Officer is attached.

8 COVID GRANTS FINANCIAL SUPPORT *(Pages 139 - 148)*

Report is attached for information.

9 INTERNAL AUDIT UPDATE *(Pages 149 - 180)*

A report from the Acting Head of Internal Audit is attached.

10 EXCLUSION OF PRESS AND PUBLIC

To consider passing the appropriate resolution under Section 100(A)(4) of the Local Government Act 1972 that the press and public be excluded from the meeting during consideration of the following items of business since they involve the likely disclosure of the exempt information stated.

11 INTERNAL AUDIT PROGRESS REPORT *(Pages 181 - 342)*

A report from the Acting Head of Internal Audit is attached.

12 INTEGRATED COMMUNITY EQUIPMENT STORES *(Pages 343 - 372)*

Will Blandamer Executive Director Strategic Commissioning and Adrian Crook Director Adult Social Care Services and Community Commissioning will be in attendance. Internal Audit report attached.

13 MEMBERS' FEEDBACK

The Chair will provide a verbal update.

This page is intentionally left blank

Agenda Item 3

Minutes of: **AUDIT COMMITTEE**

Date of Meeting: 21 July 2021

Present: Councillor M Whitby (in the Chair)
Councillors S Butler, I Gartside, M Hayes, B Mortenson, J Rydeheard, M Smith and S Wright

Also in attendance: Karen Murray – Mazars
Amelia Payton - Mazars

Public Attendance: No members of the public were present at the meeting.

Apologies for Absence: J Dennis and Councillor U Farooq

AU.1 APOLOGIES FOR ABSENCE

AU.2 DECLARATIONS OF INTEREST

Councillor Steve Wright declared a personal interest in any item relating toschools in the Borough as his wife is employed at a local school.

Councillor Sam Butler declared a personal interest in any reference to Homes England as his Fiancée was employed by them.

AU.3 MINUTES OF THE LAST MEETING

It was agreed:

That the Minutes of the last meeting held on 18 March 2021 be approved as a correct record and signed by the Chair.

AU.4 MATTERS ARISING

There were no matters arising

AU.5 DRAFT STATEMENT OF ACCOUNTS 2020/21

Sam Evans, Joint Chief Finance Officer presented a briefing note setting out the unaudited Statement of Accounts for the 2020/21 financial year. The report highlights the overall financial position for the year.

Whilst there is no longer a requirement to present the unaudited accounts to Members before the external audit process commences, the Council has continued this practice as it gives Members early notification of the financial outcome of the previous financial year and is considered to be good practice.

There is a requirement to obtain certification of the accounts by the responsible financial officer, for the Council this is the Executive Director of Finance and S151 Officer.

The accounts will be available for public scrutiny from 2 August to 13 September. This will be advertised on the Council's website. The unaudited accounts will be placed on the Council's website on 31 July in line with the Government's policy of increased transparency in the public sector. And the accounts will be subject to external audit.

The style and format of the accounts is largely prescribed by the CIPFA Code of Practice (The Code). Audit Committee should assure themselves that the Narrative Report is consistent with the core financial statements.

The Statement of Accounts for Bury Council comprises of:

- A narrative statement by the Executive Director of Finance and S151 Officer
- The statement of responsibilities for the accounts
- The core financial statements, comprising:
- The movement in reserves statement
- The comprehensive income and expenditure statement
- The balance sheet as at 31 March 2021
- The cash flow statement
- The notes to the core financial statements
- The Housing Revenue Account
- The Collection Fund
- The Group Accounts

It was explained that Elected members are not expected to be financial experts, but they are responsible for approving and issuing the Council's financial statements. In doing this they are playing a key role in ensuring accountability and value for money are demonstrated to the public. However, local authority financial statements are complex and can be difficult to understand: they must comply with CIPFA's Local Authority Code of Practice, which is based on International Financial Reporting Standards and also the accounting and financing regulations of central government

This covering report explains the key features of the primary statements and notes that make up the 2020/21 Statement of Accounts. The narrative statement provides further information on the key issues for the benefit of readers of the statements.

Sam explained that the narrative statement provided information on the financial statements and gave an explanation of key events and their effect on the financial statements. It was reported that the information in the narrative statement is consistent with budget information provided during the year and reconciles to the year-end financial position reported to Cabinet on 21st July 2021.

Those present were given the opportunity to ask questions and make comments and the following points were raised:-

- Councillor Butler referred to the Government grants that had been

received in relation to COVID and asked whether this was making the accounts look better than had they not been received.

Sam confirmed that this was the case and that the Council would be working to build back the reserves that they would be using to support loss of income particularly in relation to the airport dividend.

- Councillor Butler referred to the Local Government Pension Scheme and the fact that this was a big liability and asked whether the scheme was still taking new members.

It was reported that this was the case.

- Councillor Rydeheard referred to the £12m use of reserves and asked whether this was sustainable.

Sam explained that this was not sustainable and that a 3 year programme was in place to get the Council back into financial balance.

- A question was asked with regard to the school reserves being down £21.5m through the DSG.

Sam reported that the Council was fortunate to secure funding through the Safety Valve Project with the Department for Education. This is a 4 year programme of work that would look at getting back into financial surplus by 2024/25 year end.

- Councillor Gartside explained that before consolidated reserves there were the minimum level of reserves. Councillor Gartside asked whether a minimum figure of reserves would be set in relation to risk management and the risks set out within the Risk Register.

Sam explained that this would be part of the Medium Term Financial Strategy which was one of the documents that was currently undergoing a refresh. This was due to Sam being very new to post.

- Councillor Rydeheard asked when the COVID grants would be expected to be used by.

Sam reported that the Council had up to the end of the 2021/22 financial year. Some of the grants already had commitments against them but not all were committed at the current time.

- Councillor Hayes referred to the Business Retention Pilot which allowed GM authorities to retain 100% of the business grants it collected. Councillor Hayes referred to the statement that this would change to

75% and asked if it was known when this would happen.

Sam explained that the 75% retention was initially planned to commence in 2021/2022, but this was delayed so that GM Authorities continued the 100% retention in 2021/2022. It was also explained that this was under constant review to ensure that it meets with the needs of localities.

- Councillor Gartside explained that the Council used to have Star Chambers where the heads of departments attended and were asked to account in relation to overspends.

Sam explained that this was a monthly item on the agenda at the Executive Team Meeting. There was also a Finance specific Overview and Scrutiny Committee being established.

- Councillor Rydeheard referred to the receipts from sales and assets and asked why the value was significantly higher than the forecast in this area.

Sam explained there were capital programme receipts that would be built into the reports in future but hadn't been included as yet.

- Councillor Whitby asked whether the cost of Covid would be met through government grants.

Sam stated that not all costs would be funded via grants and there would be a shortfall.

Delegated decision:

That the Draft Statement of Accounts be noted.

AU.6 EXTERNAL AUDITOR'S ANNUAL AUDIT LETTER 2019-20

Karen Murray from the External Auditors Mazars presented the Committee with the External Auditor's Annual Letter. The report had been presented to the Committee at it's meeting in March and this was now the final version. The report confirmed the completion of the work carried out by Mazars for the 2019/2020 audit year and had been issued following certification of the whole of Government Accounts return.

The report would be available for public access on the Council website.

Mazars had issued an unqualified opinion on the Council's accounts on the 25 March and the work on the whole of Government accounts return was completed on 21 June 2021.

Those present were given the opportunity to ask questions and make comments and the following points were raised:-

- Councillor Gartside referred to weaknesses in the Governance arrangements and asked what the current view of the External Auditors was.

Karen reported that the work had been carried out in relation to governance arrangements, but Mazars had not been able to confirm that arrangements had been embedded in the day to day work of the Council. There was nothing that External Auditors were concerned about, and work would be carried out during the course of the 2020/2021 audit to confirm this.

Delegated decision:

That the report be noted.

AU.7 EXTERNAL AUDIT PROGRESS REPORT

Karen Murray presented the Committee with an update of the progress made by Mazars in relation to the work for the 20/2021 financial year. The report had two purposes, firstly to ensure that the audit work is on track and secondly to ensure that the Committee were satisfied with the governance of the council.

Karen reported that the External Auditors would not be able to deliver the audit work in line with the deadline of the end of September as set out in the regulations, but would be reporting back to the Committee in November.

A notice would be published on the Council website which would state that the work was ongoing, as long as this was done then the Council will have complied with its statutory duties.

As at end of June 2021 there were still 100 authorities who were waiting on their 2019/2020 accounts to be audited and work hadn't even started on their 20/2021 accounts.

Karen referred to the work that was ongoing in relation to the findings of the Redmond Review and how this would inform the audit regime going forward.

Karen also referred to other information that was provided in section two of the report that set out the guidance from the National Audit Office relating to changes in respect of the VFM that the external auditors carried out and how from 2021the new code of practice will direct the external auditors to provide a commentary and not give a conclusion as previously.

Karen also referred to the Government Office report on the response to the pandemic and explained how this was useful as it set out the challenges that had been faced and would be faced by local authorities and S.151 Officers going forward.

The Audit Strategy will be brought to the next meeting of the Audit Committee

Those present were given the opportunity to ask questions and make comments and the following points were raised:-

- Councillor Whitby stated that it was disappointing that the work would not be completed in the required timescales. Councillor Whitby referred to the work that had been carried out by the Council Officers.

- Councillor Gartside referred to the number of Councils that still not had their 2019/2020 audits completed.

Karen explained that there were a number of Councils that not had their 2019/2020 Audit of accounts completed which meant that work could not start on the 2020/2021 accounts. Bury were not within this group and therefore the 2020/2021 accounts would be audited but the work would be completed late.

- Councillor Gartside asked what the issues were regarding the lateness of the audit last year.

Karen explained that this was the first year that Mazars were working remotely due to the pandemic. It was also explained that the Council had agreed that they would complete the work later to enable the Council to deal with the issues highlighted the previous year.

- Councillor Gartside asked if the audit completion work should be back on track for the following year.

Karen explained that measures were in place to deal with the back log at a national level as 60% of Council's would not have their accounts audited within the timescales. Actions were in place and proposals were currently being consulted on. It was explained that it was anticipated that it would take a couple of years to get back on track.

- Councillor Rydeheard referred to the background behind the issues around the deadlines and Council's not meeting these.

Karen explained the background around this and how deadlines had been changed to assist with the work being completed.

Councillor Whitby referred to the fact that the national situation was worsening as the numbers of councils not meeting the deadlines had increased.

Delegated decision:

That the contents of the report be noted.

AU.8 ANNUAL GOVERNANCE STATEMENT & HEAD OF AUDIT OPINION

The Audit Committee were presented with the draft Annual Governance Statement and Head of Audit Opinion report.

The draft AGS is presented for an initial review by the Audit Committee and a

final document will be presentedto Committee in September for recommendation for approval at Full Council later in the year.

Those present were given the opportunity to make comments and ask questions and the following points were raised:

- Councillor Butler referred to the training that had been provided to the Audit Committee Members at the start of the Municipal Year and asked that this be expanded upon to ensure that the Committee members received all relevant training that was available.

It was explained that the Committee would be receiving information provided by Mazars which they would find useful and that training sessions would be built into each scheduled meeting.

Sam explained that she would be holding a training workshop event in relation to Council finances and it was anticipated that this would be towards the end of September.

Councillor Whitby referred to the Audit training that that she had attended which had been provided by the LGA and recommended that Members attend if it is provided again.

Delegated decision:

That the Audit Committee

1. Notes the draft AGS and provide initial comments,

2. Notes that the AGS will be available on theCouncil's website from the end of July andavailable for public inspection;

3. Notes that a final AGS will be presented to Committee in September for approval and forrecommendation to Full Council.

AU.9 RISK REGISTER

It was reported that this item would be deferred to a future meeting of the Audit Committee. A review was currently being undertaken to ensure that there was consistency across the Council in relation to risk management and how it was calculated and reported.

It was explained that the report would contain details of the Council risks and the Audit Committee would be given the opportunity to carry out a 'deep dive' exercise on whichever risk the Committee identified.

AU.10 INFORMATION GOVERNANCE

Lynne Ridsdale presented a report providing an update to the Audit Committee on the work of the IGSG, the IG work programme and associated activity that has been progressed during the first quarter of 2021/22.

It was explained that Information Governance (IG) is the strategy or framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards, ensuring compliance with the relevant statutory and regulatory requirements.
It is of paramount importance to ensure that information is efficiently and legally managed, and that the appropriate policies, procedures, guidance and management accountability and structures provide a robust governance framework for information management.

IG within the Council is delivered through a distributed model of responsibility rather than through a specific or dedicated team, with key roles identified and assigned to ensure appropriate oversight and accountability. These roles include for example, the Senior Information Risk Officer (SIRO), the Data Protection Officer (DPO), Information Asset Owners (IAO) and Information Asset Managers (IAM).

The Information Governance Steering Group (IGSG) will provide assurance on IG within the Council, to the Committee through strategic and operational oversight and delivery of its wide-reaching work programme, which includes compliance with all statutory requirements and annual compliance with the Data Security and Protection Toolkit (DSPT).

The Audit Committee is responsible for providing assurance on the Council's governance (including risk and information governance) and as set out in the Council's Constitution, is required to annually review the IG requirements.

It was explained that in 2019, Bury Council invited the Information Commissioner's Office (ICO) to undertake a supportive review and audit of the Council's IG arrangements in place to ensure the organisation's compliance with the GDPR. The review was due to take place in May 2020 but was deferred due to the pandemic and rearranged for June 2021.

The report also gave updates in the following areas:

- Data Security and Protection Toolkit
- Information Governance Steering Group
- GDPR Internal Audit
- Information Governance Framework

Delegated decision:

That the Audit Committee:

1. Note the update provided;

2. Note the re-establishment of the IGSG and its formal reporting to the Audit Committee;

3. Approve the Terms of Reference of the IGSG; and

4. Endorse the Information Governance Framework as presented.

AU.11 ANNUAL INTERNAL AUDIT YEAR END UPDATE

Janet Spelzini presented a report summarising the results of internal audit work during 2020/21 and giving an overall opinion of the Authority's control environment as required by the Accounts and Audit Regulations 2015.

It was reported that based upon the results of audit work undertaken during the year, the Acting Head of Internal Audit's opinion is that the Authority's control environment provides substantial assurance that the significant risks facing the Authority are addressed.

Members were given the opportunity to ask question and the following points were raised:

- Councillor Rydeheard asked about the grading system.

Sam explained that the Audit Committee could request the officer responsible for a specific service area attend a meeting of the committee if that service had received a report with the outcome showing a limited level of assurance.

- Councillor Whitby explained that the Committee would receive a summary of all internal Audit reports with the Audit Update reports.

Delegated decision:

That the contents of the report be noted.

AU.12 INTERNAL AUDIT PLAN 2021.2022

The Acting Head of Internal Audit presented a report setting out the context of the Internal Audit Service explaining the approach to the compilation of the 2021/22 internal audit annual plan. The annual plan was incorporated at Annex 1 to the report.

Delegated decision:

1. That the contents of the report be noted

2. That the annual audit plan for 2021/22 be approved.

COUNCILLOR M WHITBY
Chair

(Note: The meeting started at 7.30 pm and ended at 9.00 pm)

This page is intentionally left blank

Agenda Item 5

Classification Open	Item No.

Meeting:	Audit Committee
Meeting date:	30th September 2021
Title of report:	Information Governance – ICO Update & Q2 delivery Update
Report by:	Lynne Ridsdale – Deputy Chief Executive
Decision Type:	
Ward(s) to which report relates	**All**

Executive Summary:

Information Governance (IG) is the strategy or framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards, ensuring compliance with the relevant statutory and regulatory requirements. At its last meeting the Audit Committee received the Q1 update on IG activity and approved the Information Governance Framework through which these functions are discharged within the Council.

During Q2 the Council has prepared and delivered a consensual audit of IG practice form the industry regulator, the Information Commissioner's office. This report:

- sets out the findings of the ICO audit;
- provides a Q2 update to the Information Governance workplan;
- proposes an improvement plan for adoption, which will also form the work plan for Quarters 3 and 4 2021/22; and
- sets out the requirements for the 2021/22 Data Security Protection Toolkit (DSPT).

Key considerations

1.0 Introduction

1.1 This report is the update on Information Governance work completed during Quarter 2 of 2021/22. The report focusses on the preparation for and findings of a consensual audit undertaken during this time by the Information Commissioner's Office (ICO). The full report is appended.

2.0 Background

2.1 The Information Commissioner is responsible for enforcing and promoting compliance with data protection legislation. Article 58(1) of the UK General Data Protection Regulation (UK GDPR) states that the Information Commissioner's Office (ICO) has the power to carry out investigations in the form of data protection audits. Section 129 of the Data Protection Act 2018 (DPA 18) also provides provision to carry out consensual audits. Additionally, Section 146 of the DPA 18 allows the ICO, through a written "assessment notice", to carry out an assessment of compliance with the data protection legislation.

2.2 Bury Council agreed to a consensual audit by the ICO of its processing of personal data. This was originally scheduled for June 2020; however, this was paused in response to the Covid-19 pandemic and was subsequently re-scheduled for 22nd – 24th June 2021.

2.3 The primary purpose of the audit was to provide the ICO and Bury Council with an independent opinion of the extent to which Bury Council, within the scope of the agreed audit, is complying with data protection legislation.

2.4 A report has been provided to Bury Council which, along with a series of recommended actions, also reflected on areas of good practice.

3.0 ICO Audit Approach

3.1 The ICO audit was structured as an evaluation of three areas of IG activity:

- Information security
- Freedom of Information
- Governance and Assurance

3.2 The Audit involved:

- Desk top review of over 100 pieces of written evidence including staff training materials, leadership job descriptions, policies, procedures, staff guidance and records of processing activity

- Over 30 stakeholder interviews with a range of staff involved in information governance activity

3.3 To inform the Audit the Council provided a copy of the Council's Information Governance Framework and internal improvement plan, which includes the actions from the recent Internal Audit review.

4.0 ICO Audit Findings

4.1 The ICO report is provided at Appendix A. The summary opinion is provided below

Audit Scope area	Assurance Rating	Overall Opinion
Governance & Accountability	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Information Security	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Freedom of Information	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering freedom of information compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with freedom of information legislation.

4.2 The audit also highlighted the following areas of best practice:

- BMBC have integrated communications around information governance into weekly executive emails, ensuring data protection matters are visible to all levels of staff.
- Departments hold a library of responses to frequent FOI/EIR requests to reduce workload, reduce response times and capitalise on any effort already expended on similar requests.
- BMBC has metacompliance software in place to ensure all staff have read and completed the Personal Commitment Statement. The statement outlines key information security requirements that staff must

4.3 The summary areas for improvement were found to be:

- BMBC does not currently maintain a central log of its lawful bases for processing, meaning there is no oversight on whether the appropriate lawful

basis is being used. BMBC should establish a central log of lawful bases, including details of any law, statute, or other obligation for that processing.

- The Records of Processing Activities (RoPA) held by BMBC does not include certain categories of information required by the UK GDPR. BMBC should ensure that its RoPA is updated to include all details specified by the legislation.
- BMBC does not have a Legitimate Interests Assessment (LIA) in place for the processing it carries out under the lawful basis of Legitimate Interest. BMBC should undertake an LIA on this processing to ensure it has adequately balanced its interests against the rights and freedoms of the data subject.
- BMBC should gain assurance from suppliers that they will notify BMBC within a reasonable timeframe of any information security breaches or personal data breaches. All breaches should be notified to a nominated person.
- BMBC should separate out the key elements of FOI/EIR legislation from the existing Data Protection eLearning module to create a new FOI module. Use the new module for mandatory FOI induction and refresher training for all staff.
- A specialist training programme should be created for all those staff with responsibility for responding to FOI/EIR requests. The training should be recorded and refreshed on a regular basis.
- BMBC should review the existing FOI pages on the council web site to demonstrate and ensure compliance with current guidance whilst ensuring the benefits gained from the web request form are not diminished.

5.0 Improvement Plan

5.1 The ICO have made 78 recommendations across the three themes of the audit, which have also been categorised by level of priority as follows

	Urgent	High	Medium	Low	Total
Governance and Assurance	7	15	14	2	38
Information Security	-	5	18	8	31
Freedom of Information	-	4	5	1	10

5.2 The recommendations have been translated into a detailed improvement plan for delivery by the end of the 2021/22 financial year. The detailed plan, which is performance managed by the Information Governance Steering Group, is available for inspection. A synopsis of activity underway is as follows

By end August	• Resolve Legitimate Interest Assessment – HR • ROPA refreshed • Review responsibilities/resources for IG • Refresh & re-establish network IG champions • Risk management strategy approved

	• Individual rights policy & procedure drafted • IG Policies updated to reflect GDPR • Induction updated & systems access only granted once e-learning complete • Contacts reviewed re data processing • DPIA screening, template and log established
By end Sept	• Resolve IS responsibilities within ICT • Update agile policy re information security • PEN test and review PSN requirements • Update personal breach policy • policy document template & schedule approved, including Information Security • policy availability to non front line staff addressed • IG KPIs reviewed • IAR reviewed following ROPA refresh • ROPA review process agreed • Privacy notice log established • FOIA policy and procedure updated
By end Oct	• Review GDPR e-learning module • Update Information Security policy in full • Establish end use asset register • Port controls designed within Enterprise Agreement • Specialist role training delivered to IG leadership roles • Internal audit plan
By end Nov	• Process for reviewing systems access in place • Resolve information security within buildings including floor walks of office sites
By end Dec	• End user device policy in place • Starter/leavers process reviewed and induction updated • Plans in place for independent assurance of IG • Audit of consent processes and recording • Review PETS

6.0 Information Governance Update 2021/22 Quarter 2

6.1 The following updates are provided in respect to the overall work programme.

- **Data Security and Protection Toolkit**

The 2021/22 iteration of the Data Security and Protection Toolkit (DSPT) was formally released by NHS Digital at the end of August 2021.

This Toolkit is a self-assessment implemented all organisations accessing NHS patient data and provides assurance as to the level of best practice in terms of the processing, storage and transfer of patient data. This is reflected in the Information Standards Notice DCB0086 Amd 9/2019.

For the 2021/22 reporting period, the submission deadline has been confirmed as 30 June 2022. As with the previous 2020/21 DSPT, there is acknowledgement of the continuing pressures resulting from the Covid-19 pandemic and as such, the deadline has been extended beyond 31 March for the 2021/22 submission.

With the recent release of the 2021/22 requirements which include additions to previous years (attached at Appendix B), work is currently progressing to incorporate these actions into the comprehensive IG workplan.

- **Information Governance Framework**

The Information Governance Framework endorsed by the Audit Committee at the June 2021 meeting is undergoing implementation to evidence assurance of effective governance practices across all Council departments. Key updates are noted below:
Information Governance Steering Group – the Group has been established as detailed above and continue to supervise and monitor all work in relation to the delivery of the workplan.

- **Information Governance Delivery Group**

This Group held their first meeting on 8th September 2021 and have been tasked with the coordination and delivery of individual actions on the workplan. The constitution reflects direct reports of Information Asset Owners (IAOS) whose departments have specific actions assigned to them. As such, there is no defined membership as the colleague best placed to progress the task in question is invited to attend.

- **Information Governance Resource**

Following a review of available resource, an Information Governance and Risk Strategic Advisor has been engaged to provide leadership direction across both the Council and CCG on a part-time, fixed term basis until January 2022; additionally supporting the seconded IG Support Officer role.

- **Policy**

Existing Information Governance and Data Security policies have been refreshed and updated in accordance with ICO recommendations. The documents currently undergoing review and approval by the IGSG include, but are not limited to the following:

- Data Subject Rights Policy
- Anonymisation and Pseudonymisation Policy
- Data Quality Policy

- Confidential Waste Disposal Policy
- Data Protection Impact Assessment (DPIA) Policy

- **Standards, including Training**

Alternative E-Learning modules within the existing training platform covering Information Governance and Cyber Security have been reviewed against National Cyber Security and ICO guidance and assurance provided they meet requirements of the audit recommendations. Work continues to progress, having identified, and now reviewing appropriate training materials for specialised IG roles.

7.0 Recommendations

4.1 The Audit Committee is required to:

- Note the 2021/22 Quarter 2 Update provided;
- Note the findings of the ICO audit at Appendix A;
- Note the 2021/22 requirements of the Data Security and Protection Toolkit provided at Appendix B.

Other alternative options considered

None.

Community impact / Contribution to the Bury 2030 Strategy

Good Information Governance practices enables the Council to deliver its statutory requirements and therefore contributes across all the themes of the Bury 2030 Strategy.

Equality Impact and considerations:

24. *Under section 149 of the Equality Act 2010, the 'general duty' on public authorities is set out as follows:*

A public authority must, in the exercise of its functions, have due regard to the need to -

(a) *eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act;*

(b) *advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;*

(c) *foster good relations between persons who share a relevant protected characteristic and persons who do not share it.*

25. *The public sector equality duty (specific duty) requires us to consider how we can positively contribute to the advancement of equality and good relations, and demonstrate that we are paying 'due regard' in our decision making in the design of policies and in the delivery of services*.

Assessment of Risk:

The following risks apply to the decision:

Risk / opportunity	Mitigation
Without a robust framework in place to support good Information Governance practice, there is a risk that the Council may not comply with the duties set out in the General Data Protection Regulations (GDPR) 2018 or Data Protection Act leading to possible data breaches, loss of public confidence, reputational damage and prosecution / fines by the Information Commissioner	Approval and Implement of the Information Governance Framework Implementation of a comprehensive Information Governance work programme

---

Consultation: N/a

Legal Implications:

The report references the Council's statutory duties and obligations under the UK GDPR, Data protection Act 2018, FOIA and associated legislation and guidance. The Council has duties under this legislation in terms of accountability and compliance and must ensure it has appropriate policies and procedures in place. A Failure to ensure compliance could result in enforcement action by the ICO.

Legal advice and support will be required in terms of the action plan outlined in the report as well as ongoing DPO oversight and support.

Financial Implications:

With the exception of the procurement of appropriate training there are no direct financial implications arising from this report. However, there are implications in relation to a potential ICO fine if the Council had a data breach and the ICO found that we as an organisation were negligent.

Report Author and Contact Details:

Lynne Ridsdale – Deputy Chief Executive

l.ridsdale@bury.gov.uk

Background papers: N/A

Please include a glossary of terms, abbreviations and acronyms used in this report.

Term	Meaning
DFM	Data Flow Mapping
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSPT	Data Security and Protection Toolkit
EIR	Environmental Information Regulations 2004
FOIA	Freedom of Information Act 2000
GDPR	General Data Protection Regulations 2018
IAM	Information Asset Manager
IAO	Information Asset Owner
IAR	Information Asset Registers
ICT	Information Communication and Technology

IG	Information Governance
IS	Information Security
IGSG	Information Governance Steering Group
KPI	Key Performance Indicator
LIA	Legitimate Interest Assessment
NHS	National Health Service
PEN	Penetration Testing
PETS	People Equipment Technology and Services
ROPA	Record of Processing activity
SAR	Subject Access Request
SIRO	Senior Information Risk Officer

Bury Metropolitan Borough Council

Data protection audit report

July 2021

Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

Bury Metropolitan Borough Council (BMBC) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 23 March 2021 with representatives of BMBC to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and BMBC with an independent assurance of the extent to which BMBC, within the scope of this agreed audit, is complying with data protection legislation.

The scope areas covered by this audit are determined following a risk based analysis of BMBC processing of personal data and Freedom of Information requests. The scope may take into account any data protection issues or risks which are specific to BMBC, identified from ICO intelligence or BMBC's own concerns, and/or any data protection issues or risks which affect their specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of BMBC, the

nature and extent of BMBC's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to BMBC.
It was agreed that the audit would focus on the following area(s)

Scope area	Description
Governance & Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the UK GDPR and national data protection legislation are in place and in operation throughout the organisation.
Information Security	There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.
Freedom of Information	The extent to which FOI/EIR accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor compliance are in place and in operation throughout the organisation.

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are normally a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

However, due to the outbreak of Covid -19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore, BMBC agreed to continue with the audit on a remote basis. A desk based review of selected policies and procedures and remote telephone interviews were conducted from 22 June to 24 June 2021 The ICO would like to thank BMBC for its flexibility and commitment to the audit during difficult and challenging circumstances.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection and freedom of information legislation. In order to assist

BMBC in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. BMBC'S priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

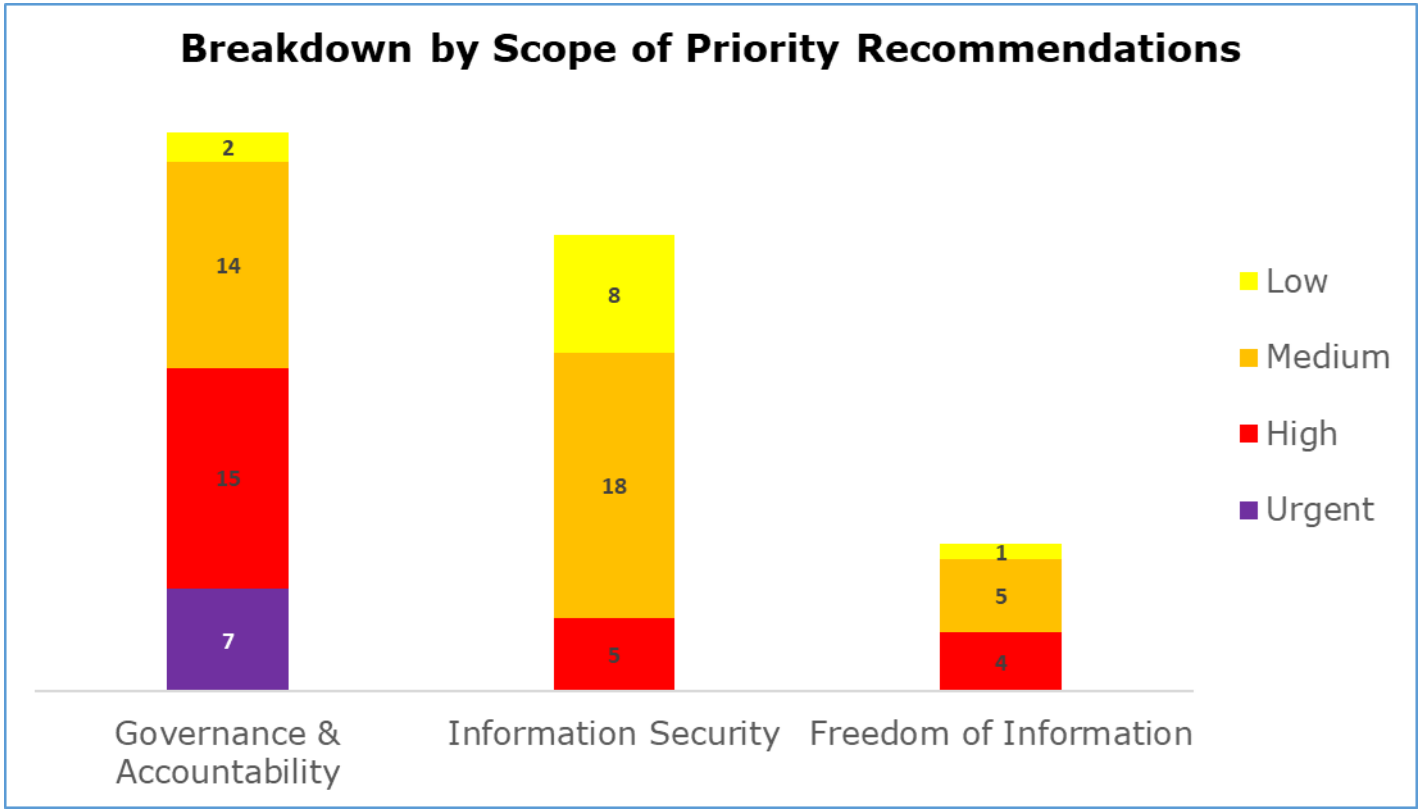
Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Governance & Accountability	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Information Security	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Freedom of Information	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering freedom of information compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with freedom of information legislation.

*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

Priority Recommendations

A bar chart showing a breakdown by scope area of the priorities assigned to the recommendations made.



The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance & Accountability has seven urgent, 15 high, 14 medium and two low priority recommendations
- Information Security has five high, 18 medium and eight low priority recommendations
- Freedom of Information has four high, five medium and one low priority recommendations

Areas for Improvement

BMBC does not currently maintain a central log of its lawful bases for processing, meaning there is no oversight on whether the appropriate lawful basis is being used. BMBC should establish a central log of lawful bases, including details of any law, statute, or other obligation for that processing.

The Records of Processing Activities (RoPA) held by BMBC does not include certain categories of information required by the UK GDPR. BMBC should ensure that its RoPA is updated to include all details specified by the legislation.

BMBC does not have a Legitimate Interests Assessment (LIA) in place for the processing it carries out under the lawful basis of Legitimate Interest. BMBC should undertake an LIA on this processing to ensure it has adequately balanced its interests against the rights and freedoms of the data subject.

BMBC should gain assurance from suppliers that they will notify BMBC within a reasonable timeframe of any information security breaches or personal data breaches. All breaches should be notified to a nominated person.

BMBC should separate out the key elements of FOI/EIR legislation from the existing Data Protection eLearning module to create a new FOI module. Use the new module for mandatory FOI induction and refresher training for all staff.

A specialist training programme should be created for all those staff with responsibility for responding to FOI/EIR requests. The training should be recorded and refreshed on a regular basis.

BMBC should review the existing FOI pages on the council web site to demonstrate and ensure compliance with current guidance whilst ensuring the benefits gained from the web request form are not diminished.

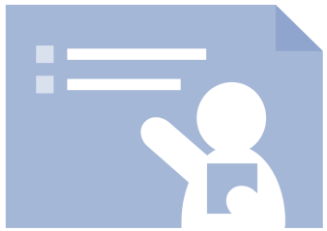
Best Practice

BMBC have integrated communications around information governance into weekly executive emails, ensuring data protection matters are visible to all levels of staff.

Departments hold a library of responses to frequent FOI/EIR requests to reduce workload, reduce response times and capitalise on any effort already expended on similar requests.

BMBC has metacompliance software in place to ensure all staff have read and completed the Personal Commitment Statement. The statement outlines key information security requirements that staff must follow

Audit findings



The tables below identify areas for improvement that were identified in the course of our audit; they include recommendations in relation to how those improvements might be achieved.

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
There is a Data Protection Officer in place with designated responsibility for data protection compliance.	a.1.A. There is a blurring of responsibilities between the Deputy Director of Governance and Assurance (DDGA) at Bury CCG, and BMBC's DPO. There is a confusion on expectations - it was reported to ICO auditors that the DDGA carries out the operational aspects of IG and DP and the DPO sits in a statutory role, however separately the DDGA was described as a specialist advisor to help implement measures but not run them. There is a risk that areas of DPO responsibility as delegated in Articles 37, 38, and 39 of the UK GDPR will be missed as there are not clear lines on who is responsible for them. B. See a.3. C. The DPO is not sufficiently well-resourced. There is no DP or IG department, and as a result	a.1.A. Clear delineation between the DPO's role and the advisory position of the DDGA is required. BMBC needs to clarify exactly what is required of a DPO by the UK GDPR and ensure its DPO is fulfilling those duties, then it will be able to provide clarity on whether the DPO or DDGA is responsible for specific aspects of DP or IG. This will ensure BMBC is fulfilling its obligations under Articles 37, 38, and 39 of the UK GDPR. B. see a.3. C. BMBC have plans in place to adequately resource IG projects and should implement them as soon as they are reasonably able to do so. By ensuring that there are specialised staff available to assist in responding to	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	many operational aspects of IG, such as responding to individual rights requests, is managed within services. BMBC have advised of resourcing plans that were put on hold due to the pandemic. There is a risk that the DPO is prevented from carrying out their role effectively, due to lack of resourcing.	individual rights requests, or provide help and guidance on data protection matters, the DPO will be able to carry out their role effectively.	
The DPO role has operational independence and appropriate reporting mechanisms are in place to senior management	a.2. BMBC's DPO also holds many other roles, including Head of Legal Services and Deputy Monitoring Officer. By holding several senior management roles, BMBC is unable to provide assurance that its DPO has operational independence and that there is no conflict with the DPO's numerous other duties as part of their role. This could result in non-compliance with Article 38(6) of the UK GDPR, which highlights that whilst DPOs may fulfil other tasks or duties, "the controller or processor shall ensure that any such tasks and duties do not result in a conflict of interest".	a.2. BMBC should consider creating documentation to account for the possibility of a conflict of interest arising, and the backup reporting measures in place to mitigate this risk, e.g. designating responsibility to another staff member on matters which could be perceived as a conflict of interest for the DPO. This will ensure BMBC can demonstrate compliance with Article 38(6) of the UK GDPR.	Medium
Operational roles and responsibilities have been assigned to support the day to day management of all aspects of information governance	a.3. The responsibility for day-to-day management of IG is not centralised or standardised - each department manages their duties individually, so there are no processes in place to ensure the DPO is involved in DP issues in a timely manner. There is no oversight by the DPO on individual department IG management and performance. ICO Auditors were advised that there is a network of IG leads, although this was unable to be evidenced, and there have previously been DP champions in departments but this has not been maintained due to the pandemic. This means there are no assurances the correct staff are in place and are trained	a.3. BMBC should implement processes to ensure the DPO has oversight of IG management and performance across individual departments. BMBC should consider reinstating DP champions and facilitating DP champion meetings in and across departments. This will allow good practice and lessons learnt to be shared across departments and provide an opportunity for the DPO to attend to ask and answer any questions there may be around the operational aspects of IG. This will ensure that the correct staff are in place and	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	accordingly, or that BMBC is fulfilling its obligations under the UK GDPR.	that BMBC is fulfilling its obligations under the UK GDPR.	
There are processes in place to ensure information risks are managed throughout the organisation in a structured way.	a.4. A mixed awareness of risk registers was reported to ICO auditors, with some departments confirming they held their own register and others stating they were only aware of the corporate register. Without the appropriate oversight of information risks across the organisation, BMBC does not have adequate assurance they are preventing misuse of personal data, which may result in a personal data breach or non-compliance with their obligations under the UK GDPR.	a.4.Document where departmental risk registers exist and commence enquiries into where they don't and why. BMBC should ensure that all departments are aware of their risk registers, and that ownership is allocated to a suitable staff member. This will mitigate the risk of misuse of personal data and ensure BMBC are in compliance with their obligations under the UK GDPR.	Urgent
There are local level operational meetings where data protection, records management and information security matters are discussed.	See a.3.	See a.3.	
Management support and direction for data protection compliance is set out in a framework of policies and procedures.	a.5.A. Policies and procedures relating to data protection matters are in place. However, these documents are significantly out of date and have not been updated and reviewed for a number of years. There is a risk that breaches will occur as the policies and procedures do not meet the requirements of the UK GDPR and DPA18. B. BMBC does not currently have a specific individual rights policy. As a result, there is a risk that individual rights requests will not be recognised as they are not documented anywhere or included in any specific training. In addition, there is a risk BMBC will not fulfil its	a.5.A. Policies and procedures should be reviewed and updated to reflect the new requirements on controllers detailed in the UK GDPR. This will ensure that BMBC is accurately reflecting its obligations under the updated legislations. B. Implement an individual rights policy, including details on what rights individuals have, exemptions that can be applied, and how requests can be made. This will ensure BMBC fulfils its obligations under Articles 12-23 of the UK GDPR.	Medium

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	obligations under Articles 12-23 of the UK GDPR, which set out the rights of the individual.		
Where the organisation is required by Schedule 1 or Part 3 section 42 of the DPA18 to have an Appropriate Policy Document (APD) in place, the document in place is sufficient to fulfil the requirement.	a.6. No document that would constitute an Appropriate Policy Document (APD) has been provided to ICO auditors. As such, BMBC has no assurance that it has properly considered and documented their justification for processing special category or criminal offence data as required under Part 3 Section 42 or Schedule 1 of the DPA18.	a.6. BMBC must implement an APD to support the accuracy of the decisions made to process special category or criminal offence data. This will ensure BMBC meets the requirements of Part 3 Section 42 or Schedule 1 of the DPA18.	Urgent
Policies and procedures are approved by senior management and subject to routine review to ensure they remain fit-for-purpose.	a.7.A. Evidence provided to ICO auditors shows that there is no consistent document control information on policies or procedures, meaning there is no way of determining whether a document is the most recent version, or requires review. There is no accountability when it comes to ensuring documents are routinely reviewed and updated. This means BMBC is not compliant with Article 5(2) of the UK GDPR, the Accountability principle. B. BMBC does not have a formal, documented policy review process - there is no set procedure for reviewing, ratifying and approving new or updated policies. This means there is no assurance around the effectiveness of policies and procedures, and that BMBC is not compliant with Article 5(2) of the UK GDPR, the Accountability principle. C. There is no centralised policy review schedule, so there is no accountability or assurance around ensuring documents are routinely reviewed and	a.7.A. All policies, procedures and guidelines should be updated to include document control information - at minimum, this should include version number, document owner, change history, and review date. This will give ownership and accountability to policies and ensure BMBC's compliance with Article 5(2) of the UK GDPR. B. BMBC should create a formal, documented policy review process, to ensure a standardised approach to reviewing, ratifying, and approving new or updated policies. This will provide assurance around the effectiveness of policies and procedures and ensure BMBC's compliance with Article 5(2) of the UK GDPR. C. BMBC should formulate a centralised policy review schedule, to provide accountability and assurance around documents being routinely reviewed and	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	updated. This means BMBC is not compliant with Article 5(2) of the UK GDPR.	updated. This will ensure BMBC's compliance with Article 5(2) of the UK GDPR.	
Policies and procedures are readily available to staff and are communicated through various channels to maintain staff awareness	a.8. There is a lack of oversight on ensuring staff without computer access have copies of policies and procedures available to them. There are no measures in place to make sure that this is the case, as it is down to individual managers to take responsibility for documents being available. There is an uncontrolled risk that staff will act without reference to guidance, and in breach of the UK GDPR or DPA18 - meaning BMBC is not conforming to the requirements of Article 5 of the UK GDPR, the Data Protection Principles.	a.8. BMBC should ensure the relevant DP and IG policies and procedures are available to all staff without computer access - for example creating a document bundle retained by depots or offices that contains the appropriate information. This will allow staff to reference guidance as required and ensure BMBC conforms to the Data Protection Principles set out in Article 5.	Medium
There is an overarching IG training programme in place for all staff.	See c.9.	See c.9.	
Induction training is in place and delivered in a timely manner to all staff including temporary and agency staff etc.	a.9. Induction training at BMBC includes the basic GDPR training, and a requirement to read the relevant data protection policies. However, there is little assurance that staff have completed training before being granted access to systems that process or hold personal data. There is a risk of non-compliance with the Data Protection Principles, set out in Article 5(1) of the UK GDPR.	a.9. Regular reporting should be carried out on who has access to systems containing personal data, and who has completed the mandatory GDPR training. This will allow BMBC to identify if any staff who have not completed the mandatory training have access to systems holding or processing personal data. Where staff have not completed the training, access should be rescinded until the training is complete. Where the staff member is a new starter, a report should be run to confirm training has been completed before granting access to these systems. This will ensure BMBC is in compliance with Article 5(1) of the UK GDPR.	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
There is provision of more specific DP training for specialised roles (such as the DPO, SIRO, IAOs) or particular functions e.g. records management teams, SAR teams, information security teams etc.	a.10.A. The DPO has not undertaken any specific DP or IG training and cannot evidence any DP or IG certifications to qualify them for the role. Whilst Article 37(5) of the UK GDPR does not specify any qualifications a DPO should hold, it is expected that a DPO should be able to evidence their "expert knowledge of data protection law and practices". Failure to have an appropriately qualified DPO may be a breach of Article 37 of the UK GDPR. B. There is no provision of specific DP training for specialised roles or particular functions - for example Information Asset Officers (IAOs) do not have specific training on their role and its responsibilities, and there is no specialised training in how to recognise or respond to a SAR. This leaves BMBC at risk of not meeting its obligations under the UK GDPR and DPA18.	a.10.A. BMBC should facilitate the DPO attending specific, specialised DP or IG training, in order to evidence and maintain their expert knowledge, and ensure BMBC is complying with their obligations under Article 37. B. The requirement for staff in particular roles or functions to have more specific training was highlighted in BMBC's recent Training Needs Analysis (TNA). BMBC should implement a specialised training programme to meet the needs of staff in these roles - i.e. what the role and responsibilities of an IAO are, how front line staff can recognise and process a SAR. This would ensure BMBC is meeting its obligations under the UK GDPR and DPA18.	High
The organisation has considered a programme of external audit with a view to enhancing the control environment in place around data handling and information assurance	a.11. BMBC does not engage an external auditor to provide independent assurances on IG practices. External auditors are engaged for the purposes of information security only. By only assessing risk through internal audits and assurances, BMBC are at risk of inaccuracies in risk assessments and potential breaches, and non-conformance with Article 5(1) of the UK GDPR, the Data Protection Principles.	a.11. BMBC should consider engaging an external auditor to provide an independent view on its IG practices. This will provide additional assurances and cover any potential blind spots, to minimise risk of inaccurate risk assessments or any potential breaches. It will also provide additional layers of assurance that BMBC is conforming with the Data Protection Principles detailed in Article 5(1) of the UK GDPR.	Medium
There is a programme of risk- based internal audit in place covering information governance / data protection.	a.12. Data protection matters are included within the scope of all audits in BMBC's internal audit plan. However, BMBC does not routinely conduct internal audits solely around data protection compliance, and the DPO is not included in audit	a.12. BMBC should routinely conduct internal audits covering a range of data protection compliance areas. This will ensure BMBC and its DPO have continuous oversight and assurance that it is maintaining compliance	Medium

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	planning. This means BMBC and its DPO may be lacking oversight and assurance that it is maintaining compliance with its obligations under the UK GDPR and DPA18.	with its obligations under the UK GDPR and DPA18.	
The organisation actively monitors or audits its own compliance with the requirements set out in its data protection policies and procedures.	a.13. BMBC's data protection policies and procedures do not specify what the compliance monitoring process is, to ensure staff are adhering to policies. Without ongoing compliance monitoring, BMBC lacks assurance that the controls it has in place to prevent non-compliance with the UK GDPR and DPA18 are being implemented.	a.13. Establish within data protection policies and procedures how compliance will be monitored. By continuously monitoring staff compliance with policies and procedures, BMBC will have ongoing assurance that the controls it has created are being implemented correctly and preventing non-compliance with the UK GDPR and DPA18.	Medium
There are data protection Key Performance Indicators (KPI) in place	a.14. BMBC has recently implemented KPIs for FOI and SAR completion. However, there are no KPIs relating to data protection training, information security, or records management. Without KPIs in place, BMBC lacks oversight on its compliance with its statutory obligations and cannot demonstrate compliance with Article 5(2) of the UK GDPR, the Accountability principle.	a.14. BMBC should implement or expand their KPIs in the following areas: -Individual rights requests, to include breakdown by type of request, and area the request was received -Data protection training, including percentage of staff completing mandatory training -Information security, including number of security breaches, incidents, and near misses -Records management, including use of metrics such as file retrieval statistics, adherence to disposal schedules, and performance of systems in place to index and track paper files containing personal data. This will ensure that BMBC has oversight on its compliance with statutory obligations and can demonstrate accountability as required under Article 5(2) of the UK GDPR.	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
Performance to IG KPIs is reported and reviewed regularly.	See a.14.	See a.14.	
There are written contracts in place with every processor acting on behalf of the organisation which set out the details of the processing	a.15. BMBC does not have a central contract log for data processors - this is managed within services. This means there is no oversight of processor contracts by the DPO, and no assurance that contract reviews are taking place regularly and consistently.	a.15. BMBC should create a central log for data processor contracts. This will provide oversight on processor contracts by the DPO and provide assurance that contract reviews take place regularly and consistently.	High
Written contracts include all the details, terms and clauses required under the UKGDPR	a.16. Evidence provided to ICO auditors indicated that details of processing - e.g. the subject matter, the duration, the nature and purpose, the type of personal data - is not included as standard in a processor contract, as required by Article 28(3) of the UK GDPR. There is a risk that BMBC may lose control of personal data, resulting in a breach, or that BMBC may be unable to respond to individual rights requests within the statutory timeframe. There is also non-compliance with Article 5(2) of the UK GDPR, the Accountability principle.	a.16. BMBC should ensure that the categories of information set out in Article 28(3) of the UK GDPR are included in all processor contracts - consider implementing a standard contract in order to achieve this. Once contracts have been updated, BMBC should ensure that compliance checks are carried out on updated contracts. This reduces the risk that BMBC may lose control of personal data or be unable to respond to individual rights requests within the timeframe designated by the UK GDPR. This will also ensure compliance with Article 5(2) of the UK GDPR.	Urgent
The organisation takes accountability for ensuring all processors comply with the terms of the written contract(s)	See a.16.	See a .16.	
The organisation has a process to ensure all processing activities are documented accurately and effectively	a.17. BMBC does not currently have any robust data mapping or information audit processes in place. This means that the Record of Processing Activities (RoPA), Information Asset Registers, or	a.17. Auditors are aware BMBC is currently working to implement more comprehensive data flow mapping, as evidenced in the template provided to ICO auditors. BMBC should work to implement this new data	Medium

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	risk assessments may be incomplete or inaccurate.	mapping process to ensure that its RoPA, IARs, and risk assessments are complete and accurate reflections of their processing.	
There is an internal record of all processing activities undertaken by the organisation	a.18. BMBC does not have a central review log for their RoPA - this is managed within services. This means there is no oversight of reviews by the DPO, and no assurance that reviews are taking place regularly and consistently.	a.18. BMBC should introduce a centralised review log for the RoPA, to make sure there is oversight on the review process and that reviews are taking place regularly and consistently.	Medium
The information documented within the internal record of all processing activities is in line with the requirements set out in Article 30 of the UKGDPR	a.19. BMBC's RoPA does not include the name and contact details of the controller, a lawful basis for processing for all records, or processing carried out by processors. This means BMBC is in non-conformance with Article 30 of the UK GDPR - which designates the responsibility for controllers to maintain a RoPA and includes details on what should be recorded.	a.19. BMBC should ensure their RoPA contains all the information required by Article 30 of the UK GDPR, and details processing undertaken by processors. This will ensure that BMBC is conforming with Article 30.	Urgent
The lawful basis and condition(s) for processing personal data, special category data and data relating to criminal convictions and offences has been identified appropriately, defined and documented internally.	a.20. ICO auditors were advised that the lawful basis for processing for each activity is documented in privacy notices, and BMBC does not maintain a centralised internal log of lawful bases for processing. In cases where Legal Obligation is the basis for processing, there is no central record of what the obligation under law is for that type of processing. Where Public Task is the lawful basis for processing, there is no central record of the task or function, and the associated law or statute. Where special category data is processed, there is no central record of the additional information required to undertake this processing. This means there is no assurance that BMBC is choosing the correct basis for processing, or that BMBC is processing personal data in compliance	a.20. Implement a central log of lawful bases for processing for all processing activities - including details of any law, statute, or additional obligation for that processing. This could be incorporated into the RoPA, the APD, or in a separate document or record. This will provide assurance that BMBC is selecting the right basis for processing and is compliant with Articles (5)(1)(a) and 5(2) of the UK GDPR.	Urgent

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	with Article 5(1)(a) and 5(2) of the UK GDPR- personal data should be processed lawfully, fairly and transparently, and that controllers should be able to demonstrate their compliance with the legislation.		
There are records of when and how consent was obtained from individuals.	a.21. ICO auditors were advised that records for consent were managed within services, and there is no oversight by the DPO of how these are managed or reviewed. There is also currently no mechanism to prompt a review of consent. This means that there is no assurance that records of consent include the correct information - i.e. who gave consent, when, what was consented to, how it was given, and that it is still valid. This creates a risk that BMBC could be processing personal data in non-conformance with UK GDPR Articles 6(1)(a) and 9(2)(a), which state that processing of personal data is only lawful when the data subject has given their consent for specific purposes.	a.21. BMBC should create a central log and review schedule of consent records. This will provide oversight on how records are managed and reviewed and give assurance that BMBC is processing personal data in conformance with UK GDPR Articles 6(1)(a) and 9(2)(a).	Medium
Consents are regularly reviewed to check that the relationship, the processing and the purposes have not changed and there are processes in place to refresh consent at appropriate intervals.	See a.21. a.22.There is no assurance around consent that is given verbally as part of a new episode of care. ICO auditors were informed that there is a requirement for consent to be recorded, however there is no assurance that the conversation takes place. There is a risk that BMBC could be processing personal data in non-conformance with UK GDPR Articles 6(1)(a) and 9(2)(a).	See a.21. a.22. BMBC should consider ways it can record this type of consent more thoroughly and accurately, and methods of providing assurance around these records. This will ensure that BMBC is processing personal data in line with UK GDPR Articles 6(1)(a) and 9(2)(a).	Medium
Where the lawful basis is Legal Obligation, the organisation has clearly	See a.20.	See a.20.	

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
documented the obligation under law for that type of processing activity for transparency purposes.			
Where the lawful basis is Legitimate Interests, the organisation has conducted a legitimate interests assessment (LIA) and kept a record of it.	a.23. ICO auditors were advised that HR functions are often carried out using the lawful basis of Legitimate Interest, however no formal documented Legitimate Interests Assessment (LIA) has been carried out. This means that BMBC is processing personal information without properly assessing the balance against the interests of the controller. BMBC is also in breach of Article 5(2) of the UK GDPR, the Accountability principle.	a.23. BMBC should undertake an LIA to ensure that the interests of the controller are adequately balanced against the rights and freedoms of the data subject.	Urgent
Where the lawful basis is Public Task, the organisations is able to specify the relevant task, function or power, and identify its statutory or common law basis for processing.	See a.20.	See a.20.	
The organisations privacy information or notice includes all the information as required under Articles 13 & 14 of the UKGDPR.	a.24. It was noted while reviewing BMBC's privacy information that in order to submit a contact form - which BMBC directs users to when they wish to make an individual rights or FOI request - that allowing all cookies is mandatory in order to submit the form. By not providing additional contact details should individuals need to convey their request in writing, consent for these cookies does not meet the thresholds set by the UK GDPR. This extends to cookies across	a.24. Consider implementing a pop-up or dashboard that allows users to actively choose which cookies they consent to. Provide additional contact details such as postal address or an email address where individuals can submit their requests, so that the online form is not the only way individuals are able to contact BMBC regarding a request. This will ensure that individuals are not forced into accepting	Medium

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	BMBC's website, where consent for cookies is assumed rather than active. This is not compliant with Regulation 6 of PECR, which requires consent for cookies to meet the UK GDPR threshold - consent should be freely given, specific, and informed.	cookies they do not want to and means that BMBC will comply with Regulation 6 of PECR.	
The organisation actively publishes or communicates privacy information to keep their service users or customers informed on how their data is collected, processed and / or shared.	a.25. It was reported to ICO auditors that no privacy dashboards were offered to individuals. This means that individuals are unable to manage their privacy preferences and are not fully aware of how their personal data is being used, meaning they may not be aware of their rights or how their information is being processed.	a.25. Consider introducing a privacy dashboard, where individuals can manage their preferences, and can gain more insight into how their personal data is used - which will ensure individuals are fully informed of their rights and how their personal information is being processed.	Low
Privacy information is concise, transparent, intelligible and uses clear and plain language	a.26.A. There is currently no DPO oversight of privacy information, and it is up to individual services to create their privacy notice from a provided template. There is a distinct disparity between services as to what information is included. The lack of oversight means that they are not moderated or standardised, and they may fail to meet the requirements of the UK GDPR. B. Privacy information is not currently provided in other languages. This presents a barrier to individuals who are not fluent in English - if they cannot understand the privacy information, it has effectively not been provided.	a.26.A. BMBC should introduce a centralised log of privacy notices, in order to both maintain a historic log and to provide DPO oversight. This will provide an opportunity for the DPO to moderate and standardise what information is included, ensuring they meet the full requirements of the UK GDPR. B. Privacy information in other languages should be available to individuals, to ensure that they fully understand how their data is being processed.	Medium
Existing privacy information is regularly reviewed and, where	a.27.A. There is no review schedule for privacy information, so there is a risk that the information is out of date and individuals are not	a.27.A Introduce a review schedule for privacy information, including reviewing alongside the RoPA, to ensure that the	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
necessary, updated appropriately.	being adequately informed of how their personal data is being processed. B. BMBC does not have a log of historic privacy notices, meaning there is no assurance around what privacy information has been provided to individuals on certain dates. C. BMBC does not currently conduct user testing on its privacy information. This means BMBC has no assurance on the effectiveness of the communication of its privacy information.	information given to individuals is up to date and explains how personal data is being processed. B. See a.26.A. C. BMBC should conduct user testing on its privacy information, which will ensure that BMBC has assurance that its privacy information is effective and understood.	
Fair processing policies and privacy information are understood by all staff and there is periodic training provided to front line staff whose role includes the collection of personal data on a regular basis.	a.28. Fair processing and privacy information is not included as part of the basic GDPR training across BMBC, nor is specialised training provided to front line staff. If staff are not fully informed and trained, individuals may not be provided with the correct information, risking a breach of UK GDPR.	a.28. Fair processing and privacy information should be incorporated into basic GDPR training, and specific training should be provided to front line staff. This will make sure that the correct information is provided, and a breach of the UK GDPR does not occur.	Low
Systems, services and products have data protection 'built in' by design.	a.29.A. It was reported that BMBC do not currently use any privacy-enhancing technologies (PETs), nor are there specific system functions that are designed to protect personal data automatically. BMBC are at risk of not adequately considering the privacy rights of individuals and prioritising functionality over privacy, therefore not meeting the requirements of Article 25 of the UK GDPR which states that the controller shall "implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as	a.29.A. BMBC should consider what PETs are available to them and how they can implement PETs within their own systems, including introducing specific system functions to automatically protect personal data. They should also ensure that individuals have access to tools to find out how their personal data is being used and consider what measures can be put in place, so individuals do not have to take any specific action to protect it. This will provide assurance that BMBC are fully considering the rights of individuals and meeting the	Medium

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects." B. BMBC does not currently have any tools to assist individuals in determining how their personal data is being used, nor are there any demonstrable measures in place to ensure individuals do not have to take specific action to protect their privacy. BMBC are at risk of not adequately considering the privacy rights of individuals and prioritising functionality over privacy, therefore not meeting the requirements of Article 25 of the UK GDPR.	requirements of Article 25 of the UK GDPR. B. BMBC should ensure that individuals have access to tools to find out how their personal data is being used and consider what measures can be put in place, so individuals do not have to take any specific action to protect it. This will provide assurance that BMBC are fully considering the rights of individuals and meeting the requirements of Article 25 of the UK GDPR.	
The organisation proactively takes steps to ensure that through the lifecycle of the processing activities they only process, share and store the data they need in order to provide their products or services.	a.30. There are not currently any policies in place regarding data minimisation or pseudonymisation/anonymisation, and as such data is not periodically reviewed to consider whether minimisation or pseudonymisation is appropriate. By not considering where it can reduce the amount of personal data being processed, BMBC is not compliant with Article 5(b and e) of the UK GDPR - which state that personal data should be limited to what is necessary and kept in a form that identifies individuals for longer than necessary.	a.30. Create a policy or policies documenting when and how data minimisation or pseudonymisation should occur and implement a review schedule to make sure that data is reviewed for opportunities to minimise or pseudonymise on a regular basis. This will ensure BMBC are compliant with Article 5(b and e) of the UK GDPR.	Medium
Existing policies, processes and procedures include references to DPIA requirements	a.31. BMBC have been unable to evidence any reference to DPIAs within change or project management policies. If the requirements for a DPIA are not integrated in the early stages of planning, there is a likelihood that the requirement of privacy by design and default will	a.31. BMBC should ensure that DPIA requirements are detailed in all change or project management policies. This will ensure DPIAs are considered in the earliest stages of a project, and that privacy by design and default is integrated from the	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	not be met, and BMBC is at risk of non-conformance with Article 35 of the UK GDPR - "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."	start - ensuring they conform with the requirements of Article 35 of the UK GDPR.	
The organisation understands the types of processing that requires a DPIA and uses a screening checklist to identify the need for a DPIA, where necessary.	a.32.A. Evidence provided to ICO auditors of BMBC's DPIA template showed that the template does not refer to the most current legislation. This means that BMBC's DPIA process is unlikely to meet the standards required by the UK GDPR, and there is a risk that a DPIA is not carried out when it should be. B. BMBC do not keep records of occasions where, following completion of the DPIA screening checklist, the decision is made not to undertake a full DPIA. This means the rights and freedoms of individuals may not be taken into account, and there is a risk of non-compliance with Article 35 of the UK GDPR.	a.32.A. BMBC should update their DPIA template to incorporate the requirements of the UK GDPR. This will ensure that their process is compliant with the most up-to-date legislation. B. BMBC should start documenting the decision not to undertake a DPIA. This will ensure that reasons are evidenced and considered fully, minimising risk of infringing the rights and freedoms of individuals and non-compliance with Article 35 of the UK GDPR.	High
The organisation has created and documented a DPIA process	a.33. BMBC has been unable to evidence a documented DPIA policy or procedure. The Privacy Impact Assessment Guidance provided has not been updated since the introduction of the UK GDPR and DPA18, and there is a likelihood that the DPIA process may not sufficiently meet the requirements of Article 35 or 39 of the UK GDPR.	a.33. Create a documented DPIA policy or procedure, updated to include the requirements of the UK GDPR and DPA18. This gives assurance that the process meets the requirements of Articles 35 and 39 of the UK GDPR.	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
DPIAs are undertaken before carrying out types of processing likely to result in high risk to individuals' rights and freedoms and meet the requirements as set out in Article 35 of the UKGDPR.	a.34. There is minimal oversight of DPIAs by the DPO, and there is no set requirement to consult them during the DPIA process. There is a risk that Article 35(2) of the UK GDPR - "The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment" - is not met.	a.34. DPIAs should be overseen by the DPO and contain an area to record their advice and recommendations. The DPIA policy or procedure should reference the requirement to consult the DPO for advice during the process. This will ensure that Article 35(2) is met.	High
The organisation acts on the outputs of a DPIA to effectively mitigate or manage any risks identified.	a.35. There are no set parameters for when a DPIA needs reviewing, and the DPO does not have any oversight of DPIA reviews. This creates a risk of BMBC being in breach of the UK GDPR as they are not sufficiently mitigating the risks of processing.	a.35. The DPIA policy or procedure should detail when a DPIA needs reviewing, e.g. on an annual basis or when a parameter of processing changes. The DPO should have regular oversight of DPIA reviews to ensure they are being completed correctly. This will ensure BMBC is adequately mitigating the risks of processing in compliance with the UK GDPR.	High
The organisation has implemented appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively	a.36.A. The Personal Data Breach Reporting Policy and Procedure is out of date, and as such refers to the DPA98 rather than UK GDPR or DPA18. There is a significant risk that the policy does not accurately reflect BMBC's obligations under the newer legislations, such as the threshold for reporting a data breach and what information needs to be included in a report to the ICO. B. BMBC does not have specific training in place to ensure staff recognise a personal data breach or near miss, so there cannot be assurance that they are recording, reporting, and preventing data breaches correctly. This could result in a breach of Article 33 of the UK GDPR, which says "in the case of a personal data breach, the	a.36.A. BMBC should update their Personal Data Breach Reporting Policy and Procedure to include the UK GDPR and DPA18, and the obligations they place on controllers regarding personal data breaches. This will ensure that BMBC has a clear, consistent approach to data breaches and can fulfil their obligations under Article 33 and 34 of the UK GDPR. B. Formulate a specific training module around data breaches and near misses. By ensuring staff have appropriate training around recognising, reporting, and preventing data breaches, BMBC will have ongoing assurance that they are maintaining compliance with Articles 33 and 34 of the UK	Urgent

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority", and/or Article 34 of the UK GDPR - "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay." C. BMBC's Personal Data Breach Log does not include near misses at present, nor does it include details on the effects of the breach or any remedial action taken. The absence of specific training or a documented procedure means near misses are unlikely to be recognised and reported. This means BMBC is unable to ensure that they are adequately documenting data breaches. Where specific details such as effects or remedial action are not included, it means that BMBC are unable to carry out any analysis on individual incidents or trend analysis more broadly. As such, measures cannot be taken to prevent the same incident recurring, or to identify and remedy themes or trends.	GPDR. C. Create an area for recording near misses, effects of the breach, and remedial action taken on the Personal Data Breach Log. This will ensure that BMBC are recording breaches and near misses appropriately and can conduct analysis on both an individual and broad scale to inform mitigating and remedial actions.	
There are mechanisms in place to assess and then report relevant breaches to the ICO (within the statutory timeframe) where the individual is likely to suffer some form of damage e.g. through	a.37.A BMBC does not have a formal, documented process in place for considering whether to report a data breach to the ICO, meaning there is a risk the correct decision may not be made. If BMBC fails to report a breach that should have been reported, it would be in breach of Article 33 of the UK GDPR.	a.37.A. See b.31. B. BMBC should update their Personal Data Breach Log to include an area for recording whether a breach has been reported and details of the decision-making process. This would ensure that they are in compliance with Article 33(5) of the UK GDPR.	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
identity theft or confidentiality breach.	B. BMBC's Personal Data Breach Log does not include an area to record if a breach has been reported and the reasoning behind the decision. This means that in the event the breach was required to be reported, BMBC is unable to evidence the reasoning for the decision to not report. This means BMBC could breach Article 33(5) of the UK GDPR, which states "The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."		
There are mechanisms in place to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms	a.38.A. BMBC does not have a formal, documented process in place to inform affected individuals about a data breach that is likely to result in high risk to their rights or freedoms. This means that BMBC may fail to properly notify an individual, resulting in a breach of Article 34(1) of the UK GDPR. B. There is no oversight by the DPO of responses to individuals involved in a data breach, meaning there is little assurance that the response is compliant with Article 34(2) of the UK GDPR, which states that "The communication to the data subject...shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)".	a.38.A. Create a formal process for responding to individuals involved in a data breach, including when individuals need to be notified and what information needs to be incorporated in the communication to them. This will ensure that BMBC can demonstrate its compliance with Article 34 of the UK GDPR. B. Include the requirement to have sign-off from the DPO before sending out a notification to an individual. Alternatively, consider creating a standard template for notifying individuals that is DPO-approved, to ensure that the correct information is included and BMBC is complying with its obligations under Article 34 of the UK GDPR.	High

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
There is an Information Security Policy in place, which is approved by management, published, communicated to employees and subject to regular review.	b.1. There is an Information Security (IS) Policy in place which covers the main expected topics. However there is a lack of version control or summary table. It was not clear when this policy was last reviewed. Key elements of the policy are communicated to staff via the Personal Commitment Statement which they must confirm they have read and understood. If policies are not version controlled and regularly reviewed there is a risk that policies may not reflect current practice, latest sector guidance or legal guidance. Lack of evidence and review means that BMBC cannot demonstrate that it is acting in line with its legal responsibilities under UK GDPR Article 5.2 ('Accountability Principle') and UK GDPR Article 24.1 which says that controllers should have appropriate technical and organisational measures in place and that these should be 'reviewed and updated where necessary'.	b.1.Ensure that all policies have version control and summary tables in place to record details such as owner, date of review and updates to the policy. This will help BMBC meet its obligations under UK GDPR Articles 5.2 and 24.1. See also a.7.	High
Information security is incorporated within a formal training programme	b.2. There is mandatory GDPR eLearning in place for all staff. The training includes key elements of IS and has a quiz at the end with a set minimum pass rate of 80%. The training was designed by the Association of Greater Manchester Authorities in 2018. It is not clear whether the content has been reviewed or updated since.	b.2. The content of the GDPR training should be reviewed and where necessary updated or if this isn't possible additional training should be rolled out to staff to cover any gaps in the GDPR module. When reviewing eLearning content, consideration should be given to the latest threat, sector guidance and trend analysis of the BMBC data breach log to understand which key topics should be covered. The National Cyber Security Centre has produced some training for Cyber Security which may be useful to gain an understanding	Medium

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
		of which key topics should be covered for cyber threats. See NCSC Cyber Security Training.	
Lead responsibility for the strategic direction and oversight of IS has been assigned to an executive board member (e.g. Chief Information Officer or IT Director).	b.3. Staff interviewed demonstrated an understanding of their roles and responsibilities. However, this wasn't always clearly recorded within key documentation. Overall IG responsibilities have been documented in the IG Framework. However, not all roles with responsibilities specific to IS have been documented in IS Policy. For example the Chief Information Officer (CIO), the Senior Information Risk Owner (SIRO) and the Data Protection Officer (DPO). Some roles with operational responsibilities have been documented within the IS Policy, however there is no reference to the role of Buildings/ Facilities Management, the Operations Safety & Resilience Manager, Information Asset Owners (IAOs) and Information Asset Administrators (IAAs). If roles are not correctly documented and understood by key staff, there is the risk of responsibility drift and a lack of long term strategic focus and direction. This could lead to a lack of a central compliance culture across the council and ultimately non-compliance with IG legislation.	b.3. Review the IS Policy to ensure all staff with strategic and operational responsibilities for IS are included. Alternatively the roles and responsibilities within the IG Framework could be expanded to include clear IS roles and responsibilities. The IS Policy could then refer back to the IG Framework for further detail. See also a.7.	Medium
Operational responsibility has been assigned for the development and the	See b.3.	see b.3.	

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
implementation of information security within the organisation.			
A steering group meets regularly to mandate, and monitor IS improvements.	b.4.A. There are several groups which consider IG and IS matters. There is an IG Group which is chaired by the SIRO and attended by the DPO and CIO. The SIRO has responsibilities for Core Corporate Services and has good oversight of these areas. The Caldicott Guardians for Children's Services and Adult Services also attend. It is possible other service areas may not have the same input or be able to feedback to the same extent on IG matters. If services are not able to feedback on these issues, there is a risk BMBC will lack central oversight of issues and risks across the organisation. There is also a risk that service areas may take divergent or non standardised approaches to promoting IG policies and compliance. B. There is also the IT & Digital Weekly Operations Board which is attended by key IT staff including the Head of ICT and the Information Security Manager and the ICT Unit Management Team which meets monthly and is attended by key staff from operational areas. The IS Policy appears to be outdated and refers to an ICT Security Working Party. C. There appears to be no documented or oversight link between the IT Governance groups and the IG Group. However the CIO who has responsibility for IT security does sit	b.4. A. BMBC should consider either adding representatives from other key services areas to the IG Group or creating an IG Steering Group which sits under and reports into the IG Group with key representatives from all services areas of the Council. This will help to ensure that overview of IG risks is more rounded and help to embed a more centralised version of compliance across the council. B. Update the IS Policy to refer to the IT & Digital Weekly Operations Board and the ICT Unit Management Team Meetings C. Ensure that either the minutes from the IT & Digital Weekly Operations Board and the ICT Unit Management Team Meetings are made available to members of the IG Group or the CIO should consider giving a summarised update of key issues/ concerns from these groups at each IG Group meeting. This will ensure a connection between IG and ICT security is maintained and fully documented. D. BMBC should ensure that IAOs and IAAs carry out periodic checks on the security of personal data once staff are allowed to work on a more regular basis within the Council buildings. The checks could include security	Medium

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
	on the IG Group. If there is no clear governance link between these groups, then there is a risk of a disconnected approach to governance and oversight of IG and ICT security issues. This could lead to duality or divergence in how compliance with IS should be managed. D. It wasn't clear to what extent physical security of personal data was considered by these groups as a standing agenda item. It is likely that physical security will be discussed as a side product of records management and compliance with information security standards such as PSN and the Data Security & Protection Assessment Toolkit. Security walk arounds were carried out as part of the GDPR internal audit. However, there is no regular reporting around standard information security compliance checks.	walk arounds to check storage areas are locked, that desks are clear, and screen are locked when staff are away from desks and that documents are not left lying around at printers or in other areas. Results should be recorded and feedback back to staff involved and the IG Group.	
There are appropriate security controls in place for home or remote working.	b.5. It was reported that Remote Working and Home Working requirements were assessed as part of the Covid - 19 contingency plans asking staff to work from home. The Remote Working Policy says it was last reviewed in 2013. It was not clear when the Individual Homeworking Policy was last reviewed or updated as it didn't include version control or a summary table. If version control information is not updated BMBC will not be able to evidence that it has reviewed its technical and organisational measures to ensure they remain adequate and in line with UK GDPR Article 24.1.	b.5. Update the Remote Working Policy to include up to date version control information and the date of review. The Individual Homeworking Policy should be updated to include version control and a summary table to detail any reviews of updates. This will help BMBC to evidence its reviews of these security arrangements.	Medium

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
Hardware and software assets have been identified, documented and classified; and appropriate protection responsibilities have been defined.	b.6.ICO auditors were provided with evidence of centralised asset management for hardware & devices, servers and applications. The IS Policy references asset registers held by a nominated officer in each service area. It wasn't clear to what extent service areas would hold and manage local hardware registers now that the most staff have an assigned a Multimedia Device (laptop or tablet) via IT and a log of these is maintained on Support Works by the Service Desk.	b.6. Review and update the IS Policy to ensure that it reflects current practice with regards to the management of IT hardware and software assets.	Low
Hardware and software asset registers/inventories are subject to periodic risk assessment	b.7. There is no formally documented risk assessment methodology within the IS Policy around assessment of risks to hardware and software assets. The Applications Inventory includes a risk status based on the importance of the application to core services. However, there doesn't seem to have been a risk assessment documented for IT hardware and server assets. If risks to assets which store or process personal data have not been assessed this may be in breach of UK GDPR Article 5.1.(f) 'Integrity and confidentiality principle'. Also UK GDPR Article 32.1 says there should be a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures. It is also important to review these measures as the context of the organisation changes, the risks applied to different assets may alter in severity or likelihood, and controls may become outdated.	b.7. Create and document a risk assessment methodology within the IS Policy for assessing IT hardware (including servers) and software assets. Assessments could include the owner of the asset, location, a risk assessment based on the criticality of the asset to the organisation, security category and estimated value, any key threats and vulnerabilities, likelihood and impact, existing controls and gap analysis. A generic assessment may be applicable for some assets and should be referenced. These risk assessments should be revisited periodically to check whether the threat status has changed.	Medium

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
There are procedures in place to ensure all employees (permanent and temporary staff) and third party users return all hardware assets upon termination of their employment, contract or agreement.	b.8. Evidence was provided to ICO auditors on the return of IT hardware/ assets when a member of staff leaves BMBC. However, the IS Policy doesn't document the process. If processes aren't adequately documented, there is a risk that BMBC cannot demonstrate it has appropriate polices in place for the management of its devices/hardware. There is also the risk that different staff or service areas may diverge from the expected processes to varying degrees.	b.8. Update the IS Policy to include details of the process for allocation and return of IT assets.	Low
There is a documented governance structure surrounding the use of removable media.	b.9. It was reported that BMBC may not keep an up to date list of all USB sticks. It is felt the risk is low due to the devices being encrypted. Whilst the risk of data breaches may be lower through the use of encrypted devices, a list should be maintained for audit/evidence purposes. It will also help BMBC to know which USB stick devices are in use and who has access to these. Without an up to date list BMBC may be a risk of not being able to evidence control of these devices.	b.9.Ensure that an updated list of all USB sticks provided by the BMBC is maintained.	Low
Media containing information is protected against unauthorised access, misuse or corruption during transportation.	b.10. There are documented rules in place around the transportation of data via removable media within the IS Policy, the Personal Commitment Statement and the Records Management Policy. However, no formal risk assessment has been documented around how data should be safely transported. It was reported that staff do assess the risks, but this was on an ad hoc and informal basis. If risk assessments are not clearly	b10. Document a formal risk assessment around methods of transporting removable media. These assessments should be periodically reviewed.	Low

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
	documented and reviewed periodically there is a risk that BMBC may not be able to evidence that sufficient consideration was given to the risks involved in transportation of certain times of removable media in compliance with UK GDPR Article 32.1 which says that measures in place should be assessed and reviewed to ensure they remain sufficient.		
There are endpoint (port) controls in place to prevent unauthorised use of removeable media or the upload or download of unauthorised information.	b.11.There are currently no endpoint controls in place to prevent unauthorised use of removable media. If there is no endpoint control, the organisation risks that personal data may be removed from its systems or systems may be compromised. It may also be in breach of UK GDPR Articles 24 and 32 which says that appropriate technical and organisational measures should be in place.	b.11. BMBC should consider adopting Group Policy controls to manage access to endpoint devices. This will allow BMBC to select which devices are able to use endpoints/ ports.	High
Removeable media is disposed of securely when no longer required, using formal procedures.	b.12.Devices and hardware are securely disposed of. However, BMBC don't receive a certificate of destruction from their third party disposal service provider. This means that BMBC is unable to evidence secure destruction of hardware and devices or be able trace destruction for audit and investigation purposes.	b.12.Ensure that a receipt of certificate of destruction is obtained from the third party disposal service provider. This should record the date, either list or provide detail of the weight or number of devices taken, method of destruction and date of destruction. This is normally signed off by an appropriate person from the supplier. BMBC should keep the receipt or destruction certificate for audit purposes. Certificates or receipts can be disposed of in line with the corporate retention schedule.	Medium
Appropriate background checks are carried out on personnel (employees, contractors, and third-party users) if required for	b.13.The requirements for some staff roles to undertake security clearance checks prior to commencement of employment is not referenced within the ICT Access Control Policy or Records Management Policy.	b.13. Ensure requirements around security clearance checks for certain staff roles and access to certain systems is reflected in the Access Control Policy and Records Management Policy.	Low

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
their duties and responsibilities.	The practice of undertaking security checks on some staff roles should be referenced within key IS policies to evidence that consideration has been given to these requirements in line with UK GDPR Articles 5.1.(f) ' Integrity and confidentiality principle' and 32 'Security of processing'.		
The allocation and use of privileged access rights is restricted and controlled.	b.14.Interviewees described that the process for allocation of and removal of privileged access rights. However, the ICT Access Policy doesn't reference this process. It also isn't clear whether service areas have a documented process for management of privilege access rights for their service specific applications. Without a formally documented process, there is the risk that access rights will be granted in an inconsistent or incorrect fashion, and that poor records will be kept.	b.14. Ensure that a documented process is in place around the granting and removal of privileged access rights for both central IT systems and applications managed at service level.	Medium
User access rights are reviewed at regular intervals	b.15. No formal regular reviews of user access rights have been carried out. System owners may request sight of users with access to systems on an ad hoc basis. If users change role and retain all their previous rights, they may keep access to personal data which is no longer relevant to their job role. Retention of key system access rights should be caught partially by the internal movers process which is managed by the IT Service Desk. However this may not capture access rights to service	b.15. BMBC should carry out regular sample checks of staff access rights on key systems to check that staff have the correct access based on their role. The results of any checks should be recorded and reported back to the relevant service area and governance groups. This will help to provide assurance that access management processes are working as expected.	Medium

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
	specific applications. Further, if the context of a role has changed, those staff may no longer require the same level of access previously needed. This may lead to a breach of UK GDPR Article 5.1(f)'Integrity and confidentiality' principle.		
Access rights are restricted or removed in a timely fashion for all staff	b.16.Interviewees were able to describe how movers and leavers access rights were granted, altered or removed. However, no formally documented IT movers and leavers process was provided as evidence. If processes are not formally documented there is a risk that BMBC cannot demonstrate that it has appropriate technical and organisational controls in place to govern access to systems which hold and process personal data. There is also the possibility that practices may diverge between expected practice and reality and may be applied differently between service areas.	b.16.Document the movers and leavers process for altering and removing access rights to systems and applications.	Medium
Access rights are adjusted upon a change of assignment/role	see b.16.	see b.16.	
Secure areas (areas that contain either sensitive or critical information) are protected by appropriate entry controls to ensure that only authorised personnel are allowed access.	b.17. All staff are provided with electronic card passes to access non public areas of the main council buildings and workspaces. Further security such as fobs and pin code access are required to access more sensitive areas. The IS Policy contains some details around physical security and access controls. However, these seem to be focused on access to the Computer Suite rather than general building access controls. UK GDPR Article 5.2	b.17. Either expand on physical access controls for buildings within the IS Policy or create a separate physical access policy which sets out all the access controls measures in place around BMBC's offices and buildings where personal data or It systems may be accessed.	Medium

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
	requires the controller to evidence compliance with the principles set out in Article 5.1(f) Integrity and confidentiality Principle. As the IS Policy doesn't clearly document these requirements BMBC are at risk of non compliance.		
Regular risk assessments and testing are undertaken to provide assurances that effective physical security controls are in place	b.18.A. In the past, the SIRO has carried out an ad hoc security walk-around and clear screen and desk check within the Town Hall. Internal Audit also conducted an after hours walk around to check on security of devices and information in Town Hall and 3 Knowsley Place. There was no evidence that IAOs and IAAs were undertaking similar periodic checks at service level. B. No evidence of formal risk assessments around physical security of IT equipment and information storage areas has been provided. The majority of staff are currently homeworking. Regular risk assessment and security testing should be undertaken and reviewed to ensure that effective physical security controls are in place. UK GDPR Article 32 states that security measures should be reviewed to test their effectiveness.	b.18.A. Whilst we recognise most staff are currently working from home, once staff return to working in BMBC's buildings, an improved schedule of regular security checks to include those at service level should be created, carried out, results documented and should also include checks done at service level by IAOs or IAAs. Other tests could also include testing of tailgating and whether staff ask for ID for an unknown person. Results should be recorded and reported back to relevant staff and the IG Group. B. A formal risk assessment should be documented for all key BMBC buildings and should include what security measures are in place and provide a gap analysis for any risks which have not been mitigated. This should be reviewed on a periodic basis or when changes occur to the layout or the use within the building.	Medium
Granting of entry / access rights is controlled, and those rights are reviewed on a regular basis to ensure that only	b.19.A. It was reported that a record of all staff with access to BMBC buildings via the electronic card is maintained. It was not clear whether access rights are ever reviewed or audited.	b.19. A & B. Document a procedure around the granting and revoking of physical access to BMBC offices and buildings. A regular sample check should be conducted to ensure that staff have the correct access permissions.	High

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
authorised personnel are allowed access	B. There is some information around buildings security which is available to staff on the intranet. This is more in the form of guidance to staff on how to apply for an access card rather than a formal Physical Access Policy. If Physical Access Controls have not been formally been documented there is a risk that BMBC cannot demonstrate it have effective organisational controls and measures in place around the protection and security of personal data. If physical access rights and processes are not reviewed on a regular basis there is no reassurance that access to restricted information is not retained by staff who should no longer have access to it.		
Manual records are stored securely and access to them is controlled.	b.20. It was reported that some staff in the Town Hall may not have access to a key safe. Keys were hidden away within a container within a drawer. If keys are not stored safely and securely there is a risk that they could be lost or stolen and access to information impeded or accessed without authorisation.	b20.Consider installing key safes for all key office areas. This will allow central and safe storage of keys to lockers and secure storage areas.	Medium
A clear desk policy is in operation across the organisation where personal data is processed.	b.21.There are clear desk and screen requirements in place. However no regular for checks are carried out.	see b.18.A.	
There is a 'clear screen' policy in operation across the organisation where personal data is processed.	See b.21. b.22.The IS Policy says that screens auto lock after 30 minutes of inactivity. This means that	See b.21. b.22.BMBC should explore the possibility of ensuring auto screen lock is engaged after a	Medium

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
	if someone forgets to lock their screen and leaves their desk there is a risk that someone main gain unauthorised access to the staff members' laptop, emails and applications.	shorter period of inactivity. This will help to reduce the risk of authorised access to staff members' devices, emails and applications.	
There are records showing secure disposal of equipment (e.g. destruction logs and certificates)	see b.12.	see b.12.	
Logging and monitoring is in place to record events and generate evidence.	b.23. There is no event logging policy in place. The need for event logging is only briefly referenced within the IS Policy. This means BMBC hasn't set out its formal approach to event logging and its responsibilities in line with UK GDPR Article 32. Policies help to evidence compliance with the legislation.	b.23.Include a policy covering event logging within the IS Policy. This should set out what elements should be logged at a minimum and how these logs should be stored and when they should be consulted.	Low
The organisation has an awareness of the lifespan of current operating systems and software and has taken appropriate measures to mitigate any risks	b.24. The Software Applications Register doesn't record whether applications are approaching end of life status. Systems which are outside of their support lifespan are vulnerable to cyberattack, as they are no longer updated when new vulnerabilities are discovered.	b.24.BMBC need to keep an up to date list of any applications near end of life status so it is aware of any threats or issues this may pose and take appropriate measures to mitigate this risk.	Medium
Networks undergo regular vulnerability scanning	b.25. It was reported that any vulnerabilities detected via Nessus, McAfee and OCS would be discussed at IMT and the IT & Digital Operations Board meetings. However there is no documented process explaining how vulnerabilities detected are managed and risk assessed. If procedures are not documented, then BMBC may not be able to evidence how it manages	b.25.Document how any vulnerabilities detected are managed, risk assessed and mitigated. This should be included in the IS Policy.	Low

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
	security threats in line with its responsibilities under UK GDPR Article 32.		
Patch management practices are established and effective	b.26. ICO auditors have seen evidence of patch management processes. However this has not been documented in the IS policy. Patch management processes should be documented for evidential purposes to demonstrate that BMBC has given consideration to its compliance responsibilities under UK GDPR Article 32.	b.26. Document BMBC's approach to patch management within the IS Policy.	Low
The installation of new software is controlled, and risk assessed	See b.27.	see b.27.	0
DPIAs have been carried out to understand and mitigate risks prior to IT suppliers being granted access to the organisation's assets	b.27.A. A copy of the Standard Procurement Pre Qualification Questionnaire was provided. It contained some standard security questions, particularly around previous experience. However the questions could have been expanded on to check basic UK GDPR and information security requirements. Checks should be made to ensure that risks associated with IT suppliers have been foreseen and controlled. B. A copy of the Privacy Impact Assessment (PIA) Guidance was provided. This appears to be outdated and refers to the DPA 98. The guidance doesn't reference the fact that the ICO need to be notified where risks cannot be mitigated. A PIA form was provided alongside	b.27.A. BMBC should expand their Pre Qualification Questionnaire to include more questions around GDPR and IS compliance. For example check if suppliers adhere to any recognised standards, For example ISO27001. BMBC could also ask for copies of DP Policies and IS Policies for details of what security measures suppliers have in place and what IG training staff have received. This should help to provide a baseline check of the suppliers security measures. More detailed and tailored questions should be asked where the processing may involve special category data, large amounts of personal data or where the type of processing may produce risks to security, rights and freedoms of individuals. B. See a.32.A & a.33. and a.34. Ensure there is an area of the form to also record guidance from IT where appropriate. See our guidance on DPIAs	Medium

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
	the guidance. The form doesn't seem include an area to record DPO and IT staff comments. If the DPIA doesn't meet the requirements set out under UK GDPR Article 35 then BMBC is at risk of non compliance.		
Contracts and agreements are in place with IT suppliers, and include relevant information security requirements	b.28. The iTrent Contract was submitted as evidence to ICO auditors. The contract is governed under the G-Cloud framework. However, there didn't seem to be any reference in the contract to reporting of information security or personal data breaches. If information security and personal data breach reporting processes are not clearly outlined in the contract there is a risk that breaches may not be reported within statuary timescales. This may lead to non compliance with UK GDPR Article 33.	b.28.Gain assurance from the supplier that it will notify BMBC within a reasonable timeframe of any information security breached or personal data breaches. All breaches should be notified to a nominated person.	High
There are processes in place to ensure that information security incidents are internally reported, assessed, classified, recorded, and analysed as quickly as possible	b.29.The Personal Data Breach Reporting Guidance doesn't reference how personal data breaches should be investigated, escalated and risk assessed. No risk scoring matrix has been included in the guidance. If there are no clear processes in place, the organisation may not effectively respond to incidents, creating greater risks to personal data in the process.	b.29. Update the Personal Data Breach Reporting Guidance document to include reference to how personal data breaches are investigated, risk assessed and escalated. A risk matrix should be included to explain how risks should be measured.	Medium
There is an incident log in place to capture all reported incidents and near misses	b.30.The data breach log doesn't include any details of a risk assessment of the incidents, categorisation of incidents or lessons learned and whether the ICO and individuals have been notified. This means BMBC may not be able to pull	b.30. BMBC should record the information detailed opposite and carry out trend analysis reports. Reports should be provided to the IG Group. See also a.37. b.	Medium

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
	trend analysis and compliance information around its performance on personal data breach reporting process and incidents.		
There are processes in place to ensure incidents are reported to the ICO as appropriate and within the required statutory timeframes (72 hrs) under the UKGDPR	b.31. There is nothing referenced within the Personal Data Breach Reporting Guidance around when BMBC are required to report incidents to the ICO and what information needs to be provided. If the process is not clearly documented BMBC may not report incidents when required and may be at risk of non compliance with UK GDPR Article 33.	b.31. Update the Personal Data Breach Reporting Guidance document to refer to the fact that the ICO needs to be notified within 72 hours of BMBC becoming aware of an incident and where the breach is likely to result in a risk to the rights and freedoms of individuals. It should also set out the information that needs to be provided to the ICO as part of the notification process (see UK GDPR Article 33.3)	High
There are mechanisms in place to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms	b.32. Some guidance is provided within the Personal Data Breach Reporting Guidance about notifying individuals of a personal data breach. However, there is no reference to the threshold under UK GDPR Article 34.1 which says that if a personal data breach is likely to result in a high risk to the rights and freedoms of individuals then they should be notified. If this requirement isn't documented, then BMBC is at risk of not complying with this requirement as staff may not realise when individuals have to be notified (and when it is not just discretionary).	b.32.Update the Personal Data Breach Reporting Guidance document to include reference to the need to notify individuals when the risk is likely to result in a high risk to the rights and freedoms of the individual. See also a38.A.	Medium

Freedom of Information			
Control measure	**Non-conformity**	**Recommendation**	**Priority**
Policies and procedures are in place which explain the organisation's approach to, and responsibilities for, FOI and EIR regulations	c.1.A. Whilst FOI policies and procedures are in place the documents are out of date and need updating to reflect current BMBC practice. B. Not all policy and procedure documents have owners and are not adequately controlled. This may lead to staff following incorrect or using out of date policies and procedures.	c.1.A. BMBC should review and update its current policy and procedure documents for FOI so as to provide an accurate and cohesive range of documents for staff use. B. BMBC should apply comprehensive document controls to its published policies and procedures and then review those documents on a regular basis.	Medium
Policies and procedures are easily accessible by staff	c.2. No explicit provision has been made to make policies and procedures easily accessible to staff who do not use computers. This may result in them taking non-compliant actions on behalf of BMBC.	c.2. BMBC should make provision to ensure staff who do not use computers are aware of how they can access FOI procedures. Managers should make staff aware they can request a hard copy or can make provision for them to use the BMBC intranet.	Medium
The organisation ensures that staff are informed of any changes to policies and procedures regarding FOI/EIR regulations	c.3. Whilst updates to policies and procedures are cascaded by managers, there is no assurance that staff have read and understood them. This means that staff, particularly those who process requests in different delivery service areas may not be following current guidance and risk non-compliance with FOI/EIR legislation.	c.3. BMBC should gain assurance that staff have understood FOI/EIR updates to policies and procedures and will be able carry out their role in line with internal or statutory requirements.	Medium
There are procedures publicly available to direct individuals in how to request information under FOI / EIR.	c.4. The BMBC website only details using the online form or writing to the council to make an FOI request. This published guidance could prevent a request being made and lead to complaints being raised. Requestors may prefer to use email or other electronic means and could see this as potentially restricting their rights.	c.5. BMBC should review the web page to take into account current ICO guidance and the Section 45 Code of Practice for access to ensure that they maintain compliance with the legislation and can be seen to be acting in line with current guidance.	High

Freedom of Information			
Control measure	**Non-conformity**	**Recommendation**	**Priority**
The organisation maintains a documented record of their receipt and handling of requests	c.5. BMBC has an FOI Case Management System (CMS) which is effective in managing and monitoring the statutory timescales for requests but has no functionality to easily report on exemptions used, refusals etc. This prevents the council form carrying out any trend analysis on requests for quality monitoring purposes.	c.5. When evaluating an upgrade or replacement for the current CMS BMBC should consider adding functions to enable trends to be easily identified for quality monitoring purposes as an aid to maintaining compliance.	Low
There are mechanisms to monitor the quality of responses to requests	See c.5.	See c.5.	
Exemptions/Exceptions should be applied on a case-by-case basis, by appropriately trained staff, with no evidence of the use of blanket exemptions/exceptions.	c.6. There is no universal formal training programme for staff with responsibility for dealing with FOI and EIR requests for information. If staff do not have the necessary skills to handle tasks such as applying exemptions and redactions, BMBC may find itself acting without compliance, and/or responding to requests in an inconsistent manner. In addition this training should be regularly refreshed to ensure the quality of responses continue to maintain compliance.	c.6. BMBC should formalise a training programme for all staff with responsibility for handling FOI/EIR requests. The training should be recorded within the staff training system. Regular refresher training should also be implemented, which again should be recorded to give assurance.	High
There is evidence of an oversight or approval process for the use of exemptions/exceptions.	c.7. There is no program of sampling of completed requests for the purposes of quality monitoring. This prevents BMBC form having any oversight as to where issues in FOI compliance may be developing.	c.7. BMBC should instigate a sampling programme for FOI responses in order to ensure a consistent quality of response and to maintain compliance.	Medium
Redactions should be applied on a case-by-case basis, by appropriately trained staff, and records should be maintained of what has been redacted.	See c.6.	See c.6.	

Freedom of Information			
Control measure	**Non-conformity**	**Recommendation**	**Priority**
There is evidence of an oversight or approval process for the use of redactions.	See c.7.	See c.7.	
There is an induction training programme, with input from Information Governance or equivalent, which includes general training on how FOI/EIR applies to the organisation, what they currently do to comply, and how to recognise an FOI/EIR request.	c.8. By combining FOI and DP training into one module staff appear unsure as whether they have received training in FOI. This may cause confusion for staff when working with the legislation(s) that in turn could lead to non-compliance in either DP or FOI.	c.8. To ensure staff can clearly differentiate the requirements of both types of legislation the FOI training should be developed into its own mandatory eLearning module. This FOI module should be mandatory and refreshed annually in line with the DP training.	High
Staff receive refresher training in the requirements of FOI/EIR, including, where appropriate, updates from the relevant decisions of the ICO and the Information Tribunal.	See c.8.	See c.8.	
There is specific training for staff with responsibility for handling requests for information, on FOI, EIR and Codes of Practice.	c.9. There is no universal specialised formal training programme for staff with responsibility for handling requests for information, on FOI, EIR and Codes of Practice. If staff do not have the necessary skills to handle specialist tasks, BMBC may find itself acting without compliance, and/or responding to requests in an inconsistent manner. In addition there is no formal periodic refresher training for these staff, this	c.9. BMBC should formalise a specialist training programme for all staff with responsibility for handling FOI/EIR requests. The training should be recorded within the staff training system and refreshed on a regular basis to give continued assurance.	High

Freedom of Information			
Control measure	**Non-conformity**	**Recommendation**	**Priority**
	potentially could lead to responses that are non-compliant.		
Staff receive regular reminders of how to recognise FOI/EIR requests	c.10. BMBC does not use periodic communication methods such as newsletters or reminder emails to remind all staff of how to recognise and react to FOI/EIR requests. If staff do not recognise requests, they may not inform the contact centre the request has been submitted, which may prevent it being responded to within the statutory timescale.	c.10. BMBC should undertake a programme of periodic communications to remind staff of how to recognise and respond to FOI/EIR requests.	Medium

Observations

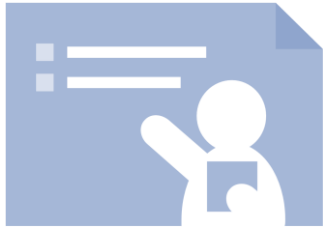
The tables below list observations made by ICO auditors during the course of the audit along with suggestions to assist BMBC with possible changes.

Governance & Accountability	
Control	**Observation**
Privacy information is concise, transparent, intelligible and uses clear and plain language	The Assistant Director for Children's Care and Safeguarding highlighted that his directorate were planning ahead and considering working alongside SEND provision parent groups around privacy information. They currently work with these group to coproduce policies and procedures, which has been effective, and this could be an opportunity to ensure privacy information is accessible and useful.

Information Security	
Control	**Observation**
Good information security practices are promoted across the organisation.	There is no formal information governance (IG) communication plan in place. A communication plan will help coordinate and focus on key IG topics and reminders to be rolled out across the year.
There is a policy that documents the process and supports the security measures the organisation uses to manage the risks introduced by using mobile devices.	To add an additional layer of compliance, BMBC could consider asking staff to check and state that they have certain security requirements before being allowed to work from home (once normal working practices resume). This could cover for example checks that Wi-Fi passwords have been reset, that certain security standards are in place regarding locks on doors and windows.

There are procedures in place to ensure all employees (permanent and temporary staff) and third party users return all hardware assets upon termination of their employment, contract or agreement.	BMBC should consider carrying out sample checks on historic leavers to check that all hardware has been returned. This is in line with good practice
Key systems, applications and data are backed up to protect against loss of personal data.	When normal operations are resumed, BMBC should consider scheduling periodic full systems tests of the back-up of key systems to check that back-ups can be restored as expected.
The plans are tested on a periodic basis to ensure they remain up to date and fit for purpose	Following a return to normal operations BMBC should consider implementing periodic unscheduled tests of the Business Continuity Plans.

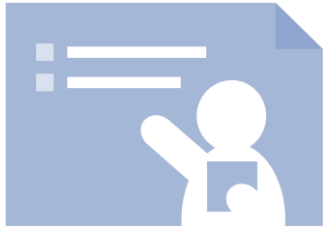
Appendices



Appendix One – Recommendation Priority Ratings Descriptions

Urgent Priority Recommendations - These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of data protection legislation.
High Priority Recommendations - These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of data protection legislation.
Medium Priority Recommendations - These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced.
Low Priority Recommendations – These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to completion.

Credits



ICO Team Manager – Paul Hamill
ICO Engagement Lead Auditor – Helen Oldham
ICO Lead Auditor – Amelia Walsh
ICO Lead Auditor – Ian Dale

Thanks

The ICO would like to thank Sally Lever, IG Project support and Business Support Manager, Lisa Featherstone, Deputy Director Governance and Assurance and Janet Witkowski, Head Legal Services and Data Protection Officer for their help in the audit engagement.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Bury Metropolitan Borough Council.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of Bury Metropolitan Borough Council. The scope areas and controls covered by the audit have been tailored to Bury Metropolitan Borough Council and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.

This page is intentionally left blank

Assertion	Input Type	OLD v3 20-21 Evidence ref	v4 21-22 Evidence ref	Change summary	Evidence Text - NHS Trusts and CSUs (Category 1)	Tool Tips - NHS Trusts (Category 1)	Required to meet standard (mandatory) - NHS Trusts and CSUs (Category 1)	Evidence Text - CCG and ALBs" (Category 2)	Tool Tips - CCG and ALBs (Category 2)	Required to meet standard (mandatory) - CCG and ALBs (category 2)	Evidence text - Others (Category 3)	Tool tips - Others (Category 3)	Required to meet standard (mandatory) - Others (Category 3)	Evidence text - GP (Category 4)	Tool tips - GP (Category 4)	Required to meet standard (mandatory) - GP (Category 4)
The organisation has a framework in place to support Lawfulness, Fairness and Transparency	Text	1.3.1	**1.1.1**	No changes	What is your organisation's Information Commissioner's Office (ICO) registration number?	You can get this number from the [Information Commissioner's Office website](https://ico.org.uk/esdwebpages/search)	Yes	What is your organisation's Information Commissioner's Office (ICO) registration number?	You can get this number from the [Information Commissioner's Office website](https://ico.org.uk/esdwebpages/search)	Yes	What is your organisation's Information Commissioner's Office (ICO) registration number?	Registration with the ICO is a legal requirement for every organisation that processes personal information, unless they are exempt as a small charity. If your organisation is not already registered, you should [register as a matter of urgency](https://ico.org.uk/for-organisations/data-protection-fee/). You can check whether you are registered and what your ICO registration number is on the [Information Commissioner's Office website](https://ico.org.uk/esdwebpages/search)	Yes	What is your ICO registration number?	You can get this number from the [Information Commissioner's Office website](https://ico.org.uk/esdwebpages/search)	Yes
	Document	1.4.1	**1.1.2**	Reword for cat 1 and 2	Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.	Please see [additional guidance.](https://www.dsptoolkit.nhs.uk/Help/88)	Yes	Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.	Please see [additional guidance.](https://www.dsptoolkit.nhs.uk/Help/88)	Yes	Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?	To be compliant with data protection legislation you must have a list or lists of the different ways in which your organisation holds personal and sensitive information (e.g. filing cabinet, care planning system, laptop). This list is called an Information Asset Register (IAR) and it should detail where and how the information is held and how you keep it safe. You should also have a list or lists of the types of personal data that are shared with others, for example needs assessments, prescriptions, payslips, care plans. This list is called a Record of Processing Activities (ROPA) and should detail how the data is shared and how your organisation keeps it safe. It is fine to have either two separate documents or a single document that combines both lists. The list(s) should be reviewed and approved by the management team or equivalent since 1st July 2021. Upload the document(s) or link to the document or specify where it is saved. Example IARs and ROPAs are available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/).	Yes	Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?	To be compliant with data protection legislation you must have a list or lists of the different ways in which your organisation holds personal and sensitive information (e.g. filing cabinet, care planning system, laptop). This list is called an Information Asset Register (IAR) and it should detail where and how the information is held and how you keep it safe. You should also have a list or lists of the types of personal data that are shared with others, for example needs assessments, prescriptions, payslips, care plans. This list is called a Record of Processing Activities (ROPA) and should detail how the data is shared and how your organisation keeps it safe. It is fine to have either two separate documents or a single document that combines both lists. The list(s) should be reviewed and approved by the management team or equivalent since 1st April 2020. Upload the document(s) or link to the document or specify where it is saved. Example IARs and ROPAs are available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/).	Yes
	Document	New	**1.1.3**	New	Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.	Please provide documentary evidence.	Yes	Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.	Please provide documentary evidence.	Yes						
	Date	1.4.2	**1.1.4**	No changes	When did your organisation last review both the list of all systems/information assets holding or sharing personal information and data flows?	The list should be reviewed since 1st July 2021 to ensure it is still up to date and correct. It should be approved by the SIRO or equivalent.	Yes	When did your organisation last review both the list of all systems/information assets holding or sharing personal information and data flows?	The list should be reviewed since 1st July 2021 to ensure it is still up to date and correct. It should be approved by the SIRO or equivalent.	Yes						
	Text	1.1.2	**1.1.5**	No changes	List the names and job titles of your key staff with responsibility for data protection and/or security.	Details are required only for staff who have a specialised role.	Yes	List the names and job titles of your key staff with responsibility for data protection and/or security.	Details are required only for staff who have a specialised role.	Yes	Who has responsibility for data security and protection and how has this responsibility been formally assigned?	Whilst data security and protection is everybody's business, someone within your organisation must take overall senior responsibility for it. There must be at least one named person who leads on data security and protection. Their responsibility is to provide leadership and guidance from a senior level. In the text box, write the name(s) of the person or people within your organisation with overall responsibility for data security and protection. Then, for each person, describe how this responsibility has been formally assigned to them. For instance, this responsibility could form part of their job description, or be noted in the minutes of a management meeting, or be in an email from the appropriate director in your organisation. Your organisation may also have additional specialised roles, for example a Data Protection Officer (DPO). [Read more about data security and protection responsibilities and specialised roles](https://www.digitalsocialcare.co.uk/resource/data-security-and-protection-responsibilities/)	Yes	Who has responsibility for data security and protection and how has this responsibility been formally assigned?	Whilst data security and protection is everybody's business, someone within your organisation must take overall senior responsibility for it. There must be at least one named person who leads on data security and protection. Their responsibility is to provide leadership and guidance from a senior level. In the text box, write the name(s) of the person or people within your organisation with overall responsibility for data security and protection. Then, for each person, describe how this responsibility has been formally assigned to them. For instance, this responsibility could form part of their job description, or be noted in the minutes of a management meeting, or be in an email from the appropriate director in your organisation. Your organisation may also have additional specialised roles, for example a Data Protection Officer (DPO). [Read more about data security and protection responsibilities and specialised roles.](https://www.digitalsocialcare.co.uk/resource/data-security-and-protection-responsibilities/)	Yes
	Yes/No	New	**1.1.6**	New	Your organisation has reviewed how you ask for and record consent.	Provide details in the comments. Further guidance is available on the [ICO website](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).		Your organisation has reviewed how you ask for and record consent. And has systems to record and manage ongoing consent.	Provide details in the comments. Further guidance is available on the [ICO website](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).		Your organisation has reviewed how you ask for and record consent. And has systems to record and manage ongoing consent.			Your organisation has reviewed how you ask for and record consent. And has systems to record and manage ongoing consent.	Further guidance is available on the [ICO website](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).	
	Yes/No	1.7.2	**1.1.7**	Removed from Cat 3	Data quality metrics and reports are used to assess and improve data quality.	Published data quality metrics and reports such as the Data Quality Maturity Index (DQMI) are reviewed and actioned in a timely manner to continually improve data quality.	Yes	Was the scope of the last data quality audit in line with guidelines.	The data quality audit should be in the last twelve months and scoped to the [Service User Data Audit guidance.](https://www.dsptoolkit.nhs.uk/help/1	Yes						
	Text	New	**1.1.8**	New	A data quality forum monitors the effectiveness of data quality assurance processes.	Guidance on establishing internal data quality assurance processes and undertaking Clinical Coding Audits can be found in the [Data Security Standard 01 big picture guide](https://www.dsptoolkit.nhs.uk/Help/23).	Yes	A data quality forum monitors the effectiveness of data quality assurance processes.	Guidance on establishing internal data quality assurance processes and undertaking Clinical Coding Audits can be found in the [Data Security Standard 01 big picture guide](https://www.dsptoolkit.nhs.uk/Help/23).	Yes						
Individuals' rights are respected and supported	Document	1.3.2	**1.2.1**	No changes	How is transparency information (e.g. your Privacy Notice and Rights for individuals) published and available to the public?	This covers personal information you collect or manage for patients including children, and the public, include a list of rights and when/whether they apply to the processing undertaken, contact details and procedure for subject access, right to rectification and other rights requests. Provide a weblink if possible or other publicly available document.	Yes	How is transparency information (e.g. your privacy notice) published and available to the public?	This covers personal information you collect or manage for patients and the public, include a list of rights and when/whether they apply to the processing undertaken, contact details and procedure for subject access and other rights requests. Provide a weblink if possible or other publicly available document.	Yes	Does your organisation have a privacy notice?	If you use and share personal data then you must tell people what you are doing with it. This includes why you need the data, what you'll do with it, who you're going to share it with and individual's rights under data protection legislation e.g. to access the information. This should be set out in writing in 'a privacy notice'. You should provide this information in a clear, open and honest way using easily understood language. Privacy notice should cover all data you process for example the data relating to the people you support and their relatives, staff, volunteers, members of the public. You may have more than one privacy notice e.g. one for staff and another one for the people you support. An example privacy notice is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/)	Yes	Does your organisation have a privacy notice?	Your organisation must set out in clear and easily understood language what it does with the personal data it processes regarding the people it supports, staff and volunteers, and members of the public, for example relatives or other professionals etc. This is called a privacy notice and there may be more than one privacy notice e.g. one notice for staff and one for the people you support. Your organisation's privacy notice(s) should be made available to these people and inform them about their rights under data protection legislation and how to exercise them. It is good practice to publish your privacy notice on your website if you have one. An example privacy notice is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/).	Yes
	Yes/No	New	**1.2.2**	New	Your organisation has a process to recognise and respond to individuals' requests to access their personal data.	Further guidance is available on the [NHSx website](https://www.nhsx.nhs.uk/information-governance/guidance/subject-access-requests/)	Yes	Your organisation has a process to recognise and respond to individuals' requests to access their personal data.	Further guidance is available on the [NHSx website](https://www.nhsx.nhs.uk/information-governance/guidance/subject-access-requests/)	Yes						
	Yes/No	New	**1.2.3**	New	Your organisation has procedures to handle an individual's objection to the processing of their personal data.	Further guidance is available on the [ICO website](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/)	Yes									
	Yes/No	1.4.4	**1.2.4**	Newly mandatory cat 1 2, 3 and 4	Is your organisation compliant with the national data opt-out policy?	Please provide your published [compliance statement](https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out) e.g. within a privacy notice and/or Published Data Release Register in the comments box.	Yes	Is your organisation compliant with the national data opt-out policy?	Please provide your published [compliance statement](https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out) e.g. within a privacy notice and/or Published Data Release Register in the comments box.	Yes	Is your organisation compliant with the national data opt-out policy?	The national data opt-out gives everyone the ability to stop health and social care organisations from sharing their confidential information for research and planning purposes, with some exceptions such as where there is a legal mandate/direction or an overriding public interest for example to help manage the covid-19 pandemic. As a provider, you should help the people who use your services to understand that they can opt out of their data being used for other purposes. You should check that your policies, procedures, and privacy notice cover the opt out. All health and social care CQC-registered organisations in England must be compliant with the national data opt out by 30 September 2021. More detailed guidance that gives advice about compliance with the national data opt-out policy is available from [NHS Digital](https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out) and [Digital Social Care](https://www.digitalsocialcare.co.uk/national-data-opt-out/).	Yes	Is your organisation compliant with the national data opt-out policy?	The national data opt-out gives everyone the ability to stop health and social care organisations from sharing their confidential information for research and planning purposes, with some exceptions such as where there is a legal mandate/direction or an overriding public interest for example to help manage the covid-19 pandemic. As a provider, you should help the people who use your services to understand that they can opt out of their data being used for other purposes. You should check that your policies, procedures, and privacy notice cover the opt out. All health and social care CQC-registered organisations in England must be compliant with the national data opt out by 30 September 2021. More detailed guidance that gives advice about compliance with the national data opt-out policy is available from [NHS Digital](https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out) and [Digital Social Care](https://www.digitalsocialcare.co.uk/national-data-opt-out/).	Yes
Accountability and Governance in place for data protection and data security	Yes/No	1.2.1	**1.3.1**	No changes	Are there board-approved data security and protection policies in place that follow relevant guidance?	Confirm that you have policies, procedures and staff guidance in place that explain the organisation's plan or principles for data protection, DPIAs, Data protection by default, data sharing, data quality, records management, data security, registration authority, national data opt out, common law duties, professional codes, subject access requests, Freedom of Information and network security. Provide details of when each policy was updated.	Yes	Are there board-approved data security and protection policies in place that follow relevant guidance?	Confirm that you have policies, procedures and staff guidance in place that explain the organisation's plan or principles for data protection, data sharing, data quality, records management, data security, registration authority, national data opt out, common law duties, professional codes, subject access requests, Freedom of Information and network security. Provide details of when each policy was updated.	Yes	Does your organisation have up to date policies in place for data protection and for data and cyber security?	Confirm that your organisation has a policy or policies in place to cover: - data protection - data quality - record keeping - data security - where relevant, network security The policy or policies should be reviewed and approved by the management team or equivalent within the last 12 months. There is no set number of how many policies your organisation has to have on these topics as the different sizes and complexity of organisations means that some will have one all-encompassing policy, whilst others may have multiple policies. Policy templates are available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/)	Yes	Are there approved data security and protection policies in place that follow relevant guidance?	Confirm that you have policies in place that explain the organisation's plan or principles for data protection, data quality, records management, data security, registration authority, Subject access requests, Freedom of Information and network security.	Yes

Yes/No	1.5.2	**1.3.2**	Reword for cat 1 and 2	Your organisation monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.	Your organisation should carry out spot checks that staff are doing what it says in the data protection, records management and/or staff confidentiality policy or guidance. These should be undertaken at least every year. They could be part of other audits that you carry out. It is good practice to keep evidence that spot checks have been carried out, including details of any actions, who has approved the actions and who is taking them forward.	Yes	Your organisation monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.	The spot checks should check that staff are doing what it says in your staff Confidentiality and Data Protection guidance and the response should include details of any actions, who has approved the actions and who is taking them forward.	Yes	Does your organisation carry out regular data protection spot checks?	Your organisation should carry out spot checks that staff are doing what it says in the data protection and/or staff confidentiality policy or guidance. These should be undertaken at least every year. They could be part of other audits that you carry out. It is good practice to keep evidence that spot checks have been carried out, including details of any actions, who has approved the actions and who is taking them forward, if applicable. There is an example audit checklist that you can download from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/).	Yes	Does your organisation carry out regular data protection spot checks?	Your organisation should carry out spot checks that staff are doing what it says in the data protection and/or staff confidentiality policy or guidance. These should be undertaken at least every year. They could be part of other audits that you carry out. It is good practice to keep evidence that spot checks have been carried out, including details of any actions, who has approved the actions and who is taking them forward, if applicable. There is an example audit checklist that you can download from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/)	Yes
Yes/No	1.1.1	**1.3.3**	No changes	Has SIRO responsibility for data security been assigned?	There is a board-level individual who has overall accountability for the security of networks and information systems and drives regular discussion at board-level.	Yes	Has SIRO responsibility for data security been assigned?	There is a board-level individual who has overall accountability for the security of networks and information systems and drives regular discussion at board-level.	Yes								
Yes/No	1.1.3	**1.3.4**	Reword for cat 1 and 2	Are there clear lines of responsibility and accountability to named individuals for data security and data protection?	Please provide details in the comments field.	Yes	Are there clear lines of responsibility and accountability to named individuals for data security and data protection?	Please provide details in the comments field.	Yes								
Text	1.8.1	**1.3.5**	No changes	Does your organisation operate and maintain a data security risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility?	Further guidance is available from the [National Cyber Security Centre.](https://www.ncsc.gov.uk/collection/risk-management-collection)	Yes	Does your organisation operate and maintain a data security risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility?	Further guidance is available from the [National Cyber Security Centre.](https://www.ncsc.gov.uk/collection/risk-management-collection)	Yes								
Text	1.8.3	**1.3.6**	No longer mandatory cat 3	What are your top three data security and protection risks?	Record at a heading level	Yes	What are your top three data security and protection risks?	Record at a heading level	Yes	What are the top three data and cyber security risks in your organisation and how does your organisation plan to reduce those risks?	All organisations have risks and should be able to identify what they are. Thinking about your responses to all of the questions in the toolkit, consider which three areas carry the most risk for your organisation. Provide a brief headline for each risk and say what your organisation plans to do to reduce that risk.		What are the top three data and cyber security risks in your organisation and how does it plan to reduce those risks?	All organisations have risks and should be able to identify what they are. Thinking about your responses to all of the questions in the toolkit, consider which three areas carry the most risk for your organisation. Provide a brief headline for each risk and say what your organisation plans to do to reduce that risk.	
Yes/No	1.6.1	**1.3.7**	Reword for cat 1 and 2. Removed from cat 4	Your organisation has implemented appropriate technical and organisational measures to integrate data protection into your processing activities.	The procedures should be approved by the board or equivalent and aim to ensure that only the minimum necessary personal data are processed and that processing is transparent allowing individuals to monitor what is being done with their data.	Yes	Your organisation has implemented appropriate technical and organisational measures to integrate data protection into your processing activities.	The procedures should be approved by the board or equivalent and aim to ensure that only the minimum necessary personal data are processed and that processing is transparent allowing individuals to monitor what is being done with their data.	Yes	Does your organisation's data protection policy describe how you keep personal data safe and secure?	Your policy should describe how your organisation considers privacy and data protection issues right at the start when embarking on a new project or process. This is called Data protection by design. This might be a new data sharing initiative for example if becoming part of a shared care record or if you are using personal data for a new purpose such as research. Your policy should also describe how your organisation only collect, use and share the minimum amount of data you need, how you limit access to only those how need to know, keep the data for a short time as possible and how you let people know what you do with their data. This is called 'data protection by default'. There is guidance on data protection by design and by default on the [ICO's website](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/). The Data Protection Policy template that is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/) covers this subject.	Yes				
Yes/No	1.6.5	**1.3.8**	Newly mandatory cat 1 and 2. Reword for cat 1 and 2	Your organisation understands when you must conduct a Data Protection Impact Assessment and has processes in place, which links to your existing risk management and project management, to action this.	[Information commissioner's office guidance](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/) is available	Yes	Your organisation understands when you must conduct a Data Protection Impact Assessment and has processes in place, which links to your existing risk management and project management, to action this.	[Information commissioner's office guidance](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/) is available	Yes	Does your organisation's data protection policy describe how you identify and minimise risks to personal data when introducing, or changing, a process or starting a new project involving personal data?	Your policy should describe the process that your organisation has in place to make sure that it systematically identifies and minimises the data protection risks of any new project or plan that involves processing personal data. For example, when you introduce a new care recording system; if you install CCTV; if you use new remote care or monitoring technology; if you share data for research or marketing purposes. This type of risk assessment is called a Data Protection Impact Assessment (DPIA). Your organisation should consider whether it needs to carry out a DPIA at the early stages of any new project if it plans to process personal data. A DPIA should follow relevant guidance from the [Information Commissioner's Office (ICO)](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/).	Yes	Does your organisation's data protection policy describe how you identify and minimise risks to personal data when introducing, or changing, a process or starting a new project involving personal data?	Your policy should describe the process that your organisation has in place to make sure that it systematically identifies and minimises the data protection risks of any new project or plan that involves processing personal data. For example, when you introduce a new care recording system; if you install CCTV; if you use new remote care or monitoring technology; if you share data for research or marketing purposes. This type of risk assessment is called a Data Protection Impact Assessment (DPIA). Your organisation should consider whether it needs to carry out a DPIA at the early stages of any new project if it plans to process personal data. A DPIA should follow relevant guidance from the [Information Commissioner's Office (ICO)](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/).	
Yes/No	1.1.4	**1.3.9**	No changes	Is data security direction set at board level and translated into effective organisational practices?		Yes	Is data security direction set at board level and translated into effective organisational practices?		Yes	Is data security direction set at management level and translated into effective organisational practices?							
Document	1.2.3	**1.3.10**	Reword cat 1 and 2	How are data security and protection policies and Data Protection Impact Assessments made available to the public?	Provide the web link, but if not available online then record where they are available. Making your policies and DPIAs available to the public will assist you to meet the transparency requirements of GDPR unless this causes a security risk to the organisation.		How are data security and protection policies and Data Protection Impact Assessments made available to the public?	Provide the web link, but if not available online then record where they are available. Making your policies and DPIAs available to the public will assist you to meet the transparency requirements of GDPR unless this causes a security risk to the organisation.		How are data security and protection policies available to the public?	Provide the web link, but if not available online then record where they are available. Publishing your policies will assist you to meet the transparency requirements of GDPR unless this causes a security risk to the organisation.		How are data security and protection policies available to the public?	Provide the web link, but if not available online then record where they are available. Publishing your policies will assist you to meet the transparency requirements of GDPR unless this causes a security risk to the organisation.	
Yes/No	1.6.6	**1.3.11**	Removed from cat 1 and 2							If staff, directors, trustees and volunteers use their own devices (e.g. phones) for work purposes, does your organisation have a bring your own device policy and is there evidence of how this policy is enforced?	The devices referred in this question include laptops, tablets, mobile phones, CDs, USB sticks etc. This applies to use of devices whether the person is on duty or not e.g. if they access your system(s) when not on shift. Please upload your Bring Your Own Device policy and any associated guidance, and evidence of how this policy is enforced. If nobody uses their own devices, then tick and write "Not applicable" in the comments box. A template Bring Your Own Device (BYOD) policy, and examples of how this policy might be enforced, is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/social-care-technology/mobile-devices)	Yes				
Text	1.6.2	**1.3.12**	Removed from cat 1 and 2							How does your organisation make sure that paper records are safe when taken out of the building?	Paper records may be taken out of your organisation's building(s), for example for hospital appointments or visits to people's homes. Leaving documents in cars, for instance, can be risky. How does your organisation make sure paper records are kept safe when 'on the move'? If you do not have any paper records or do not take them off site, write "Not applicable" in the text box.	Yes				
Text	1.6.3	**1.3.13**	Removed from cat 1 and 2							Briefly describe the physical controls your buildings have that prevent unauthorised access to personal data.	Physical controls that support data protection include lockable doors, windows and cupboards, clear desk procedure, security badges, key coded locks to access secure areas etc. Provide details at high level and, if you have more than one building, summarise how compliance is assured across your	Yes	There are physical controls that prevent unauthorised access to buildings and locations where personal data are stored or processed.	Physical controls that can support data protection include lockable doors, windows and cupboards, clear desk procedure, security badges, key coded locks to access secure areas, records libraries, etc. Provide details at high level.	Yes
Text	1.6.4	**1.3.14**	Removed from cat 1 and 2							What does your organisation have in place to minimise the risks if mobile phones are lost, stolen, hacked or used inappropriately?	Smartphones are especially vulnerable to being lost or stolen. What has been put in place by your organisation to protect them to prevent unauthorised access? E.g. is there a PIN or fingerprint or facial scan? Is there an app set up to track the location of a lost/ stolen smartphone, and 'wipe' its contents remotely? You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any mobile phones, write "Not applicable" in the text box. Guidance is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/social-care-technology/mobile-devices)	Yes				
Records are maintained appropriately	Yes/No	1.7.4	**1.4.1**	Reword cat 1 and 2	The organisation has a records management policy including a records retention schedule	The policy which sets out records management responsibilities, covers the whole record lifecycle including secure storage, tracking, transfer and disposal. The retention schedule is based on business need with reference to statutory requirements and [other guidance](https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/).	Yes	The organisation has a records management policy including a records retention schedule	The policy which sets out records management responsibilities, covers the whole record lifecycle including secure storage, tracking, transfer and disposal. The retention schedule is based on business need with reference to statutory requirements and [other guidance](https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/).	Yes	Does your organisation have a timetable which sets out how long you retain records for?	Your organisation should have in place and follow a retention timetable for all the different types of records that it holds, including finance, staffing and care records. The timetable, or schedule as it sometimes called, should be based on [statutory requirements or other guidance](https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/).	Yes	Has a records retention schedule been produced?	Your organisation should have in place and follow a retention timetable for all the different types of records that it holds, including finance, staffing and care records. The timetable, or schedule as it sometimes called, should be based on [statutory requirements or other guidance](https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/).	Yes
Text	1.7.5	**1.4.2**	Removed cat 1 and 2, new for cat 3.							If your organisation uses third parties to destroy records or equipment that hold personal data, is there a written contract in place that has been reviewed since 1st July 2021? This contract should meet the requirements set out in data protection regulations.	It is important that when there is no longer a valid reason to keep personal data that it is disposed of securely. This applies to paper documents, electronic records and equipment, such as old computers and laptops, mobile phones, CDs and memory sticks. If your organisation uses a contractor to destroy any records or equipment, such as a document shredding company or IT recycling organisation, then the contract(s) or other written confirmation with third parties must include the requirement to have appropriate security measures and the facility to allow audit by your organisation. Further information about the destruction of records is in chapter 5 of the Records Management Code of Practice. If you do not use third parties to destroy records or equipment, then tick and write "Not applicable" in the comments box. Advice on contracts for secure disposal of personal data is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latestguidance/contract-guidance/).	Yes				

	Text	1.7.3	**1.4.3**	Removed from Cat 1 and 2 (which becomes new question 1.1.8)							If your organisation destroys any records or equipment that hold personal data, how does it make sure that this is done securely?	It is important that when there is no longer a valid reason to keep personal data that it is disposed of securely. This applies to paper documents, electronic records and equipment, such as old computers and laptops, mobile phones, CDs and memory sticks. If anyone in your organisation destroys any records or equipment themselves, such as shredding documents, briefly describe how the organisation makes sure that this is done securely. If you do not destroy records or equipment yourselves, or only use a third party to do so, write "Not applicable" in the text box. [Digital Social Care](https://www.digitalsocialcare.co.uk//latest-	Yes	If your organisation destroys any records or equipment that hold personal data, how does it make sure that this is done securely?	It is important that when there is no longer a valid reason to keep personal data that it is disposed of securely. This applies to paper documents, electronic records and equipment, such as old computers and laptops, mobile phones, CDs and memory sticks. If anyone in your organisation destroys any records or equipment themselves, such as shredding documents, briefly describe how the organisation makes sure that this is done securely. If you do not destroy records or equipment yourselves, or only use a third party to do so, write "Not applicable" in the text box.	
Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards	Yes/No	2.2.1	**2.1.1**	No changes	Is there a data protection and security induction in place for all new entrants to the organisation?	The induction can be delivered face to face or digitally. Records are maintained and the induction is reviewed on a regular basis to ensure its effectiveness.	Yes	Is there a data protection and security induction in place for all new entrants to the organisation?	The induction can be delivered face to face or digitally. Records are maintained and the induction is reviewed on a regular basis to ensure its effectiveness.	Yes	Does your organisation have an induction process that covers data security and protection, and cyber security?	All new staff, directors, trustees and volunteers who have access to personal data, should have an induction that covers data security and protection as well as cyber security. It is good practice to keep records of who has been inducted and to review the induction process on a regular basis to ensure it is effective and up to date. There is an 'Introduction to Information Sharing for Staff' available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latestguidance/staff-guidance/).	Yes	Does your organisation have an induction process that covers data security and protection, and cyber security?	All new staff, directors, trustees and volunteers who have access to personal data, should have an induction that covers data security and protection as well as cyber security. It is good practice to keep records of who has been inducted and to review the induction process on a regular basis to ensure it is effective and up to date.	Yes
	Yes/No	2.2.2	**2.1.2**	No changes	Do all employment contracts contain data security requirements?	Please provide any explanatory text in the comments box	Yes	Do all employment contracts contain data security requirements?	Please provide any explanatory text in the comments box	Yes	Do all employment contracts, and volunteer agreements, contain data security requirements?	Clauses in contracts or agreements should reference data security (confidentiality, integrity and availability). Many contracts commonly focus on just confidentiality. Your organisation's staff employment contracts, and volunteer and trustee agreements if you have them, should be reviewed to see if they need to be updated to include a clause on data security. There is an example staff contract clause available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/staff-guidance/).	Yes	Do all employment contracts, and volunteer agreements, contain data security requirements?	Clauses in contracts or agreements should reference data security (confidentiality, integrity and availability). Many contracts commonly focus on just confidentiality. Your organisation's staff employment contracts, and volunteer and trustee agreements if you have them, should be reviewed to see if they need to be updated to include a clause on data security.	Yes
	Text	2.2.3	**2.1.3**	No changes	The results of staff awareness surveys on staff understanding of data security are reviewed to improve data security.	Using the [staff awareness questions](https://www.dsptoolkit.nhs.uk/Help/21) either through the Data Security Awareness training or local materials.		The results of staff awareness surveys on staff understanding of data security are reviewed to improve data security.	Using the [staff awareness questions](https://www.dsptoolkit.nhs.uk/Help/21) either through the Data Security Awareness training or local materials.		The results of staff awareness surveys on staff understanding of data security are reviewed to improve data security.	Using the [staff awareness questions](https://www.dsptoolkit.nhs.uk/Help/21) either through the Data Security Awareness training or local materials.		The results of staff awareness surveys on staff understanding of data security are reviewed to improve data security.	Using the [staff awareness questions](https://www.dsptoolkit.nhs.uk/Help/21) either through the Data Security Awareness training or local materials.	
There has been an assessment of data security and protection training needs across the organisation	Yes/No	3.1.1	**3.1.1**	Wording change (date only)	Has an approved organisation-wide data security and protection training needs analysis been completed after 1 July 2021?	This is an assessment of data security and protection training (including records management and Subject access requests) and development needs for all your staff including Board Members. Approved by your SIRO or equivalent.	Yes	Has an approved organisation-wide data security and protection training needs analysis been completed after 1 July 2021?	This is an assessment of data security and protection training and development needs for all your staff including Board Members. Approved by your SIRO or equivalent.	Yes	Has a training needs analysis covering data security and protection, and cyber security, been completed since 1st July 2021?	A training needs analysis is a process which helps identify the data security and protection, and cyber security, training and development needs across your organisation. Your organisation's training needs analysis should identify the level of training or awareness raising required by your staff, directors, trustees and volunteers if you have them. It should be reviewed and/or approved annually by the person(s) with overall responsibility for data security and protection within your organisation. An example training needs analysis is available to download from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/staff-guidance/).	Yes			
Staff pass the data security and protection mandatory test	Yes/No	3.2.1	**3.2.1**	Wording change (date only)	Have at least 95% of all staff, completed their annual Data Security Awareness Training?	Please provide your highest percentage figure for the period 1st July 2021 - 30th June 2022 in the space below with an explanation of how you have calculated the figure. This can be calculated from local materials/E Learning system and/or the national Data Security Awareness E-Learning system.	Yes	Have at least 95% of all staff, completed their annual Data Security Awareness Training?	Please provide your highest percentage figure for the period 1st July 2021 - 30th June 2022 in the space below with an explanation of how you have calculated the figure. This can be calculated from local materials/E Learning system and/or the national Data Security Awareness E-Learning system.	Yes	Have at least 95% of staff, directors, trustees and volunteers in your organisation completed training on data security and protection, and cyber security, since 1st July 2021?	All people in your organisation with access to personal data must complete appropriate data security and protection, and cyber security, training every year. Your organisation's training needs analysis should identify the level of training or awareness raising that people need. There is an understanding that due to illness, maternity/paternity leave, attrition or other reasons it might not be possible for 100% of people to receive training every year. Therefore, the target is 95% of people with access to personal data. [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/train-staff-to-be-cyber-aware/) provides guidance on training, including sources of free online data and cyber security training.	Yes	Have at least 95% of staff, completed training on data security and protection, and cyber security, since 1st July 2021?	All people in your organisation with access to personal data must complete appropriate data security and protection, and cyber security, training every year. Your organisation's training needs analysis should identify the level of training or awareness raising that people need. There is an understanding that due to illness, maternity/paternity leave, attrition or other reasons it might not be possible for 100% of people to receive training every year. Therefore, the target is 95% of people with access to personal data.	Yes
Staff with specialist roles receive data security and protection training suitable to their role	Text	3.3.1	**3.3.1**	No changes	Provide details of any specialist data security and protection training undertaken.	Details of any additional training as identified by your Data Security Training Needs analysis. Such as staff with roles in Informatics (IT and Information areas), Records Management, Clinical Coding & Information Governance (including privacy / confidentiality & data protection).	Yes	Provide details of any specialist data security and protection training undertaken.	Details of any additional training as identified by your Data Security Training Needs analysis. Such as staff with roles in Informatics (IT and Information areas), Medical Records, Clinical Coding & Information Governance (including privacy / confidentiality & data protection).	Yes	Provide details of any specialist data security and protection training undertaken.	Details of any additional training as identified by your Data Security Training Needs analysis. Such as staff with roles as Caldicott Guardian, in Informatics (IT and Information areas), Medical Records, Clinical Coding & Information Governance (including privacy / confidentiality & data protection).				
	Yes/No	3.3.2	**3.3.2**	No changes	The organisation has appropriately-qualified technical cyber security specialist staff and/or service.	See guidance within [big picture guide 3.](https://www.dsptoolkit.nhs.uk/Help/23)	Yes	The organisation has appropriately-qualified technical cyber security specialist staff and/or service.	See guidance within [big picture guide 3.](https://www.dsptoolkit.nhs.uk/Help/23)	Yes						
	Yes/No	3.3.3	**3.3.3**	No changes	The organisation has a nominated member of the Cyber Associates Network.	Further details are available on the [NHS Digital website.](https://digital.nhs.uk/services/data-security-centre/cyber-associates-network)	Yes	The organisation has a nominated member of the Cyber Associates Network.	Further details are available on the [NHS Digital website.](https://digital.nhs.uk/services/data-security-centre/cyber-associates-network)	Yes						
Leaders and board members receive suitable data protection and security training	Yes/No	3.4.1	**3.4.1**	No changes	Have your SIRO and Caldicott Guardian received appropriate data security and protection training?	As defined in your organisations data security and protection training needs analysis.	Yes	Have your SIRO and Caldicott Guardian received appropriate data security and protection training?	As defined in your organisations data security and protection training needs analysis.	Yes	Have the people with responsibility for data security and protection received training suitable for their role?	It is likely that the person or people within your organisation who are responsible for data security and protection will need additional and more in depth training than the majority of your staff. Your organisation's training needs analysis should identify any additional training required by people with increased data security and protection responsibilities or specialist roles, for example a Data Protection Officer (DPO).	Yes			
	Yes/No	New	**3.4.2**	New	All board members have completed appropriate data security and protection training?	As defined in your organisation's data security and protection training needs analysis. All Board members are current permanent working board members (for example board members who are sick should not be included).	Yes	All board members have completed appropriate data security and protection training.	As defined in your organisations data security and protection training needs analysis. All Board members are current permanent working board members (for example board members who are sick should not be included).	Yes						
The organisation maintains a current record of staff and their roles	Yes/No	4.1.1	**4.1.1**	No changes	Your organisation maintains a record of staff and their roles.		Yes	Your organisation maintains a record of staff and their roles.		Yes	Does your organisation have an up to date record of staff, and volunteers if you have them, and their roles?	Your organisation must have a list of all staff, and volunteers if you have them, and their current role. This list should be kept up to date, including any change of role, new starters and removal of leavers. This might be linked to your existing payroll or rostering system.	Yes	Does your organisation have an up to date record of people and their roles?	Your organisation must have a list of all staff, and volunteers if you have them, and their current role. This list should be kept up to date, including any change of role, new starters and removal of leavers. This might be linked to your existing payroll or rostering system.	Yes
	Yes/No	4.1.2	**4.1.2**	No changes	Does the organisation understand who has access to personal and confidential data through your systems, including any systems which do not support individual logins?	Each system may use its own user list(s) or use federated access. There may be systems where technically or operationally it is not possible to have individual logins but there are alternative methods of maintaining user lists. Where this occurs, it is understood and risk assessed by the organisation.	Yes	Does the organisation understand who has access to personal and confidential data through your systems, including any systems which do not support individual logins?	Each system may use its own user list(s) or use federated access. There may be systems where technically or operationally it is not possible to have individual logins but there are alternative methods of maintaining user lists. Where this occurs, it is understood and risk assessed by the organisation.	Yes	Does your organisation know who has access to personal and confidential data through its IT system(s)?	Your organisation should know who has access to the personal and confidential data in its IT system(s). Each person needs to have their own account to access a system. If that is not currently possible, and users share a login, the organisation must risk assess the situation and agree a plan to end the use of shared logins. If your organisation does not use any IT systems, then tick and write "Not applicable" in the comments box.	Yes	Does the organisation understand who has access to personal and confidential data through your systems, including any systems which do not support individual logins?	A list of all systems, showing your staff roles and numbers split by the system access level they have.	Yes
	Yes/No	4.1.3	**4.1.3**	No changes	Are users in your organisation only given the minimum access to sensitive information or systems necessary for their role?			Are users in your organisation only given the minimum access to sensitive information or systems necessary for their role?								
The organisation assures good management and maintenance of identity and access control for it's networks and information systems	Date	4.2.1	**4.2.1**	No changes	When was the last audit of user accounts held?	An audit of staff accounts from your organisation, to make sure there aren't any inappropriate access permissions. Record the date when the last user audit was held. This should be completed annually as a minimum.	Yes	When was the last audit of user accounts held?	An audit of staff accounts from your organisation, to make sure there aren't any inappropriate access permissions. Record the date when the last user audit was held. This should be completed annually as a minimum.	Yes						
	Document	4.2.2	**4.2.2**	No changes	Provide a summary of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted.	This can be an incident either where the staff member's rights to data were too high or too low. Do not name individuals.		Provide a summary of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted.	This can be an incident either where the staff member's rights to data were too high or too low. Do not name individuals.		Provide a summary of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted.	This can be an incident either where the staff member's rights to data were too high or too low. Do not name individuals.				
	Yes/No	4.2.3	**4.2.3**	Wording change cat 1 and 2.	Logs are retained for a sufficient period, managed securely, reviewed regularly and can be searched to identify malicious activity.	Organisational policy should set out the rules defining log retention. The average time to detect a cyber attack is over three months and it is not uncommon for incidents to take significantly longer to detect. The most important logs for identifying malicious activity should be held for six months as a minimum. Organisations should consider the ability to trace an incident end to end e.g. network address translation. Please refer to [National Cyber Security Centre guidance.](https://www.ncsc.gov.uk/files/NCSC_SOC_Feeds.pdf)	Yes	Logs are retained for a sufficient period, managed securely, reviewed regularly and can be searched to identify malicious activity.	Organisational policy should set out the rules defining log retention. The average time to detect a cyber attack is over three months and it is not uncommon for incidents to take significantly longer to detect. The most important logs for identifying malicious activity should be held for six months as a minimum. Organisations should consider the ability to trace an incident end to end e.g. network address translation. Please refer to [National Cyber Security Centre guidance.](https://www.ncsc.gov.uk/files/NCSC							
	Yes/No	4.2.5	**4.2.4**	No changes	Are unnecessary user accounts removed or disabled?	Former employees', guest and other unnecessary accounts are routinely and promptly removed or disabled from internal workstations, Active Directory domains and other user directories. Privileged user access is also removed when no longer required or appropriate.	Yes	Are unnecessary user accounts removed or disabled?	Former employees', guest and other unnecessary accounts are routinely and promptly removed or disabled from internal workstations, Active Directory domains and other user directories. Privileged user access is also removed when no longer required or appropriate.	Yes	Does your organisation have a reliable way of removing or amending people's access to IT systems when they leave or change roles?	When people change roles or leave your organisation, there needs to be a reliable way to amend or remove their access to your IT system(s). This could be by periodic audit to make sure that people's access rights are at the right level. It is important that leavers who had access to personal data have their access rights revoked in line with your policies and procedures. This includes access to shared email addresses. If your organisation does not use any IT systems, then tick and write "Not applicable" in the comments box	Yes	Does your organisation have a reliable way of removing or amending people's access to IT systems when they leave or change roles?	When people change roles or leave your organisation, there needs to be a reliable way to amend or remove their access to your IT system(s). This could be by periodic audit to make sure that people's access rights are at the right level. It is important that leavers who had access to personal data have their access rights revoked in line with your policies and procedures. This includes access to shared email addresses.	Yes
All staff understand that their activities on IT systems will be monitored and recorded for security purposes	Yes/No	4.3.1	**4.3.1**	No longer mandatory cat 3	All system administrators have signed an agreement which holds them accountable to the highest standards of use.	With great power comes great responsibility and all administrators should attest to that responsibility by being signatory to a agreement affirming the highest standard of use.	Yes	All system administrators have signed an agreement which holds them accountable to the highest standards of use.	With great power comes great responsibility and all administrators should attest to that responsibility by being signatory to a agreement affirming the highest standard of use.	Yes	Have all the administrators of your organisation's IT system(s) signed an agreement to hold them accountable to higher standards?	The people within your organisation who are IT system administrators may have access to more information than other staff. Therefore, they need to be held accountable in a formal way to higher standards of confidentiality than others. This requirement applies to IT system administrators working in external companies who support your organisation's IT systems. This formal agreement could be part of a job description or a contract with your IT support company and/or systems supplier/s. If your organisation does not use any IT systems, then 'tick' and write "Not applicable" in the comments box.		Have all the administrators of your organisation's IT system(s) signed an agreement to hold them accountable to higher standards?	The people within your organisation who are IT system administrators may have access to more information than other staff. Therefore, they need to be held accountable in a formal way to higher standards of confidentiality than others. This requirement applies to IT system administrators working in external companies who support your organisation's IT systems This formal agreement could be part of a job description or a contract with your IT support company and/or systems supplier/s. If your organisation does not use any IT systems, then 'tick' and write "Not applicable" in the comments box.	Yes

	Text	4.3.2	**4.3.2**	No changes	Are users, systems and (where appropriate) devices always identified and authenticated prior to being permitted access to information or systems?	Please provide details. For critical systems you should consider if device authentication is required.	Yes	Are users, systems and (where appropriate) devices always identified and authenticated prior to being permitted access to information or systems?	Please provide details. For critical systems you should consider if device authentication is required.	Yes							
	Yes/No	4.3.5	**4.3.3**	No changes	Have all staff been notified that their system use could be monitored?	Staff are informed and understand that their system use can be monitored and recorded. The notification method is periodic.		Have all staff been notified that their system use could be monitored?	Staff are informed and understand that their system use can be monitored and recorded. The notification method is periodic.		Have all staff been notified that their system use could be monitored?	Staff are informed and understand that their system use can be monitored and recorded. The notification method is periodic.		Have all staff been notified that their system use could be monitored?	Staff are informed and understand that their system use can be monitored and recorded. The notification method is periodic.	Yes	
You closely manage privileged user access to networks and information systems supporting the essential service	Yes/No	New	**4.4.1**	New	The organisation ensures that logs, including privileged account use, are kept securely and only accessible to appropriate personnel. They are stored in a read only format, tamper proof and managed according to the organisation information life cycle policy with disposal as appropriate.	Organisational policy should set out the rules defining log retention. The average time to detect a cyber attack is over three months and it is not uncommon for incidents to take significantly longer to detect. The most important logs for identifying malicious activity should be held for six months as a minimum. [Guidance from NCSC](https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide) on maintaining security of logs is available. Note: you are not expected to purchase a CSOC.	Yes	The organisation ensures that logs, including privileged account use, are kept securely and only accessible to appropriate personnel. They are stored in a read only format, tamper proof and managed according to the organisation information life cycle policy with disposal as appropriate.	Organisational policy should set out the rules defining log retention. The average time to detect a cyber attack is over three months and it is not uncommon for incidents to take significantly longer to detect. The most important logs for identifying malicious activity should be held for six months as a minimum. [Guidance from NCSC](https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide) on maintaining security of logs is available. Note: you are not expected to purchase a CSOC.		The person with responsibility for IT confirms that IT administrator activities are logged and those logs are only accessible to appropriate personnel. If your organisation does not use any IT systems, then 'tick' and write "Not applicable" in the comments box.	IT Support staff typically have high level access to systems. The activities of these users should be logged and only available to appropriate personnel. If your organisation does not use any IT systems, then 'tick' and write "Not applicable" in the comments box.		The person with responsibility for IT confirms that IT administrator activities are logged and those logs are only accessible to appropriate personnel.	IT Support staff typically have high level access to systems. The activities of these users should be logged and only available to appropriate personnel. If your organisation does not use any IT systems, then 'tick' and write "Not applicable" in the comments box.	
	Yes/No	4.4.3	**4.4.2**	Non-material wording change cat 1 and 2	The organisation does not allow users with wide ranging or extensive system privilege to use their highly privileged accounts for high-risk functions, in particular email and web browsing.	Provide details in the comments section	Yes	The organisation does not allow users with wide ranging or extensive system privilege to use their highly privileged accounts for high-risk functions; in particular email and web browsing.	Provide details in the comments section	Yes							
	Yes/No	4.4.4	**4.4.3**	Non-material wording change cat 1 and 2	The organisation only allows privileged access to be initiated from devices owned and managed or assured by your organisation	Explain any exceptions or risk management applied.		The organisation only allows privileged access to be initiated from devices owned and managed or assured by your organisation	Explain any exceptions or risk management applied.								
You ensure your passwords are suitable for the information you are protecting	Yes/No	4.5.1	**4.5.1**	Newly mandatory cat 2	Do you have a password policy giving staff advice on managing their passwords?	The password policy must cover: (a) How to avoid choosing obvious passwords (such as those based on easily-discoverable information). (b) Not to choose common passwords (use of technical means, such as using a password blacklist, is recommended). (c) No password reuse. (d) Where and how they may record passwords to store and retrieve them securely. (e) If password management software is allowed, and if so, which. (f) Which passwords they really must memorise and not record anywhere. (g) Assessing risks to ensure systems use appropriate authentication measures e.g. high-strength passwords enforced technically for all users of internet-facing authentication services.	Yes	Do you have a password policy giving staff advice on managing their passwords?	The password policy must cover: (a) How to avoid choosing obvious passwords (such as those based on easily-discoverable information). (b) Not to choose common passwords (use of technical means, such as using a password blacklist, is recommended). (c) No password reuse. (d) Where and how they may record passwords to store and retrieve them securely. (e) If password management software is allowed, and if so, which. (f) Which passwords they really must memorise and not record anywhere. (g) Assessing risks to ensure systems use appropriate authentication measures e.g. high-strength passwords enforced technically for all users of internet-facing authentication services.	Yes							
	Yes/No	4.5.2	**4.5.2**	Newly mandatory cat 2	Technical controls enforce password policy and mitigate against password-guessing attacks.	Examples of technical controls are [provided by the National Cyber Security Centre.](https://www.ncsc.gov.uk/collection/passwords)	Yes	Technical controls enforce password policy and mitigate against password-guessing attacks.	Examples of technical controls are [provided by the National Cyber Security Centre.](https://www.ncsc.gov.uk/collection/passwords)	Yes							
	Yes/No	4.5.3	**4.5.3**	No changes	Multifactor authentication is used [wherever technically feasible].	Multifactor authentication can include hardware-based certificates. This applies to end user devices. [Where it is not possible to apply multifactor authentication, this should be considered in your response to 9.5.9]	Yes	Multifactor authentication is used [wherever technically feasible].	Multifactor authentication can include hardware-based certificates. This applies to end user devices.								
	Text	4.5.4	**4.5.4**	No changes	Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.		Yes	Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.		Yes	How does your organisation make sure that staff, directors, trustees and volunteers use good password practice?	If your organisation has any IT systems or computers, it should provide advice for setting and managing passwords. Each person should have their own password to access the computer, laptop or tablet that they are using and a separate password for other systems. These passwords should be 'strong' i.e. hard to guess. This could be enforced through technical controls i.e. your system(s) require a minimum number of characters or a mixture of letters and numbers in a password. If your organisation does not use any IT systems, computers or other devices, write "Not applicable" in the text box. Information about good password practice is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/use-strong-passwords/).	Yes					
	Yes/No	4.5.5	**4.5.5**	Reword cat 1 and 2	Does your organisation, or your supply chain with access to your systems, grant limited privileged access and third party access only for a limited time period, or is it planning to do so?			Does your organisation, or your supply chain with access to your systems, grant limited privileged access and third party access only for a limited time period, or is it planning to do so?			Do you ensure that passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength?						
Process reviews are held at least once per year where data security is put at risk and following data security incidents	Yes/No	5.1.1	**5.1.1**	Non-material wording change cat 1 and 2	Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security or protection incident, with findings acted upon.	Explain, in the comments, how any incident response and management tests/process review findings tests have informed the immediate future technical protection and remediated any systemic vulnerabilities of the system or service, to ensure identified issues cannot arise in the same way again.	Yes	Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security or protection incident, with findings acted upon.	Explain, in the comments, how any incident response and management tests/process review findings tests have informed the immediate future technical protection and remediated any systemic vulnerabilities of the system or service, to ensure identified issues cannot arise in the same way again.	Yes	If your organisation has had a data breach or a near miss in the last year, has the organisation reviewed the process that may have allowed the breach to occur?	Confirm that your organisation has reviewed any processes that have caused a breach or a near miss, or which force people to use unauthorised workarounds that could compromise your organisation's data and cyber security. Workarounds could be things such as using unauthorised devices such as home computers or personal memory sticks or forwarding emails to personal email addresses. It is good practice to review processes annually even if a breach or near miss has not taken place. If no breaches or near misses in the last 12 months then please tick and write "Not applicable" in the comments box.	Yes	If your organisation has had a data breach or a near miss in the last year, has the organisation reviewed the process that may have allowed the breach to occur?	Confirm that your organisation has reviewed any processes that have caused a breach or a near miss, or which force people to use unauthorised workarounds that could compromise your organisation's data and cyber security. Workarounds could be things such as using unauthorised devices such as home computers or personal memory sticks or forwarding emails to personal email addresses. It is good practice to review processes annually even if a breach or near miss has not taken place. If no breaches or near misses in the last 12 months then please tick and write "Not applicable" in the comments box.	Yes
	Document	5.1.3	**5.1.3**	No changes	List of actions arising from each process review, with names of actionees.	For each process review a list of actions should be produced with each action having an owner. If no actions mark none in other text.		List of actions arising from each process review, with names of actionees.	For each process review a list of actions should be produced with each action having an owner. If no actions mark none in other text.		List of actions arising from each process review, with names of actionees.	For each process review a list of actions should be produced with each action having an owner. If no actions mark none in other text.					
Participation in reviews is comprehensive, and clinicians are actively involved	Document	5.2.1	**5.2.1**	No changes	Provide a scanned copy of the process review meeting registration sheet with attendee signatures and roles held.	An example of a scanned registration sheet, photo or minutes. The attendees should be from a multi-disciplinary team with active clinical involvement for care related processes and systems.		Provide a scanned copy of the process review meeting registration sheet with attendee signatures and roles held.	An example of a scanned registration sheet, photo or minutes. The attendees should be from a multi-disciplinary team with active clinical involvement for care related processes and systems.		Provide a scanned copy of the process review meeting registration sheet with attendee signatures and roles held.	An example of a scanned registration sheet, photo or minutes. The attendees should be from a multi-disciplinary team with active clinical involvement for care related processes and systems.					
Action is taken to address problem processes as a result of feedback at meetings or in year	Yes/No	5.3.1	**5.3.1**	No changes	Are the actions to address problem processes, being monitored and assurance given to the board or equivalent senior team?	Explain the governance around escalation of any issues and findings to the board, or equivalent, such as through reports and briefing notes, during the last twelve months.		Are the actions to address problem processes, being monitored and assurance given to the board or equivalent senior team?	Explain the governance around escalation of any issues and findings to the board, or equivalent, such as through reports and briefing notes, during the last twelve months.		Are the actions to address problem processes, being monitored and assurance given to the senior team?	Explain the governance around escalation of any issues and findings to the board, or equivalent, such as through reports and briefing notes, during the last twelve months.		Are the actions to address problem processes, being monitored and assurance given to the senior team?	Explain the governance around escalation of any issues to management through reports and briefing notes during the last twelve months.		
A confidential system for reporting data security and protection breaches and near misses is in place and actively used	Yes/No	6.1.1	**6.1.1**	No changes	A policy/procedure is in place to ensure data security and protection incidents are managed/reported appropriately.	Confirmation that a functioning data security and protection breach reporting and management mechanism is in place including use of the DSP Toolkit incident reporting tool	Yes	A policy/procedure is in place to ensure data security and protection incidents are managed/reported appropriately.	Confirmation that a functioning data security and protection breach reporting and management mechanism is in place including use of the DSP Toolkit incident reporting tool	Yes	Does your organisation have a system in place to report data breaches?	All staff, and volunteers if you have them, are responsible for noticing and reporting data breaches and it is vital that you have a robust reporting system in your organisation. There is an incident reporting tool within this toolkit which should be used to report health and care incidents to Information Commissioner's Office ICO. If you are not sure whether or not to inform the Information Commissioner's Office of a breach, the toolkit's incident reporting tool and guide can help you to decide.	Yes	A data security and protection breach reporting system is in place.	Confirmation that a functioning data security and protection breach reporting mechanism is in place including use of the DSP Toolkit incident reporting tool.	Yes
	Yes/No	6.1.4	**6.1.3**	No changes	Is the board or equivalent notified of the action plan for all data security and protection breaches?	Outline in the comments, the processes of notifying the board.	Yes	Is the board or equivalent notified of the action plan for all data security and protection breaches?	Outline in the comments, the processes of notifying the board.	Yes	If your organisation has had a data breach, were the management team notified, and did they approve the actions planned to minimise the risk of a recurrence?	In the event of a data breach the management team of your organisation, or nominated person, should be notified of the breach and any associated action plans or lessons learnt. If no breaches in the last 12 months then please tick and write "Not applicable" in the comments box.	Yes	If your organisation has had a data breach, were the management team notified, and did they approve the actions planned to minimise the risk of a recurrence?	In the event of a data breach the management team of your organisation, or nominated person, should be notified of the breach and any associated action plans or lessons learnt. If no breaches have occurred in the last 12 months then please tick and write "Not applicable" in the comments box.	
	Yes/No	6.1.5	**6.1.4**	No changes	Individuals affected by a breach are appropriately informed.	Data subjects are appropriately informed of data breaches in [accordance with guidance](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/). If no breaches then please tick and state "No breaches".	Yes	Individuals affected by a breach are appropriately informed.	Data subjects are appropriately informed of data breaches in [accordance with guidance](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/). If no breaches then please tick and state "No breaches".	Yes	If your organisation has had a data breach, were all individuals who were affected informed?	If your organisation has had a data breach that is likely to result in a high risk of adversely affecting individuals' rights and freedoms - e.g. damage to reputation, financial loss, unfair discrimination, or other significant loss - you must inform the individual(s) affected as soon as possible. If your organisation has had no such breaches in the last 12 months then please tick and write "Not applicable" in the comments box. More information is available from the [Information Commissioner's Office](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/).	Yes	If your organisation has had a data breach, were all individuals who were affected informed?	If your organisation has had a data breach that is likely to result in a high risk of adversely affecting individuals' rights and freedoms - e.g. damage to reputation, financial loss, unfair discrimination, or other significant loss - you must inform the individual(s) affected as soon as possible. If your organisation has had no such breaches in the last 12 months then please tick and write "Not applicable" in the comments box. More information is available from the [Information Commissioner's Office](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/).	Yes
All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway	Yes/No	6.2.3	**6.2.1**	No changes	Has antivirus/anti-malware software been installed on all computers that are connected to or capable of connecting to the Internet?	This applies to: application servers; desktop computers; laptop computers, tablets and mobile devices running windows desktop operating systems. Please include the name of your anti-virus product in the comments.	Yes	Has antivirus/anti-malware software been installed on all computers that are connected to or capable of connecting to the Internet?	This applies to: application servers; desktop computers; laptop computers, tablets and mobile devices running windows desktop operating systems. Please include the name of your anti-virus product in the comments.	Yes	Do all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date?	This applies to all servers, desktop computers, laptop computers, and tablets. Note that antivirus software and antimalware software are the same thing – they both perform the same functions. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or other devices, then tick and write "Not applicable" in the comments box. Further information is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/have-up-to-date-antivirus-software/).	Yes	Do all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date?	This applies to all servers, desktop computers, laptop computers, and tablets. Note that antivirus software and antimalware software are the same thing – they both perform the same functions. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or other devices, then tick and write "Not applicable" in the comments box. Further information is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/have-up-to-date-antivirus-software/).	Yes

	Yes/No	6.2.4	**6.2.3**	Newly mandatory cat 2	Antivirus/anti-malware is kept continually up to date.	Provide an explanation of how this is achieved. This could be through automatic update, central deployment, ATP etc.	Yes	Antivirus/anti-malware is kept continually up to date.	Provide an explanation of how this is achieved. This could be through automatic update, central deployment, ATP etc.	Yes						
	Yes/No	6.2.5	**6.2.4**	No changes	Antivirus/anti-malware software scans files automatically upon access.	This includes when files are downloaded and opened, and when they are accessed from a network folder.	Yes	Antivirus/anti-malware software scans files automatically upon access.	This includes when files are downloaded and opened, and when they are accessed from a network folder.							
	Yes/No	6.2.6	**6.2.5**	No changes	Connections to malicious websites on the Internet are prevented.	This applies to all corporate devices. It may be achieved by one or more of the following using a web proxy, antivirus/anti-malware, browser tools, Protective DNS services, blacklisting or other mechanisms.	Yes	Connections to malicious websites on the Internet are prevented.	This applies to all corporate devices. It may be achieved by one or more of the following using a web proxy, antivirus/anti-malware, browser tools, Protective DNS services, blacklisting or other mechanisms.							
	Text	6.2.9	**6.2.6**	No changes	Number of phishing emails reported by staff per month.	From your service desk system or service the number of reported phishing mails.		Number of phishing emails reported by staff per month.	From your service desk system or service the number of reported phishing mails.		Number of phishing emails reported by staff per month.	From your service desk system or service the number of reported phishing mails.				
	Yes/No	6.2.10	**6.2.7**	No changes	Does the organisation maintain a list of approved applications, and are users prevented from installing any application that is unsigned or has an invalid signature?	This applies to: email, Servers, desktop computers, laptop computers; tablets and mobile phones. Provide details of how this is enforced.	Yes									
	Yes/No	6.2.11	**6.2.8**	No changes	You have implemented on your email, Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) for your organisation's domains to make email spoofing difficult.	This applies to email systems	Yes	You have implemented on your email, Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) for your organisation's domains to make email spoofing difficult.	This applies to email systems	Yes						
	Yes/No	6.2.12	**6.2.9**	No changes	You have implemented spam and malware filtering, and enforce DMARC on inbound email.	This applies to email systems and should include the name of the filtering product.	Yes	You have implemented spam and malware filtering, and enforce DMARC on inbound email.	This applies to email systems and should include the name of the filtering product.	Yes						
Known vulnerabilities are acted on based on advice from NHS Digital, and lessons are learned from previous incidents and near misses	Text	6.3.1	**6.3.1**	No changes	If you have had a data security incident, was it caused by a known vulnerability?	Provide details of incidents over the reporting period (a year). Known vulnerabilities are those listed on the [Cyber alerts portal](https://digital.nhs.uk/cyber-alerts). If no incidents have occurred, state: "None".	Yes	If you have had a data security incident, was it caused by a known vulnerability?	Provide details of incidents over the reporting period (a year). Known vulnerabilities are those listed on the [Cyber alerts portal](https://digital.nhs.uk/cyber-alerts). If no incidents have occurred, state: "None".	Yes	If you have had a data security incident, was it caused by a known vulnerability?	Provide details of incidents over the reporting period (a year). If no incidents have occurred state "None".				
	Yes/No	6.3.2	**6.3.2**	Reword cat 1 and 2	The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service.	Your response should cover 'high severity' cyber alerts issued over the last 12 months.	Yes	The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service.	Your response should cover 'high severity' cyber alerts issued over the last 12 months.	Yes	Have staff, directors, trustees and volunteers been advised that use of public Wi-Fi for work purposes is unsafe?	Use of public Wi-Fi (e.g. Wi-Fi freely available at cafes and train stations etc) or unsecured Wi-Fi (Wi-Fi where no password is required to access it) could be unsafe and lead to unauthorised access of personal data. Staff, directors, trustees and volunteers if you have them, should be advised of this. If nobody uses mobile devices for work purposes out of your building/offices, then tick and write "Not applicable" in the comments box.	Yes			
	Text	6.3.3	**6.3.3**	No changes	The organisation has a proportionate monitoring solution to detect cyber events on systems and services.	Since 1st July 2021, all systems monitoring requirements have been assessed.	Yes	The organisation has a proportionate monitoring solution to detect cyber events on systems and services.	Since 1st July 2021, all systems monitoring requirements have been assessed.	Yes						
	Yes/No	6.3.5	**6.3.4**	No changes	Are all new digital services that are attractive to cyber criminals (such as for fraud) implementing transactional monitoring techniques from the outset?	Includes an assessment of which services are susceptible to fraud. If none, please 'tick' and explain in the comments section.	Yes	Are all new digital services that are attractive to cyber criminals (such as for fraud) implementing transactional monitoring techniques from the outset?	Includes an assessment of which services are susceptible to fraud. If none, please 'tick' and explain in the comments section.	Yes						
	Text	6.3.6	**6.3.5**	No changes	Have you had any repeat data security incidents within the organisation during the past twelve months?	A repeat incident is defined as an exploitation of the same vulnerability on the same systems or different ones, that occurs within three calendar months of a previous occurrence. Provide details.		Have you had any repeat data security incidents within the organisation during the past twelve months?	A repeat incident is defined as an exploitation of the same vulnerability on the same systems or different ones, that occurs within three calendar months of a previous occurrence. Provide details.		Have you had any repeat data security incidents within the organisation during the past twelve months?	A repeat incident is defined as an exploitation of the same vulnerability on the same systems or different ones, that occurs within three calendar months of a previous occurrence. Provide details.		Have you had any repeat data security incidents within the organisation during the past twelve months?	A repeat incident is defined as an exploitation of the same vulnerability on the same systems or different ones, that occurs within three calendar months of a previous occurrence. Provide details.	
Organisations have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services	Document	7.1.1	**7.1.1**	No changes	Your organisation understands the health and care services it provides.	This should cover: i. What their key operational services are, ii. What technologies and services their operational services rely on to remain available and secure, iii. What other dependencies the operational services have (power, cooling, data, people etc.), iv. The impact of loss of availability of the service	Yes	Your organisation understands the health and care services it provides.	This should cover: i. What their key operational services are, ii. What technologies and services their operational services rely on to remain available and secure, iii. What other dependencies the operational services have (power, cooling, data, people etc.), iv. The impact of loss of availability of the service	Yes	Organisations understand the health and care services they provide.	This should cover: i. What their key operational services are, ii. What technologies and services their operational services rely on to remain available and secure, iii. What other dependencies the operational services have (power, cooling, data, people etc.), iv. The impact of loss of availability of the service				
	Yes/No	7.1.2	**7.1.2**	No changes	Do you have well defined processes in place to ensure the continuity of services in the event of a data security incident, failure or compromise?	This may include the preservation of manual processes for essential services.	Yes	Do you have well defined processes in place to ensure the continuity of services in the event of a data security incident, failure or compromise?	This may include the preservation of manual processes for essential services.	Yes	Does your organisation have a business continuity plan that covers data and cyber security?	Your organisation's business continuity plan should cover data and cyber security – for example what would you do to ensure continuity of service if: you had a power cut; the phone line/internet went down; you were hacked; a computer broke down; the office became unavailable (e.g. through fire). An example business continuity plan is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/).	Yes	Does your organisation have a business continuity plan that covers data and cyber security?	Your organisation's business continuity plan should cover data and cyber security – for example what would you do to ensure continuity of service if: you had a power cut; the phone line/internet went down; you were hacked; a computer broke down; the office became unavailable (e.g. through fire).	Yes
	Yes/No	7.1.3	**7.1.3**	No changes	You understand the resources and information that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available.			You understand the resources and information that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available.			You understand the resources and information that will be needed if there is a data security incident and arrangements are in place to make these resources available.					
	Text	7.1.4	**7.1.4**	No changes	You use your security awareness, e.g. threat intelligence sources, to make temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.			You use your security awareness, e.g. threat intelligence sources, to make temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.								
There is an effective test of the continuity plan and disaster recovery plan for data security incidents	Text	7.2.1	**7.2.1**	No changes	Explain how your data security incident response and management plan has been tested to ensure all parties understand their roles and responsibilities as part of the plan.	This should be since 1st July 2021 with active board and business representation. Exercise scenarios should be based on incidents experienced by your and other organisations, or are composed using threat intelligence.	Yes	Explain how your data security incident response and management plan has been tested to ensure all parties understand their roles and responsibilities as part of the plan.	This should be since 1st July 2021 with active board and business representation. Exercise scenarios should be based on incidents experienced by your and other organisations, or are composed using threat intelligence.	Yes	How does your organisation test the data and cyber security aspects of its business continuity plan?	Describe how your organisation tests these aspects of its plan and what the outcome of the exercise was the last time you did this. This should be since 1st July 2021. Guidance for testing your business continuity plan for the data and cyber security aspects is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/).	Yes			
	Document	7.2.4	**7.2.2**	No changes	From the business continuity exercise, explain what issues and actions were documented, with names of actionees listed against each item.	Each action should have an owner and timescale.	Yes	From the business continuity exercise, explain what issues and actions were documented, with names of actionees listed against each item.	Each action should have an owner and timescale.	Yes	From the business continuity exercise, explain what issues and actions were documented, with names of actionees listed against each item.	Each action should have an owner and timescale.				
You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions	Text	7.3.1	**7.3.1**	No changes	On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary.	Advice is available from NHS Digital or a cyber incident response company.	Yes	On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary.	Advice is available from NHS Digital or a cyber incident response company.	Yes	How does your organisation make sure that there are working backups of all important data and information?	It is important to make sure that backups are being done regularly, that they are successful and that they include the right files and systems. Briefly explain how your organisation's back up systems work and how you have tested them. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or IT systems, write "Not applicable" in the text box. For advice about backups, see [Digital Social	Yes			
	Yes/No	7.3.2	**7.3.2**	No changes	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Contacts include phone number as well as email.	Yes	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Contacts include phone number as well as email.	Yes	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Contacts include phone number as well as email.	Yes	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Contacts include phone number as well as email.	Yes
	Yes/No	7.3.3	**7.3.3**	No changes	Are draft press materials for data security incidents ready?	The press materials you have such as skeleton press statements in the eventuality of an incident.		Are draft press materials for data security incidents ready?	The press materials you have such as skeleton press statements in the eventuality of an							
	Yes/No	7.3.4	**7.3.4**	No changes	Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed.	Provide evidence that your backup, testing and review process is effective.	Yes	Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed.	Provide evidence that your backup, testing and review process is effective.	Yes	Are backups routinely tested to make sure that data and information can be restored?	It is important that your organisation's backups are tested at least annually to make sure data and information can be restored (in the event of equipment breakdown for example). You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or IT systems, then tick and write "Not applicable" in the	Yes	How does your organisation make sure that there are working backups of all important data and information?	It is important to make sure that backups are being done regularly, that they are successful and that they include the right files and systems. Briefly explain how your organisation's back up systems work and how you have tested them. You may need to ask your IT supplier to assist with answering this question.	Yes
	Text	7.3.5	**7.3.5**	Reword for cat 1 and 2	Do you test your backups regularly to ensure you can restore the service from a backup?	Backups should be tested frequently. The example provided may relate to a live or test environment.	Yes	Do you test your backups regularly to ensure you can restore the service from a backup?	Backups should be tested frequently. The example provided may relate to a live or test environment.	Yes						
	Yes/No	7.3.6	**7.3.6**	Reword for cat 1, 2 and 3	Are your backups kept securely and separate from your network ('offline'), or in a cloud service designed for this purpose?	Cloud synching services, such as OneDrive, SharePoint or Google Drive, should not be used as your only backup and stored backup should not be permanently connected to your network. Further guidance is available from the [National Cyber Security Centre](https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world)	Yes	Are your backups kept securely and separate from your network ('offline'), or in a cloud service designed for this purpose?	Cloud synching services, such as OneDrive, SharePoint or Google Drive, should not be used as your only backup and stored backup should not be permanently connected to your network. Further guidance is available from the [National Cyber Security Centre](https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world)	Yes	Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose?	Cloud synching services, such as OneDrive, SharePoint or Google Drive, should not be used as your only backup and stored backup should not be permanently connected to your network. Further guidance is available from the [National Cyber Security Centre](https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world)				
All software and hardware has been surveyed to understand if it is supported and up to date	Document	8.1.1	**8.1.1**	No changes	Provide evidence of how the organisation tracks and records all software assets and their configuration.	This is a list of all the software that is used in the organisation including version numbers and whether the software is supported i.e. it still receives security updates.	Yes	Provide evidence of how the organisation tracks and records all software assets and their configuration.	This is a list of all the software that is used in the organisation including version numbers and whether the software is supported i.e. it still receives security updates.	Yes						
	Yes/No	8.1.2	**8.1.2**	No changes	Does the organisation track and record all end user devices and removable media assets?	e.g. You hold an up to date list of all your end user devices and removable media.	Yes	Does the organisation track and record all end user devices and removable media assets?	e.g. You hold an up to date list of all your end user devices and removable media.	Yes	Does the organisation track and record all end user devices and removable media assets?	e.g. You hold an up to date list of all your end user devices and removable media.				
	Yes/No	8.1.3	**8.1.3**	Newly mandatory cat 2	Devices that are running out-of-date unsupported software and no longer receive security updates (patches) are removed from the network, or the software in question is uninstalled. Where this is not possible, the device should be isolated and have limited connectivity to the network, and the risk assessed, documented, accepted and signed off by the SIRO.	Provide summary details in the comments box. Documentation should be held locally for protections for these devices . This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers; desktop computers; laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services. Devices that are standalone or air-gapped should be captured under 9.5.9.	Yes	Devices that are running out-of-date unsupported software and no longer receive security updates (patches) are removed from the network, or the software in question is uninstalled. Where this is not possible, the device should be isolated and have limited connectivity to the network, and the risk assessed, documented, accepted and signed off by the SIRO.	Provide summary details in the comments box. Documentation should be held locally for protections for these devices . This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers; desktop computers; laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services. Devices that are standalone or air-gapped should be captured under 9.5.9.	Yes						

	Yes/No	8.1.4	**8.1.4**	No changes	The organisation ensures that software that is no longer within support or receiving security updates is uninstalled. Where this is impractical, the endpoint should be isolated and have limited connectivity to the network.	Covers software running on computers that are connected to the internet.						Are all the IT systems and the software used in your organisation still supported by the manufacturer or the risks are understood and managed?	Systems and software that are no longer supported by the manufacturer can be unsafe as they are no longer being updated to protect against viruses for example. You may need to ask your IT supplier to assist with answering this question. Examples of unsupported software include: Windows XP, Windows Vista, Windows 7, Java or Windows Server 2008. Windows 8.1 is supported until January 2023. Windows 10 is supported and is the most up to date version of Windows. This question also applies to software systems such as rostering, care planning or electronic medicine administration record (MAR) charts for example. If your organisation does not use any IT systems or software, then tick and write "Not applicable" in the comments box. For guidance (including information on how to check which software versions you have), see [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/install-the-latest-	Yes			
Unsupported software and hardware is categorised and documented, and data security risks are identified and managed	Document	8.2.1	**8.2.1**	No changes	List any unsupported software prioritised according to business risk, with remediation plan against each item.	Unsupported software is software which is no longer receiving security updates e.g. Windows XP, Java or Windows Server 2008. Unsupported software is less secure and so poses a larger risk to your organisation. The unsupported software list will comprise of the results of the software survey where the software is not supported/updated.	Yes	List any unsupported software prioritised according to business risk, with remediation plan against each item.	Unsupported software is software which is no longer receiving security updates e.g. Windows XP, Java or Windows Server 2008. Unsupported software is less secure and so poses a larger risk to your organisation. The unsupported software list will comprise of the results of the software survey where the software is not supported/updated.	Yes	If your answer to 8.1.4 (on IT systems and software being supported by the manufacturer) was that software risks are being managed, please provide a document that summarises the risk of continuing to use each unsupported item, the reasons for doing so and a summary of the action your organisation is taking to minimise the risk.	This is a conscious decision to accept and manage the associated risks of unsupported systems. This document should indicate that your board or management team have formally considered the risks of continuing to use unsupported items and have concluded that the risks are acceptable. If your answer to the previous question was yes, write "Not	Yes			
	Yes/No	8.2.2	**8.2.2**	Reword cat 1 and 2	The SIRO confirms that the risks of using unsupported systems are being managed and the scale of unsupported software is reported to your board along with the plans to address.	The SIRO has been briefed on the unsupported systems and has made a conscious decision to accept and manage the associated risks. A report has been provided to the board in the last 12 months. If no unsupported systems please tick and state "No unsupported systems" as a comment.	Yes	The SIRO confirms that the risks of using unsupported systems are being managed and the scale of unsupported software is reported to your board along with the plans to address.	The SIRO has been briefed on the unsupported systems and has made a conscious decision to accept and manage the associated risks. A report has been provided to the board in the last 12 months. If no unsupported systems please tick and state "No unsupported systems" as a comment.	Yes						
Supported systems are kept up-to-date with the latest security patches	Document	8.3.1	**8.3.1**	No changes	How do your systems receive updates and how often?	This is your strategy for system updates. You may need your IT supplier/s to assist with this.	Yes	How do your systems receive updates and how often?	This is your strategy for system updates. You may need your IT supplier/s to assist with this.	Yes				How do your systems receive updates and how often?	This is your strategy for system updates. You may need your IT supplier/s to assist with this.	Yes
	Text	8.3.2	**8.3.2**	No changes	How often, in days, is automatic patching typically being pushed out to remote endpoints?	Remote endpoints being those devices or computers that are not on the core network (such as home or mobile workers). Provide the usual number of days between one wave of remote patching and the next.	Yes	How often, in days, is automatic patching typically being pushed out to remote endpoints?	Remote endpoints being those devices or computers that are not on the core network (such as home or mobile workers). Provide the usual number of days between one wave of remote patching and the next.	Yes	How often, in days, is automatic patching typically being pushed out to remote endpoints?	Remote endpoints being those devices or computers that are not on the core network (such as home or mobile workers). Provide the usual number of days between one wave of remote patching and the next.				
	Yes/No	8.3.3	**8.3.3**	No changes	There is a documented approach to applying security updates (patches) agreed by the SIRO.	Provide details in the comments box. This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers, desktop computers, laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services.	Yes	There is a documented approach to applying security updates (patches) agreed by the SIRO.	Provide details in the comments box. This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers, desktop computers, laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud	Yes						
	Yes/No	8.3.4	**8.3.4**	No changes	Where a security patch has been classed as critical or high-risk vulnerability it is applied within 14 days, or the risk has been assessed, documented, accepted and signed off by the SIRO with an auditor agreeing a robust risk management process has been applied.	Provide summary details in the comments box. Documentation should be held locally for all security patches. This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers, desktop computers, laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services. Devices that are unable to be patched should be captured under 8.1.3. Devices that are standalone or air-gapped should be captured under 9.5.9.	Yes	Where a security patch has been classed as critical or high-risk vulnerability it is applied within 14 days, or the risk has been assessed, documented, accepted and signed off by the SIRO with an auditor agreeing a robust risk management process has been applied.	Provide summary details in the comments box. Documentation should be held locally for all security patches. This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers, desktop computers, laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services. Devices that are unable to be patched should be captured under 8.1.3. Devices that are standalone or air-gapped should be captured under 9.5.9.	Yes						
	Text	New	**8.3.5**	New	Where a security patch has been classed as critical or high-risk vulnerability has not been applied, explain the technical remediation and risk management that has been undertaken.	Provide details for each patch not applied. This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers, desktop computers, laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services.	**Yes**				How does your organisation make sure that the latest software updates are downloaded and installed?	It is important that your organisation's IT system(s) and devices have the latest software and application updates installed. Most software can be set to apply automatic updates when they become available from the manufacturer. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any IT systems, devices or software, write "Not applicable" in the text box. Further information is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/install-the-latest-software-updates/).	Yes			
	Yes/No	8.3.5	**8.3.6**	Changed to yes/no	Is your organisation actively using and managing Advanced Threat Protection (ATP) or equivalent?	e.g. using NHS Digital Endpoint Detection and Response. Please provide details of the product used in the comments.		Is your organisation actively using and managing Advanced Threat Protection (ATP) or equivalent?	e.g. using NHS Digital Endpoint Detection and Response. Please provide details of the product used in the comments.							
	Document	New	**8.3.7**	New	Are 95% of your server estate and 98% of your desktop estate on supported versions of operating systems?	Please upload a screenshot/s from Advanced Threat Protection (ATP) demonstrating the percentage of servers and desktops on supported versions of operating systems. If not met, please provide details in the comments on the plan to achieve 95% of your server estate and 98% of your desktop estate on supported versions of operating systems.		Are 95% of your server estate and 98% of your desktop estate on supported versions of operating systems?	Please upload a screenshot/s from Advanced Threat Protection (ATP) demonstrating the percentage of servers and desktops on supported versions of operating systems. If not met, please provide details in the comments on the plan to achieve 95% of your server estate and 98% of your desktop estate on supported versions of operating systems.							
You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service	Text	8.4.1	**8.4.1**	No changes	Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?	Explain at a summary level. Where it is not possible to apply these measures, explain any mitigations (such as logical separation).	Yes	Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?	Explain at a summary level. Where it is not possible to apply these measures, explain any mitigations (such as logical separation).	Yes	Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?	Explain at a summary level. Where it is not possible to apply these measures, explain any mitigations (such as logical separation).				
	Yes/No	8.4.2	**8.4.2**	No changes	All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.	Covers software running on computers that are connected to or capable of connecting to the Internet. Unsupported software should be covered under 8.3.4.	Yes	All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.	Covers software running on computers that are connected to or capable of connecting to the Internet. Unsupported software should be covered under 8.3.4.	Yes	All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.	Covers software running on computers that are connected to or capable of connecting to the Internet.				
	Yes/No	8.4.3	**8.4.3**	No changes	You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.	This may include NHS Digital's VMS and / or Bitsight service.		You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.	This may include NHS Digital's VMS and / or Bitsight service.		You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.					
All networking components have had their default passwords changed	Yes/No	9.1.1	**9.1.1**	No changes	The Head of IT, or equivalent role, confirms all networking components have had their default passwords changed to a high strength password.	This covers all network components under the organisation's control.	Yes	The Head of IT, or equivalent role, confirms all networking components have had their default passwords changed to a high strength password.	This covers all network components under the organisation's control.	Yes	Does your organisation make sure that the passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords?	Networking components include routers, switches, hubs and firewalls at all of your organisation's locations. Your organisation may just have a Wi-Fi router. This does not apply to Wi-Fi routers for people working from home. You may need to ask your IT supplier to assist with answering this question. If your organisation does not have a network or internet access, then tick and write "Not applicable" in the comments	Yes	The Head of IT, or equivalent role confirms all networking components have had their default passwords changed.	If you don't have network or internet access please contact the helpdesk to request an exemption.	Yes
	Yes/No	9.1.2	**9.1.2**	Newly mandatory cat 2	The Head of IT, or equivalent role, confirms all organisational devices have had their default passwords changed.	This covers the organisation's servers, desktop computers, laptop computers, tablets and mobile phones.	Yes	The Head of IT, or equivalent role, confirms all organisational devices have had their default passwords changed.	This covers the organisation's servers, desktop computers, laptop computers, tablets and mobile phones.	Yes						
A penetration test has been scoped and undertaken	Yes/No	9.2.1	**9.2.1**	No changes	The annual IT penetration testing is scoped in negotiation between the SIRO, business and testing team including a vulnerability scan and checking that all networking components have had their default passwords changed to a high strength password.	Please include the scope and redact any elements of the results that are sensitive.	Yes	Annual IT penetration testing is scoped through negotiation between the SIRO, business and testing team, and includes a vulnerability scan and a check that all networking components have had their default passwords changed.	Please include the scope and redact any elements of the results that are sensitive.	Yes	Annual IT penetration testing is scoped through negotiation between the person responsible for IT, management and testing team, and includes a vulnerability scan and a check that all networking components have had their default passwords changed.	This should be since 1st July 2021. Please include the scope and redact any elements of the results that are sensitive.		Annual IT penetration testing is scoped through negotiation between the SIRO, business and testing team, and includes a vulnerability scan and a check that all networking components have had their default passwords changed.	This should be since 1st July 2021. Please include the scope and redact any elements of the results that are sensitive.	
	Date	9.2.2	**9.2.2**	No changes	The date the penetration test and vulnerability scan was undertaken.	This should be since 1st July 2021.	Yes	The date the penetration test was undertaken.	This should be since 1st July 2021.	Yes	The date the penetration test was undertaken.	This should be since 1st July 2021.				
Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities	Yes/No	9.3.1	**9.3.1**	No changes	All web applications are protected and not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities.	If no web applications, 'tick' yes and explain in the comments.	Yes	All web applications are protected and not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities.	If no web applications, 'tick' yes and explain in the comments.	Yes	All web applications are protected and not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities.	If no web applications, 'tick' yes and explain in the comments.				
	Document	9.3.2	**9.3.2**	No changes	The SIRO or equivalent senior role has reviewed the results of latest penetration testing, with an action plan for its findings.	Provide the action plan with confirmation of SIRO review.	Yes	The SIRO or equivalent senior role has reviewed the results of latest penetration testing, with an action plan for its findings.	Provide the action plan with confirmation of SIRO review.		The person responsible for IT has reviewed the results of latest penetration testing, with an action plan for its findings.	Provide the action plan with confirmation of SIRO review.				
	Yes/No	9.3.3	**9.3.3**	No changes	The organisation uses the UK Public Sector DNS service, or equivalent protective DNS service, to resolve Internet DNS queries.		Yes	The organisation uses the UK Public Sector DNS service, or equivalent protective DNS service, to resolve Internet DNS queries.		Yes						
	Yes/No	9.3.4	**9.3.4**	No changes	The organisation ensures that changes to its authoritative DNS entries can only be made by strongly authenticated and authorised administrators.		Yes	The organisation ensures that changes to its authoritative DNS entries can only be made by strongly authenticated and authorised administrators.		Yes	The organisation ensures that changes to its authoritative DNS entries can only be made by strongly authenticated and authorised administrators.					
	Yes/No	9.3.5	**9.3.5**	No changes	The organisation understands and records all IP ranges in use across the organisation.		Yes	The organisation understands and records all IP ranges in use across the organisation.		Yes	The organisation understands and records all IP ranges in use across the organisation.					
	Yes/No	9.3.6	**9.3.6**	No changes	The organisation is protecting it's data in transit (including email) using well-configured TLS v1.2 or better.		Yes	The organisation is protecting it's data in transit (including email) using well-configured TLS v1.2 or better.		Yes	The organisation is protecting it's data in transit (including email) using well-configured TLS v1.2 or better.					
	Yes/No	9.3.7	**9.3.7**	No changes	The organisation has registered and uses the National Cyber Security Centre (NCSC) Web Check service, or equivalent web check service, for its publicly-visible applications.		Yes	The organisation has registered and uses the National Cyber Security Centre (NCSC) Web Check service, or equivalent web check service, for its publicly-visible applications.		Yes						
	Document	New	**9.3.8**	New	The organisation maintains a register of medical devices connected to its network.	The register should be uploaded and include Vendor, maintenance arrangements, any network segmentation is in place and whether network access is given to supplier/maintainer.	Yes	The organisation maintains a register of medical devices connected to its network.	The register should include Vendor, maintenance arrangements and whether network access is given to supplier/maintainer.		The organisation maintains a register of medical devices connected to its network.	The register should include Vendor, maintenance arrangements and whether network access is given to supplier/maintainer.		The organisation maintains a register of medical devices connected to its network.	The register should include Vendor, maintenance arrangements and whether network access is given to supplier/maintainer.	
	Document	New	**9.3.9**	New	What is the organisation's data security assurance process for medical devices connected to the network.	This should be a policy / process document or full explanation covering how the organisation assures data security during the full life cycle of the medical device.										

You have demonstrable confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services	Text	9.4.1	**9.4.1**	Removed from Cat 3	You validate that the security measures in place to protect the networks and information systems are effective, and remain effective for the lifetime over which they are needed.	Please provide an explanation.		You validate that the security measures in place to protect the networks and information systems are effective, and remain effective for the lifetime over which they are needed.	Please provide an explanation.							
	Yes/No	9.4.2	**9.4.2**	Removed from Cat 3	You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential services.	The review period for assurance methods should be in the last twelve months.		You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential services.	The review period for assurance methods should be in the last twelve months.							
	Text	9.4.3	**9.4.3**	No changes	Your confidence in your security as it relates to your technology, people, and processes has been demonstrated to, and verified by, a third party onsite assessment.	Using an on-site technical assessment from [NHS Digital's Cyber Security Support Model](https://digital.nhs.uk/services/data-security-centre/data-security-onsite-assessment) or equivalent. Organisations receiving IT provision from an NHS organisation may provide evidence from the supplying organisations assessment, subject to appropriate scope.		Your confidence in your security as it relates to your technology, people, and processes has been demonstrated to, and verified by, a third party onsite assessment.	Using an on-site technical assessment from [NHS Digital's Cyber Security Support Model](https://digital.nhs.uk/services/data-security-centre/data-security-onsite-assessment) or equivalent. Organisations receiving IT provision from an NHS organisation may provide evidence from the supplying organisations assessment, subject to appropriate scope.		Your confidence in your security as it relates to your technology, people, and processes has been demonstrated to, and verified by, a third party onsite assessment.	Organisations that have outsourced their entire IT function may be covered by their supplier's assessment.				
	Text	9.4.4	**9.4.4**	No changes	Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.		Yes	Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.		Yes	Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.					
	Document	9.4.6	**9.4.5**	Removed from Cat 3	What level of assurance (overall risk rating & confidence level rating) did the independent audit of your Data Security and Protection Toolkit provide to your organisation?	Upload a copy of your full DSPT audit/independent assessment report, which should cover the mandatory audit-scope set out in the ['Strengthening Assurance Independent Assessment Guide'](https://www.dsptoolkit.nhs.uk/Help/Independent-Assessment-Guides)	Yes	What level of assurance did the independent audit of your Data Security and Protection Toolkit provide to your organisation?	Upload a copy of your full DSPT audit/independent assessment report, which should cover the mandatory audit-scope set out in the ['Strengthening Assurance Independent Assessment Guide'](https://www.dsptoolkit.nhs.uk/Help/Independent-Assessment-Guides)	Yes						
You securely configure the network and information systems that support the delivery of essential services	Yes/No	9.6.1	**9.5.1**	No changes	All devices in your organisation have technical controls that manage the installation of software on the device.	Describe how this is managed across your devices with detail of any exceptions.	Yes	All devices in your organisation have technical controls that manage the installation of software on the device.	Describe how this is managed across your devices with detail of any exceptions.	Yes	All devices in your organisation have technical controls that manage the installation of software on the device	Describe how this is managed across your devices with detail of any exceptions.				
	Yes/No	9.6.2	**9.5.2**	No changes	Confirm all data are encrypted at rest on all mobile devices and removable media and you have the ability to remotely wipe and/or revoke access from an end user device.		Yes	Confirm all data are encrypted at rest on all mobile devices and removable media and you have the ability to remotely wipe and/or revoke access from an end user device.		Yes	Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?	Mobile computers like laptops and tablets and removable devices like memory sticks/cards/CDs are vulnerable as they can be lost or stolen. To make these devices especially difficult to get into, they can be encrypted (this protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people). Devices can be further protected, for example, by preventing the use of removable devices like memory sticks. This is called computer port control. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any mobile devices, or equivalent security arrangements are in place, then tick and write "Not applicable" in the comments box. For advice on encrypting mobile devices and equivalent security arrangements, see [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/protect-mobile-devices-and-tablets/).	Yes	Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?	Mobile computers like laptops and tablets and removable devices like memory sticks/cards/CDs are vulnerable as they can be lost or stolen. To make these devices especially difficult to get into, they can be encrypted (this protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people). Devices can be further protected, for example, by preventing the use of removable devices like memory sticks. This is called computer port control. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any mobile devices, or equivalent security arrangements are in place, then tick and write "Not applicable" in the comments box.	Yes
	Text	9.6.3	**9.5.3**	No changes	You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.			You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.			You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.					
	Yes/No	9.6.4	**9.5.4**	No changes	Only approved software can be installed and run and unnecessary software is removed.	This is for all devices in your organisation including servers, desktop computers; laptop computers, tablets, mobile phones. This could be a whitelisting solution.	Yes	Only approved software can be installed and run and unnecessary software is removed.	This is for all devices in your organisation including servers, desktop computers; laptop computers, tablets, mobile phones. This could be a whitelisting solution.							
	Yes/No	9.6.5	**9.5.5**	No changes	End user devices are built from a consistent and approved base image.	Applies to the organisation's desktop computers, laptop computers and tablets.	Yes	End user devices are built from a consistent and approved base image.	Applies to the organisation's desktop computers, laptop computers and tablets.							
	Yes/No	9.6.6	**9.5.6**	No changes	End user device security settings are managed and deployed centrally.	Applies to the organisation's desktop computers, laptop computers and tablets. This could be achieved using Group policy, mobile device management or similar mechanisms.	Yes	End user device security settings are managed and deployed centrally.	Applies to the organisation's desktop computers, laptop computers and tablets. This could be achieved using Group policy, mobile device management or similar mechanisms.							
	Yes/No	9.6.7	**9.5.7**	No changes	AutoRun is disabled.	This applies to servers, desktop and laptop computers. AutoRun relates to automatic execution of files without user interaction, and should not be confused with AutoPlay (which requires user interaction).	Yes	AutoRun is disabled.	This applies to servers, desktop and laptop computers. AutoRun relates to automatic execution of files without user interaction, and should not be confused with AutoPlay (which requires user interaction).							
	Yes/No	9.6.9	**9.5.8**	No changes	All remote access is authenticated.	Strong (ideally multifactor) authentication is required to remotely access personal, confidential information. This includes both web applications and remote access to corporate networks.	Yes	All remote access is authenticated.	Strong (ideally multifactor) authentication is required to remotely access personal, confidential information. This includes both web applications and remote access to corporate networks.							
	Yes/No	9.6.10	**9.5.9**	No changes	You have a plan for protecting devices that are natively unable to connect to the Internet, and the risk has been assessed, documented, accepted and signed off by the SIRO.	This applies to any device (managed internally or by a third party) that does not have a route to/from the Internet, such as air-gapped networks or stand-alone devices. Such as an MRI Scanner.	Yes	You have a plan for protecting devices that are natively unable to connect to the Internet, and the risk has been assessed, documented, accepted and signed off by the SIRO.	This applies to any device (managed internally or by a third party) that does not have a route to/from the Internet, such as air-gapped networks or stand-alone devices. Such as an MRI Scanner.	Yes						
	Yes/No	9.6.11	**9.5.10**	No changes	Does your organisation meet the secure email standard?	[Further detail on the standard](https://digital.nhs.uk/services/nhsmail/the-secure-email-standard) is available on the NHS Digital website.		Does your organisation meet the secure email standard?	[Further detail on the standard](https://digital.nhs.uk/services/nhsmail/the-secure-email-standard) is available on the NHS Digital website.							
The organisation is protected by a well managed firewall	Yes/No	9.7.1	**9.6.1**	No changes	Have one or more firewalls (or similar network device) been installed on all the boundaries of the organisation's internal network(s)?	This may include NHS Digital's Secure Boundary cloud-based firewall. IT Healthcheck would provide suitable evidence.	Yes	Have one or more firewalls (or similar network device) been installed on all the boundaries of the organisation's internal network(s)?	This may include NHS Digital's Secure Boundary cloud-based firewall. IT Healthcheck would provide suitable evidence.	Yes						
	Yes/No	9.7.2	**9.6.2**	No changes	Has the administrative interface used to manage the boundary firewall been configured such that; it is not accessible from the Internet, it requires second factor authentication or is access limited to a specific address?		Yes	Has the administrative interface used to manage the boundary firewall been configured such that; it is not accessible from the Internet, it requires second factor authentication or is access limited to a specific address?								
	Yes/No	9.7.3	**9.6.3**	No changes	The organisation has checked and verified that firewall rules ensure that all unauthenticated inbound connections are blocked by default.	All protocols (such as HTTP/S, SMB, NetBIOS, Telnet, TFTP, RPC, rlogin, rsh, rexec etc.) are blocked by default.	Yes	The organisation has checked and verified that firewall rules ensure that all unauthenticated inbound connections are blocked by default.	All protocols (such as HTTP/S, SMB, NetBIOS, Telnet, TFTP, RPC, rlogin, rsh, rexec etc.) are blocked by default							
	Yes/No	9.7.4	**9.6.4**	No changes	All inbound firewall rules (other than default deny) are documented with business justification and approval by an authorised individual.	Confirm documentation of approval is available. This must be accurate and up to date.	Yes	All inbound firewall rules (other than default deny) are documented with business justification and approval by an authorised individual.	Confirm documentation of approval is available. This must be accurate and up to date.							
	Yes/No	9.7.5	**9.6.5**	No changes	Have firewall rules that are no longer required been removed or disabled?	Explain the process of removal and be ready to demonstrate to an onsite assessment.	Yes	Have firewall rules that are no longer required been removed or disabled?	Explain the process of removal and be ready to demonstrate to an onsite assessment.							
	Yes/No	9.7.6	**9.6.6**	No changes	Do all of your desktop and laptop computers have personal firewalls (or equivalent) enabled and configured to block unapproved connections by default?	Provide details of how you have implemented this and describe the confirmation process.	Yes	Do all of your desktop and laptop computers have personal firewalls (or equivalent) enabled and configured to block unapproved connections by default?	Provide details of how you have implemented this and describe the confirmation process.							
The organisation can name its suppliers, the products and services they deliver and the contract durations	Document	10.1.1	**10.1.1**	No changes	The organisation has a list of its suppliers that handle personal information, the products and services they deliver, their contact details and the contract duration.	A list containing suppliers that handle personal information, systems/services and contract start and end dates.	Yes	The organisation has a list of its suppliers that handle personal information, the products and services they deliver, their contact details and the contract duration.	A list containing suppliers that handle personal information, systems/services and contract start and end dates.	Yes						
	Yes/No	10.1.2	**10.1.2**	No changes	Contracts with all third parties that handle personal information are compliant with ICO guidance.	A review of all contracts has been undertaken to ensure that they comply with the requirements set out in Article 28 of the GDPR. If you have no such suppliers, then 'tick' and write "Not applicable" in the comments box.		Contracts with all third parties that handle personal information are compliant with ICO guidance.	A review of all contracts has been undertaken to ensure that they comply with the requirements set out in Article 28 of the GDPR. If you have no such suppliers, then 'tick' and write "Not applicable" in the comments box.		Does your organisation have a list of its suppliers that handle personal information, the products and services they deliver, and their contact details?	Your organisation should have a list or lists of the external suppliers that handle personal information such as IT or care planning systems suppliers, IT support, accountancy, DBS checks, HR and payroll services, showing the system or services provided. If you have no such suppliers, then 'tick' and write "Not applicable" in the comments box. A template example is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/manage-your-suppliers/).	Yes	Does your organisation have a list of its suppliers that handle personal information, the products and services they deliver, and their contact details?	Your organisation should have a list or lists of the external suppliers that handle personal information such as IT or care planning systems suppliers, IT support, accountancy, DBS checks, HR and payroll services, showing the system or services provided. If you have no such suppliers, then 'tick' and write "Not applicable" in the comments box. A template example is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/manage-your-suppliers/).	Yes
Basic due diligence has been undertaken against each supplier that handles personal information	Yes/No	10.2.1	**10.2.1**	No changes	Your organisation ensures that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.	For more information see the [2017/18 Data Security Protection Requirements guidance](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/675420/17-18_statement_of_requirements_Branded_template_final_22_11_18-1.pdf).	Yes	Your organisation ensures that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.	For more information see the [2017/18 Data Security Protection Requirements guidance](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/675420/17-18_statement_of_requirements_Branded_template_final_22_11_18-1.pdf).	Yes	Do your organisation's IT system suppliers have cyber security certification?	Your organisation should ensure that any supplier of IT systems has cyber security certification. For example, external certification such as Cyber Essentials, or ISO27001, or by being listed on Digital marketplace, or by completing this Toolkit. An IT systems supplier would include suppliers of systems such as rostering, care planning or electronic medicine administration record (MAR) charts for example. If your organisation does not use any IT systems, then tick and write "Not applicable" in the comments box. Guidance is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/manage-your-suppliers/).	Yes	Do your organisation's IT system suppliers have cyber security certification?	Your organisation should ensure that any supplier of IT systems has cyber security certification. For example, external certification such as Cyber Essentials, or ISO27001, or by being listed on Digital marketplace, or by completing this Toolkit. An IT systems supplier would include suppliers of systems such as rostering, care planning or electronic medicine administration record (MAR) charts for example. If your organisation does not use any IT systems, then tick and write "Not applicable" in the comments box.	Yes
	Yes/No	10.2.2	**10.2.2**	Removed from cat 1 and 2							Contracts with all third parties that handle personal information are compliant with ICO guidance.	A review of all contracts has been undertaken to ensure that they comply with the requirements set out in Article 28 of the GDPR. If you have no such suppliers, then 'tick' and write "Not applicable" in the comments box.		Contracts with all third parties that handle personal information are compliant with ICO guidance.	A review of all contracts has been undertaken to ensure that they comply with the requirements set out in Article 28 of the GDPR. If you have no such suppliers, then 'tick' and write "Not applicable" in the comments box.	
	text	10.2.3	**10.2.3**	No changes	Percentage of suppliers with data security contract clauses in place.	The percentage snapshot of current suppliers handling personal data that currently have security clauses.		Percentage of suppliers with data security contract clauses in place.	The percentage snapshot of current suppliers handling personal data that currently have security clauses.							
	Yes/No	10.2.4	**10.2.4**	No changes	Where services are outsourced (for example by use of cloud infrastructure or services), the organisation understands and accurately records which security related responsibilities remain with the organisation and which are the supplier's responsibility.		Yes	Where services are outsourced (for example by use of cloud infrastructure or services), the organisation understands and accurately records which security related responsibilities remain with the organisation and which are the supplier's responsibility.		Yes						
	Yes/No	10.2.5	**10.2.5**	No changes	All suppliers that process or have access to health or care personal confidential information have completed a Data Security and Protection Toolkit, or equivalent.	Provide confirmation that all suppliers have successfully completed a Data Security and Protection Toolkit or the organisation has assured itself separately that they reach a similar or higher data security standard.		All suppliers that process or have access to health or care personal confidential information have completed a Data Security and Protection Toolkit, or equivalent.	Provide confirmation that all suppliers have successfully completed a Data Security and Protection Toolkit or the organisation has assured itself separately that they reach a similar or higher data security standard.		All Suppliers that process or have access to health or care personal confidential information have completed a Data Security and Protection Toolkit, or equivalent.	All suppliers have successfully completed a Data Security and Protection Toolkit or the organisation has assured itself separately that they reach a similar or higher data security standard.				

All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented	Document	10.3.1	**10.3.1**	No changes	List of data security incidents – past or present – with current suppliers who handle personal information.	All current ongoing incidents are listed and all historical incidents (up to 2 calendar rolling years). Redact any sensitive information.		List of data security incidents – past or present – with current suppliers who handle personal information.	All current ongoing incidents are listed and all historical incidents (up to 2 calendar rolling years). Redact any sensitive information.		List of data security incidents – past or present – with current suppliers who handle personal information.	All current ongoing incidents are listed and all historical incidents (up to 2 calendar rolling years). Redact any sensitive information.				
All instances where organisations cannot comply with the NDG Standards because of supplier-related issues are recorded and discussed at board	Text	10.4.1	**10.4.1**	No changes	List of instances of suppliers who handle health and care data not complying with National Data Guardian standards, with date discussed at board or equivalent level.	Where an organisation finds itself unable to comply with National Data Guardian standards and this is purely due to supplier related issues, these issues should be raised at the board.		List of instances of suppliers who handle health and care data not complying with National Data Guardian standards, with date discussed at board or equivalent level.	Where an organisation finds itself unable to comply with National Data Guardian standards and this is purely due to supplier related issues, these issues should be raised at the board.		List of instances of suppliers who handle health and care data not complying with National Data Guardian standards, with date discussed at board or equivalent level.	Where an organisation finds themselves unable to comply with National Data Guardian standards and this is purely due to supplier related issues, these issues should be raised at the board.				
The organisation understands and manages security risks to networks and information systems from your supply chain	Text	10.5.2	**10.5.1**	No changes	Where appropriate, you offer support to suppliers to resolve incidents.			Where appropriate, you offer support to suppliers to resolve incidents.								
		1.3.5	**N/A**	Removed												
		1.6.7	**N/A**	Removed												
		1.6.8	**N/A**	Removed												
		3.2.2	**N/A**	Removed												
		3.4.2	**N/A**	Removed												
		4.4.5	**N/A**	Removed												
		4.5.6	**N/A**	Removed												
		5.1.2	**N/A**	Removed												
		6.1.2	**N/A**	Removed												
		4.4.1	**N/A**	Removed												
		6.2.2	**N/A**	Removed												

Audit Strategy Memorandum

Bury Metropolitan Borough Council

Year ending 31 March 2021

mazars

Contents

mazars

Members of the Audit Committee
Bury Metropolitan Borough Council

Mazars LLP
One St Peter's Square
Manchester
M2 3DE

September 2021

Dear Audit Committee Members

Audit Strategy Memorandum – Year ending 31 March 2021

We are pleased to present our Audit Strategy Memorandum for Bury Metropolitan Borough Council for the year ending 31 March 2021. The purpose of this document is to summarise our audit approach, highlight significant audit risks and areas of key judgements and provide you with the details of our audit team. As it is a fundamental requirement that an auditor is, and is seen to be, independent of its clients, section 8 of this document also summarises our considerations and conclusions on our independence as auditors. We consider two-way communication with you to be key to a successful audit and important in:

- reaching a mutual understanding of the scope of the audit and the responsibilities of each of us;
- sharing information to assist each of us to fulfil our respective responsibilities;
- providing you with constructive observations arising from the audit process; and
- ensuring that we, as external auditors, gain an understanding of your attitude and views in respect of the internal and external operational, financial, compliance and other risks facing Bury Metropolitan Borough Council which may affect the audit, including the likelihood of those risks materialising and how they are monitored and managed.

With that in mind, we see this document, which has been prepared following our initial planning discussions with management, as being the basis for a discussion around our audit approach, any questions, concerns or input you may have on our approach or role as auditor. This document also contains an appendix that outlines our key communications with you during the course of the audit,

Client service is extremely important to us and we strive to provide technical excellence with the highest level of service quality, together with continuous improvement to exceed your expectations so, if you have any concerns or comments about this document or audit approach, please contact me on 07721 234 043.

Yours faithfully

Signed: {{_es_:signer1:signature }}

Karen Murray

Mazars LLP

01

Section 01:

Engagement and responsibilities summary

1. Engagement and responsibilities summary

Overview of engagement

We are appointed to perform the external audit of Bury Metropolitan Borough Council (the Council) for the year to 31 March 2021. The scope of our engagement is set out in the Statement of Responsibilities of Auditors and Audited Bodies, issued by Public Sector Audit Appointments Ltd (PSAA) available from the PSAA website: https://www.psaa.co.uk/managing-audit-quality/statement-of-responsibilities-of-auditors-and-audited-bodies/. Our responsibilities are principally derived from the Local Audit and Accountability Act 2014 (the 2014 Act) and the Code of Audit Practice issued by the National Audit Office (NAO), as outlined below.

Audit opinion

We are responsible for forming and expressing an opinion on the financial statements. Our audit does not relieve management or the members of the Audit Committee, as those charged with governance, of their responsibilities.

Going concern

The Council is required to prepare its financial statements on a going concern basis by the Code of Practice on Local Authority Accounting. The Chief Finance Officer is responsible for the assessment of whether is it appropriate for the Council to prepare it's accounts on a going concern. basis As auditors, we are required to obtain sufficient appropriate audit evidence regarding, and conclude on the appropriateness of the Chief Finance Officer's use of the going concern basis of accounting in the preparation of the financial statements and the adequacy of disclosures made.

Value for money

We are also responsible for forming a view on the arrangements that the Council has in place to secure economy, efficiency and effectiveness in its use of resources. We discuss our approach to Value for Money work further in section 5 of this report.

Fraud

The responsibility for safeguarding assets and for the prevention and detection of fraud, error and non-compliance with law or regulations rests with both those charged with governance and management. This includes establishing and maintaining internal controls over reliability of financial reporting.

As part of our audit procedures in relation to fraud we are required to enquire of those charged with governance, including key management and internal audit as to their knowledge of instances of fraud, the risk of fraud and their views on internal controls that mitigate the fraud risks. In accordance with International Standards on Auditing (UK), we plan and perform our audit so as to obtain reasonable assurance that the financial statements taken as a whole are free from material misstatement, whether caused by fraud or error. However our audit should not be relied upon to identify all such misstatements.

Reporting to the NAO

We report to the NAO on the consistency of the Council's financial statements with its Whole of Government Accounts (WGA) submission.

Electors' rights

The 2014 Act requires us to give an elector, or any representative of the elector, the opportunity to question us about the accounting records of the Council and consider any objection made to the accounts. We also have a broad range of reporting responsibilities and powers that are unique to the audit of local authorities in the United Kingdom

Section 02:

Your audit engagement team

2. Your audit engagement team

Your external audit service continues to be led by Karen Murray. A summary of key team members are detailed below:

Who	Role	E-mail
Karen Murray	Partner	karen.murray@mazars.co.uk
Amelia Payton	Manager	amelia.payton@mazars.co.uk

In addition an engagement quality control reviewer has been appointed for this engagement.

Section 03:

Audit scope, approach and timeline

3. Audit scope, approach and timeline

Audit scope

Our audit is designed to comply with all professional requirements.

Our audit of the financial statements will be conducted in accordance with International Standards on Auditing (UK), relevant ethical and professional standards, our own audit approach and in accordance with the terms of our engagement. Our work is focused on those aspects of your business which we consider to have a higher risk of material misstatement, such as those impacted by management judgement and estimation, application of new accounting standards, changes of accounting policy, changes to operations or areas which have been found to contain material errors in the past.

Audit approach

Our audit approach is risk based. It is primarily driven by the risks we consider could result in a higher risk of material misstatement of the financial statements. Once we have completed our risk assessment, we develop our audit strategy and design audit procedures in response to this assessment.

We plan to take a wholly substantive approach to our audit testing. Substantive procedures are audit procedures designed to detect material misstatements at the assertion level and comprise: tests of details (of classes of transactions, account balances, and disclosures); and substantive analytical procedures. Irrespective of the assessed risks of material misstatement, which take into account our evaluation of the operating effectiveness of controls, we are required to design and perform substantive procedures for each material class of transactions, account balance, and disclosure.

Our audit will be planned and performed so as to provide reasonable assurance that the financial statements are free from material misstatement and give a true and fair view. The concept of materiality and how we define a misstatement is explained in more detail in section 8.

The diagram on the next page outlines the procedures we perform at the different stages of the audit.

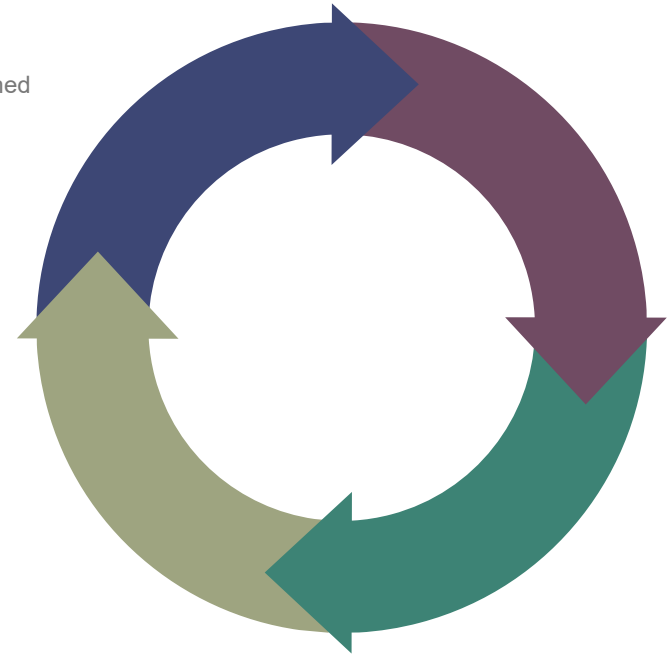
3. Audit scope, approach and timeline

Planning – April

- Initial opinion and value for money planning
- Considering proposed accounting treatments and accounting policies
- Initial risk assessment for opinion and risk assessment
- Developing the audit strategy and planning the audit work to be performed
- Preliminary analytical review
- Planning visit and developing our understanding of the Council

Interim – September

- Documenting systems and controls
- Performing walkthroughs
- Interim controls testing including tests of IT general controls



Completion – November

- Final review and disclosure checklist of financial statements
- Final partner review
- Agreeing content of letter of representation
- Reporting to the Audit Committee
- Reviewing subsequent events
- Signing the auditor's report

Fieldwork – October

- Receiving and reviewing draft financial statements
- Reassessment of audit plan and revision if necessary
- Executing the strategy starting with significant risks and high risk areas
- Communicating progress and issues
- Clearance meeting

3. Audit scope, approach and timeline

Management's and our experts

Management makes use of experts in specific areas when preparing the Council's financial statements.

We also use experts to assist us to obtain sufficient appropriate audit evidence on specific items of account.

Item of account	Management's expert	Our expert
Long Term Investments: Valuation of Share Holding in Manchester Airport Holdings Ltd	BDO	Mazars internal Valuations Team
Investment Property: Valuation of Manchester Airport Land	Jacobs	Mazars internal Valuations Team
Property, Plant & Equipment and Investment Property	Bury in-house valuation team and Align Property Partners	We will use available third party information to challenge the key valuations assumptions We will consider whether our internal valuations team will be required
Defined Benefit Liability	Hymans Robertson Actuaries	PwC (Consulting actuary on behalf of the National Audit Office)
Financial Instruments: Fair Value Disclosures	Link Asset Services	We will review the methodology used by the expert to gain assurance that the fair value disclosures are materially correct

3. Audit scope, approach and timeline

Group audit approach

The Council prepares Group accounts and consolidates the following bodies

- Six Town Housing Ltd
- Bury MBC Townside Fields Ltd
- The Persona group of companies (Persona Care and Support Ltd and Persona Group Ltd)

Mazars UK are the appointed auditor for the Council only. As such we are the appointed auditor for 94% of the Group's total expenditure and 88% of the Group's total net assets. We do not plan to obtain specific assurance from the component auditors of the Council's subsidiary companies, on the grounds of materiality.

The approach to the Group audit is set out below:

Entity	Auditor	Scope	Planned audit approach
Six Town Housing Ltd	RSM UK Audit LLP	Targeted procedures	We will: • complete analytical procedures on Six Town Housing Ltd's financial statements; • complete audit procedures over the LGPS pension liability in line with our group significant risk; and • review the consolidation process and adjustments made by the Council in preparing group financial statements.
Bury MBC Townside Fields Ltd	Horsfield & Smith	Targeted procedures	We will: • complete analytical procedures on Bury MBC Townside Fields Ltd's financial statements; • request third party confirmation of the company's bank balance; and • review the consolidation process and adjustments made by the Council in preparing group financial statements.
The Persona group of companies	Horsfield & Smith	Targeted procedures	We will: • complete analytical procedures on The Persona group of companies' financial statements; • complete audit procedures over the LGPS pension liability in line with our group significant risk; and • review the consolidation process and adjustments made by the Council in preparing group financial statements.

Section 04:

Significant risks and other key judgement areas

4. Significant risks and other key judgement areas

Following the risk assessment approach discussed in section 3 of this document, we have identified relevant risks to the audit of financial statements. The risks that we identify are categorised as significant, enhanced or standard. The definitions of the level of risk rating are given below:

Significant risk

A significant risk is an identified and assessed risk of material misstatement that, in the auditor's judgment, requires special audit consideration. For any significant risk, the auditor shall obtain an understanding of the entity's controls, including control activities relevant to that risk.

Enhanced risk

An enhanced risk is an area of higher assessed risk of material misstatement ('RMM') at audit assertion level other than a significant risk. Enhanced risks require additional consideration but does not rise to the level of a significant risk, these include but may not be limited to:

- key areas of management judgement, including accounting estimates which are material but are not considered to give rise to a significant risk of material misstatement; and
- other audit assertion risks arising from significant events or transactions that occurred during the period.

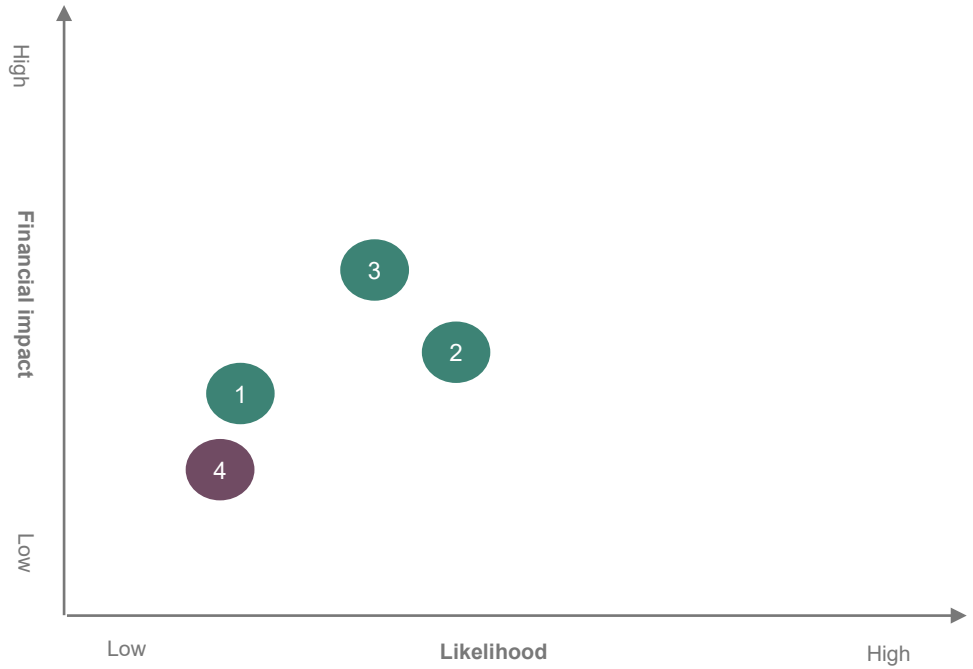
Standard risk

This is related to relatively routine, non-complex transactions that tend to be subject to systematic processing and require little management judgement. Although it is considered that there is a risk of material misstatement (RMM), there are no elevated or special factors related to the nature, the likely magnitude of the potential misstatements or the likelihood of the risk occurring.

4. Significant risks and other key judgement areas

Summary risk assessment

The summary risk assessment, illustrated in the table below, highlights those risks which we deem to be significant and other enhanced risks in respect of the Council. We have summarised our audit response to these risks on the next page.



1. Management override of controls
2. Net defined benefit liability valuation (Group)
3. Valuation of property, plant and equipment including investment properties
4. Valuation of Airport Shareholding

Key: Significant risk Enhanced risk / significant management judgement

4. Significant risks and other key judgement areas

Specific identified audit risks and planned testing strategy

We have presented below in more detail the reasons for the risk assessment highlighted above, and also our testing approach with respect to significant risks. An audit is a dynamic process, should we change our view of risk or approach to address the identified risks during the course of our audit, we will report this to the members of the Audit Committee.

Significant risks

	Description	Fraud	Error	Judgement	Planned response
1	**Management override of controls** This is a mandatory significant risk on all audits due to the unpredictable way in which such override could occur. Management at various levels within an organisation is in a unique position to perpetrate fraud because of the ability to manipulate accounting records and prepare fraudulent financial statements by overriding controls that otherwise appear to be operating effectively. Due to the unpredictable way in which such override could occur there is a risk of material misstatement due to fraud on all audits.	●	○	○	We plan to address the management override of controls risk through performing audit work over accounting estimates, journal entries and significant transactions outside the normal course of business or otherwise unusual.

4. Significant risks and other key judgement areas

Significant risks

	Description	Fraud	Error	Judgement	Planned response
2	**Net defined benefit liability valuation** The net pension liability represents a material element of the Council and the Group balance sheet. The Council and its consolidated subsidiaries are admitted bodies of Greater Manchester Pension Fund, which had its last triennial valuation completed as at 31 March 2019. The valuation of the Local Government Pension Scheme relies on a number of assumptions, most notably around the actuarial assumptions, and actuarial methodology which results in the Council's and the subsidiaries' overall valuations. There are financial assumptions and demographic assumptions used in the calculation of the valuation, such as the discount rate, inflation rates and mortality rates. The assumptions should also reflect the profile of the Council's and the subsidiaries' employees, and should be based on appropriate data. The basis of the assumptions is derived on a consistent basis year to year, or updated to reflect any changes. There is a risk that the assumptions and methodology used in valuing the pension obligations are not reasonable or appropriate to the Council's or the subsidiaries' circumstances. This could have a material impact to the Council and Group net pension liability in 2020/21	○	●	●	Our audit procedures will include: • Obtaining an understanding of the skills, experience and qualifications of the actuary, and considering the appropriateness of the instructions to the actuary from the Council. • Obtaining confirmation from the auditor of the Greater Manchester Pension Fund that the controls in place at the Pension Fund are free from material deficiencies. • Reviewing a summary of the work performed by the Pension Fund auditor on the Pension Fund investment assets, and evaluating whether the outcome of their work would affect our consideration of the Council's share of Pension Fund assets. • Reviewing the actuarial allocation of Pension Fund assets to the Council by the actuary, including comparing the Council's share of the assets to other corroborative information. • Reviewing the appropriateness of the Pension Asset and Liability valuation methodology applied by the Pension Fund Actuary, and the key assumptions included within the valuation. This includes comparing them to expected ranges, utilising information provided by PwC, consulting actuary engaged by the National Audit Office. • Agreeing the data in the IAS 19 valuation report provided by the Pension Fund Actuary for accounting purposes to the pension accounting entries and disclosures in the Council's and Group's financial statements.

4. Significant risks and other key judgement areas

Significant risks

	Description	Fraud	Error	Judgement	Planned response
3	**Valuation of property, plant and equipment including investment properties** The CIPFA Code requires that where assets are subject to revaluation, their year end carrying value should reflect the fair value at that date. The Council has adopted a rolling revaluation model which sees all land and buildings revalued in a five year cycle. The valuation of Property, Plant & Equipment involves the use of a management expert (the valuer), and incorporates assumptions and estimates which impact materially on the reported value. There are risks relating to the valuation process which reflect the significant impact of the valuation judgements and assumptions and the degree of estimation uncertainty. As a result of the rolling programme of revaluations, there is a risk that individual assets which have not been revalued for up to three years are not valued at their materially correct fair value. In addition, as the valuations are undertaken at the start of the year there is a risk that the fair value as the assets is materially different at the year end.	○	●	●	Our audit procedures will include: • Obtaining an understanding of the skills, experience and qualifications of the valuers, and considering the appropriateness of the Council's instructions to the valuers. • Obtaining an understanding of the basis of valuation applied by the valuers in the year. • Consider whether the overall revaluation methodology used by the Council's valuers is in line with industry practice, social housing statutory guidance, the CIPFA Code of Practice and the Council's accounting policies. • Obtaining an understanding of the Council's approach to ensure that assets not subject to revaluation in 2020/21 are materially fairly stated. • Obtaining an understanding of the Council's approach to ensure that assets revalued through 2020/21 are materially fairly stated at the year end. • Sample testing the completeness and accuracy of underlying data provided by the Council and used by the valuers as part of their valuations. • Comparing the valuation of the land at Manchester Airport to our internal valuation expert's estimate of the valuation. • Critically assess the appropriateness of the social housing factor applied to the valuation of the Council Dwellings. • Using relevant market and cost data to assess the reasonableness of the valuation as at 31 March 2021. • Testing the accuracy of how valuation movements were presented and disclosed in the financial statements. • Testing a sample of items of capital expenditure in 2020/21 to confirm that the additions are appropriately valued in the financial statements

4. Significant risks and other key judgement areas

Other key areas of management judgement and enhanced risks

	Description	Fraud	Error	Judgement	Planned response
4	**Valuation of Airport Shareholding** The Council's shareholding in the Manchester Airport Holdings Group Limited (MAHG Ltd.) has been valued by a firm of financial experts, engaged by management, based on assumptions about financial performance, stability, and key business projections. The figure disclosed in your accounts in relation to MAHG Ltd. is at fair value. There is a risk that the assumptions and methodology used by your experts are not appropriate and we will need to obtain assurance that accounting entries are not materially misstated.	○	●	●	We plan to address this risk by: • Assessing the scope of work/terms of engagement, qualifications, objectivity and independence of the expert engaged to carry out the valuation assessment of the airport shares. • Utilising the services of our internal valuation expert to review the work completed by management's expert and evaluate the appropriateness of the assumptions applied to arrive at the figure in the financial statements

Section 05:

Value for Money

5. Value for Money

The framework for Value for Money work

We are required to form a view as to whether the Council has made proper arrangements for securing economy, efficiency and effectiveness in its use of resources. The NAO issues guidance to auditors that underpins the work we are required to carry out in order to form our view, and sets out the overall criterion and sub-criteria that we are required to consider.

The new Code of Audit Practice (the Code) has changed the way in which we report our findings in relation to Value for Money (VFM) arrangements from 2020/21. Whilst we are still required to be satisfied that the Council has proper arrangements in place, we will now report by exception in our auditor's report where we have identified significant weakness in those arrangements. This is a significant change to the requirements under the previous Code which required us to give a conclusion on the Council's arrangements as part of our auditor's report.

Under the new Code, the key output of our work on VFM arrangements will be a commentary on those arrangements which will form part of the Auditor's Annual Report.

Specified reporting criteria

The Code requires us to structure our commentary to report under three specified criteria:

1. **Financial sustainability** – how the Council plans and manages its resources to ensure it can continue to deliver its services
2. **Governance** – how the Council ensures that it makes informed decisions and properly manages its risks
3. **Improving economy, efficiency and effectiveness** – how the Council uses information about its costs and performance to improve the way it manages and delivers its services

Our approach

Our work falls into three primary phases as outlined opposite. We need to gather sufficient evidence to support our commentary on the Council's arrangements and to identify and report on any significant weaknesses in arrangements. Where significant weaknesses are identified we are required to report these to the Council and make recommendations for improvement. Such recommendations can be made at any point during the audit cycle and we are not expected to wait until issuing our overall commentary to do so.

Planning and risk assessment	Obtaining an understanding of the Council's arrangements for each specified reporting criteria. Relevant information sources will include: • NAO guidance and supporting information • Information from internal and external sources including regulators • Knowledge from previous audits and other audit work undertaken in the year • Interviews and discussions with staff and members
Additional risk based procedures and evaluation	Where our planning work identifies risks of significant weaknesses, we will undertake additional procedures to determine whether there is a significant weakness.
Reporting	We will provide a summary of the work we have undertaken and our judgements against each of the specified reporting criteria as part of our commentary on arrangements. This will form part of the Auditor's Annual Report. Our commentary will also highlight: • Significant weaknesses identified and our recommendations for improvement • Emerging issues or other matters that do not represent significant weaknesses but still require attention from the Council.

5. Value for Money

Identified risks of significant weaknesses in arrangements

The NAO's guidance requires us to carry out work at the planning stage to understand the Council's arrangements and to identify risks that significant weaknesses in arrangements may exist.

We have not yet fully completed our planning and risk assessment work. We will report the results of our planning and risk assessment work to the Audit Committee as soon as they become apparent.

Section 06:

Fees for audit and other services

6. Fees for audit and other services

Fees for work as the Council's appointed auditor

Details of the proposed 2019/20 and 2020/21 fees are set out below:

Area of work	2020/21 Proposed Fee	2019/20 Proposed Fee
Scale audit fee	£89,882	£89,882
Fee variations:		
Additional Testing on Property, Plant & Equipment and Defined Benefit Pensions Schemes as a result of changes in regulatory expectations	£17,250 [1]	£17,250
Additional testing as a result of the implementation of new auditing standards: ISA 220 (Revised): Quality control of an audit of financial statements; ISA 540 (Revised): Auditing accounting estimates and related disclosures; ISA570 (Revised) Going Concern; and ISA 600 (Revised): Specific considerations – audit of group financial statements	£2,000 [2]	-
Other additional costs	TBC	£7,250 [3]
Sub-total	**£107,332**	**£114,322**
Additional work arising from the change in the Code of Audit Practice	Expected to be at least £10,000 (or 20% of the revised fee) [4]	-
Total	£107,332 [5]	£114,322(*)

[1] The scale fee has been adjusted to take into account the additional work required as a result of increased regulatory expectations in these areas.

[2] For 2020/21, new auditing standards have been introduced which will lead to additional audit work not reflected in the scale fee. The implementation of IFRS 16 Leases is deferred to the financial year 2021/22.

[3] This mainly relates to additional testing and reporting of uncertainties in key estimates as a result of Covid-19. This also includes additional work relating to the VFM issue in respect of governance issues.

[4] As explained in section 5, the revised Code of Audit Practice will lead to a substantial amount of additional audit work to support the new value for money conclusion and the changes in reporting requirements. Our review of the Code and supporting guidance notes shows that the additional fee impact at all public sector entities is expected to be at least £10,000 [or 20% of the post fee variation 2020/21 fee]. The final fee will take into account the extent and complexity of any significant weaknesses in arrangements we identify.

[5] This is a proposed fee for 2020/21 at the point of the issue of our ASM. This figure is subject to change and additional costs will be discussed with management.

*Final proposed fee for 2019/20 to be confirmed with PSAA.

PSAA have issued a consultation on the 2021/22 audit fee scale. We will revisit our fee proposal in line with the outcome of this consultation to ensure we are consistent with sector wide changes.

07

Section 07:

Our commitment to independence

7. Our commitment to independence

We are committed to independence and are required by the Financial Reporting Council to confirm to you at least annually in writing that we comply with the FRC's Ethical Standard. In addition, we communicate any matters or relationship which we believe may have a bearing on our independence or the objectivity of the audit team.

Based on the information provided by you and our own internal procedures to safeguard our independence as auditors, we confirm that in our professional judgement there are no relationships between us and any of our related or subsidiary entities, and you and your related entities creating any unacceptable threats to our independence within the regulatory or professional requirements governing us as your auditors.

We have policies and procedures in place which are designed to ensure that we carry out our work with integrity, objectivity and independence. These policies include:

- All partners and staff are required to complete an annual independence declaration;
- All new partners and staff are required to complete an independence confirmation and also complete computer based ethical training;
- Rotation policies covering audit engagement partners and other key members of the audit team; and
- Use by managers and partners of our client and engagement acceptance system which requires all non-audit services to be approved in advance by the audit engagement partner.

We confirm, as at the date of this document, that the engagement team and others in the firm as appropriate, Mazars LLP are independent and comply with relevant ethical requirements. However, if at any time you have concerns or questions about our integrity, objectivity or independence please discuss these with Karen Murray in the first instance.

Prior to the provision of any non-audit services Karen Murray will undertake appropriate procedures to consider and fully assess the impact that providing the service may have on our auditor independence.

No threats to our independence have been identified.

Any emerging independence threats and associated identified safeguards will be communicated in our Audit Completion Report.

08

Section 08:

Materiality and other misstatements

8. Materiality and misstatements

Summary of initial materiality thresholds

Threshold –	Council £'000s	Group £'000s
Overall materiality	10,900	10,950
Performance materiality	7,630	7,665
Specific materiality for Senior Officers Remuneration	5	N/a
Trivial threshold for errors to be reported to Audit Committee	327	329

Materiality

Materiality is an expression of the relative significance or importance of a particular matter in the context of financial statements as a whole.

Misstatements in financial statements are considered to be material if they, individually or in aggregate, could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements.

Judgements on materiality are made in light of surrounding circumstances and are affected by the size and nature of a misstatement, or a combination of both. Judgements about materiality are based on consideration of the common financial information needs of users as a group and not on specific individual users.

The assessment of what is material is a matter of professional judgement and is affected by our perception of the financial information needs of the users of the financial statements. In making our assessment we assume that users:

- Have a reasonable knowledge of business, economic activities and accounts;
- Have a willingness to study the information in the financial statements with reasonable diligence;
- Understand that financial statements are prepared, presented and audited to levels of materiality;
- Recognise the uncertainties inherent in the measurement of amounts based on the use of estimates, judgement and the consideration of future events; and
- Will make reasonable economic decisions on the basis of the information in the financial statements.

We consider materiality whilst planning and performing our audit based on quantitative and qualitative factors.

Whilst planning, we make judgements about the size of misstatements which we consider to be material and which provides a basis for determining the nature, timing and extent of risk assessment procedures, identifying and assessing the risk of material misstatement and determining the nature, timing and extent of further audit procedures.

The materiality determined at the planning stage does not necessarily establish an amount below which uncorrected misstatements, either individually or in aggregate, will be considered as immaterial.

We revise materiality for the financial statements as our audit progresses should we become aware of information that would have caused us to determine a different amount had we been aware of that information at the planning stage.

Our provisional materiality is set based on a benchmark of gross revenue expenditure. We will identify a figure for materiality but identify separate levels for procedures design to detect individual errors, and also a level above which all identified errors will be reported to Audit Committee.

We consider that gross revenue expenditure remains the key focus of users of the financial statements and, as such, we base our materiality levels around this benchmark.

8. Materiality and misstatements

Materiality (continued)

We expect to set a materiality threshold at 2% of gross revenue expenditure. Based on the 2020/21 unaudited group accounts gross revenue expenditure we anticipate the overall materiality for the year ending 31 March 2021 to be in the region of £10,950k for the Group and £10,900k on the Council (£11,900k in the prior year).

After setting initial materiality, we continue to monitor materiality throughout the audit to ensure that it is set at an appropriate level.

Performance Materiality

Performance materiality is the amount or amounts set by the auditor at less than materiality for the financial statements as a whole to reduce, to an appropriately low level, the probability that the aggregate of uncorrected and undetected misstatements exceeds materiality for the financial statements as a whole. Our initial assessment of performance materiality is based on low inherent risk, meaning that we have applied 70% of overall materiality as performance materiality.

Misstatements

We accumulate misstatements identified during the audit that are other than clearly trivial. We set a level of triviality for individual errors identified (a reporting threshold) for reporting to Audit Committee that is consistent with the level of triviality that we consider would not need to be accumulated because we expect that the accumulation of such amounts would not have a material effect on the financial statements. Based on our preliminary assessment of overall materiality, our proposed triviality threshold is £336k for the Group and £327k for the Council based on 3% of overall materiality. If you have any queries about this please do not hesitate to raise these with Karen Murray.

Reporting to the Audit Committee

The following three types of audit differences will be presented to the Audit Committee:

- summary of adjusted audit differences;
- summary of unadjusted audit differences; and
- summary of disclosure differences (adjusted and unadjusted).

Appendix: Key communication points

Appendix: Key communication points

We value communication with Those Charged With Governance as a two way feedback process at the heart of our client service commitment. ISA 260 (UK) 'Communication with Those Charged with Governance' and ISA 265 (UK) 'Communicating Deficiencies In Internal Control To Those Charged With Governance And Management' specifically require us to communicate a number of points with you.

Relevant points that need to be communicated with you at each stage of the audit are outlined below.

Form, timing and content of our communications

We will present the following reports:

- Our Audit Strategy Memorandum;
- Our Audit Completion Report; and
- Auditor's Annual Report

These documents will be discussed with management prior to being presented to yourselves and their comments will be incorporated as appropriate.

Key communication points at the planning stage as included in this Audit Strategy Memorandum

- Our responsibilities in relation to the audit of the financial statements;
- The planned scope and timing of the audit;
- Significant audit risks and areas of management judgement;
- Our commitment to independence;
- Responsibilities for preventing and detecting errors;
- Materiality and misstatements; and
- Fees for audit and other services.

Key communication points at the completion stage to be included in our Audit Completion Report

- Significant deficiencies in internal control;
- Significant findings from the audit;
- Significant matters discussed with management;
- Our conclusions on the significant audit risks and areas of management judgement;
- Summary of misstatements;
- Management representation letter;
- Our proposed draft audit report; and
- Independence.

Appendix: Key communication points

ISA (UK) 260 'Communication with Those Charged with Governance', ISA (UK) 265 'Communicating Deficiencies In Internal Control To Those Charged With Governance And Management' and other ISAs (UK) specifically require us to communicate the following:

Required communication	Where addressed
Our responsibilities in relation to the financial statement audit and those of management and those charged with governance.	Audit Strategy Memorandum
The planned scope and timing of the audit including any limitations, specifically including with respect to significant risks.	Audit Strategy Memorandum
With respect to misstatements: • Uncorrected misstatements and their effect on our audit opinion; • The effect of uncorrected misstatements related to prior periods; • A request that any uncorrected misstatement is corrected; and • In writing, corrected misstatements that are significant.	Audit Completion Report
With respect to fraud communications: • Enquiries of Audit Committee members to determine whether they have a knowledge of any actual, suspected or alleged fraud affecting the entity; • Any fraud that we have identified or information we have obtained that indicates that fraud may exist; and • A discussion of any other matters related to fraud.	Audit Completion Report and discussion at Audit Committee Audit Planning and Clearance meetings

Appendix: Key communication points

Required communication	Where addressed
Significant matters arising during the audit in connection with the entity's related parties including, when applicable: • Non-disclosure by management; • Inappropriate authorisation and approval of transactions; • Disagreement over disclosures; • Non-compliance with laws and regulations; and • Difficulty in identifying the party that ultimately controls the entity.	Audit Completion Report
Significant findings from the audit including: • Our view about the significant qualitative aspects of accounting practices including accounting policies, accounting estimates and financial statement disclosures; • Significant difficulties, if any, encountered during the audit; • Significant matters, if any, arising from the audit that were discussed with management or were the subject of correspondence with management; • Written representations that we are seeking; • Expected modifications to the audit report; and • Other matters, if any, significant to the oversight of the financial reporting process or otherwise identified in the course of the audit that we believe will be relevant to the Audit Committee in the context of fulfilling their responsibilities.	Audit Completion Report
Significant deficiencies in internal controls identified during the audit.	Audit Completion Report
Where relevant, any issues identified with respect to authority to obtain external confirmations or inability to obtain relevant and reliable audit evidence from other procedures.	Audit Completion Report

Appendix: Key communication points

Required communication	Where addressed
Audit findings regarding non-compliance with laws and regulations where the non-compliance is material and believed to be intentional (subject to compliance with legislation on tipping off) and enquiry of the Audit Committee into possible instances of non-compliance with laws and regulations that may have a material effect on the financial statements and that the Audit Committee may be aware of.	Audit Completion Report and Audit Committee meetings
With respect to going concern, events or conditions identified that may cast significant doubt on the entity's ability to continue as a going concern, including: • Whether the events or conditions constitute a material uncertainty; • Whether the use of the going concern assumption is appropriate in the preparation and presentation of the financial statements; and • The adequacy of related disclosures in the financial statements.	Audit Completion Report
Reporting on the valuation methods applied to the various items in the annual financial statements including any impact of changes of such methods	Audit Completion Report
Indication of whether all requested explanations and documents were provided by the entity	Audit Completion Report

Karen Murray

Partner

Mazars

One St. Peter’s Square

Manchester

M2 3DE

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of 40,400 professionals – 24,400 in Mazars’ integrated partnership and 16,000 via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*where permitted under applicable country laws.

This page is intentionally left blank

Agenda Item 7

Classification Open	Item No.

Meeting:	Audit Committee
Meeting date:	30th September 2021
Title of report:	Risk Register
Report by:	Sam Evans Executive Director of Finance
Decision Type:	Non Key
Ward(s) to which report relates	**All**

Executive Summary:

Risk Management is a key part of Bury Council's Code of Corporate Governance and underpins its system of internal control.

This report provides an update on the work progressed to date and demonstrates that efforts are ongoing to embed a culture of good risk management across the Council.

The Audit Committee are tasked with the responsibility of reviewing and scrutinising risks where the impact has the potential to disrupt achievement of the Council's Priorities. This report identifies those risks which are on departmental risk registers. Further work is required by the Executive team to produce a corporate risk register from not only those risks which are identified on individual departmental risk registers but also those of a genuine corporate nature. The corporate risk register will be brought to a future Audit Committee.

Recommendation(s)

That the Audit Committee:

- Note the update provided.
- Support the approach progressed to date to update the departmental risk registers into meaningful and dynamic documents.

- Support the approach that a further corporate risk register will be developed which will incorporate not only departmental risks but overarching organisational risks
- Review the Risk Matrix (in Appendix A) and the Risk Register in the main report.

Key Considerations

At the previous meeting of the Audit Committee, it was agreed that a refreshed approach to the identification, analysis and review of risk would be rolled-out across all departments in order to implement a cohesive, uniformed approach to the management of organisational risk.

The work progressed to date reflects progress on the embedding of good risk management practice as part of routine day-to-day delivery, however there is more work to be done to provide adequate assurance to the Audit Committee that risk remains dynamic within the Council.

1. Introduction

1.1. This report provides an updated position in respect to the management of risk review, analysis and reporting across departments of the Council.

1.2. The report presents the risk position and status as at **September 2021.**

2. Background

2.1. Over the last 2 years, the Council has reviewed its approach to Risk Management.

2.2. In late 2019, a revised Risk Management Strategy was introduced, which reinforced the use of a 5x5 matrix (see Appendix A) and provided some descriptors of risk to aid quantification of both impact and likelihood, however the advent of Covid-19 in March 2020 meant that the strategy was not fully rolled out.

2.3. In 2020, CIPFA were commissioned to create a Corporate Risk Register and also develop a simple framework that could be adopted across all departments for the capture, monitoring and management of departmental risks. This work has significantly progressed, with each directorate / department risk register collated into a single Master Risk Register.

2.4. At the Audit Committee in June 2021, it was agreed that some further work would be undertaken to collate and refresh the Council's risk registers and to support the embedding of risk as a core aspect of good strategic and operational management through a process of regular review and oversight.

2.5. The development of the risk management arrangements will also enable Bury Council to move from the self-assessed 'risk aware' organisation with a scattered, silo-based approach to risk management through standalone and reactive processes to one that

is inclusive, holistic and proactive. Not only will it enable corporate oversight, it also ensures review and scrutiny of the process, consistency in application and supports regular review, reporting and strengthening of risk management in practice.

2.6. All departmental risk registers have now been pulled into one Master repository, from which the "Red Risk" Register has been extracted.

2.7. The Red Risk Register, which is presented to Audit Committee for review and scrutiny, captures risks across the Council that have been assessed at a level of 15 or above.

2.8. Further work will be performed by the Executive Team to discuss and identify those risks that will eventually constitute the "Corporate Risk Register". The first iteration of this register will be presented to Audit Committee at the November meeting.

2.9. When reviewing the attached Red Risk Register, Audit Committee are requested to note that there is further specific work to be performed in providing guidance to Risk Owners, not limited to the definition of mitigating actions and inclusion of relevant dates, to enable timeframes to be considered in the analysis of organisational risk.

2.10. These issues will be addressed as a priority and evidenced in the forthcoming quarterly report to the Audit Committee.

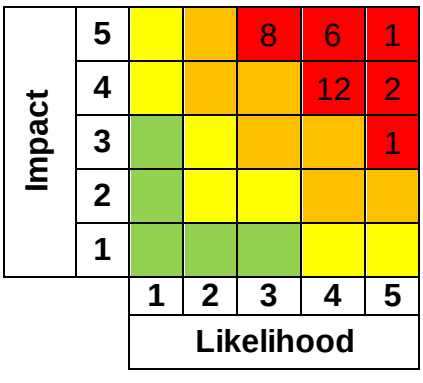
2.11. There are currently a total of 114 risks on the departmental risk register, of which 26% (30 risks) are included within the Red Risk Register, split across the departments of the Council as follows:

Department	No. Risks	Low (1-3)	Moderate (4-6)	High (8-12)	Significant (15-25)
BGI	26	2	8	14	2
CC	34	0	3	20	11
CYP	4	0	0	2	2
Finance	22	0	0	16	5
OCO	11	0	0	7	4
Operations	18	1	4	7	6
TOTAL	**114**	**3**	**15**	**66**	**30**

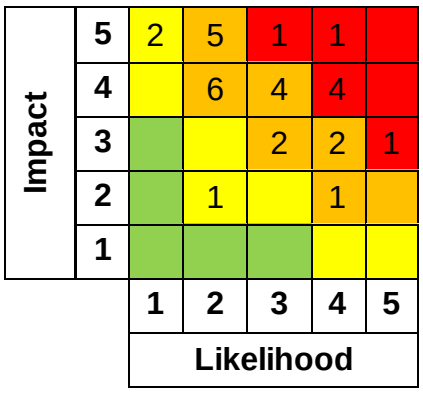
3. Red Risk Register

3.1 The following heat maps reflects the current and target risk profile in respect to those risks on the register:

Current



Target



3.2 All departments have been asked to review their risks and update accordingly, including the addition of a number of new fields. Further work is required in children's services following the peer review and we anticipate that the number of risks on the departmental register will increase following this piece of work.

3.3 The updated position is therefore presented as:

Risks that have remained static:

3.4 The following **21** risks have not seen any change in their assessed level at the last review:

- BGI/PAM/3 - Reduced revenue income to the Council due to COVID-19 – impacting on programme of rent reviews and lease renewals, and effects on businesses that lease our commercial portfolio
- CC/DS/1 - Failure to meet the requirements of data protection legislation and good information governance practice / serious data breach
- CC/HOUSING/1 - Failure to meet Homelessness Statutory Function & Delivery
- CC/HR/1 - Workforce capability and capacity is insufficient to deliver against the Council's ambitious priorities
- CC/HR/2 - The Council's Pay Structure and JE approach impacts on delivery
- CC/HR/3 - Inability of HR to provide robust advice and support
- CC/HR/4 - Opportunities for improvement and to assure compliance through the development of iTrent are not realised
- CC/IT/1 - Failure of infrastructure
- CC/IT/3 - Failure of Town Hall Data Centre
- CC/IT/4 - Failure to delivery new Digital Strategy
- CC/IT/5 - Cyber attack
- CC/1- Breach of health and safety legislation leading to prosecution under the Corporate Manslaughter Act and other Health and Safety Regulations
- CYP/1 – Ofsted Inspection
- CYP2 - Recruitment and retention of Social Workers and Managers (added as a new risk in May 2021, second risk assessment saw no change to the risk score)
- FIN/3 - Dedicated Schools Grant (DSG) Deficit increases significantly
- FIN/4 – Capital Schemes not delivered in line with programme
- FIN/5 Financial Resilience and Sustainability not achieved therefore Section 151 Officer compelled to issue a Section 114 Notice
- OCO/1 - Covid-19 Global Pandemic – Future waves and new variants
- OCO/4 – Health and Care Transformation
- OPS/1 - Continued provision of Leisure Services
- OPS/13 - Springwater Park landslip

New Risks:

3.5 The following **9** risks are reported as new, as they have not been included on previous departmental risk registers at the last review:

- BGI/SPED/1 - Failure to adopt an up to date statutory development plan
- OCO/2 Disruption to the health and care system caused by the Integrated Care System (ICS) and winter pressures leading to demands on the Adult Social Care budget
- OCO/3 Market failure of care providers and or risk of reduced workforce availability
- OPS/14 - Carbon Neutrality / Climate Agenda
- OPS/16 - Shortage of staff, particularly LGV Class II drivers required to drive RCVs, sweepers and tippers, also Vehicle Workshop staff from Manager to Mechanics. In addition, national shortage of HGV drivers because of Brexit impacting on waste collection and high market rate and also potential fuel disruption may impact on service deliver
- OPS/17 - Provision of Public Protection services
- OPS/18 - Impact on the taxi trade from the introduction of Minimum Licensing Standards
- Fin/1 Public sector spending cuts from the next Comprehensive Spending Review and then the Local Government Settlement
- Fin/2 Inflation

4.0 Next Steps

4.1 The work progressed to date reflects progress on the embedding of good risk management practice as part of routine day-to-day delivery, however there is more work to be done and therefore the audit Committee is advised that the following actions will be progressed so that risk remains dynamic:

- Additional information sharing and guidance sessions to be delivered to risk owners on a department by department basis, to support the full population of the risk register template;
- Consideration as to whether the domains review and potential re-basing of risks based on new descriptors should be completed at this time;
- Areas where information not yet captured to be updated as a priority;
- Risks due for review in October completed accordingly;
- Quality Assurance exercise to be undertaken on risks, actions and assessment to ensure register is complete and ‘tells the story’;
- Risk to be a standing item on department team meetings and Executive Team agenda (monthly);
- Corporate Risk Register extracted and presented to Audit Committee on quarterly basis from November 2021;
- Audit Committee to identify a number of risks for ‘deep dive’ analysis discussion at each meeting.

Community impact / Contribution to the Bury 2030 Strategy

Ensuring compliance with Financial Procedures and Policies

Equality Impact and considerations:

24. *Under section 149 of the Equality Act 2010, the 'general duty' on public authorities is set out as follows:*

    A public authority must, in the exercise of its functions, have due regard to the need to -

    (a) *eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act;*

    (b) *advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;*

    (c) *foster good relations between persons who share a relevant protected characteristic and persons who do not share it.*

25. *The public sector equality duty (specific duty) requires us to consider how we can positively contribute to the advancement of equality and good relations, and demonstrate that we are paying 'due regard' in our decision making in the design of policies and in the delivery of services*.

Assessment of Risk:

The following risks apply to the decision:

Risk / opportunity	Mitigation
• Failure to identify and own major risks that may prevent the Council from achieving one or more of its objectives. • Failure to ensure that the major risks are being managed.	• Review of risk management arrangements at Corporate level. • Review of the Council's risk management strategy and arrangements for the maintenance of risk registers. • Review the associated information management system and reporting arrangements.

Consultation:

N/A

Legal Implications:

The Council constitution sets out that the Audit Committee is responsible for providing assurance on the council's audit, governance (including risk management and information governance) and financial processes in accordance with the functions scheme.

Under the Account and Audit Regulations 2015, Authorities must undertake an effective internal audit to evaluate the effectiveness of their risk management, control and governance processes. Consideration must be given to the Public Internal Audit Standards (PIAS) and sector specific guidance.

Financial Implications:

Mitigating some of the risks may require financial resources and a number of risks are around organisational and services financial resilience and loss of income following the pandemic.

Report Author and Contact Details:

Sam Evans, Executive Director of Finance

sam.evans5@nhs.net

Glossary of terms, abbreviations and acronyms used in this report.

Term	Meaning
CPFA	Independent Consultancy
BGI	Business Growth and Infrastructure department
CC	Corporate Core department

CYP	Children and Young People's department
OCO	One Commissioning Organisation

Appendix A – Risk Matrix
Quantitative Measure of Risk – Impact / Consequence Score

	Impact / Consequence score (severity levels) and examples of descriptors				
	1	2	3	4	5
AT RISK	Very Low	Minor	Moderate	High	Severe
EXAMPLES : NEW POLITICAL ARRANGEMENTS, POLITICAL PERSONALITIES, POLITICAL MAKE-UP					
POLITICAL Associated with the failure to deliver either local or central government policy or meet the local administrations manifest commitment	The risk will result in a minor delay, inconvenience Can be managed no real impact upon service.	The risk will result in a minor loss, delay, inconvenience, interruption. Opportunity to innovate/make minor improvements missed. Short term effect.	The risk will result in a waste of time and resources. Good opportunity to innovate/improve missed. Moderate impact on efficiency, output, quality. Medium term effect which may be costly to recover from.	The risk will have a major impact on the achievement of ambitions/priorities, serious impact on costs, income, performance, reputation, substantial opportunities missed. Medium to long term effect and expensive to recover from	The risk will have a critical impact on the achievement of ambitions and priorities, huge impact on costs, income, performance, reputation, critical opportunities missed. Difficult to recover from and may require a long-term recovery plan/period.
EXAMPLES : COST OF LIVING, CHANGES IN INTEREST RATES, INFLATION, POVERTY INDICATORS					
ECONOMICAL Affecting the ability to meet financial commitments. These include budgetary pressures, the failure to purchase adequate insurance cover, external macro level economic changes or proposed investment decisions	The risk will result in a minor delay, inconvenience Can be managed no real impact upon service.	The risk will result in a minor loss, delay, inconvenience, interruption. Opportunity to innovate/make minor improvements missed. Short term effect.	The risk will result in a waste of time and resources. Good opportunity to innovate/improve missed. Moderate impact on efficiency, output, quality. Medium term effect which may be costly to recover from.	The risk will have a major impact on the achievement of ambitions/priorities, serious impact on costs, income, performance, reputation, substantial opportunities missed. Medium to long term effect and expensive to recover from	The risk will have a critical impact on the achievement of ambitions and priorities, huge impact on costs, income, performance, reputation, critical opportunities missed. Difficult to recover from and may require a long-term recovery plan/period.
EXAMPLES : STAFF LEVELS FROM AVAILABLE WORKFORCE, AGEING POPULATION, HEALTH STATISTICS					
SOCIAL Relating to the effects of changes in demographic, residential or social economic trends on council's ability to meet its objectives	The risk will result in a minor delay, inconvenience Can be managed no real impact upon service.	The risk will result in a minor loss, delay, inconvenience, interruption. Opportunity to innovate/make minor improvements missed. Short term effect.	The risk will result in a waste of time and resources. Good opportunity to innovate/improve missed. Moderate impact on efficiency, output, quality. Medium term effect which may be costly to recover from.	The risk will have a major impact on the achievement of ambitions/priorities, serious impact on costs, income, performance, reputation, substantial opportunities missed. Medium to long term effect and expensive to recover from	The risk will have a critical impact on the achievement of ambitions and priorities, huge impact on costs, income, performance, reputation, critical opportunities missed. Difficult to recover from and may require a long-term recovery plan/period.

	Impact / Consequence score (severity levels) and examples of descriptors				
	1	2	3	4	5
AT RISK	Very Low	Minor	Moderate	High	Severe
TECHNOLOGICAL Associated with the capacity of the Council to deal with the pace/scale of technological change, or its ability to use technology to address changing demands. May also include consequences of internal technological failures on the Council's ability to deliver its objectives	The risk will result in a minor delay, inconvenience Can be managed no real impact upon service.	The risk will result in a minor loss, delay, inconvenience, interruption. Opportunity to innovate/make minor improvements missed. Short term effect.	The risk will result in a waste of time and resources. Good opportunity to innovate/improve missed. Moderate impact on efficiency, output, quality. Medium term effect which may be costly to recover from.	The risk will have a major impact on the achievement of ambitions/priorities, serious impact on costs, income, performance, reputation, substantial opportunities missed. Medium to long term effect and expensive to recover from	The risk will have a critical impact on the achievement of ambitions and priorities, huge impact on costs, income, performance, reputation, critical opportunities missed. Difficult to recover from and may require a long-term recovery plan/period.
EXAMPLES : HUMAN RIGHTS, TUPE REGULATIONS, DATA PROTECTION					
LEGISLATIVE/LEGAL Associated with current or potential changes in national or European law	The risk will result in a minor delay, inconvenience Can be managed no real impact upon service.	The risk will result in a minor loss, delay, inconvenience, interruption. Opportunity to innovate/make minor improvements missed. Short term effect.	The risk will result in a waste of time and resources. Good opportunity to innovate/improve missed. Moderate impact on efficiency, output, quality. Medium term effect which may be costly to recover from.	The risk will have a major impact on the achievement of ambitions/priorities, serious impact on costs, income, performance, reputation, substantial opportunities missed. Medium to long term effect and expensive to recover from	The risk will have a critical impact on the achievement of ambitions and priorities, huge impact on costs, income, performance, reputation, critical opportunities missed. Difficult to recover from and may require a long-term recovery plan/period.
EXAMPLES : LAND USE, RECYCLING, POLLUTION, WASTE MANAGEMENT					

	Impact / Consequence score (severity levels) and examples of descriptors				
	1	2	3	4	5
AT RISK	Very Low	Minor	Moderate	High	Severe
ENVIOROMENTAL Relating to the environmental consequences of progressing the council's strategic objectives	The risk will result in a minor delay, inconvenience Can be managed no real impact upon service.	The risk will result in a minor loss, delay, inconvenience, interruption. Opportunity to innovate/make minor improvements missed. Short term effect.	The risk will result in a waste of time and resources. Good opportunity to innovate/improve missed. Moderate impact on efficiency, output, quality. Medium term effect which may be costly to recover from.	The risk will have a major impact on the achievement of ambitions/priorities, serious impact on costs, income, performance, reputation, substantial opportunities missed. Medium to long term effect and expensive to recover from	The risk will have a critical impact on the achievement of ambitions and priorities, huge impact on costs, income, performance, reputation, critical opportunities missed. Difficult to recover from and may require a long-term recovery plan/period.

	Impact / Consequence score (severity levels) and examples of descriptors				
	1	2	3	4	5
AT RISK	Very Low	Minor	Moderate	High	Severe
EXAMPLES : STAFF RESTRUCTURE, CAPACITY, TRAINING, WORKFORCE NEEDS					
PROFESSIONAL / MANAGERIAL Associated with the particular nature of each profession, internal protocols and managerial abilities	The risk will result in a minor delay, inconvenience Can be managed no real impact upon service.	The risk will result in a minor loss, delay, inconvenience, interruption. Opportunity to innovate/make minor improvements missed. Short term effect.	The risk will result in a waste of time and resources. Good opportunity to innovate/improve missed. Moderate impact on efficiency, output, quality. Medium term effect which may be costly to recover from.	The risk will have a major impact on the achievement of ambitions/priorities, serious impact on costs, income, performance, reputation, substantial opportunities missed. Medium to long term effect and expensive to recover from	The risk will have a critical impact on the achievement of ambitions and priorities, huge impact on costs, income, performance, reputation, critical opportunities missed. Difficult to recover from and may require a long-term recovery plan/period.
EXAMPLES : BUDGET OVERSPENDS, LEVEL OF COUNCIL TAX, LEVEL OF RESERVES					

	Impact / Consequence score (severity levels) and examples of descriptors				
	1	2	3	4	5
AT RISK	Very Low	Minor	Moderate	High	Severe
EXAMPLES : STAFF RESTRUCTURE, CAPACITY, TRAINING, WORKFORCE NEEDS					
FINANCIAL Associated with financial planning and control	Small Loss>£100 The risk will result in a minor delay, inconvenience Can be managed no real impact upon service.	Loss>£1,000 The risk will result in a minor loss, delay, inconvenience, interruption. Opportunity to innovate/make minor improvements missed. Short term effect.	Loss>£10,000 The risk will result in a waste of time and resources. Good opportunity to innovate/improve missed. Moderate impact on efficiency, output, quality. Medium term effect which may be costly to recover from.	Loss>£100,000 . The risk will have a major impact on the achievement of ambitions/priorities, serious impact on costs, income, performance, reputation, substantial opportunities missed. Medium to long term effect and expensive to recover from	Loss>£1,000,000 The risk will have a critical impact on the achievement of ambitions and priorities, huge impact on costs, income, performance, reputation, critical opportunities missed. Difficult to recover from and may require a long-term recovery plan/period.
EXAMPLES : SECURITY, ACCIDENTS, HEALTH & SAFETY, HAZARDS, FIRE					
PHYSICAL Related to fire, security, accident prevention and health and safety	The risk will result in a minor delay, inconvenience Can be managed no real impact upon service.	The risk will result in a minor loss, delay, inconvenience, interruption. Opportunity to innovate/make minor improvements missed. Short term effect.	The risk will result in a waste of time and resources. Good opportunity to innovate/improve missed. Moderate impact on efficiency, output, quality. Medium term effect which may be costly to recover from.	The risk will have a major impact on the achievement of ambitions/priorities, serious impact on costs, income, performance, reputation, substantial opportunities missed. Medium to long term effect and expensive to recover from	The risk will have a critical impact on the achievement of ambitions and priorities, huge impact on costs, income, performance, reputation, critical opportunities missed. Difficult to recover from and may require a long-term recovery plan/period.

	Impact / Consequence score (severity levels) and examples of descriptors				
	1	2	3	4	5
AT RISK	Very Low	Minor	Moderate	High	Severe
EXAMPLES : CONTRACTOR FAILS TO DELIVER, PARTNERSHIP AGENCIS WITH CONFLICTING GOALS					
PARTNERSHIP/CONTACTUAL Associated with failure of contractors and partnership arrangements to deliver services or products to the agreed costs and specification	The risk will result in a minor delay, inconvenience Can be managed no real impact upon service.	The risk will result in a minor loss, delay, inconvenience, interruption. Opportunity to innovate/make minor improvements missed. Short term effect.	The risk will result in a waste of time and resources. Good opportunity to innovate/improve missed. Moderate impact on efficiency, output, quality. Medium term effect which may be costly to recover from.	The risk will have a major impact on the achievement of ambitions/priorities, serious impact on costs, income, performance, reputation, substantial opportunities missed. Medium to long term effect and expensive to recover from	The risk will have a critical impact on the achievement of ambitions and priorities, huge impact on costs, income, performance, reputation, critical opportunities missed. Difficult to recover from and may require a long-term recovery plan/period.
EXAMPLES : STANDARDS NOT MET, ACCREDITATION,					
COMPETITIVE Affecting the competitiveness of the service (in terms of cost or quality) and /or its ability to deliver best value	The risk will result in a minor delay, inconvenience Can be managed no real impact upon service.	The risk will result in a minor loss, delay, inconvenience, interruption. Opportunity to innovate/make minor improvements missed. Short term effect.	The risk will result in a waste of time and resources. Good opportunity to innovate/improve missed. Moderate impact on efficiency, output, quality. Medium term effect which may be costly to recover from.	The risk will have a major impact on the achievement of ambitions/priorities, serious impact on costs, income, performance, reputation, substantial opportunities missed. Medium to long term effect and expensive to recover from	The risk will have a critical impact on the achievement of ambitions and priorities, huge impact on costs, income, performance, reputation, critical opportunities missed. Difficult to recover from and may require a long-term recovery plan/period.
EXAMPLES : MANAGING EXPECTATIONS, COMPLAINTS, CONSULTATION, COMMUNICATION EXTERNALLY					
CUSTOMER/CITIZEN Associated with failure to meet the current and changing needs and expectations of customers and citizens	The risk will result in a minor delay, inconvenience Can be managed no real impact upon service.	The risk will result in a minor loss, delay, inconvenience, interruption. Opportunity to innovate/make minor improvements missed. Short term effect.	The risk will result in a waste of time and resources. Good opportunity to innovate/improve missed. Moderate impact on efficiency, output, quality. Medium term effect which may be costly to recover from.	The risk will have a major impact on the achievement of ambitions/priorities, serious impact on costs, income, performance, reputation, substantial opportunities missed. Medium to long term effect and expensive to recover from	The risk will have a critical impact on the achievement of ambitions and priorities, huge impact on costs, income, performance, reputation, critical opportunities missed. Difficult to recover from and may require a long-term recovery plan/period.

Qualitative measure of risk – Likelihood Score

Descriptor	1	2	3	4	5

	Rare	Unlikely	Possible	Likely	Almost certain
Frequency Time framed descriptors	Not expected to occur for years	Expected to occur annually	Expected to occur monthly	Expected to occur weekly	Expected to occur daily
Frequency Broad descriptors	Will only occur in exceptional circumstances	Unlikely to occur	Reasonable chance of occurring	Likely to occur	More likely to occur than not occur
Probability	1-9% chance	10-24% chance	25-50% chance	51-80% chance	81% or higher

Quantification of the Risk – Risk Rating Matrix

			Likelihood				
			1	**2**	**3**	**4**	**5**
			Rare	**Unlikely**	**Possible**	**Likely**	**Almost certain**
Impact / Consequence	**5**	**Severe**	5	10	15	20	25
	4	**High**	4	8	12	16	20
	3	**Moderate**	3	6	9	12	15
	2	**Minor**	2	4	6	8	10
	1	**Very Low**	1	2	3	4	5

Bury Council

Key: Risk Register sorted by Department, Team, Risk No.

Risk Ref								No Controls Gross Score				With Current Current Score							Target score		
Department	Team	Risk No.	Risk Owner	Risk	Cause	Effect	Domain	Date Risk Identified	Likelihood	Impact	Total Score = L*I	Current Mitigating Controls	Likelihood	Impact	Total Score = L*I	Trend (change since last review)	Current Risk Review Date	Planned Risk Actions	Action Due Date	Action Owner	Likelihood	Impact	Total Score = L*I
BGI	PAM	3	LG	**Reduced revenue income to the Council due to COVID-19 –impacting on programme of rent reviews and lease renewals, and effects on businesses that lease our commercial portfolio**	• Covid-19 • Limited capacity caused by current levels of resources within the team and need to review previous outsourced arrangement to enable a robust programme to be in place	Reduced income to the Council and potentially increased void commercial Council-owned properties in some sectors	Finance	01/04/21	4	4	16	Current outsourcing of some rent reviews and lease renewals (but needs reviewing). Tenants have received rent free periods/grants where eligible for assistance from the Council but this was a one-off agreement by Cabinet during Covid	4	4	16	**Static**	17/08/21	Review of capacity and outsourcing arrangements, plus ongoing monitoring of income budgets with Finance	31/03/22	Liz Gudgeon	4	3	12
BGI	SPED	1	CL	**Failure to adopt an up to date statutory development plan**	Difficulty of getting an up to date plan in place due to legal challenges and difficulties in meeting requitrements of the National Planniong Policy Framework.	Don't get up to date planning policies to help determine planning applications and don't secure sufficent land for housing and employment needs (including the Northern Gateway)	Operational and legal compliance	01/04/21	4	5	20	Continuing to progress development plan through to examination	3	5	15	**New**	31/10/2021	Consider and respond to consultation submissions through the Examination process	31/12/21	Cris Logue	1	5	5
CC	DS	1	LR	**Failure to meet the requirements of data protection legislation and good information governance practice / serious data breach**	• Failure to follow GDPR provisions • Polices out of date/staff capability due to lack of training/lack of staff • Failure to follow Council's own data management policies • Negligent or unlawful use of data	• Judicial or ICO Review /challenge and/or fine inability to deliver leading to reputational damage and financial impact due to fine or compensation • Inability to deliver and further reputational damage			5	5	25	• GDPR and Data Management Policy • Document retention and disposal policy • DPO/IG Lead oversight of processes • DSPT 2020/21 submission • Policies • GDPR/Data Training & Development • Fair Use Notices	4	5	20	**Static**	08/01/2022	• IG strategy to be developed • IG processes to be mapped • IG resources to be identified • Internal Audit review subject to risk assessment • Comprehensive training programme to be implemented • IG policies and Procedures to be reviewed • DPST 2020/21 requirements to be assessed	Mar 2021 June 2021 June 2021 Aug 2021 Sept 2021 Sept 2021 Sept 2021	Marcus Connor	1	5	5
CC	HOUSING	1	PC	**Failure to meet Homelessness Statutory Function & Delivery**	• Increasing pressures on the service that impacts (reduces) capacity across the service • Increase in homelessness - stat and non stat provision • Lack of affordable permanent housing supply within local housing market	• Unable to meet statutory requirements as per Homelessness & HRA legislation • Legal challenge with potential judicial reviews resulting in increased legal costs and reputation damage	Homelessness & Housing Options	01/04/21	4	5	20	• Maximise funding opportunities to increase resources & capacity • Robust processes and operating procedures in place • Direct Let priority • System & IT solutions • Successful implementation of the re-structure with realignment of services • Increase in statutory dispersed accommodation • New homelessness strategy - Development of Private Rented Sector & Landlord engagement	3	5	15	**Static**	31/08/21	• Review structure of team / service • Framework of regular monitoring and KPI reviews to be developed • External funding opportunities to be maximised • Developing new tenancy sustainment strategy to prevent homelessness and reduce cases / demand	10/04/22	Phil Cole	2	5	10
CC	HR	1	SM	**Workforce capability and capacity is insufficient to deliver against the Council's ambitious priorities**	• Inadequate appraisal and talent management arrangements • Lack of workforce planning • Failure to invest in employee development • Work demands and priorities exceed available capacity. • Workforce fatigue	• Priorities not delivered leading to reputational, financial or legal challenge • Increased costs through reliance on external resources	Business Objectives / Projects	01/04/21	4	5	20	• Investment in additional capacity in key areas • Prioritisation through the Corporate Plan • Apprenticeship strategy	4	5	20	**Static**	16/09/21	• Continued focus on prioritisation • Training and development to be considered in new People Strategy	31/10/21	Director of People and Inclusion	2	4	8
CC	HR	2	SM (CS)	**The Council's Pay Structure and JE approach impacts on delivery**	• Outdated approach to JE • Complex process • Complex pay structure • Compression linked to Living Wage application	• Potential legal challenge • Service delivery impacts through staff satisfaction issues or time taken to conduct JE • Retention through lack of competitive salaries in some areas	Financial Balance / Claims	01/04/21	4	5	20	• More regular JE moderation panels being scheduled • Move to more generic roles where opportunities present themselves	4	5	20	**Static**	16/09/21	• Pay review	31/03/22	Director of People and Inclusion	2	5	10
CC	HR	3	SM (SB)	**Inability of HR to provide robust advice and support**	• Lack of capacity and capability in the service • Historic issues not addressed • Policies and processes not sufficient and over complex Poor service to school leads to issues in relationship or lack of compliance / legal challenge	• Legal challenge, financial and service delivery risk. (Key areas of risk include: occupational health duties, employment liabilities linked to uncontrolled agency and casual usage, poor advice to schools, timeliness of operational processes)	Operational and Legal Compliance	01/04/21	5	4	20	• Work to fill existing vacancies. • Policy review • Support to transactional team • Emphasis on service engagement	5	4	20	**Static**	16/09/21	• Development of HR pledge • Investment through Transformation Programme • Review of non-core activity	31/12/21	Head of HR	3	4	12
CC	HR	4	SM	**Opportunities for improvement and to assure compliance through the development of iTrent are not realised**	• Lack of investment and capability in systems improvement • Poorly managed contract • Lack of compliance oversight - Lack of management, development and processes in transactional HR team •Poor quality workforce data	• Opportunities are not realised leading to wider organisational impact. including inability to deliver savings or increase capacity • Legal challenge re:compliance	Information and Technology (Information Governance)	01/04/21	4	4	16	• iTrent programme with refreshed structure and leadership	4	4	16	**Static**	16/09/21	• Programme refresh, including review of capacity	31/08/21	Strategic HR Lead	3	4	12
CC	IT	1	KW	**Failure of infrastructure**	• Outdated systems • Hardware failure • Lack of availability of support or maintenance due to staffing shortages or products being out of licence / support contracts	• Loss of functionality and reduction in productivity • Impact on customer and user experience	Information and Technology	01/04/21	3	5	15	• Infrastructure replacement programme • Extended support purchase for older servers	3	5	15	**Static**	31/08/21	• Infrastructure replacement programme to be rolled out / completed • Migration to cloud storage / back-up	29/03/22	Kate Waterhouse	2	5	10
CC	IT	2	KW	**Failure of Town Hall Data Centre**	• External damage e.g. fire, flood, electric supply failure	• Potential data breach if records lost on permanent basis • Loss of productivity due to quality of connection to back-up data centre	Information and Technology	01/04/21	3	5	15	• Data management strategy in place re. backups; • Textile Hall back up data centre	3	5	15	**Static**	31/08/21	• Cloud migration plan to move data into Azure now in build phase • Review of options to relocate data centre scheduled for 22/23	29/03/22	Kate Waterhouse	2	5	10
CC	IT	3	KW	**Failure to deliver Digital Strategy**	• Lack of resources e.g. funding, staff or delivery partner (e.g. GMSS)	• Inability to achieve ambition for new ways of working and improved customer and staff experience • Inability to deliver data management and business intelligence model required for improved decision making and performance management		01/04/21	4	4	16	• Placement of Digital Strategy in Transformation programme to ensure visibility and deliverability • SLA with GMSS	4	4	16	**Static**	31/08/21	• Review of resources across Council and CCG IT/Digital functions • Additional resource approved within the Transformation Strategy		Kate Waterhouse	2	4	8

Key: Risk Register sorted by Department, Team, Risk No.

Risk Ref								No Controls Gross Score					With Current Current Score								Target score		
Department	Team	Risk No.	Risk Owner	Risk	Cause	Effect	Domain	Date Risk Identified	Likelihood	Impact	Total Score = L*I	Current Mitigating Controls	Likelihood	Impact	Total Score = L*I	Trend (change since last review)	Current Risk Review Date	Planned Risk Actions	Action Due Date	Action Owner	Likelihood	Impact	Total Score = L*I
CC	IT	4	KW	**Cyber attack**	• External threat to data and systems	• Potential loss of data resulting in significant data breach • Potential significant loss of functionality if systems were damaged or shut down	Information and Technology	01/04/21	3	5	**15**	• Training and updated Cyber Essentials Toolkit in place. • PCN accreditation renewed annually	3	5	**15**	**Static**	31/08/21	• Further training and investment in cyber security to be progressed against IG Action Plan timeframes • PSN accreditation of the Council • Cyber Essentials accreditation for Council and CCG to be achieved • New TOM to be developed for Council IT Team to include strengthened cyber security function, to be approved by Feb 2022	29/01/22	Kate Waterhouse	2	4	**8**
CC		1	GL	**Breach of health and safety legislation leading to prosecution under the Corporate Manslaughter Act and other Health and Safety Regulations**	• Failure to implement appropriate health & safety measures • Failure to manage effectively • Condition of the estate	• Senior officers held accountable and potentially imprisoned • Significant reputational damage. Financial redress		01/04/21	4	5	**20**	• Health & Safety Policies including arrangements for agile workers. • Investment in office repair work • Regular maintenance and inspection scheduling • Investment in corporate landlord • Covid-19 controls • Agile working • Transformation programme • Estates rationalisation Recruitment to Head of Corporate Landlord complete • Executive Budget Asset Holders Board established • Development, Approval & Investment into a 5 year Strategic Facilities Management Model • Require immediate temporary staff to support the ask in CL and BGI - Not approved at this time • Emergency repairs being undertaken as reported, judicious Preventative corrective action being taken on priority H&S outstanding works. • £1m spend on Town Hall works • Decision taken to close the Longfield Suite. Regular monitoring of the building as it remains empty. • Mandatory training for all staff on health and safety matters. • Employee assistance programme in place which incorporates mental wellbeing support	3	5	**15**	**Static**	08/01/2021	• Establishment of Corporate Landlord function to strengthen Facilities Management - review of health and safety teams and policy to maximise impact - strengthen TU role in managing health and safety responsibilities including TU Safety Reps & establishment of joint health and safety committee - corporate performance reports to be produced to report on health and safety incidents, accidents and resultant improvement actions • Regular maintenance and inspection scheduling	31/03/22	Geoff Little	3	5	**15**
CYP		1	IB	**Ofsted Inspection**	• A poor Ofsted judgement can lead to a high staff turnover from senior leaders through to frontline staff. Creating turmoil in an already struggling local authority, making it difficult to do what is most important - turning around services for children, young people and families in need	• DfE Intervention • Increased service demand • Financial pressure of up to £10m • Increased staff churn • Political risk and reputation of the council and region		21/05/2021	5	5	**25**	• CYP leadership • CYP improvement plan • Newly appointed Director of Education and Skills to start in May 2021	3	5	**15**	**Static**	21/05/2021	Independently chaired Delivery Board in place from September ; Delivery plan in place; LGA review given clear diagnostic; interim leadership in place with increased visibility in workforce			2	4	**8**
CYP		2	IB	**Recruitment and retention of Social Workers and Managers**	• High turnover of agency staff • Bury staff are attracted to other local authorities • Recruitment Marketing is not effective at attracting people to work for Bury • Lack of skills and capacity to create and implement a workforce strategy • Performance management culture not embedded in the council	• Too high caseloads that then effect lived experience of children • Too many changes of social worker that effect the lived experience of children • Capacity to monitor recruitment trends and successfully onboard new staff in a timely way risks losing staff before they start		21/05/2021	5	4	**20**	Work through HR to ensure vacancies are recruited to; project team in place to reduce case loads	4	4	**16**	**Static**	21/05/2021	Development of delivery plan focussed on recruitment and retention and reduction of caseloads.			2	4	**8**
FIN	Fin	1	SE	**Public sector spending cuts from the next Comprehensive Spending Review and then the Local Government Settlement**	Government tries to recover some of the expenditure incurred during the pandemic Limited funding is directed to the NHS recovery of planned care waiting lists impacting on funding for other government depts	In order to produce a balanced budget savings will need to be made to services thereby impacting on what can be delivered following years of already stringent reduced budgets	Finance	01/04/21	5	5	**25**	Early work with partners and across GM LAs with GMCA to model/ lobby and anticipate potential impacts and funding models Early work with Exec team and members to identify potential savings to close the financial gap Build into the MTFS the NI levy Rationalisation of admin buildings as part of transformation programme to reduce utilities expenditure	4	4	**16**	new	31/12/21	Continuous refinement of MTFS and budget setting as more information becomes available Continue to work through efficiencies with all departments	28/02/22	Sam Evans	4	3	**12**
FIN	Fin	2	SE	**Inflation**	Increased inflationary pressures as a consequence of Brexit, supply and demand pressures and as global economies recover from the pandemic	Resources need to be redirected to fund inflation with no beneficial impact on activity and deliverables	Finance	01/04/21	5	3	**15**	Early work with Exec team and members to identify potential savings to close the financial gap Rationalisation of admin buildings as part of transformation programme to reduce utilities expenditure	5	3	**15**	new	31/12/21	Continuous refinement of MTFS and budget setting as more information becomes available Continue to work through efficiencies with all departments	28/02/02	Sam Evans	4	2	**8**
FIN	Fin	3	SE	**Dedicated Schools Grant (DSG) Deficit increases significantly**	• Demand increases • Accountability and responsibility for funding not accurately specified • Lack of capacity / inclusion in local provision	• DfE warning and intervention • Budget reductions • High Cost out of borough placements	Finance and reputation	**01/04/21**	4	4	**16**	• Medium Term Financial Strategy updated • Monthly monitoring • DfE 'Safety Valve' deficit recovery agreement • Escalation to Executive Team and Members	4	4	**16**	**Static**	31/08/2021	• DfE Recovery Plan agreed • DfE engagement • Transformation plan priorities agreed with key stakeholders • Review of expenditure and rebaselining undertaken • Additional Capital funding secured for in-borough provision	on-going	Isobel Booler Sam Evans Steven Goodwin	2	2	**4**
OCO		1	GL	**Covid-19 Global Pandemic - Future Waves and new variants**	• Social Distancing and other preventative measures not used or not effective. • Increase in localised cases due to mass gatherings, new virus strains increase risk	• New lockdown measures, potentially localised • Support/response planning commenced for most vulnerable. Significant pressure on Public Health and NHS • Excess deaths			5	5	**25**	• Local Outbreak Plan • Partnership working with CCG, AGMA • Experience and planning for first outbreak and lockdown • Lessons learned evaluation • Regular liaison with Public Health England • Social Distancing including face covering guidance • Business Continuity Planning/Review/Update • Weekly Health Protection Board and fortnightly Gold meetings (assurance)	4	5	**20**	**Static**	08/01/2021	• Review current mitigating controls • Follow PHE guidance • Keep under review • Regular and prompt communication with staff and residents		Lesley Jones	2	4	**8**

Key: Risk Register sorted by Department, Team, Risk No.

Risk Ref									No Controls Gross Score				With Current Current Score								Target score		
Department	Team	Risk No.	Risk Owner	Risk	Cause	Effect	Domain	Date Risk Identified	Likelihood	Impact	Total Score = L*I	Current Mitigating Controls	Likelihood	Impact	Total Score = L*I	Trend (change since last review)	Current Risk Review Date	Planned Risk Actions	Action Due Date	Action Owner	Likelihood	Impact	Total Score = L*I
OCO		2	WB	**Disruption to the health and care system caused by the Integrated Care System (ICS) and winter pressures leading to demands on the Adult Social Care budget**	Significant change and disruption to NHS system architecture disrupts what is required at a locality level as staff are establishing new governance arrangements and relationships and pooled budgets created between the council and CCG need to be revised	Loss of focus on our continuing transformation journey of integration, person and community centred services, and focus on population health gain			4	5	**20**	1)Working with colleagues across the GM system to ensure the GM ICS operating model creates the conditions for our continued placed based transformation 2)Working with NCA footprint partners to continue to advocate for the place based approach 3)Building and starting to operate the new Bury health and care system partnership arrangements (including the Locality Board) to provide confidence and assurance of our arrangements	4	4	**16**	**New**					4	4	**16**
OCO		3	WB	**Market failure of care providers and or risk of reduced workforce availability**	Challenging circumstances for care providers, including availability and attractiveness of other jobs	Residential and care providers close or cease to take new residents resulting in increased pressures on the domiciliary market, the NHS and families Not enough home care packages to meet demand Carer breakdown due to increased pressures		01/04/21	5	5	**25**	Working closely with all providers of care to ensure early warning are in place Real living wage agreed and funded through contracts for all social care packages	4	5	16	**New**					4	4	**16**
OCO		**4**	WB	**Health and Care Transformation**	• Nature of COVID19 will impact the delivery of the recovery and transformation programmes	• Unreformed health and care services creating sub optimal outcomes and financially unsustainable services		05/10/20	5	5	**25**	• Response managed through Bury SILVER • Issues and risks escalated to Recovery and Transformation Board • Focus on quick wins during 2nd wave	5	5	**25**	**Static**	04/01/2021			Lesley Jones	3	3	**9**

Target Date	Next Risk Review Date
01/12/2023	ongoing
01/11/2021	Mar-22
31/10/2021	Oct-21
31/03/2022	Oct-21
31/12/2021	Oct-21
31/03/2022	Oct-21
31/03/2023	Nov-21
31/03/2023	Nov-21
31/03/2023	Nov-21

Target Date	Next Risk Review Date
31/03/2022	Nov-21
28/02/22	31/12/21
28/02/22	31/12/21
2024/25	Apr-22

Next Risk Review Date			
Target Date			

Briefing Note: Bury Council 2021/22 Covid Grants/Funding Support

Background

1. This briefing note largely focusses on financial year 2021/22[1] and provides a summary of the Covid funding support Bury Council has received.

1.1. Since the beginning of the Pandemic the Government has announced multiple funding streams in recognition of the ongoing Covid related pressures on councils. **Appendix A** summarises the £115.440m funding received in financial year 2020/21. A number of these allocations now require reconciliations and any unspent monies to be returned. These reconciliations are ongoing at this time

1.2. The position on grants and Covid support has continually changed and may continue to do so for the remainder of the current financial year.

1.3. The rest of this briefing note provides a summary of the 2021/22 covid funding and support received by Bury Council which can be broadly categorised into three areas,

I. Support for expenditure as a result of Covid-19
II. Support for income loss as a result of Covid-19
III. Covid-19 Support for Business

Support for Expenditure as a result of Covid-19

2. Local Authorities have received additional support for covid related expenditure enabling councils to fulfil a critical role during the pandemic including containing outbreaks, and testing and protecting the population from Covid-19.

2.1. Bury Councils **2021/22** support for Covid related expenditure is currently c.£12m. Appendix B provides a list of the current covid grant support and an explanation of what each grant is providing support for

Support for Income Loss as a result of Covid-19

3. The council submits a monthly return (Titled 'COVID-19 local authority financial management information) to the Ministry of Housing Communities and Local Government (MHCLG) detailing Income loss as a result of Covid-19. The income losses fall into two areas:

i. Council Tax, Business Rates, and non-collection fund items
ii. Revenue Budget income losses

3.1. Table 1 below summarises the current estimated losses (or gains) for Council Tax, Business Rates, and non-collection fund items as a result of Covid 19. After Business rate losses, council tax gains and non-Collection fund losses are factored in there is a net income loss of £0.764m. The figures in table 1 below are compared against the 2021/22 budgets which were adjusted for the impact of Covid based upon best estimates at the time.

Table 1

Description	2021/22 Loss/ (Gain) (£000)
Business Rates	773

[1] The section on support for business summarises the full support received across 2020/21 and 2021/22

Council Tax	(2,310)
Total Collection Fund	**(1,537)**
Non-Collection Fund	2,301
Total Income Losses (Gains)	**764**

3.2. Table 2 Summarises the forecast £11.534m Revenue Budget income losses relative to pre covid budget forecasts

Table 2

Income source	**2021/22 Loss (£000)**
Highways and Transport Sales, Fees & Charges losses	617
Cultural & Related Sales, Fees & Charges losses	1,134
Other	777
Sales, Fees & Charges (SFC) income losses total	**2,528,**
Commercial Income losses (dividends)	6,135
Commercial Income losses total	**6,135**
Non collection fund losses sub total	**8,663**

Covid-19 Support for Business

4. Over the period of the pandemic Local authorities have received and distributed funding to support small and medium sized businesses in England. To date £79.946m has been received by Bury Council to support businesses. Table 1 below summarises the amount of money that Bury council has received for the duration of the Pandemic (i.e., 2020/21 & 2021/22)

Table 3

Business Support Grants		**Total Allocation (£000)**
Restart Grant Scheme		9,282
Small Business Grant Fund (SBGF) & Retail, Hospitality and Leisure Business Grants Fund (RHLGF)		42,920
Pubs Grant		87
Local Authority Discretionary Grant Fund		1,957
Local Restrictions Support Grant[2]	Initial Allocations	10,762
	Additional Restrictions Grant[3]	1,383
Closed Business Lockdown		13,555
Total		**79,946**

[2] The LRSG is made up of multiple grants and eligibility is subject to government criteria

[3] The ARG is available for discretionary payments to business including those not eligible for the LRSG.

Appendix A – Analysis of Grants Received in 2020/21 as a result of Covid -19

Analysis of Grants Received 2020/21 as a result of COVID -19			
Description	**Amount (£m)**	**Additional Information**	**Additional Notes**
Business Rates Grants	42.920	Grant payments of £10k and £25k to eligible business and funding for a discretionary scheme.	The scheme is now closed.
Local Restrictions Support Grant Closed (Addendum & Sector)	8.358	Funding to support businesses legally required to close during a national lockdown and those legally closed since March (e.g., nightclubs).	New Allocation received January 2021
Local Restrictions Support Grant (Closed)	0.376	Funding to support businesses in Tier 3 and 4 areas legally required to close.	
Local Restrictions Support Grant (Open)	1.653	Funding to support businesses that remain open but who are severely impacted by the restrictions.	
Christmas Support Payment – Wet-pubs	0.083	Funding to support wet-led pubs where tier 3 restrictions imposed	
National Lockdown Top-Up Grant Jan-Feb 2021	9.036	One-off top-up grant for retail, hospitality and leisure businesses closed in national lockdown Jan-Feb 2021	
Additional Restrictions Grant (ARG)	5.738	One-off funding of approx. £20/head of population for business support activities, primarily in the form of discretionary grants during restrictions in November and January.	Top Up received January 2021.
New Burdens (Revenues and benefits) for the administration of the business rates grants.	0.170	New costs to support the administration of grants to businesses and increase in welfare and benefit claimants.	Decision made and funding used to increase capacity in the revenues and benefits team.
New Burdens – Administration of Retail, Leisure and Hospitality Grants	0.076	New costs to support the administration of grants to businesses and increase in welfare	Top Up Received January 2021

		and benefit claimants.	
Local Restrictions Support Grant (RSG) allocation 16 February – 31 March	4.735		
Sub Total	**73.145**		

Analysis of Grants Received 2020/21 as a result of COVID -19			
Description	**Amount (£m)**	**Additional Information**	**Additional Notes**
Sales Fees & Charges compensation scheme 1st round	4.897	No additional costs. This grant is un-ringfenced and is available to support the Council to meet additional costs and loss of income as a result of COVID-19.	
Sub Total	**1.912**	**Additional Information**	**Additional Notes**
COVID–19 Tranche 1	5.364	un-ringfenced grant and is available to support the Council to meet additional costs and loss of income as a result of COVID-19.	
COVID-19 Tranche 2	5.253		
COVID-19 Tranche 3	1.699		
COVID-19 Tranche 4	3.324		
Sub Total	**15.640**	**Additional Information**	**Additional Notes**
Hardship Relief Fund	1.880	Criteria on how this should be allocated was provided by government. Majority to be used to fund £150 credit on council tax bills to working age residents eligible for local council tax support scheme. Remainder allocated to hardship and welfare schemes.	Currently held within the Collection Fund as most of the costs will be incurred within the fund.
DEFRA Food and Essentials Hardship Grant	0.229	Allocated to wider food offer to support vulnerable people and FSM provision at October half term, and to support those	

		suffering from hardship as a result of self-isolation. Working with Bury Community Support Network to identify vulnerable group and to target support.	

Analysis of Grants Received 2020/21 as a result of COVID -19			
Description	**Amount (£m)**	**Additional Information**	**Additional Notes**
Self-Isolation Grant	0.171	Grant payments to eligible claimants who are self-isolating	Government Criteria
Self-Isolation Grant Top Up	0.124		Received January 2021
Next Steps Accommodation Programme	0.081		
COVID Winter Grant scheme	0.619	To support families/vulnerable households particularly with food, energy, and water bills to the end of March. Was utilised to fund free school meals since Christmas holidays and for the remainder of the financial year.	
Sub Total	**3.104**	**Additional Information**	**Additional Notes**
Re-Opening High Streets	0.169	Grant offset fully by new additional costs.	This grant will be paid in arrears on qualifying expenditure.
Sub Total	**0.169**	**Additional Information**	**Additional Notes**
Infection Control Tranche 1	2.396	Monitoring assumes that the grant will be offset fully by new additional costs.	All of the grant received has been allocated to care home and other organisations as specified in the grant criteria.

Infection Control Tranche 2	1.934	Monitoring assumes that the grant will be offset fully by new additional costs.	All of the grant received has been allocated to care home and other organisations as specified in the grant criteria.
Sub Total	**4.330**		

Analysis of Grants Received 2020/21 as a result of COVID -19			
Description	**Amount (£m)**	**Additional Information**	**Additional Notes**
Test and Trace	1.080	Monitoring assumes that the grant will be offset fully by new additional costs.	Additional costs will be reflected within the OCO department
Test and Trace Enhanced Support	0.150	Monitoring assumes that new costs will be incurred. Focus on communications and approval for additional support obtained.	Report approved.
COVID Marshall Funding	0.104	Monitoring assumes that new costs will be incurred.	Report approved via Emergency Powers Group.
Test, Track & Contain grant	1.528	Allocation of resource has been submitted to MHCLG.	Additional costs will be reflected within the OCO department.
Clinically Extremely Vulnerable (CEV) funding	0.142	Monitoring assumes that the grant will be offset fully by new additional costs.	Additional costs will be reflected within the OCO department
Contain Outbreak Management Fund	0.764	Monitoring assumes that the grant will be offset fully by new additional costs.	Funding received for December 2020
Contain Outbreak Management Fund	0.764	Monitoring assumes that the grant will be offset fully by new additional costs.	Funding received for January 2021

Contain and Outbreak Management	0.764	Monitoring assumes that the grant will be offset fully by new additional costs	Funding received for February 2021
Workforce Capacity Fund	0.408	80% allocated to care homes. 20% discretionary.	EPG decision February 2021
Adult Social Care Rapid Testing Fund	0.592	80% allocated to care homes. 20% discretionary.	EPG decision February 2021
Community Champions Fund	0.467		EPG decision February 2021
Clinically Extremely Vulnerable	0.162	Monitoring assumes that the grant will be offset fully by new additional costs	
Sub Total	**6.925**		

Analysis of Grants Received 2020/21 as a result of COVID -19			
Description	**Amount (£m)**	**Additional Information**	**Additional Notes**
Wellbeing for Education Grant	0.030	Allocated to Schools	Non-ringfenced grant to better equip education settings to support wellbeing and psychological recovery as they return to full time education.
Covid catch-Up Premium	2.367	Allocated to Schools	Additional funding to help children catch up on lost learning and reach expected curriculum levels during the 2020/21 academic year. It should be noted that £0.875m of the funding was received by the council to be passported to academies. Funding will be received in 3 tranches (Autumn, Spring and Summer terms).
Covid Exceptional Cost Re- Imbursement Scheme	2.645	Allocated to Schools	Reimbursement scheme to allow schools to reclaim any exceptional costs incurred during lockdown from March – July 2020 in relation to premises, cleaning and free

			school meals plus other costs that are subject to DfE scrutiny and validation. Of the funding allocated £0.660m is for academies.
Holiday Activities and Food Programme 2020/21	0.073	Allocated to Schools	To be used for FSM and activity over Easter
Hospital Discharge Programme	5.100	Allocated Adult Social care Budgets	To facilitate the rapid transfer from hospital beds funding made available to support the cost of the first 6 weeks of community care
Sub Total	**10.215**		
TOTAL	**118.425**		

Appendix B - Support for expenditure as a result of Covid

Title		Description	Full Year Cost (£)
Covid 19 Funding for Adult Social Care	**Hospital Discharge Programme**	Relates to enhance the NHS discharge process so patients who no longer need urgent treatment can return home safely and quickly. Agreement with Bury CCG is as follows: **Qtr 1(April - June)** - Council able to Recharge DHSC funding pot for the first 6 weeks of Care Package Costs **Qtr 2 (July -September)** Council Can Recharge the DHSC funding for the first 4 weeks of Care Package Costs **Qtr3 &Qtr 4 (October-March)** Council Can Recharge the DHSC funding for the first 4 weeks of Care Package Costs	**2,200,000**
	Infection Control	To distribute the fund in accordance with the grant conditions to continue to reduce the rate of transmission of Covid-19 within and between care settings through effective infection prevention and control practices and increase the uptake of staff vaccination	**732,510**
	Infection Control - Extension		**513,130**
	Rapid testing	Funding to support additional rapid testing of staff in care homes, and to support visiting professionals and enable indoors, close contact visiting where possible.	**472,426**
	Rapid testing - Extension		**383,970**
Other Government Funding For Local Authorities	**DWP Covid Winter Grant Scheme 2021-22 (extension / top-up)**	Additional funding to support those most in need with the cost of food, energy, water and other essentials.	**582,982**
	Welcome Back Fund (formerly Reopeing high streets Fund)	The Welcome Back Fund is providing councils across England a share of £56 million from the European Regional Development Fund (ERDF) to support the safe return to high streets and help build back better from the pandemic.	**170,000**
	Covid 19 Unringfenced Funding	Emergency funding for Local Governement in 21/22 announced in Decmber 2020. £1.55bn unringfrenced funding for Local authorities to use to respond to the Covid 19 pandemic	**5,330,086**
	Additional Funding for Local Elections	£15m grant alloacted across local authorities to cover the additional costs of the local elections in England (i.e ensuring polls are covid secure)	**97,639**
Containment Outbreak Management Fund (COMF)	**Containment Outbreak Management Fund**	The Fund is ring-fenced for public health purposes to tackle COVID-19, working to break the chain of transmission and protecting the most vulnerable. Whilst the specific public health activities that can be funded are subject to local decision making a list of activities that this funding could be used for is included in the general Contain Outbreak Management Fund policy letter of 1 December 2020.	**1,375,000**
Total			**11,857,743**

This page is intentionally left blank

Agenda Item 9

Classification Open	Item No.

Meeting:	Audit Committee
Meeting date:	30th September 2021
Title of report:	Internal Audit Progress Report – 1st April 2021 to 10th September 2021
Report by:	Acting Head of Internal Audit
Decision Type:	Council
Ward(s) to which report relates	**All**

Executive Summary:

This report sets out the progress to date against the annual audit plan 2021/22. The report enables Members to monitor the work of the Internal Audit service, raise any issues for further consideration and also provide an opportunity to request further information or to suggest areas for additional or follow up work.

The conclusions drawn from the report are:

- The majority of work outstanding from the 2020/21 plan has now been completed and work on 2021/22 plan is progressing. Ten reports have been issued to Members since the beginning of the financial year.
- One report with a Limited assurance has been issued to date. This report will need to be considered within the Annual Governance Statement produced at the end of the financial year 2021/22.
- In response to the impact of COVID 19 and the positive response for the requirement from Internal Audit to support other priority services, the level of audit coverage for the remainder of 2021/22 may need to be reviewed.
- A team member has been supported to commence professional accountancy studies, an element of this support requires providing time in the working week for study and to gain work experience, this may also require an adjustment to the planned audit coverage.

Recommendation(s)

That:

- Members note this report and the work undertaken by Internal Audit;

Key Considerations

1. Background

1.1 This report outlines the work undertaken by Internal Audit between 1st April 2021 to 10th September 2021.

1.2 Management is responsible for establishing and maintaining appropriate risk management processes, control systems, accounting records and governance arrangements i.e. the control environment. Internal Audit plays a vital role in reviewing whether these arrangements are in place and operating properly and providing advice to managers. On behalf of the Council, Internal Audit review, appraise and report on the efficiency, effectiveness and economy of these arrangements and provide assurance to the organisation (Chief Executive, Executive Directors and the Audit Committee) and ultimately the taxpayers, that the Council maintains an effective control environment that enables it to significantly manage its business risks. The service helps the Council achieve its objectives and provides assurance that effective and efficient operations are maintained.

1.3 The assurance work culminates in an annual opinion given by the Head of Internal Audit on the adequacy of the Council's control environment, based on the work undertaken, and this opinion feeds into the Annual Governance Statement.

1.4 The Internal Audit Plan for 2021/22 provides for 806 days to be delivered throughout the 2021/22 year across all Council Departments, and group companies i.e. Six Town Housing and Persona. The Audit plan covers a range of themes.

1.5 The 2021/22 plan was not approved by Audit Committee at the meeting on 21 July 2021 as Committee requested sight of the Council risk register, so they have the opportunity to be assured that items within the annual plan, do address some of the risks on the register, and also to give the Committee the opportunity to request for specific pieces of work to be included in the annual audit plan.

1.6 Work has been continuing throughout the year to date, addressing audits in the original 2021/22 plan. Regular progress reports are produced, informing Members of audit activities, and this is the first report of the 2021/22 financial year covering the period from 1st April 2021 to 10th September 2021 which includes 24 completed weeks.

2.0 ISSUES

2.1 Annual Audit Plan

2.1.1 The annual plan for 2021/22 was presented to Audit Committee in July 2021 and provided for 806 audit days to be delivered throughout the year. The plan was not approved as Committee requested sight of the risk register, to be assured that the audit plan focussed on risks faced by the Council, and also to give the Committee opportunity to request specific pieces of work to be included in the annual plan.

The original plan is shown at appendix 1.

Since the plan was produced specific requests for work have been received from Departments and these are:-

Childrens Services

- Recruitment of staff within schools
- Recruitment of School Governors

A revised plan will be brought to November committee, reflecting any changes from the risk register, Committee requests, Departmental requests, and adjustments required for staffing issues which are referred to later in this report.

2.2 Audit Plan Progress

This report details the outcome of reviews undertaken, including work reported to Audit Committee in this period, work currently ongoing and draft reports which have been issued to Aduit clients.

Audits completed and Reports Issued.

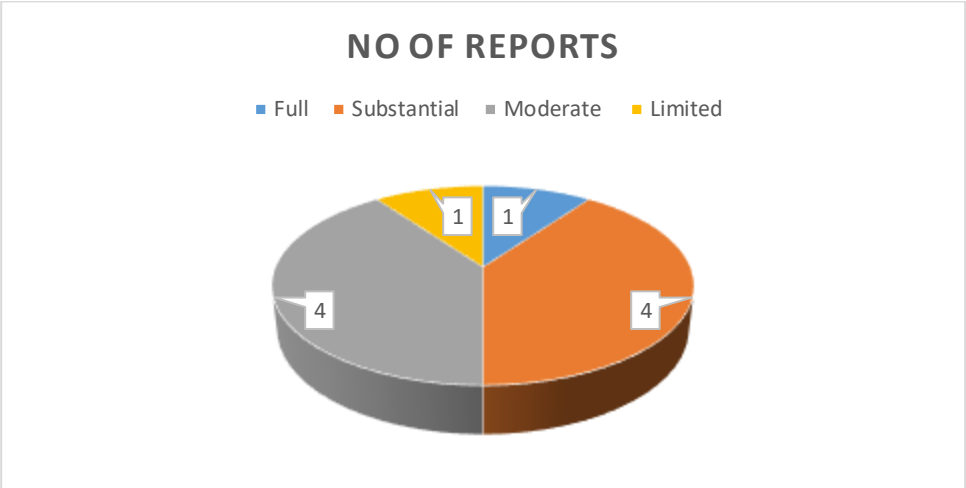
2.2.1 Table 1 below summarises the 10 audits that have been finalised and issued since the last progress report to Audit Committee in March 2021, and the corresponding number of agreed actions and overall level of assurance provided for each of those audits. All of these relate to audits included within the 2020/21 audit plan but finalised since 31st March 2021.

Full reports have been provided to Committee Members for each of these reviews. Summary reports detailing the overall opinion, the findings, recommendations and action plans of these reviews, are also presented in part B of the Audit Committee meeting. The summary reports are exempt from publication as they may contain information which is likely to reveal the identity of an individual or information relating to the financial or business affairs of any particular person (including the Authority).

Table 1: Final Reports Issued

Audit	Number of agreed actions and priority				Level of Assurance
	Fundamental	Signifciant	Merits Attention	Total	
GDPR	0	15	9	24	Moderate
Budget Setting and Monitoring in Schools	0	2	0	2	Substantial
Purchase Cards	0	4	8	12	Moderate
Car Allowances	0	6	5	11	Moderate
Adoption Services	0	2	0	2	Substantial
Six Town Housing - Treasury Management	0	1	2	3	Substantial
Integrated Community equipment Store (ICES)	3	10	9	22	Limited
Members Allowances	0	3	1	4	Moderate
Pupil Premium Grant	0	0	2	2	Full
Pooled Budget	0	1	0	1	Substantial
Total	3	44	36	83	

Number of assurance levels given in Final Audit reports.



2.2.2 Any level of assurance given to each audit is a balanced judgement based upon the established system of controls, the subject's approach to risk management and the nature of any recommendations and actions agreed. (See appendix for explanations of the different levels of assurance).

Actions are classified over the categories of Fundamental, Significant and Merits Attention. See appendix for explanations of the different levels of priority.

2.2.3 The agreed actions are designed to improve the control environment and / or improve "value for money" within the client's area of responsibility and we can report that the actions made in this period have been agreed by management.

Our audit reports include an action plan that records the detail of our findings, the agreed action that management intend to take in response to these findings and the timescale to undertake such action. This provides a record that progress can be measured against when we undertake our Post Implementation Reviews or follow up work.

2.3 Other work

This section details other work completed by the audit team during the period.

2.3.1 Assurance work - Ongoing reviews

There are some audits still being finalised from the 2020/21 plan and work has also commenced to deliver the audits detailed in the audit plan for 2021/22. It is expected that draft reports will have been issued for these areas before the next Audit Committee meets in November 2021. Audits which are currently taking place are:-

<u>2020/21</u>

- Six Town Housing Disabled Facilities Adaptations
- Estates Property Management
- Members Delegated Funds

2021/22

- Cash and Bank Key Controls
- Creditors Key Controls
- Payroll Key Controls
- Main Accounting Key Controls
- Council Tax Key Controls
- Treasury Management Key Controls
- Six Town Housing Rents Key Controls
- Housing Development Program
- Complaints (Childrens Services)
- GM Supporting Families (TFG)Troubled Families
- Residential Payments
- Petty Cash – Choices for Well Living Team
- Leisure Services – Income Review
- Six Town Housing Electrical Safety
- Six Town Housing Arrears Prevention
- Six Town Housing -Fire Safety

2.3.2 Assurance work – Draft reports

Draft reports have been issued to Audit clients and it is expected that final reports will be issued to Audit Committee Members before the next meeting of the Committee in November 2021. Draft reports have been issued for the following areas:-

2020/21

- Corporate Health and Safety
- Operations Procurement
- Mobile Phones
- Six Town Housing – Fraud and Business Controls
- Six Town housing - Procurement Repairs and Maintenance Improvement Works
- Six Town Housing Data Quality
- Six Town Housing Payroll

2021/22

- Housing Benefit Key Controls
- NNDR Key Controls
- Petty Cash Accommodation Team

2.4 Information Governance and Data / Digital

2.4.1 Internal Audit provide advice and consultative support to the council's arrangements for information governance and its response to the Information Commissioners Office (ICO) inspection in June 2021. An IG Delivery Group has been established and Internal Audit are represented on this group.

2.5 Supporting Transformation and Change

2.5.1 The Internal Audit Plan includes a provision of days to be made available to support services throughout the year by providing consultancy advice or independent assurance as / when our input is appropriate.

- Payroll: Support and advice has been given to the HR and Payroll Teams as they develop the use of the i-trent payroll system.
- Petty cash: Reviews of the use of petty cash floats for two establishments are being undertaken, and recommendations when implemented will assist the Council to make changes required to support the Making Tax Digital agenda.

2.6 Resources

2.6.1 Covid-19 Response

Since the middle of March 2020, and the onset of the Covid 19 pandemic the internal audit team have supported the council's response to the pandemic by:-

- Working with the revenue and benefits team on the Governments small business, retail and hospitality, and discretionary grants.
- Working with the Housing Benefits team processing the Government's track and trace /isolation payments to eligible members of the public.

2.6.2 Staffing

There has been no sickness reported in the team for the current financial year.

A team member has been seconded for 8 weeks, to provide support to the Housing Benefits Team in response to the pandemic. This poses a minor risk that the planned audits for 2021/22 may not be delivered. This situation will be monitored as the year progresses and updates will be brought to Audit Committee.

A team member has recently enrolled on a professional accountancy course, supported by the organisation via the apprenticeship levy. Part of the support includes providing time within the working week to undertake study and gain work experience. The annual audit plan may need to be adjusted to reflect this requirement, and this may reduce the number of days available to deliver audit assignments.

The adjustments to the plan if required will be made for the report to be provided to Audit Committee in November 2021.

2.6.3 Investigations

The team continues to be available to support the business with internal investigations providing technical skills and advice when called upon and managing the whistleblowing hotline / online referrals.

2.6.4 Collaboration

We have ongoing representation on sub-groups of the North West Heads of Internal Audit Group. The groups have been established to share good practice across the region.

- Contract Auditt Group
- IT Audit Group
- Schools Audit Group.
- Fraud Group (attended by members of the Counter-Fraud Team, information shared with Internal Audit)

2.6.5 School Audits

Individual School Audits are not incorporated in the 2021/22 plan, they have been replaced with thematic reviews of areas which were covered in the school audit reviews.

There are however arrangements in place that Internal Audit will undertake School Audits on request from the Executive Director of Education and / Childrens Services or Executive Director of Finance, where it is thought an audit review would be beneficial to the School and the Council. There have been no requests to date for individual schools to be audited.

A Schools Assurance Group has been established within the Council and Internal Audit are represented on this group.

<u>School funds</u>

The annual accounts for two School Voluntary funds have been examined as requested by the schools. A small fee was collected for these pieces of work.

Community impact / Contribution to the Bury 2030 Strategy

Ensuring compliance with Financial Procedures and Policies

Equality Impact and considerations:

24. *Under section 149 of the Equality Act 2010, the 'general duty' on public authorities is set out as follows:*

A public authority must, in the exercise of its functions, have due regard to the need to -

(a) *eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act;*

(b) *advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;*

(c) *foster good relations between persons who share a relevant protected characteristic and persons who do not share it.*

25. *The public sector equality duty (specific duty) requires us to consider how we can positively contribute to the advancement of equality and good relations, and demonstrate that we are paying 'due regard' in our decision making in the design of policies and in the delivery of services*.

Assessment of Risk:

The following risks apply to the decision:

Risk / opportunity	Mitigation
Risks are highlighted in Audit Plans and in the terms of reference for each Audit review.	Internal Controls are reviewed in each audit to mitigate identified risks. Actions are reported to managers and progress is monitored and reported on a regular basis.

Consultation:

N/a

Legal Implications:

Internal Audit forms one of the sources of assurance for a Local Authority. Under the Account and Audit Regulations 2015, Authorities must undertake an effective internal audit to evaluate the effectiveness of their risk management, control and governance processes. Consideration must be given to the Public Internal Audit Standards (PIAS) and sector specific guidance. The Council must also comply with requirements as set out in the Council's constitution.

Financial Implications:

There are no financial implications arising from this report. The work of the Internal Audit Service however supports the governance framework and the work on business grants has also ensured that the risk of fraud to the Council is minimised.

Report Author and Contact Details:

Janet Spelzini, Acting Head of Internal Audit,
Tel: 0161 253 5085
Email: j.spelzini@bury.gov.uk

Background papers:

Internal Audit Plan 2021/22

Internal Audit Reports issued throughout the course of the year.

Please include a glossary of terms, abbreviations and acronyms used in this report.

Term	Meaning

CORPORATE GOVERNANCE AND RISK								
Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Corporate Core	Risk Management and Assurance Framework	Failure to identify major risks that may prevent the Council from achieving one or more of its objectives. Failure to ensure that the major risks are being managed.	Review of risk management arrangements at Corporate level – review of the Council's risk management strategy and arrangements for the maintenance of risk registers. Review the associated information management system and reporting arrangements.	15	QTR2			
Corporate Core	Complaints Procedures	Failure to comply with Council policy and regulations, potential for reputational damage should a complaint be taken to the Ombudsman.	Review of system for receiving and dealing with complaints.	15	QTR3			Audit brought forward and commenced as received a specific request to look at the process in Childrens services
Corporate Core	FOI /Subject access	Failure to comply with Council policy and regulations, potential for reputational damage should a complaint be taken to the Ombudsman.	Review of system for receiving and dealing with FOI / SAR requests. Specific request to focus testing on Childrens' Services.	15	QTR4			

Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Corporate Core	Recruitment Process	Failure to undertake robust pre-employment checks (right to work in the UK etc.) which may result in reputational damage or financial penalties.	Review of recruitment process – including assurance over the design and operation of the recruitment process including: 1 completeness and timeliness of pre-employment checks 2 completeness, accuracy and timeliness of adding new employees to the payroll 3 monitoring by HR of compliance with pre-employment and recruitment processes 4 an appropriate division of duties is enforced by the system.	15	QTR4			
Corporate Core	Governance arrangements / AGS	Loss of accountability, lack of corporate ownership of decision making and possible failure to deliver the expected level of services to residents.	Review the methodology for producing the annual governance statement, ensuring that it reflects the code of governance, is in line with CPFA guidance and is adequately supported by evidence.	26	QTR2/3			Planning underway

Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Operations	Health and Safety	Potential damage to health / wellbeing or loss of life which may result in claims, reputational damage, litigation or corporate manslaughter	Review of Health and Safety arrangements within Operational Services, including the identification of services provided, the risk assessments in place action to address any remedial action identified.	15	QTR3			

SERVICE REFORM (Core Financial Systems)								
Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Corporate Finance	Finance Systems - key controls	Errors and omissions resulting in weaknesses in the integrity of financial data and statements	Routine annual review of high level controls within the key finance systems, retrospective review looking at transactions in 2020/21, to support closure of accounts process. Council Tax NNDR Housing Benefits Treasury Management Payroll Creditors Main Accounting Debtors Cash Collection and Banking.	80	QTR 1			Draft reports issued to client: • NNDR • Housing Benefits Draft reports in review process to be issued to client before October:- • Treasury Management • Payroll • Creditors • Main Accounting • Debtors • Cash Collection and Banking • Council Tax

Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Corporate Finance	National Fraud Initiative	Statutory requirements are not complied with	Manage and co-ordinate the NFI including additional checks on data matches where appropriate.	15	QTR3 and QTR 4	N/A		Ongoing exercise, NFI data matching results being examined
Corporate Finance	Establishment Budgets and alignment with HR records	Establishment budgets and HR information may become out of line, creating budget pressures elsewhere if funds have to be released to meet payroll costs/ alternatively staffing levels/payments to employees may have to be reduced so funds can be released to deliver services.	Review the arrangements in place to ensure that budgets for establishments remain aligned with HR systems.	5	QTR 3 / 4			

Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Corporate Finance	I-Trent - Payroll – Additional hours / overtime payments	Failure to respond effectively and efficiently to any major incident.	Review arrangements to manage and process timekeeping and overtime effectively as the self-serve module is introduced in i-trent. Cover all directorates, and report to each Executive Director with results of findings.	15	QTR2			
Corporate Finance	Unit 4 - Land and Property Valuations	Inaccurate information may be held in the financial accounts.	Review the process for valuing land and property and the updating of records in the CONCERTO system and the subsequent reconciliation of the CONCERTO system with Unit 4.	15	QTR 2 /3			

SERVICE REFORM (Grants and Verification)								
Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Corporate Finance	Grant Claims	Failure to comply with grant arrangements.	Certification of those grant claims required to be certified by the Council's head of internal audit. Anticipated during 2021/22 include:- Local Growth Fund Transport – Bus subsidy Cycle City Highways, Potholes and Flood Resilience	16	QTR 3			
Corporate Finance	NNDR – Business Grants	Failure to comply with grant arrangements.	Review the process for the administration of the Business Grants awarded as a result of COVID 19, ensuring that grants awarded were within the government set criteria.	20	QTR 3			

Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Children and Young People	Dedicated School Grant	The Council may fail to address the recommendations made by the DFE, and DSG recovery may not be achieved.	Review work being undertaken to ensure that recommendations identified during the Safety Valve project are being addressed and DSG recovery is being achieved.	20	QTR3 / 4			
Communities and Wellbeing / One Commissioning Organisation	GM Supporting Familes (TFG)	Failure to comply with grant requirements and failure to deliver programme objectives.	Routine annual review. GMCA have been granted devolved powers over the programme and are collaborating to develop a more traditional / risk- based approach to the annual assurance work. Reviews to be undertaken once / twice a year as directed by GMCA and the devolution agreement.	10	QTR2/3			Audit commenced

PLACE AND PEOPLE								
Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Corporate Core	CCTV	Failure to adhere to the agreement and follow the CCTV Code of Practice could impact on the Council's reputation and reliance placed on the CCTV function in supporting other agencies and community safety.	Annual review as required by CCTV agreement.	5	QTR4			
Children and Young People	Independent Foster Agency	Inability to place "looked after children" with suitable families or promptly as the need arises.	Review of the use of IFA's, including the controls in place to help ensure cost effectiveness and manage quality and quantity of placements.	10	QTR2			Planning underway

Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Children and Young People	Care Packages	Failure to comply with Council policy and legislation when procuring goods / services / administering contracts with suppliers. Best value may not be achieved and high cost care packages may not be challenged.	A review of the process for the calculation and award of care packages for vulnerable children, and the billing and payment processes around care processes to provide assurance that financial risks are mitigated. Review arrangements in place for ongoing reviews of care packages to ensure they are still appropriate and consider the financial controls in particular authorisation for changes to rates and providers. Determine if any benchmarking processes are in place and review.	15	QTR3			

Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Children and Young People	Residential Placements	Failure to comply with Council policy and legislation when procuring goods / services / administering contracts with suppliers. Best value may not be achieved and high cost care packages may not be challenged.	A review of the processes and associated costs relating to Looked After Children who are placed into residential care.	15	QTR2			Planning underway
Children and Young People	School and College Transport	Children with special educational needs may be excluded from Education as they may not have any available transport / support to enable them to be able to travel to and from school.	Review the management and contractual arrangements over SEN transport to ensure outcomes for service users are achieved and risks to the service users and the Council are mitigated.	15	QTR3			

Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Communities and Wellbeing / One Commissioning Organisation	Home care packages	Failure to comply with Council policy and legislation when procuring goods / services / administering contracts with suppliers. Best value may not be achieved and high cost care packages may not be challenged.	A review of the process for the calculation and award of care packages for vulnerable adults, and the billing and payment processes around homecare processes to provide assurance that financial risks are mitigated. Review arrangements in place for ongoing reviews of care packages to ensure they are still appropriate and consider the financial controls in particular authorisation for changes to rates and providers. Determine if any benchmarking processes are in place and review.	15	QTR3			

Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Operations	Highways and Footway Maintenance	Budget cuts may have led to a reduced ability to maintain a safe and passable highway, - risk of fatality. This may lead to increased reputational damage as there is the potential for claims to be made against the Council which may incur significant financial penalties.	Review of highways maintenance – work programmes, allocation of works and subsequent monitoring, and costs.	20	QTR3			
Operations	Fleet Management	Vehicles and plant may be mis–used / mis-appropriated	Review to assess the security of the vehicle and plant equipment and the arrangements in place to ensure that all items can be accounted for.	10	QTR2			Planning underway

Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Operations	Taxi Licences	Potential damage to health / wellbeing or loss of life. Reputational damage to the Council and potential financial claims.	Review the system in place for the issue of licences to taxi driver licences to applicants, ensuring that appropriate checks are made to ensure that individuals have a right to work in the UK and hold the appropriate driving licence.	10	QTR2			Planning underway
Operations	Architectural Practice Fee Income	Income due may not be collected, effecting cash flow of the Council. Additionally errors and omissions resulting in weaknesses in the integrity of financial data and statements	Review the processes in place to ensure that income due to the service is correctly calculated in line with any agreements in place, and that the income is collected and posted to the accounts promptly.	10	QTR3			
Operations	Income	Income due may not be collected, effecting cash flow of the Council. Additionally errors and omissions resulting in weaknesses in the integrity of financial data and statements.	Work to be undertaken as part of COVID 19 recovery, to look at areas including Leisure Memberships, Civic Centre bookings and Markets	25	QTR3 /4			Specific request to look at income within leisure centres received from client, audit brought forward and work is ongoing.

CONTRACTS								
Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Corporate Finance	STH Client Management arrangements	Failure to implement the clauses in place in the management agreement could provide a risk of financial loss to the Council in addition to reputational damage.	A new agreement has been implemented and a review is required to ensure that the terms of the agreement are being adhered to.	15	QTR2			Planning underway
Corporate Finance	Persona	Failure to implement the clauses in place in the management agreement could provide a risk of financial loss to the Council in addition to reputational damage.	A new agreement has been implemented and a review is required to ensure that the terms of the agreement are being adhered to.	15	QTR2			Planning underway

Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Business Growth and Infrastructure	Regeneration Projects	Failure to comply with Council policy and legislation	Identify regeneration projects that have / are taking place. Review a project to ensure that best practice was followed, considering project initiation, procurement of works, ongoing monitoring, and administration of payments, record keeping and post project implementation review.	10	QTR3			Audit brought forward as specific request to examine a project received from client – audit ongoing
All Services	Contract register	Failure to comply with Council policy and legislation when procuring goods / administering contracts with suppliers.	Review the arrangements to identify contracts in place and ensure adequate information is held to ensure that contracts are renewed on a timely basis.	10	QTR2			Planning underway

SUPPORT / SYSTEMS IMPLEMENTATION								
Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Corporate Core	GDPR	Failure to comply with Council policy and regulation and legislation, potential for reputational damage and financial penalties should a complaint be taken to the ICO.	Follow up work following issue of internal audit work, and ICO visit.	10	QTR3 / 4			
Communities and Wellbeing	CONTROCC	Failure to adequately secure systems could result in a data breach, loss of service / downtime and loss of data.	Provision to support system implementation	5	TBA	N/A		
Communities and Wellbeing / One Commissioning Organisation	Direct Payments	Funds provided to meet individuals social care and support needs are not being used as agreed and fail to deliver anticipated outcomes.	The service is planning to undertake a beginning to end review of the Direct Payment process and have asked for Internal support with this.	5	TBA	N/A		

Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Corporate Core Finance	I-Trent	Failure to adequately secure systems could result in a data breach, loss of service / downtime and loss of data.	Provision to support system implementation	5	TBA	N/A		
Corporate Core Finance	Income collection / Debtors and Write off procedures	Errors and omissions resulting in weaknesses in the integrity of financial data and statements. Legislation may be breached. Inappropriate debts may be written off.	Request for audit support to Treasury Management function to identify income sources, document collection and banking procedures and to determine if making tax digital agenda is being adhered to. Additional work includes a review of the revised write off procedures when they have been updated.	15	TBA	N/A		

Directorate	Topic	Potential Control / Governance Issue	Proposed Audit Coverage	Indicative Days	Proposed Timing	Reported	Assurance	Comments
Corporate Core Finance	Unit 4 - Making Tax Digital	Failure to comply with legislation could result in reputational damage and financial penalties.	Provision included to support the Management Accountancy Team in systems development to ensure that the making tax digital agenda is adhered to. The work will need to focus on expenditure, including petty cash and income streams which feed the annual accounts.	15	TBA	N/A		Petty cash reviews being undertaken in two areas as requested by Management t Accountancy Team. Issues have been identified and reports will be produced and presented to Audit Committee.
			TOTAL	552				

OTHER COMMITMENTS		
Activity	***Indicative Days***	***Comments***
Completion of audits commenced during 2020/21: **Health and Safety** **GDPR** **Pooled Budgets** **Budget Setting and Monitoring in Schools** **Purchase Cards** **Car Allowances** **Adoption** **Integrated Community Equipment Stores** **Members Allowances** **Members Delegated Funds** **Pupil Premium** **Operations Procurement** **Mobile Phones**	25	Indicative days were set too low • Final Audit reports now issued for: • GDPR • Pooled Budgets • Budget Setting and Monitoring in Schools • Purchase Cards • Car Allowances • Adoption • Integrated Equipment Store • Pupil Premium • Members Allowances Final reports are due to be issued for: • Mobile Phones • Operations Procurement Draft report being finalised for • Members Delegated Funds
External Traded Services - -perform audits of School Fund and Out of School Club accounts	10	Two school fund accounts have been reviewed to date
Audit work for Six Town Housing and Persona (separate audit plans)	120	Work is underway to deliver the STH audit plan.
Post Implementation Reviews and Action Tracking	24	

Contingency for GMCA Collaboration / reactive GM assurance work	5	Completion
Contingency for Investigations and supporting the council's counter fraud strategy	30	
Contingency for reactive or unplanned work, management request, consultancy work	20	
Audit Service Management and administration, including service development, assurance mapping, Quality Assurance and Improvement Programme (QAIP), anti-fraud and corruption strategy, audit planning and Committee's support	199	Indicative days may need to be revised as team member seconded to P1 service, and team member now commenced CPFA studies.
Provisions for annual leave / training / sickness	243	Indicative days may need to be revised as team member seconded to P1 service, and team member now commenced CPFA studies.
Provision of ICT review – by Salford Computer Audit Services (System Licencing)	20	
Total:	696	
Combined Total:	1248	
Audit days to be delivered	**806**	(Exclude 199+243)

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank