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, 25 November 2021
Place:	Town Hall
Time:	7.00 pm – Training at 6pm
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:	**There will be pre meeting training at 6pm**

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 - 12)*

The Minutes of the last meeting of the Audit Committee held on 30 September 2021 are attached.

4 MATTERS ARISING

5 FINAL ACCOUNTS

Sam Evans, the Council's Section 151 Officer will give an update at the meeting.

6 RISK REGISTER *(Pages 13 - 42)*

A report from Sam Evans, Executive Director of Finance is attached
Appendix A attached
Appendix B attached
Appendix C attached
Appendix D attached

7 INFORMATION GOVERNANCE UPDATE *(Pages 43 - 108)*

A report from the Deputy Chief Executive is attached

8 COVID 19 UPDATE *(Pages 109 - 132)*

A report from the Leader of the Council and Cabinet Member for Finance and Growth is attached.

The Section 151 Officer will report at the Meeting

9 INTERNAL AUDIT UPDATE REPORT *(Pages 133 - 168)*

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 - AUDIT REPORTS *(Pages 169 - 298)*

A report from the Acting Head of Internal Audit is attached
Appendices 1 – 6 attached
Officers will attend in relation to the following reports:

- Health and Safety
- Members Discretionary Budgets
- Creditors Key Controls
- Cash and Bank Key Controls
- Debtors Key Controls
- Main Accounting Key Controls

This page is intentionally left blank

Agenda Item 3

Minutes of: **AUDIT COMMITTEE**

Date of Meeting: 30 September 2021

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

Also in attendance: Lynne Ridsdale, Deputy Chief Executive
Sam Evans, Section 151 Officer
Will Blandamer - Executive Director of Strategic Commissioning
Adrian Crook - Assistant Director of Adult Social Care (Operations)
Janet Spelzini – Interim Head of Internal Audit
Marcus Connor – Corporate Policy Manager
Amelia Payton – Mazars
Julie Gallagher – Head of Democratic Services

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

Apologies for Absence:

AU.1 DECLARATIONS OF INTEREST

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

AU.2 MINUTES OF THE LAST MEETING

It was agreed:

That the Minutes of the last meeting held on 21 July 2021 be approved as a correct record and signed by the Chair.

AU.3 MATTERS ARISING

Sam Evans Section 151 Officer provided Members of the Committee with an update in respect of the Council's minimum level of balances/financial reserves. CIPFA benchmarking recommends that Councils hold reserves of between five and ten percent, 10% would equate to £17.1 million, the position at March 2022 is the Council current level of reserves are circa 20%.
On current projections it is expected that by 2023 the levels will be between 11 and 17% this is dependent on delivery of budget savings and the effective operation of the safety valve project.

The Section 151 reported that she will facilitate financial training for all Elected Member prior to the next meeting of the Audit Committee.

AU.4 INFORMATION GOVERNANCE PROGRESS REPORT

Lynne Ridsdale, Deputy Chief Executive and Marcus Connor the recently appointed

Information Governance Manager following consideration of this item at the last meeting, the Deputy Chief Executive provided Members of the Committee with an update. An accompanying report had been circulated prior to the meeting and provided details of the 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)

A detailed action plan has been developed as a result of the consensual audit by the ICO which had been carried out 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.

The ICO have made 79 recommendations across the three themes of the audit.

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.

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

The Deputy Chief Executive confirmed that there had been a lack of corporate oversight of the information governance function as well as a lack of follow up on actions when breaches had occurred. The Corporate Management Team are committed to ensure that Information Governance is an area of focus and has been included in the Risk Register.

Responding to a Member question in relation to the timetable for delivery of the recommendations, the Deputy Chief Executive reported that these are necessary timescales. There is a huge amount of work to be undertaken, the action plan will be subject to a monthly review and if necessary timescales can be reviewed/amended.

It was agreed:

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, therefore this item will be a standing agenda item.

AU.5 MAZARS AUDIT STRATEGY MEMORANDUM

Amelia Payton representing the External Auditors Mazars, presented the Committee with the External Auditor's Strategy Memorandum, for the year ending 31 March 2021. The purpose of this document is to summarise Mazars audit

approach, highlight significant audit risks and areas of key judgements and provide you with the details of the Mazars audit team.

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 the considerations and conclusions on Mazars independence as auditors.

The report provided information in respect of:

- Engagement and responsibilities
- Audit engagement team
- Audit scope, approach and timeline
- Significant risks and other key judgement areas
- Value for Money
- Fees for audit and other services

Responding to a question from the Chair, the Mazars representative reported that Mazars will provide a team of staff to commence the audit on the 4th October 2021 and to be completed by the end of November 2021. Of the 10 GM audits, Mazars have been instructed to complete, three have currently been signed off.

Delegated decision:

That the report be noted.

AU.6 REDMOND REVIEW

Delegated decision:

The External Auditors will provide an update report at the next scheduled meeting of Audit Committee.

AU.7 RISK REGISTER UPDATE

Following deferment of this item from the previous meeting, Sam Evans, Section 151 Officer presented the risk register for Members consideration. An accompanying report had been circulated to Members prior to the meeting providing information in relation to:

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**

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.

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

In considering the risk register Members of the Committee raised concerns that there were a number of fields that didn't have action owners as well as a number of areas that did not have a due date for completion. The Section 151 Officer

reported that there is still a great deal of work to do in developing the risk register, a training programme for staff will commence imminently.

Delegated decision:

That the Audit Committee:

- Note the update provided
- Support the approach progressed to date to update the departmental risk registers
- Support the approach that a further corporate risk register will be developed which will incorporate not only departmental risks but overarching organisational risks
- Request the Executive team review the areas without an action owner and or a completion date and an updated document be presented at the next Audit Committee
- Identify health and safety and the shortage of HGV drivers as areas for further scrutiny and in doing so, the two lead officers for these areas be invited to the next meeting of the Audit Committee scheduled to be held on 25th November 2021

AU.8 COVID GRANTS FINANCIAL SUPPORT

A Covid Grants Financial Support report that had been prepared for consideration at the Overview and Scrutiny Committee was shared with Members of the Audit Committee for their oversight. The report provided details of:

- Support for Expenditure as a result of Covid-19
- Support for Income Loss as a result of Covid-19
- Covid-19 Support for Business
- Analysis of Grants Received in 2020/21 as a result of Covid -19

Responding to a Member's question, the Section 151 Officer reported that the term unspent grants relates to those grants not claimed by businesses within the Borough. The Council continues to work proactively to contact business to ensure if they are entitled to a grant they receive it.

The Section 151 Officer reported that not all loss of income would be re-imbursed by central government and the Council will only be able to recover 75% of 95% of the budget. There remains elements of some baseline expenditure that will not be funded.

In response to a Members question in relation to loss of Council Tax income of £2.3 million; the Section 151 Officer reported that that the charge deficit could be recouped over three years. The Council remains optimistic that they will be able to recover the majority of the monies, the bigger challenge remains with the collection of Business Rates.

Delegated decision:

That the report be noted and further report will be considered at the next meeting of the Audit Committee.

Further information in respect of a breakdown of spend in relation to;

- the £ 15.4 million pounds of funding, Covid Marshalls, Community Champions and Local Election funding will be provided to Members of the Committee

AU.9 INTERNAL AUDIT UPDATE

Janet Spelzini, Acting Head of Internal Audit presented a report setting 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 Acting Head of Internal Audit reported that 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 reviewing the plan Members of the Committee requested that:

- An update on the information obtained via the whistleblowing hotline
- If the proposed highway maintenance review could be brought forward
- the scope of the complaints review be broadened to include waste management complaints.
- Details of the scope of the internal review in respect of the Unit 4 - Land and Property Valuations be shared with the Audit Committee

Delegated decision:

That the contents of the report be noted

AU.10 EXCLUSION OF PRESS AND PUBLIC

Delegated decision:

That in accordance with Section 100(A)(4) of the Local Government Act 1972, the press and public be excluded from the meeting during consideration of the following items of business since they involved the likely disclosure of exempt information, relating to any action taken, or to be taken in connection with the prevention, investigation and prosecution of crime.

AU.11 INTERNAL AUDIT PROGRESS REPORT

Janet Spelzini presented a report setting out the work undertaken by Internal Audit between 1st April 2021 to 10th September 2021 to the end of quarter 2 2021/2022.

Appended to the report was a list of the Internal Audit Reports that had been issued and recommendations that had been made.

Delegated decision:

That the contents of the report be noted

AU.12 INTEGRATED COMMUNITY EQUIPMENT STORES

Will Blandamer - Executive Director of Strategic Commissioning and Adrian Crook - Assistant Director of Adult Social Care (Operations) attended the meeting to update and provide assurance to Members following the internal audit review of the Integrated Community Equipment Stores.

Delegated decision:

That the contents of the report be noted

AU.13 MEMBERS' FEEDBACK

It was agreed:

- Internal audit reports to be shared with members of the audit committee in one tranche two weeks prior to the Committee dates to be confirmed
- Members to consider shadowing an internal audit review
- Section 151 Officer to scope with the Chair an Annual Report on Fraud

COUNCILLOR M WHITBY
Chair

(Note: The meeting started at 7.00 pm and ended at 8.50 pm)

This page is intentionally left blank

Agenda Item 6

Classification Open	Item No.

Meeting:	Audit Committee
Meeting date:	25th November 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 scrutinizing risks where the impact has the potential to disrupt achievement of the Council's priorities.

This report presents the first iteration of the Council's Corporate Risk Register, in accordance with the refreshed Risk Management Strategy initially introduced in late 2019. The risks identified are a collation of strategic risks currently present on the departmental "Red Risk" register, together with additional events determined by the Executive Team to pose a threat to the Council's strategic objectives and service delivery.

A total of 17 risks have been identified as those of a genuine corporate nature and are summarised as follows:

- **17** risks are currently present on the Corporate Risk Register;
- **15** risks are currently rated as Significant (risk score 15-25)
- **2** risks are currently rated as High (risk score 8-12)
- Of these 17 risks:
    - 1 has increased in score
    - 10 have decreased in score
    - 6 have remained static.

Recommendation(s)

That:

The Audit Committee:

- Note the update provided;
- Review the Risk Matrix presented at Appendix A;
- Analyse and discuss the 2 Deep Dive Risk Reports presented at Appendix B;
- Receive the Corporate Risk Register at Appendix C;
- Review the information presented;
- Determine whether the level of assurance provided against the risks is sufficient; and,
- Review the Risk Mechanism at Appendix D and support the approach to escalating and de-escalating risks between the Council's departmental and corporate risk registers.

Key Considerations

1. Background

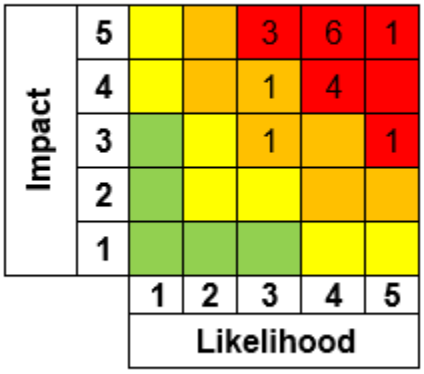
At the previous meeting of the Audit Committee, it was agreed that work would be undertaken by the Executive Team to produce a Corporate Risk Register that would result in a reduction of the Council's exposure to strategic risks, through identification and effective management.

2. Key Considerations

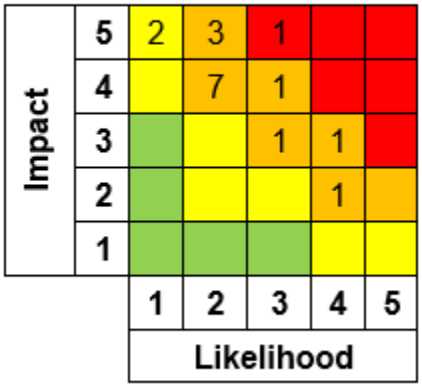
The work progressed to date reflects progress toward providing the Audit Committee with adequate assurance of dynamic corporate risk management. The Corporate Risk Register represents a collation of risks identified and assessed as significant risks to Bury Council.

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

Current



Target



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. • Creation of a Corporate Risk Register in alignment with the revised risk management strategy.

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

Background papers:

- Risk Matrix at Appendix A;
- Deep Dive Risk Reports presented at Appendix B;
- Corporate Risk Register at Appendix C;
- Risk Mechanism at Appendix D.

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

Term	Meaning
BGI	Business Growth and Infrastructure department
CC	Corporate Core department
CYP	Children and Young People's department
OCO	One Commissioning Organisation
FIN	Finance department
ICS	Integrated Care System

Risk Register Update

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 **November 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. Since June 2020, significant work has been undertaken to implement a robust approach to risk management across Bury Council, commencing with the introduction of a framework that has been rolled out across all directorates. This was later supplemented with information and guidance sessions department by department to further embed a culture of dynamic risk identification and proactive management.

2.4. All departmental risks are now collated, monitored and managed from a single repository, the Master Risk Register. Risk Owners are moving toward a comfortable rhythm of analysing risks due for review in the relevant reporting month and including risk as a standing item on departmental team meetings.

2.5. At the September meeting, the risks assessed at a level 15 or above on the Master Register were captured and presented to the Audit Committee as the "Red Risk Register". From the resulting discussion, the following two risks were identified for "deep dive" analysis discussion at the forthcoming meeting:

- **CC/1**- Council liability for the death of an employee or member of the public.
- **OPS/17** - 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 and high market rate.

2.6. The corresponding reports at Appendix B provide an increased level of detail on these two selected risks, including existing controls, assurances and mitigating actions to facilitate reduction of the risk to a tolerable scoring.

2.7. Furthermore, it was agreed at the September meeting that work would be performed by the Executive Team to discuss and identify those risks that would constitute the "Corporate Risk Register".

3. Corporate Risk Register

3.1 The Corporate Risk Register (Appendix C) captures the Council's key strategic risks, details the existing controls that provide some level of assurance and identifies planned actions being undertaken to mitigate these risks.

3.2 The Corporate Risk Register is not intended to cover all risks, rather those that are cross cutting and strategic. These risks are identified as those with the potential to disrupt the Council's ability to meet its strategic and operational objectives; and as such, have been discussed and agreed by the Executive Team and categorised as warranting regular scrutiny to help the Council minimise future financial risks and adverse implications. Risks such as Aging Vehicles and Continued Provision of Leisure Services are managed at directorate or service level and remain on the Master Risk Register. The document at Appendix D depicts the relationship between Bury Council's risk registers mechanism by which risks are escalated and de-escalated accordingly.

3.3 The live document will be reviewed by the Executive Team on a quarterly basis in alignment with the schedule of meetings for the Audit Committee, where it will be presented for scrutiny and identification of risks for "deep dive" analysis from November 2021.

3.4 For each risk present on the Corporate Risk Register, the following information is given:

- Risk Reference
- Risk Title
- Strategic Outcome
- Current Score (Likelihood x Impact)
- Target Score (Likelihood x Impact)
- Risk Owner
- Key Potential Impacts
- Current Controls
- Departmental Risk Register reference (if applicable)
- Planned Actions
- Responsible Officer
- Risk Action Status, and;
- Trend.

3.5 The following strategic risks have been identified and are presented on the appended register. Each has been aligned to one of the four strategic outcomes, as detailed in the Bury 2030 Community Strategy:

- **CR1/Financial Sustainability** – *Economic Growth and Inclusion*
  - Reduced budgets and public sector cuts impact the Council's ability to deliver services.
- **CR2/COVID-19 Impact** – *Strength-based Approach*
  - Risk of new variants impacting social mobility and further reduced income from commercial portfolio arising from lockdowns.
- **CR3/Security & Resilience** – *Delivering Together*
  - External threats of terrorism and cyber security incidents causing disruption to Bury communities, Councillor's and service delivery I.T systems.
- **CR4/Digital Transformation** – *Delivering Together*
  - Inability to achieve ambition for new ways of working through failed delivery of the Digital Strategy.
- **CR5/Increasing Demand Pressures** – *Economic Growth and Inclusion*
  - Significant increases in demand for services potentially resulting in failure to meet local authority statutory obligations.
- **CR6/Climate Change** – *Local Neighbourhoods*
  - Inability to meet UK 2030 Emissions Target and Bury Climate Manifesto potentially impacting future funding.
- **CR7/ICS Implementation** – *Strength-Based Approach*
  - Potential adverse effect on the health and social system caused by the implementation of the Integrated Care System (ICS).
- **CR8/Elections** – *Delivering Together*
  - Potential reputational damage if Bury Council fails to effectively deliver the May 2022 election.
- **CR9/Workforce Capability and Capability to Deliver** – *Economic Growth and Inclusion*
  - Impact on delivery of Council priorities should the workforce capability and capacity prove insufficient.
- **CR10/EU Exit Impacts** – *Economic Growth and Inclusion*
  - Social and economic programmes at risk as a result of loss of EU funding, increased inflation and further skills gaps due to restrictions on the free movement of people.
- **CR11/Asset Management (Operational Health & Safety**) – *Local Neighbourhoods*
  - Potential of prosecution resulting from a breach of health and safety legislation in relation to safe and effective buildings and facilities used by occupants.
- **CR12/Children's Social Care Services** – *Economic Growth and Inclusion*
  - Adverse impact on children, young people and families due to high Social Worker caseloads and the possibility of receiving a poor Ofsted judgement.

- **CR13/Regulatory Compliance** – *Delivering Together*
  - Failure to meet the requirements of data protection legislation and good information governance practice may result in breach incidents and potential sanctions.
- **CR14/Corporate Health & Safety** – *Economic Growth and Inclusion*
  - Potential adverse effect on service delivery resulting from sickness absence; failure to protect staff wellbeing, welfare and morale.
- **CR15/Regeneration & Development** – *Local Neighbourhoods*
  - Rising construction inflation and a slow housing market create challenges to deliver regeneration and housing programmes.
- **CR16/Special Educational Needs and Disabilities** – *Economic Growth and Inclusion*
  - An increased number of SEND tribunals may erode parental trust in the Council and result in inadequate statutory compliance.
- **CR17/Technical and Legal Compliance with Employment Law and Council Policy Framework** – *Strength-based Approach*
  - Breakdown in employee relations, legal challenge with reputational or financial impacts.

4 Trend Analysis

4.1 There are currently a total of 17 risks on the corporate risk register, split across the departments of the Council as follows. Of the 17 risks 15 (88.2%) are rated as significant:

Department	No. Risks	Low (1-3)	Moderate (4-6)	High (8-12)	Significant (15-25)	Risks Not Scored
CC	**8**	0	0	2	6	0
CYP	**2**	0	0	0	2	0
FIN	**2**	0	0	0	2	0
OCO	**1**	0	0	0	1	0
OPS	**4**	0	0	0	4	0
TOTAL	**17**	**0**	**0**	**2**	**15**	**0**

4.2 Of the 17 risks:

1 has increased in score:

- CR3 Security & Resilience.

10 have decreased in score:

- CR1 Financial Sustainability
- CR5 Increasing demand pressures
- CR7 ICS Implementation
- CR8 Elections
- CR9 Workforce Capability and Capability to Deliver
- CR10 EU Exit Impacts

- CR12 School Improvement
- CR13 Regulatory Compliance
- CR14 Corporate Health & Safety
- CR17 Technical and Legal Compliance with Employment Law and Council Policy Framework.

6 have remained static:

- CR2 COVID-19 Impact
- CR4 Digital Transformation
- CR6 Climate Change
- CR11 Asset Management (Operational Health and Safety)
- CR15 Regeneration & Development
- CR16 Special Educational Needs and Disabilities.

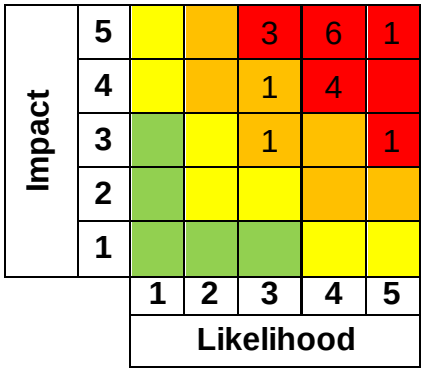
4.3 Planned actions to address the risks

Mitigating actions have been identified and are on track to deliver against 16 of the risks however some slippage has occurred in respect of addressing one risk - CR13 Regulatory Compliance.

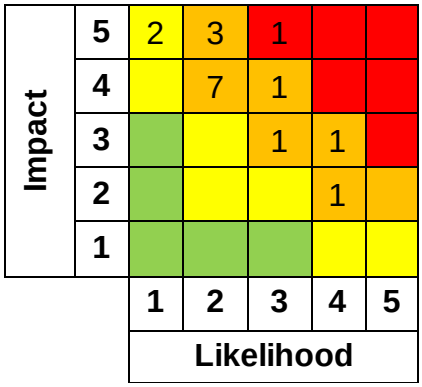
4.4 Heat Maps

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

Current



Target



5 Recommendations

5.1 The Audit Committee is asked to:

- Note the update provided;
- Review the Risk Matrix presented at Appendix A;
- Analyse and discuss the 2 Deep Dive reports presented at Appendix B;
- Receive the Corporate Risk Register at Appendix C;

- Review the information presented;
- Determine whether the level of assurance provided against the risks is sufficient; and,
- Review the document at Appendix D and support the approach to escalating and de-escalating risks between the Council's departmental and corporate risk registers.

This page is intentionally left blank

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					
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					
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

This page is intentionally left blank

Report to	**Audit Committee**
From	**Corporate Core Department**
Risk Reference	**CC/1**
Risk Description	**Council liability for the death of an employee or member of the public.**
Recommendation	**For analysis and discussion**

Context

An internal audit of Bury Council health and safety arrangements was undertaken in 2020 which gave an overall opinion of a limited level of assurance.

The report reminds the Council that failure to comply with Health and Safety legislation carries a risk of a charge of Corporate Manslaughter which, if proven, would result in unlimited fines, remedial orders and publicity orders.

Internal Audit Findings

The key concerns raised by internal audit are as follows:

- There is no formal reporting process in place to inform the Executive Team of health and safety related issues, performance or to provide assurance to the Chief Executive that the Council's responsibilities for Health and Safety are being met.
- The reporting of injuries, diseases and dangerous occurrences is not being undertaken in line with the required timescales detailed in legislation.
- A new health and safety policy was drafted in the previous financial year (2020/21). The policy has undergone Union consultation, but it has not been taken to Cabinet for formal approval, although it is accepted that this will be progressed once feedback from the audit has been provided in order that any necessary adjustments may be made.
- No assurance can be given on the level of compliance across the Council with regards to fire risk management. It is unclear on how often the Council expects fire risk assessments to be undertaken, as a corporate decision has not been taken/recorded.
- Assurance cannot be provided that the necessary health and safety risk assessments for buildings and services have been undertaken to demonstrate compliance with covid 19 requirements.

The report provided a set of recommendations to respond to these findings, of which two were classified as fundamental:

- The governance structure around health and safety requires review
- An annual health and safety report should be produced and presented to the relevant committee providing an overview of organisational and departmental issues and performance and to identify future priorities

This note provides an update on immediate actions against the fundamental recommendations above and responsibility / actions within the wider improvement plan.

Immediate Response & Assurance

Proposals against the two fundamental recommendations made by Internal Audit are as follows:

1. **Annual Report**

The framework for an annual health and safety report has been developed and work is underway to deliver the first report by the end of the 2021 calendar year. The production of real-time performance information will be maintained by the corporate health and safety team and released on a quarterly basis

2. **Governance**

Governance proposals for health and safety have been developed as follows:

- The corporate health and safety advisory team will be moved to the leadership of the Director of People and inclusion and maintain responsibility for advice to managers; internal investigations; accident reporting and staff training. The service will be subject to a structural review
- A Facilities management team will be established under the leadership of the Operations department Assistant Director of Operations (Strategy), to assume responsibility for the management of council buildings. Pending the establishment of a substantive team a short term project team will be established to support urgent compliance checks
- A proposal for a corporate Health and Safety JCC Is being developed with the Trades Unions and will also be in place by year end.

Consistent with the arrangements above it is proposed that the corporate risk owner for accident and incidents at work is moved to the Operations department.

3. **Wider priority work**

The ability to progress a number of the other recommendations is predicated on the existence of a single record of all buildings, occupancy and compliance. Work has progressed to achieve this as follows:

- Work has begun to establish a small Facilities Management (FM) service under the leadership of Head of Corporate Landlord. A minimum requirement for £100k funding has been identified of which £50k will be met by the Corporate Core but the balance is outstanding.
  Whilst the FM team is substantively established a fixed term project team will be sourced to support the compliance work, below. A 12-month team is required for which funding has been identified for the first 5 months
- a pilot 34-point compliance check list for completion in all buildings against statutory / regulatory / business requirements has been developed, including fire risk assessments which were particularly referenced by the audit report. This exercise will deliver :

- A definitive list of all operational buildings; service occupancy and identification of Building Owners. The number of buildings is understood to be c116 but details are still vague
- Location of all buildings that can be grouped into geographic hubs across the borough
- Overall % compliance and RAG rating across the estate as a basis for risk management and remedial action

Application of the compliance check list at Humphry House concluded a 44% compliance rate. This would be a typical outcome from the proposed desk top exercise across the estate. Funding will be required to address remedial works at this scale

Delivering wider recommendations through a Taskforce

The detail of all recommendations, mapped by accountability against the governance described above, is appended.

Internal audit proposed that a "Taskforce" was established to oversee production of and delivery against an improvement plan. It is proposed that the Taskforce is comprised as follows, accountable direct to the Chief Executive:

- A Unison representative
- Chris Beadsworth, head of Corporate Landlord
- Sam McVaigh, Director People & Inclusion

Key Issues

Key issues associated with immediate response are as follows:

- The work to complete a checklist for all 16 buildings is a major piece of work to complete in its entirety. Options will be required to progress a proportionate approach
- The totality of funding for a facilities management team has not yet been resolved. Options must be considered to identify the balance of both fixed term and substantive resource requirements as described above
- Funding will also be required to address the schedule of improvements to work places which the compliance audit is likely to identify. Options for reinvestment of capital receipts from the current schedule of accelerated disposals will be explored.

Annex – All recommendations by accountable service

Facilities Health and Safety improvements (Corporate Landlord)	**Workforce Health and Safety improvements (Corporate Core)**
• A decision on the frequency of fire risk assessments / reviews should be made corporately and communicated • The Health and Safety team / Facilities Management team should have a system and records in place to report and provide assurance on the level of compliance with fire risk management across the Council. • Guidance to those expected to undertake Fire risk assessments should be reviewed, it should be clear and precise and ensure that a consistent approach is applied when risk assessments are undertaken. • The review of the COVID-19 arrangements in place for buildings and staff should be completed and any services operating without the necessary risk assessments should be contacted to complete assessments as priority • The Health and Safety team should have systems/procedures in place to enable them to monitor and provide assurance on the level of compliance with facilities management risk assessments. • A central record of Council buildings and responsible officers should be held and be made available to the Health and Safety team. • The Health and Safety Team/Facilities Management Team should be able to demonstrate that statutory risk assessments are up to date at each establishment and should hold accurate information of risk assessments required, and risk assessments undertaken. • The Health and Safety Team should check and monitor to ensure that the risk assessments are in place and cover all the statutory requirements and are maintained up to date in accordance with legislation and best practice guidance • A decision should be reached on the level of PAT testing to be applied to Council equipment whilst employees are agile working.	• The governance structure around health and safety requires review including a reporting line to Members and senior managers • An annual health and safety report should be produced and presented to the relevant committee • The Health and Safety policy should undergo formal approval, publication and annual review • RIDDOR reportable incidents must be reported within the HSE specified timeframes and managers made aware of this • The system in place for recording accidents, incidents and near misses should undergo review • The guidance on the intranet, 'Instructions to use the Accident, Incident and Dangerous Occurrence Report Form HS1' should be reviewed and updated to include the current process. Checks need to be undertaken to ensure that all accident/injury reports have been captured within either the iTrent system or on the spreadsheet held by the Health and Safety team for the period between October 2019 and April 2020 • All documents relating to Health and Safety incidents should be accurately and securely filed and should be retained in line with data retention policies • The Health and Safety team should have systems/procedures in place to enable them to monitor and provide assurance on the level of compliance with display screen equipment and personal COVID risk assessments • Managers should be reminded of their responsibilities in completing all relevant risk assessments and keeping

Facilities Health and Safety improvements (Corporate Landlord)	Workforce Health and Safety improvements (Corporate Core)
• Arrangements for PAT testing should then be put in place to ensure that the Council are following statutory and best practice requirements. • The current contract for Portable Appliance Testing should be reviewed to determine if it is still appropriate for the current working arrangements, and if not, the contract should be re-tendered with a new agreement being in place from 1st March 2022	them up to date for all members of their service/team • A formal annual inspection plan for independent reviews should be put in place by the Health and Safety team to identify issues and provide assurance that Managers are complying and fulfilling their health and safety responsibilities. • A formal follow up process should be put in place to ensure that the weaknesses identified in the audit reviews are actioned by the Service Manager. • The health and safety reviews and outcomes should be reported to Senior Officers and committee Members • The Health and Safety guidance published on the intranet should be regularly reviewed to ensure all guidance is relevant and up to date. • Guidance should be re-circulated to staff • The Health and Safety team should take advantage of the e-learning modules available and consider if any modules should be mandatory for particular members of staff and/all members of staff (e.g. Health and Safety in the Workplace). • Key performance indicators should be introduced to monitor the uptake of health and safety modules • The Health and Safety team should undertake periodic assessments on the Health and Safety training undertaken by Managers across the Council and be able to provide assurance on the level of knowledge and understanding Managers have for Health and Safety responsibilities • Managers should be made aware and regularly reminded of their responsibilities to keep their knowledge up to date and retain a record of all Health and Safety training undertaken to demonstrate that they

Facilities Health and Safety improvements (Corporate Landlord)	Workforce Health and Safety improvements (Corporate Core)
	are up to date with current practices and responsibilities. • A training analysis should be undertaken to ensure that Managers/employees are receiving training appropriate to their role

Report to	**Audit Committee**
From	**Operations Department**
Risk Reference	**OPS/17**
Risk Description	**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 and high market rate.**
Recommendation	**For analysis and discussion**

Immediate Response & Assurance

The concern around the availability of HGV remains as a result of reduced availability of trained drivers, this is a National issue and many Local Authorities are experiencing the impact of these shortages.

In Bury we have reacted quickly to address the situation by securing the employment of additional HGV drivers in order to mitigate some of the risk.

We are also developing a programme for career progression initiatives in order to allow those who wish to do so to take the HGV training and progression route with financial support packages available for those who wish to do so.

This page is intentionally left blank

Risk Ref.	Risk Title	Strategic Outcome	Likelihood	Impact	Total Score = L*I	Likelihood	Impact	Total Score = L*I	Risk Owner	Key Potential Impacts	Current Controls	Dept. Risk Reg. Ref.	Planned Actions	Responsible Officer	Risk Action Status	Trend
CR1	**Financial Sustainability**	Economic Growth and Inclusion	4	4	16	3	3	9	S. Evans	• Significant deficit increase in Dedicated Schools Grant (DSG) potentially resulting in Department of Education warning and intervention and budget restrictions. • Public sector spending cuts/ rising inflation impacting ability to continue to deliver effective services. • Winter demands increasing pressure on ASC budgets.	• Medium Term Financial Strategy updated; monthly monitoring and DfE 'Safety Valve' deficit recovery agreement in place; escalation to Executive Team and Members. • Reserve Strategy and Financial Management and reporting refresh. • Budget Strategy Principles, regular monitoring of budget risk register.	FIN.1	• DfE Recovery Plan agreed; Transformation plan priorities agreed with key stakeholders; review of expenditure and rebaselining undertaken; Additional capital funding secured for in-borough provision. • Rebaseline of capital programme and closer working with directorates to identify potential pressures earlier in order to put mitigating actions into place. • Continuous refinement of MTFS and budget setting.	I. Booler/ S. Goodwin J. Bunn S. Evans	On target	Decreased
CR2	**COVID-19 Impact**	Strength-based Approach	4	4	16	4	3	12	P. Lakin	• New variants further impacting social mobility, lower earning income households and impeding economic recovery. • 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.	• Local Outbreak Plan and partnership working with CCG, AGMA; experience and planning for first outbreak and lockdown generating 'lessons learned' evaluation. Regular liaison with UKHSA; Vaccination Programme; Social Distancing including face covering guidance. Business Continuity Planning/Review/Update. Weekly Health Protection Board and fortnightly Gold meetings providing further assurance. • Current outsourcing of some rent reviews and lease renewals. • 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. • Quarterly Debtors meeting in place to review agreed payment plans and implement new payments plans appropriately.	OCO-AC.4 BGI-PAM.3	• Review current mitigating controls; follow PHE guidance; regular and prompt communication with staff and residents. Targeted comms and engagement to reduce inequalities in vaccine uptake • Continued outsourcing of some rent reviews and lease renewals. • Review of capacity and outsourcing arrangements. • Ongoing monitoring of income budgets with Finance. • Consideration to be given to allowing some business rent free periods in alignment with P26a Insolvency and Coronavirus Act 2000. • Awaiting outcomes of Government review into grants and rates relief previously provided to businesses, to identify potential fraudulent claims.	L. Jones L. Gudgeon	On target	Static
CR3	**Security & Resilience**	Delivering Together	3	5	15	2	5	10	K. Waterhouse	• Ongoing national threat from terrorism resulting in potential resurgence of terrorist activity and radicalisation of vulnerable members of community. • General threat to safety and security of Councillors. • External threat to data and systems potentially impacting system functionality/causing a data breach.	• Emergency response policies, Prevent initiative, GM Resilience Forum and Tension Monitoring Report. • Government guidance shared with parties currently exposed to such attacks. Local Government Assessment Toolkit implemented. • Training and updated Cyber Essentials Toolkit in place; PCN accreditation renewed annually.	CC-IT.4	• Continued early intervention work and community engagement through the Community Safety Partnership. • Democratic Services to undertake a security review regarding arrangements for Councillors. • Further training and investment in cyber security to be progressed against IG Action Plan timeframes; continued PSN accreditation; 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.	K. Waterhouse J. Dennis K. Waterhouse	On target	Increased
CR4	**Digital Transformation**	Delivering Together	4	4	16	2	4	8	K. Waterhouse	• Inability to achieve ambition for new ways of working, improved customer and staff experience through delivery of the Digital Strategy.	• Placement of Digital Strategy in Transformation programme to ensure visibility and deliverability; additional resource approved within the Transformation Strategy.	CC-IT.4	• Review of resources across Council and CCG IT/Digital functions.	K. Waterhouse	On target	Static
CR5	**Increasing demand pressures**	Economic Growth and Inclusion	3	5	15	2	4	8	G. Little	• Failure to meet Homelessness Statutory Function & Delivery. • Failure to transform services likely result in the Council failing to meet its statutory obligations. Adults and children's care facing a significant increase in demand for services.	• New Homelessness Strategy, increased statutory dispersed accommodation, development of private rented sector and landlord engagement. • Regular transformation programme review meetings, scrutiny of the Executive Committee and appropriate reporting to cabinet. • Fee setting exercise and cost of care comparisons carried out annually. Close working and relationship building 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.	CC-HSE.1 OCO-AC.2	• Development of regular monitoring framework and KPI review, new tenancy sustainment strategy to prevent homelessness and reduce cases in Bury. • Development of workforce strategy for the care sector.	P. Cole A.Crook	On target	Decreased
CR6	**Climate Change**	Local Neighbourhoods	4	4	16	3	4	12	D. Ball	• Inability to meet UK 2030 Emissions Target and Bury Climate Manifesto delayed due to coved, potentially impacting future funding.	• Greenhouse Gas Emissions Report produced Dec 2020; updating fleet for lower carbon emissions; recruitment to Climate Team Complete. • Climate Strategy and Action Plan approved by Cabinet in October 2021. Climate Action Board and forums under establishment. Climate Action Fund open for bids. Partnership work across GM / GM access to funding. • Public sector Decarbonisation Funding awarded to Bury.	OPS.8	• Continued partnership work across GM. • Public Sector Decarbonisation Funding to be spent by end March 2022. Climate Action Funding to be awarded and distributed by end March 2022. • First meeting of Climate Action Forums and Board to take place in Q3.	L. Swann	On target	Static
CR7	**ICS Implementation**	Strength-based Approach	4	5	20	2	4	8	W. Blandamer	• 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.	• Working with colleagues across the GM system to ensure the GM ICS operating model creates the conditions for our continued placed based transformation, and NCA footprint partners to continue to advocate for the place based approach; 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. • Response managed through Bury SILVER. • Issues and risks escalated to Integration Delivery Collaboration.	OCO-AC.2	• Transformation plans will continue to be monitored monthly through IDC Board. • Transformation Board and Adult Social Care Savings and Transformation Programme. • Bespoke communication approach to address this agenda; continued work with GM partners.	W. Blandamer	On target	Decreased
CR8	**Elections**	Delivering Together	3	3	9	1	5	5	J. Dennis	• Potential legal challenge and reputational damage if the Council is unable to effectively deliver the May 2022 Elections. • Personal liabilities to the Returning Officer.	• Election planning to commence early. • Review of polling stations and regular reports submitted to member Group. • Oversight by the Director of Law and Governance. • Legislative changes reviewed regularly to assess impact on Bury.	CC-ELC.1 CC-ELC.2	• Regular planning meeting from December 2021 to commence election planning. • Enhanced training to staff members on grass skirt count method. • Improved communication with candidates and agents. Review of polling boundaries and stations following outcome of the Local Government Boundary Commission review. • Separate issues log to track concerns as they arise. • Risk assessments of polling station to commence December 2021. • Risk assessments of polling station to commence December 2021.	Elections Manager	On target	Decreased
CR9	**Workforce Capability and Capability to Deliver**	Economic Growth and Inclusion	4	5	20	2	5	10	L. Ridsdale	• Workforce capability and capacity insufficient to deliver Council's priorities, including Corporate Plan and Let's Do It priorities and the required Budget savings.	• Prioritisation through the Corporate Plan resulting in investment in additional capacity in key areas and development of Apprenticeship strategy; policies review; improved utilisation of iTrent programme. • Transformation strategy, including agreed areas for additional investment.	CC-HR.2 CC-HR.8	• Continued prioritisation. • Delivery of transformation (Let's Do it Well) work including leadership and a management training and process simplification and improvement. • Focused work on behaviours, values and culture.	S. McVaigh	On target	Decreased
CR10	**EU Exit Impacts**	Economic Growth and Inclusion	5	3	15	4	2	8	S. Evans	• Inflation: increased inflationary pressures as a consequence of Brexit and recovery from the pandemic. • Disruption to supply chains. • Loss of EU funding may, if not replaced by Government, pose a risk to economic and social programmes of the Council. • National immigrations policies restricting free movement of people could lead to further skills gaps in the workforce.	• 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. • Complete review of all budgets with a view to a zero based budgeting approach.	FIN.5	• Continuous refinement of MTFS and budget setting as more information becomes available; engagement with and identification of efficiencies with all departments. • Piloting the use of grant finder software to ensure all potential grants to the borough are accessed where appropriate. • Use of Kickstart, apprentices and training of existing workforce to ensure a workforce which meets both current and future needs.	S. Evans	On target	Decreased
CR11	**Asset Management (Operational Health and Safety)**	Local Neighbourhoods	5	5	25	3	5	15	D. Ball	• Breach of Health and Safety legislation leading to prosecution under the Corporate Manslaughter Act and other Health and Safety Regulations. • Council buildings, facilities and premises must provide safe and effective environments for all building occupants that use them.	• Recruitment to Head of Corporate Landlord. • Corporate Health and Safety independent audit undertaken with formal report, findings and recommendations. • Establishment of Estates Transformation Board. • Establishment of a "Taskforce" to oversee delivery against internal audit recommendations implemented through an improvement plan.	CC-H&S.1	• Corporate Landlord function to be established under leadership of the Operations Department dependant on Executive Management team approving 5 year business case and budget. • Strengthen Trade Union (TU) role in managing health and safety responsibilities including TU Safety Reps and establishment of joint health and safety committee. • Performance reports to be produced to report on health and safety; incidents and accidents; and resultant improvement actions. • Accelerated disposals programme to be initiated under the Estates Transformation Project.	D. Ball/ C. Beadsworth	On target	Static
CR12	**Children's Social Care Services**	Economic Growth and Inclusion	4	5	20	2	5	10	I. Booler	• Children left in harmful situations and risk. • High case loads potentially leading to social worker high turnover which then impacts on children, families and partners. • A poor Ofsted judgement can lead to further high staff turnover from senior leaders through to frontline staff, making it difficult to do what is most important - turning around services for children, young people and families in need.	• CYP Improvement Plan. • Development of leadership delivery plan and independently chaired Delivery Board in place from September; LGA review given clear diagnostic; interim leadership in place with increased visibility in workforce. • Ofsted inspection taking place 25th - 29th October 2021. Outcome will drive further actions/ assurances. Project team in court team has reduced case loads and improved the quality of planning	CC-CYP.2	• Strengthen the Delivery Plan to ensure focus on recruitment and retention and ensuring increased stability in the workforce. • Strengthen QA processes to ensure audits lead to improved practice. • Engage a managed service for Child in Need cases from 8th November to immediately impact on reducing social worker caseloads across the service	S. Bruce	On target	Decreased
CR13	**Regulatory Compliance**	Delivering Together	4	5	20	3	4	12	J. Dennis	• Failure to meet the requirements of data protection legislation and good information governance practice / serious data breach.	• IG strategy developed and resources identified. Appropriate policies and procedures in place compliant to current legislation; DSPT 2020/21 submission; UK GDPR training.	CC-DS.1	• IG processes to be mapped; Internal Audit review subject to risk assessment; Comprehensive IG/Cyber Security training programme to be implemented; IG policies and Procedures to be reviewed; DPST 2020/21 requirements to be assessed.	M. Connor	Some slippage	Decreased
CR14	**Corporate Health & Safety**	Economic Growth and Inclusion	4	5	20	2	4	8	S. McVaigh	• Injury and absence for staff members. • Lack of compliance with legislative or regulatory requirements leading to legal action and potentially reputational and financial consequences. • Sickness absence impacting on service delivery.	• Corporate Health & Safety Advisory Team moved under the leadership of the Director of People & Inclusion. • Health & Safety Policies including arrangements for agile workers, mandatory training for all staff. • Employee assistance programme in place which incorporates mental well-being support. • Comprehensive suite of guidance.		• Review of team structure. • Refreshed governance arrangements for health and safety. • Renewed staff training and communications plan. • Renewed reporting and incident management arrangements.	S. McVaigh	On target	Decreased
CR15	**Regeneration & Development**	Local Neighbourhoods	3	5	15	1	5	5	P. Lakin	• Northern Gateway - failure to grasp opportunity presented by the largest regeneration project to impact this part of the country. • Challenges faced in driving inclusive growth within the region, impacted by a slow housing market and accessing up to date planning policies. • Rising construction inflation and interest rate shifts increasing cost of delivering town centre regeneration and housing programmes.	• Active engagement with political advocacy and links to Communications Strategy. • Progression of Development Plan through to examination.		• Continue to explore funding opportunities. • Consider and respond to consultation submissions through the Examination process.	C. Logue	On target	Static
CR16	**Special Educational Needs and Disabilities**	Economic Growth and Inclusion	4	5	20	2	5	10	I. Booler	• Increase in SEND tribunals. • Further increase in LGO ombudsman complaints. • Further loss of parental trust • Poor compliance in regard to 20 week • Review targets not met • Statutory deficit reduction targets not met impacting of the success of Project Safety Valve.	• SEND Assurance Board and plan. • Ameo/future Gov project support around transformation and delivery plan. • Recruitment plan. • Co-production with strategic partner Bury2gether. • Increased capacity in EHCP team.		• Further recruitment within SEND at a strategy level. • Over establishment of posts in Statutory assessment team to focus on historic backlog. • Co-produce and pilot work around EHCP processes bringing parents earlier in the process. • Workstreams with schools on both finance and broader inclusion. • Focussed work on graduated response across Bury to improve consistency of identification.	Director of Education	On target	Static
CR17	**Technical and Legal Compliance with Employment Law and Council Policy Framework**	Strength-based Approach	3	4	12	2	4	8	S. McVaigh	• Breakdown in employee relations, legal challenge with reputational or financial impacts.	• Improvement programme driven through the Transformation Strategy. • Additional investment in key areas. • iTrent improvement programme. • Strong TU relationships.	CC-HR.3 CC-HR.4 CC-HR.9	• Delivery of improvement work. • Review of HR structure. • Pay review as part of 'Let's Do it Well' Transformation Programme.	S. McVaigh	On target	Decreased

This page is intentionally left blank

Risk Mechanism

Master Risk Register

* Collection of departmental/operational risks.
* Risks due for review in the assigned month are assessed and appropriately updated at departmental meetings.

Red Risk Register

* Collection of departmental/operational risks rated 15+ ("red risks".
* Reviewed bi-monthly by Executive Committee.

Risk Senior Leadership Group (RSLG)

* Directors/ Assistant Directors:
  - representative from each department
  - with oversight of operational/departmental risks may discuss updates to Corporate Risk Register on a quarterly basis
  - will propose escalation of departmental risks onto Corporate Risk Register.

* Business Support:
  - notes outcomes and updates relevant fields on Corporate Risk Register following conventions implemented
  - reports Group's findings upwards to Exec Committee
  - reports Exec's findings downwards to RSLG.

Corporate Risk Register

* Collection of principle/strategic risks with the potential to disrupt the Council's ability to deliver its objectives.

* Risks identified during a "developmental meeting" and to remain on the Corporate Risk Register until such time as can be adequately mitigated before closure and de-escalation to the departmental risk register.
  - the Register is a live document where new risks are introduced or escalated from the departmental risk register, as they arise during the course of the financial year.

* 'Risk Senior Leadership Group' review Corporate Risk Register on a quarterly basis and present to the Executive three weeks prior to Audit Committee papers deadline.

* The Executive will review the Corporate Risk Register - approve for submission to Audit Committee for further scrutiny and "deep dive" selections made for the next Audit Committee meeting.

This page is intentionally left blank

Agenda Item 7

Classification Open	Item No.

Meeting:	Audit Committee
Meeting date:	25 November 2021
Title of report:	Information Governance – Update Q3, 2021/22 to date
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 Q2 update on IG activity and approved the Information Governance Framework through which these functions are discharged within the Council.

During Q3 to date the Council has continued to progress in responding to the Information Commissioner's Officer's (ICO's) recommendations. This report provides an update on progress against the Information Governance workplan for Quarter 3 to date.

Prior to the ICO's visit, a review of the Council's position in relation to IG was undertaken by the Council's Internal Audit. The key recommendations of their report were similar to those made by the ICO. A review of progress against all the recommendations from Internal Audit are also shown.

Key considerations

1.0 Introduction

1.1 This report is the update on Information Governance work completed to date in Quarter 3 of 2021/22.

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.

2.5 Since the provision of the ICO's report, Bury Council has developed a detailed workplan to respond to the issues raised. Progress against the items in the workplan is detailed below.

3.0 Improvement Plan

3.1 The ICO made 79 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

3.2 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 initially planned is as follows:

By end August	• Resolve Legitimate Interest Assessment – HR • ROPA refreshed • Review responsibilities/resources for IG • Refresh & re-establish network of 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 Information Security (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 Key Performance Indicators (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, including port controls designed within Enterprise Agreement • Establish end use asset register • 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

4.0 Information Governance Update 2021/22 Quarter 3 to date

4.1 The following updates are provided against activity which is scheduled for completion at this point within the overall work programme:

- Resolve Legitimate Interest Assessment – HR
  - Complete: The assessment concluded a legally acceptable basis on which employee personal information is processed and stored, as HR's activities do not override individual rights.

- ROPA refreshed
  - Completed by all departments. Follow up meetings with individual managers / services are currently being held to review the ROPA responses provided, and subsequently to make any further updates and additions. Plan to be developed for spot checks to take place on regular basis.

- Review responsibilities/resources for IG
  - Complete. Dedicated Information Governance Manager and Data Protection Officer post created and filled. Additional project resource in place to deliver the improvement plan on a fixed term basis

- Refresh & re-establish network IG Champions
  - Complete. Nominations received from teams and services, with 14 volunteers obtained to date. Gaps identified will be filled by line managers. Initial meeting of the Champions to be arranged for start of December to highlight role and expectations.

- Risk management strategy approved
  - Complete. An IG Risk Register has been developed. This will ensure that all areas of concern or risk relating to IG matters will be monitored and addressed in a timely manner. This document will also be reported to the IGSG on a monthly basis.

- Individual rights policy & procedure drafted
  - At final draft stage subject to review from Head of Legal Services.

- IG Policies updated to reflect GDPR
  - The following policies and procedures have all been revised and are at final draft stage subject to review by Head of Legal Services:

    - FOI and EIR Policy
    - FOI and EIR Public Interest Test (PIT)
    - Bury Privacy Notice Template.
    - Data Subject Rights.
    - Bury IG Complaints Procedure.
    - Data Quality Policy.
  - All remaining policies and procedures will be completed by end of November for review by Head of Legal Services:
    - Appropriate Policy Processing Special Category Data
    - Anonymisation and Pseudonymisation Policy
    - Information Asset Owner and Information Asset Administrator Responsibilities

- Induction updated & systems access only granted once e-learning complete
  - Complete. Onboarding processes revised to ensure ICT access only granted once IG e-learning complete. Learning to be completed within first 5 days of commencement of employment.

- Contracts reviewed re data processing
  - Ongoing. A spot-check review of existing contracts valued at under £75,000 is being undertaken in collaboration with Procurement. These have been identified to pose the highest risk of non-compliance to data protection legislation, as those at a greater value must undergo a robust process before engagement. A Data Processing Agreement containing appropriate IG clauses has been drafted by Legal and approved for appending to existing contracts as required.

- DPIA screening checklist, full assessment template and log established
  - Policy and template reviewed and awaiting approval from Legal. Log to be established by end of November.

- Resolve Information Security (IS) responsibilities within ICT
  - IS policies to be reviewed with all IG policies by the end of November. This will highlight any issues for clarification.

- Update agile policy re information security
  - To be reviewed with other IG related policies by end of November.

- PEN test and review PSN requirements
  - Ongoing. Timetable revised to test in December to align with activities in ICT calendar. External element of the PEN test (a simulated and authorised cyberattack on a computer system to evaluate the security of the system) due to complete November. Internal tests to commence and complete December.

- Update personal breach policy
  - At final draft stage subject to review from Head of Legal Services.

- Policy document template & schedule approved, including Information Security
  - Complete. Template applied to all policies in development

- Policy availability to non-front-line staff addressed
  - All staff will have a Council email by the new financial year; policy access will be available from that time. All policies will be made available for staff / customers via the intranet / internet once approved.

- IG KPIs reviewed
  - Complete. Corporate Plan PIs have been updated to include a number of complaints and data breaches. Information reported on FOIs and SARs completed in time are reported against the Business Excellence Transformation theme in the first performance report against the Bury Council and CCG integrated Corporate Plan, Quarter 3, 2020/21. Performance against indicators to be reported to Information Governance Steering Group monthly, and Audit Committee on a quarterly basis.
  - Suite to be strengthened after review of best practice in other organisations.

- Information Asset Register (IAR) to be reviewed following ROPA refresh
  - Completion of IAR moved to December on completion of ROPA follow up meetings, when full picture of all assets will be known.

- ROPA review process agreed
  - Programme of spot-checks to be developed on completion of all ROPA-related work. A rolling review of ROPA entries will be introduced. With regular updates to each meeting of the Information Governance Steering Group. Additional column added to ROPA spreadsheet to include details of any associated contracts.

- Privacy notice log established
  - Complete. Privacy notices included in ROPA.

- FOIA policy and procedure updated
  - At final draft stage subject to review from Head of Legal Services.

- Review GDPR e-learning module
  - 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.
  - New Data Breach module and test developed internally.
  - New suite of training developed to cover the issues raised by the ICO. This now includes courses of GDPR, FOI, Cyber Security, and Data

Breach process, together with overall Quiz developed.
    - Overall pass mark of 80% required for all staff.
    - Currently being reviewed prior to wider launch.
    - Launch will focus on new starters and those who have not yet completed training.
    - Approximately one month before twelve months expire since last completion of training, reminders will be sent to all staff. This is likely to be May 2022 and linked to suggested IG awareness month of communications.

- Update Information Security policy in full, including port controls designed within Enterprise Agreement
    - Information Security Policies currently being reviewed as part of IG Policy review. Due to complete by November, to then be reviewed by Head of Legal Services.

- Establish end use asset register
    - To be developed following review of IS policies and linked to ROPA due to complete December.

- Specialist role training delivered to IG leadership roles
    - SIRO training complete. Training for IG Manager to be developed and arranged. Further training programmes for senior Council officers to be identified and developed.

- Internal audit plan
    - Recommendations incorporated into IG Workplan.
    - Details of actions taken and tasks completed detailed in section 4.3 below.

4.2 Managing Data Breaches

In addition to the scheduled work plan, Data Breach monitoring and review has increased, with increased challenge to remedial actions taken by teams coming from the Information Governance Team and DPO.

A presentation on preventing and reporting data breaches has been developed and offered to all teams within the Council. A high level of take up has been achieved, with particular interest coming from nearly all teams who have recently reported a data breach.

A new training model on Data Breaches and overall Information Security Quiz, requiring an 80% pass rate, has been developed and is undergoing final amendments and testing before formal launching of the new IG E-learning Suite.

All officers making a data breach will be required to repeat the Council's training module, and will receive a letter from the Data Protection Officer to make them aware of the severity of breach and the risks to the Council and themselves; they will also meet with their Executive Director to discuss the matter and identify any further support which they might require.

4.3 Response to Internal Audit recommendations

The overall findings of the Internal Audit rated the Council as 'Moderate Risk' with respect to its approach to IG. However, 15 recommendations were identified needing 'Significant' attention, with a further 9 that were deemed to 'Merit Attention'. The key risks are shown (in bold) below, along with the specific recommendations made where action needs to be taken and the Council's current response:

1. **Risk GDPR Legislation is not complied with and the Council may be subjected to financial penalties. The Council does not control the information it holds.**

1.1 All departments should be required to update and confirm the accuracy of the ROPA (Significant)
- Complete. All departments have provided updates for the ROPA. These are currently being individually reviewed with members of the IG Team.

1.2 All departments should be required to confirm that privacy notices are in place for all systems that process personal data (Significant)
- Complete. This information is included in the ROPA.

1.3 Personal data audits should be undertaken across all services to clarify all data flows. (Significant)
- To commence on completion of all ROPA follow up meetings.

1.4 There should be a corporate approach to the management of ongoing consent to provide assurance to the Council that information held is permitted, accurate and up to date. It should be established if individual system owners have any processes in place for managing ongoing consent, the processes should be review and checked to ensure they comply with guidance. Additionally, it should be established whether Department / Systems Owners maintain records of requests to dispose of personal data and if so if these requests are held securely and have been actioned in a secure manner. (Merits Attention)
- To be addressed on completion of the IG / IS policy review.

1.5 The Council should undertake the three-part test to demonstrate it has fully considered and protected individuals rights and interests. (Merits Attention)
- To be developed as part of the IG / IS policy review.

1.6 Procedures should be introduced to ensure that the records retention schedules in each department are reviewed and updated periodically.

(Merits Attention)
- To be developed on completion of the follow up ROPA activity.

1.7 In the event of staff returning to work in the administrative buildings, management should consider introducing cross shredders across the council to enable the prompt disposal of confidential waste. Guidance also needs to be issued to staff working at home on sage disposal procedures for confidential waste. This should be incorporated into corporate homes working policies and procedures. In additional, all Council officers should be encouraging to reduce the use of paper documents. (Merits Attention)
- To be incorporated into the IG / IS policy review.
- Walk round of offices to be carried out on a routine basis to ensure compliance.
- Weekly comms to remind staff in offices and agile working of the need to dispose of documents appropriately.

2. **Individuals' Rights are Not considered in process activities**.

2.1 The individual system privacy notices should be reviewed to ensure that they are consistent and provide all the information as required by the GDPR legislation (Significant)
- Complete. Record of privacy notices included in the ROPA.

2.2 A Corporate approach to handling SARS / FOIs should be introduced and implemented as soon as possible. Staff undertaking enquiries to address SAR / FOI requests should be provided with training to ensure that all requests are dealt with appropriately and in a consistent manner, with Senior Management being required to sign off responses before they are issues (Significant)
- Process to be included as part of the IG policy review.

3. **The Council has no governance arrangement for ensuring data is protected**.

3.1 The Communities and Wellbeing (NB no longer exists) and Corporate Core departments should ensure there is appropriate representation on the IG group. The group meeting should be resurrected to ensure that the profiles of GDPR is still high on the agenda and to ensure that compliance with GDPR legislation continues to be addressed. (Significant)
- Complete. IG Steering Group contains representation from all departments.
- IG Champions network being established to ensure involvement and ownership at all levels of the organisation.

3.2 Clearly defined roles and responsibilities need to be established for the on-going management of GDPR. Once these are established, this information should be disseminated to Business Managers and staff. (Significant)
- Complete. SIRO and IG Manager / DPO identified. Support from key

senior managers identified via the IG Steering Group.

3.3 The IG Group should be encouraged to develop its protocols to ensure that information is effectively disseminated to business managers across the council. (Significant)
- Complete – IG Steering Group to own all IG related tasks.
- Complete – weekly IG communications issued to all staff.
- IG Champions network being established.

3.4a Consideration should be given to mandating a clear desk / clear wall policy in all administrative buildings to ensure that all business sensitive / personal information is not left in a place where the information could be compromised. Guidance needs to be developed for all staff working at home to ensure that Council data is kept secure. (Significant)
- To be developed as part of policy review.
- Message to be cascaded via weekly IG Communications.
- Walk-rounds of offices to commence on approval of policies.

3.4b All staff who work in the administrative buildings should be reminded on the need to maintain security regarding data and should be encouraged to challenge anyone that is not wearing an ID badge and / or acting in a suspicious manner. (Significant)
- Reminder to be included in weekly IG Communications.

3.4 The latest version of the Data Protection Policy should be published on the intranet / internet, so it is available to staff / public. (Merits Attention)
- To be completed on formal approval of revised policies.

3.5 GDPR compliance checks should be undertaken on a period basis to ensure compliance is maintained. Consideration also needs to be given to how compliance will be maintained with staff working from home on a permanent basis. (Merits Attention)
- To be developed in New Year on completion of policies review.

4. **Staff have not received training on GDPR and are not following the principles**.

4.1 Managers should be reminded of the need for all members of staff to complete the GDPR online training module and a date for all staff should be set. (Significant)
- Complete. During Summer 2021, all staff required to repeat training.
- Annual reminder to be issued by IG Manager.
- Process being finalised for all new starters to complete training within first 5 days of employment to obtain access to systems.

5. **The Council does not have contracts in place with data processors and is unaware how Council information will be handled by 3rd parties.**

5.1 System owners should be reminded of the need to ensure that there are written agreements in place for all data that is processed by outside parties (Significant)

- Ongoing. Spot-check review of existing contracts valued at under £75,000 is being undertaken in collaboration with Procurement. These have been identified to pose the highest risk of non-compliance to data protection legislation, as those at a greater value must undergo a robust process before engagement. A Data Processing Agreement containing appropriate IG clauses has been drafted by Legal and approved for appending to existing contracts as required.

5.2 The Council should review its Project Initiation Document to ensure that appropriate DP measures are incorporated into any system developments (Merits Attention)

- Complete. All policies now use this format.

6. **Data Protection privacy impact assessments are not undertaken**.

6.1 All system owners should be required to complete a Data Protection Impact Assessment to provide assurance to the Council that all risks have been identified. (Significant)

- Complete. Part of ROPA.

7. **Data Security, International Transfers and Breaches**

7.1 The Council's ICT Security should be reviewed and updated to reflect the current GDPR / DP legislation. The revised document should be circulated so all staff are again made aware of GDPR requirements. (Significant)

- To be included in review of all IG / IS policies. Due for completion end of November.

7.2 All staff should be reminded that confidential data should not be sent outside the council IT network to personal email accounts. Management should consider further compliance checks to ensure that personal data is not being sent to employees' personal email accounts. (Significant)

- Complete. Weekly IG Communications informed all staff of need to use Egress system when sending personal data outside the organisation.

7.3 The Paper Records and Data handline and Transit policy should be reviewed, and all staff should be encouraged to work in a paperless environment. The policy will need to be updated to reflect the arrangement for staff working from home. The policy should then be relaunched to all staff. (Significant)

- Included in review of all IG / IS policies.

7.4 The personal Data Breach Reporting Policy should be updated with the current DP Lead's contact information. In addition, the record of all data breaches should be forwarded to Internal Audit for review (Merits Attention)

- Complete. Awaiting input from Head of Legal Services and formal approval.

5 Recommendations

5.1 The Audit Committee is required to note the 2021/22 Quarter 3 Update provided.

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 UK General Data Protection Regulations (GDPR) 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:

Report to Audit Committee - Information Governance – ICO Update & Q2 delivery Update – 30 September 2021

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
FOIA	Freedom of Information Act 2000
GDPR	General Data Protection Regulations 2018
IAM	Information Asset Manager
IAO	Information Asset Owner
IAR	Information Asset Registers
ICO	Information Commissioner's Office
ICT	Information Communication and Technology
IG	Information Governance
IGSG	Information Governance Steering Group
IS	Information Security
NHS	National Health Service
PSN	Public Services Network

ROPA	Record of Processing activity
SAR	Subject Access Request
SIRO	Senior Information Risk Officer

This page is intentionally left blank

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.

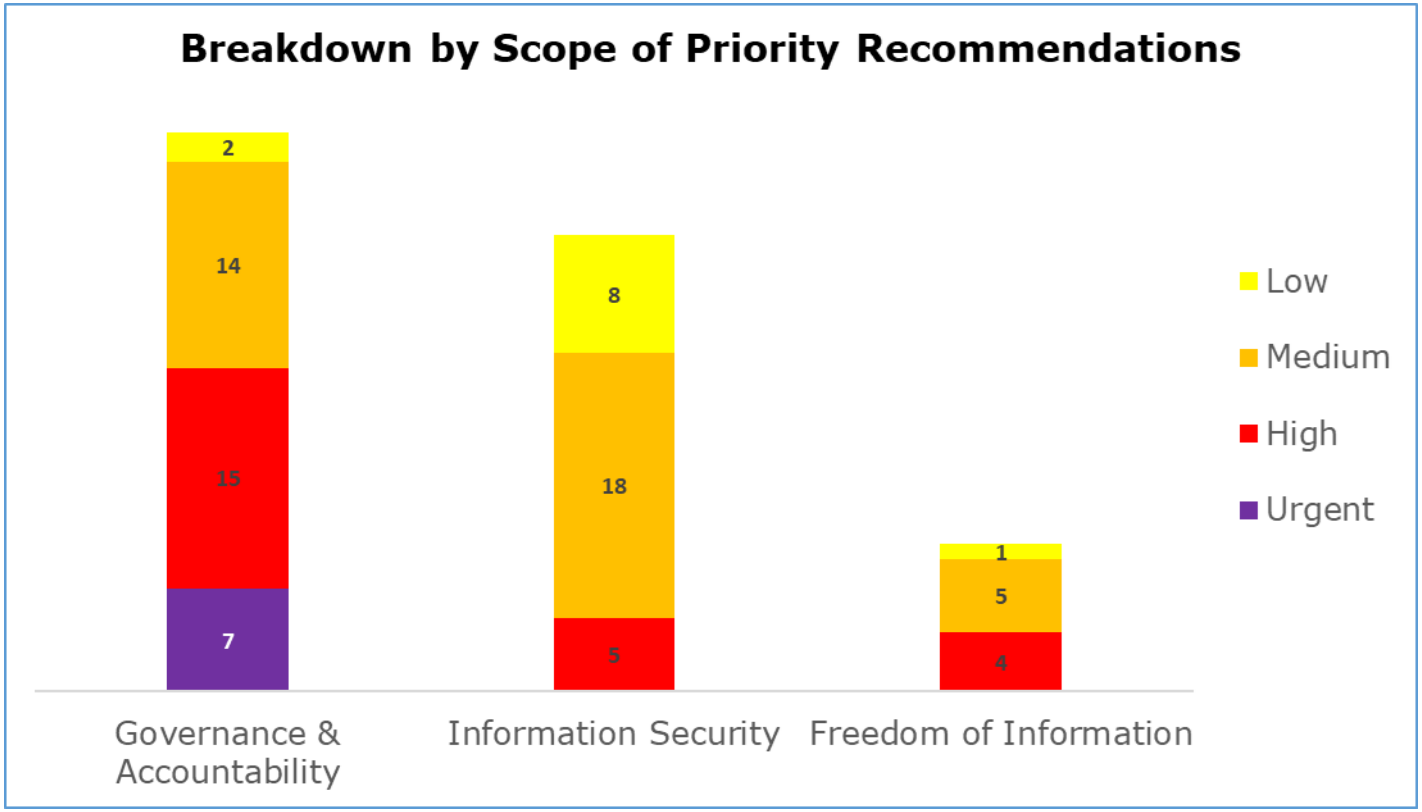
Audit Summary

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.

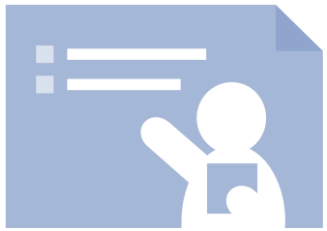
Best Practice

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

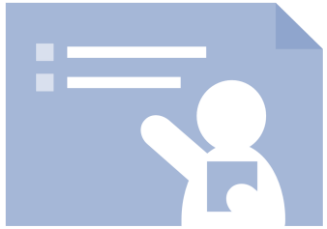
The tables below list observations made by ICO auditors during the course of the audit along with suggestions to assist BMBC with possible changes.

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.

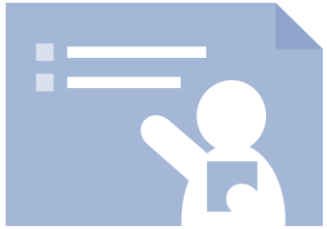
Appendices



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

Agenda Item 8

Classification Open	Item No.

Meeting:	**AUDIT COMMITTEE**
Meeting date:	**25th November 2021**
Title of report:	**Grant Support in Response to Covid**
Report by:	**Leader of the Council and Cabinet Member for Finance and Growth**
Decision Type:	**Non- Key Decision**
Ward(s) to which report relates	**All**

1 Introduction

1.1 In response to the Covid pandemic, the government has made available grants to local authorities both to support them with managing the costs and loss of income resulting from the pandemic and also to support businesses and other key sectors affected by the pandemic as well as individuals suffering from hardship.

1.2 This report sets out the position in relation to the grants received in 2020/21 and 2021/22 and where they have been utilised.

1.3 The final section of this report responds to outstanding questions tabled at the previous Overview and Scrutiny Committee

2 Background

2.1 Bury Council has received a number of grants since the pandemic and a full breakdown is attached in Appendix 1. As the pandemic continues across the period 2020/21 -2021/22 the government has announced new grant funding streams in recognition of the ongoing pressures on councils and to also fund new requirements. This means that the position on grants continues to change and is likely to for the remainder of the current financial year. As of October 22, 2021, the Council has received grant support in response to Covid totalling £151.949m.

2.2 A summary of Bury's Covid grant support for 2020/21 and 2021/22 is set out in Chart 1 and Chart 2 respectively. The largest area of Covid support in 2020/21 was Support to Business which accounted for 64% of the 2020/21 grant support . It is worth noting that there has been no further funding to support businesses in 2021/22 as all of the funding was received in 2020/21 in order to aid cashflow and to support getting monies out to businesses quickly. In 2021/22 the largest areas of support was un-ringfenced grant funding and Welfare which accounted for 26% and 25% respectively

Chart 1 – Analysis of Covid Grants Received 2020/21

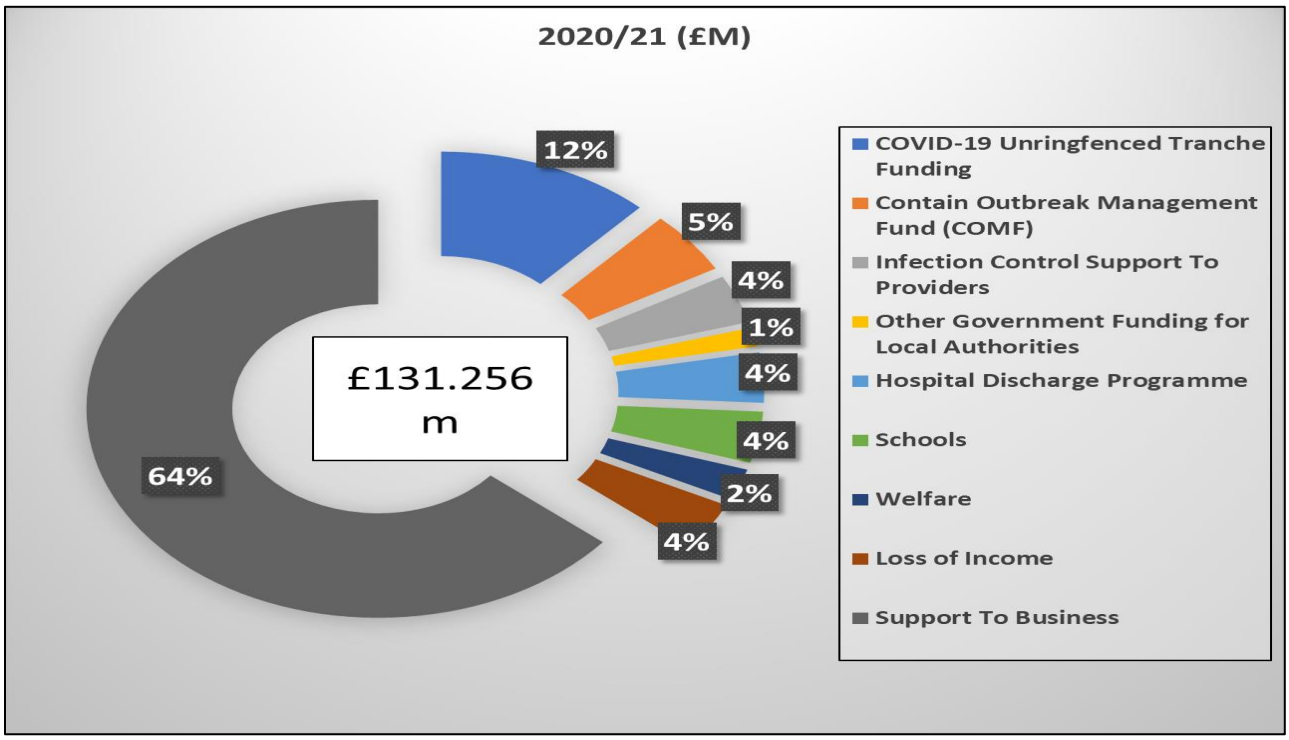
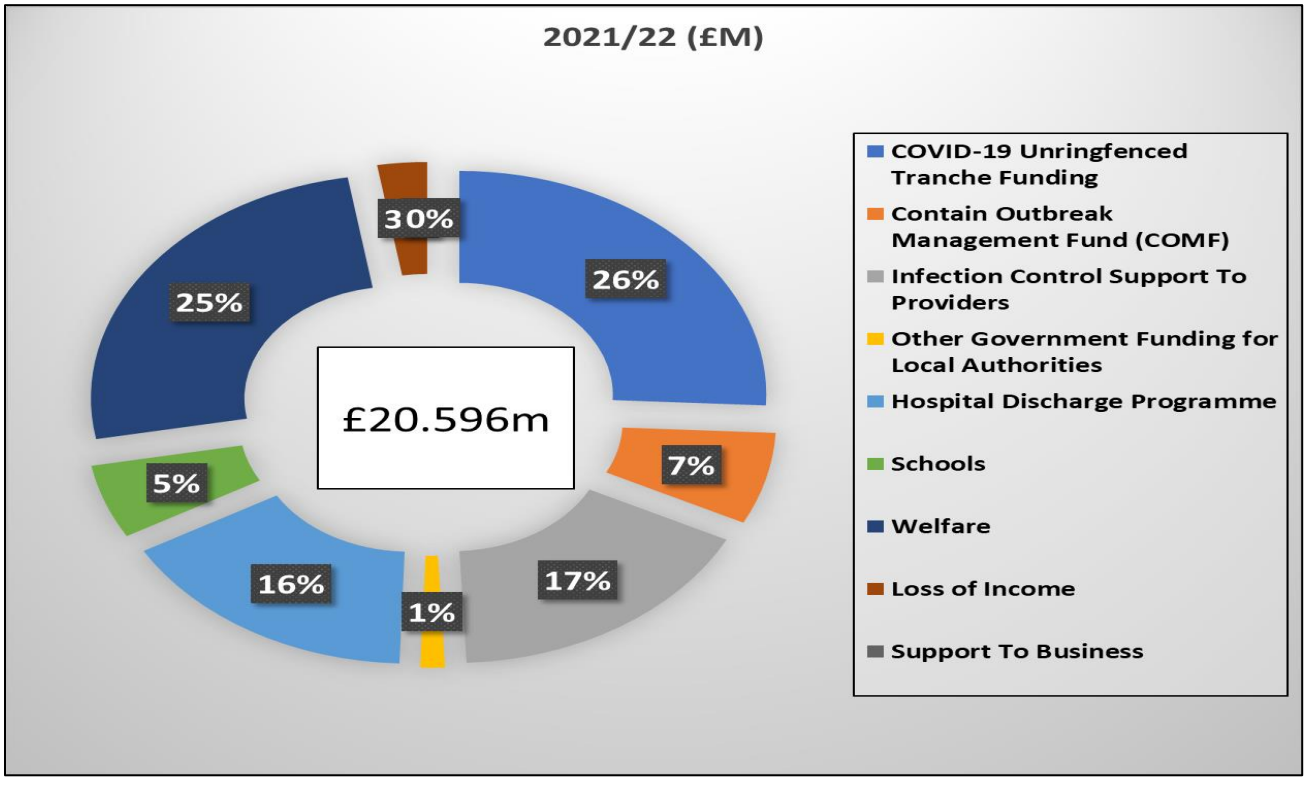


Chart 2 – Analysis of Covid Grants Received 2021/22



2.3 Table 1 shows that of the £151.949m received, a total of £144.303m (95%) has been spent or committed leaving an uncommitted grant allocation of £7.646m. The Council are now working with the government around reconciliation of the grants paid out and at the end of reconciliation any uncommitted amounts will be returned to the Government.

Table 1

Covid-19 Funding Type	2020/21 (£M)	2021/22 (£M)	Total (£M)	Spent / Committed (£M)	Uncommitted (£M)
COVID-19 Unringfenced Tranche Funding	15.640	5.330	20.970	20.970	0.000
Contain Outbreak Management Fund (COMF)	6.387	1.376	7.763	7.763	0.000
Infection Control Support To Providers	4.922	3.487	8.408	8.408	0.000
Other Government Funding for Local Authorities	1.925	0.266	2.191	2.191	0.000
Hospital Discharge Programme	5.100	3.348	8.448	8.448	0.000
Schools	5.213	1.107	6.320	6.320	0.000
Welfare	3.183	5.238	8.421	8.421	0.000
Loss of Income	4.897	0.541	5.438	5.438	0.000
Support To Business	83.989	0.000	83.989	76.343	7.646
Total	131.256	20.693	151.949	144.303	7.646

3. Covid-19 Funding Type

3.1 COVID-19 Un-ringfenced Tranche Funding

3.1.1 To date £20.970m of one off (non-recurrent) un-ringfenced Covid grant has been built into the overall funding of the Council's 2020/21 and 2021/22 revenue budget and as such is fully committed to support council services.

3.1.2 The below identifies where the Council has allocated this funding to support key services which were impacted by the pandemic either as a consequence of additional support to residents or to support the consequential impact on expenditure.

3.1.3 In 2020/21 the un-ringfenced Covid Expenditure was spent as follows:

- Business Growth & Infrastructure - £0.166m
- Children & Young People -£2.136m
- Operations - £7.324m
- Levy Equalisation -£7.102m

Total -£16.728m

Note: This will be partially offset by council income losses related to covid

3.1.4 In 2021/22 the un-ringfenced Covid Expenditure was spent as follows:

- One Commissioning Organisation - £5.102m
- Business Growth & Infrastructure - £0.150m
- Children & Young People -£ 0.078m

Total -£5.330m

3.2 Contain Outbreak Management Fund (COMF)

3.2.1 The Contain Outbreak Management Fund (COMF) provides local authorities (LAs) with financial support to be used for test, trace and contain activity. The specific public health activities that can be funded from the COMF are left to the judgement of LAs in conjunction with their Directors of Public Health.

3.2.2 Bury Councils COMF resource is £7.763m and is fully committed against a cross-directorate expenditure plan. There is specific criteria against which COMF monies can be spent. These are:

- PH interventions.
- Infection control.
- Supporting the vulnerable.

3.3 Infection Control Support to Providers

3.3.1 Bury council has received £8.408m in total to support providers of care to reduce the transmission of COVID-19 in care settings, minimising infection and keeping staff and residents safe.

3.4 Other Government Funding for Local Authorities

3.4.1 Other Covid government funding is currently £2.191m and are those Covid grants that don't fit into the specific covid grant types set out in Table 1. The £2.094m is summarised in Table 2 below.

Table 2

Description	2020/21	2021/22	Total
ASC Workforce Capacity Fund	**0.408**	**0.000**	**0.408**
Clinically Extremely Vulnerable Support Funding	**0.689**	**0.000**	**0.689**
Community Champions Fund	**0.467**	**0.000**	**0.467**
Compliance and Enforcement Grant	**0.104**	**0.000**	**0.104**
Welcome Back Fund (formerly Reopening High Streets Fund)	**0.169**	**0.169**	**0.338**
Provisional Rough Sleeping Emergency Funding	**0.002**	**0.000**	**0.002**
Next Steps Accommodation Programme	**0.081**	**0.000**	**0.081**
Additional Funding for Local Elections	**0.000**	**0.097**	**0.097**
National Leisure Recovery Fund	**0.004**	**0.000**	**0.004**
Total	**1.925**	**0.266**	**2.191**

3.4.2 Members have previously asked for further information on the use of the Community Champions funding. Please see below a brief analysis of what this funding was used for.

- Community Engagement Champions, one for each neighbourhood as part of new Community Hub structure on a 12 month basis to:
    - Identify and connect with each neighbourhood and across other hubs to ensure communities of interest are understood and represented.
    - Feed in local viewpoints, issues and opportunities to the Communications Team and wider leadership and inform the development of the community connector role design and skills profile.
    - Support the wider community network.
    - Co-ordinate wider community engagement.
    - Close gaps in community relationships and network.

- Engagement with existing community groups to strengthen awareness and use of connections and engagement channels with particular communities of interest or experience, including faith and race networks. This was to allow cascade of Covid19 information (including on testing, self-isolation and vaccination) to communities who might not ordinarily engage through mainstream communication.

- Commission to better understand our communities in a more granular and timely fashion through quantitative and qualitative social research. This included mapping of community characteristics, key focal points within neighbourhoods, insight on where communities are an outlier, changing trends within communities and exploring the variety of means with which to engage with new, emerging and future champions from each community.

3.4.3 The previous report identified the compliance and enforcement grant as COVID marshals. The information below details the remit of this work:

- Promoting social distancing and encouraging public compliance with COVID-19 public health measures.
- Educating and explaining COVID-19 Secure guidelines in the public realm and for business premises.
- Identifying and supporting businesses and premises not following guidelines, escalating as appropriate.
- Encouraging the wearing of face coverings

3.4.4 Please also see below further information on the spend in relation to delivering the elections.

- Printing - Postal Vote (25% increase predicted)
  Polling Stations - Additional Portacabin hire and land rental costs for portacabins
- Personal Protective Equipment - Equipment for making polling stations safe and additional stationery costs

- Count - Increased count costs .Increased postal vote costs (more expected). Extra space due to social distancing, additional table and chair hire for social distanced count.
  Staffing- Increased number of reserve staff required
  Communications - Extra costs of informing of new venues / safety of polling stations.

3.5 Hospital Discharge Programme

3.5.1 At the start of the pandemic central government radically changed the discharge route of hospital patients when it issued the hospital discharge and community support: policy and operating model. It did this by extending the period of health care the NHS were responsible by 6[1] weeks after they left hospital.

3.5.2 In order to deliver this new pathway, the government made available a national Hospital discharge fund to help cover the costs of the post-discharge recovery and support services, rehabilitation and reablement care that are in addition to those normally provided.

3.5.3 The Council received c£5.1m from the Hospital Discharge Fund in 2020/21 and a further £3.348m is forecast in 2021/22.

3.6 Schools

3.6.1 Recognising difficulties being faced by schools as result of the pandemic central Government have provided numerous Covid-19 grants. The initial grants introduced were intended to help schools meet any additional exceptional costs incurred for cleaning, free school meals provision, or increased premises costs. Latterly the grants have focussed on post-lockdown return to education to support all children disadvantaged through 'lost education'. These grants include Covid Catch-Up, Covid Recovery, School Led Tutoring. Additional grants have also been provided to support costs incurred for covid testing facilitated by schools.

3.6.2 Schools have also been supported with meeting the cost of free school meal vouchers for holiday periods through the national voucher scheme funded by central Government, and through LA funding provided via the Winter Grant, Holiday Activities Grant, and Household Support Fund.

3.7 Welfare

3.7.1 Bury has received £8.421m of welfare related grants. Some of the grants have specific criteria regarding how they should be used and others provide an opportunity for Local Authorities to develop schemes that address local an emerging issues related to welfare. A summary of the position is highlighted in Table 3 below

[1] Since September 2021 the period of health care the NHS is responsible for is now 4 weeks

Table 3

Funding	Description	Total
Local Council Tax Support Scheme	Support to help people who are on a low income or claiming certain benefits to pay their Council Tax bill.	**2.081**
Hardship Relief Fund	Specific to 2020/21 whereby all working age claimants eligible for the Local Council tax Support Scheme have received a £150 reduction in their council tax bill. The criteria is mandated by the government and applied locally. Some of the funding was added to the welfare scheme and the criteria expanded to support 'working poverty'	**1.880**
DEFRA Food and Essentials Hardship Grant	Specific to 2020/21 and was agreed that £0.140m would be targeted as a food offer for the Borough and the remaining £0.089m was added to the Council's Welfare Scheme, the criteria for which was expanded to provide support for those suffering hardship as result of isolation but who did not qualify for the government's scheme.	**0.229**
Self-Isolation Grant	Test and Trace Support Payment is for people on low incomes who have to self-isolate because they have Covid	**1.136**
COVID Winter Grant scheme	The majority of funding was used to cover free school meal vouchers over the holidays.	**1.561**
Household support fund Oct '21 - 31 March22	Funding covers the period 6th October to 31st March 2022. The requirements of the grant are broadly similar to the Winter Grant Scheme and delivery is intended to follow a similar path as that used for those schemes.	**1.534**
Total		**8.421**

3.8 Loss of Income

3.8.1 This funding is un-ringfenced and is to support the Council with regards to loss of income as a result of COVID-19. To date, the council has received funding of £4.897m (2020/21) and £0.541m (2021/22) to support income losses.

3.8.2 The income identified and reported to the Mistry of Housing, Communities and Local Government as being lost due to COVID in 20/21 was :-

- £17.464m for services broken down as follows:-
  - Highways £1.725m
  - Leisure £3.148m
  - Commercial losses £9.076m
  - Other Sales Fees & charges £3.515m
- £5.273m for Collection Fund (Council Tax and Business Rates)
- £0.509m for HRA (Housing Revenue Account).

The estimated income loss due to COVID in 2021/22 as reported to MHCLG in September is:-

- £11.451m for services broken down as follows:-
  - Highways £1.234m
  - Leisure £1.051m
  - Commercial Losses £9.006m
  - Other Sales Fees & charges £0.160m

- £2.219m for Collection Fund

3.9 Support to Businesses

3.9.1 Business support grants have been allocated in phases as announced by the government, but all schemes have now closed apart from the Additional Restrictions Grant (ARG), which runs until the end of March 2022.

3.9.2 In response to Wave 1, Bury received £42.920m to allocate grants of £10,000 and £25,000 to businesses in the retail, hospitality and leisure sectors. Government criteria determined eligibility for the grants. Included in the allocation was the provision for 5% of the grants paid out for a discretionary scheme.

3.9.3 The Council was responsible for administering the scheme until it closed at the end of September. In total, £41.580m was paid out to 3,715 business across the borough leaving a small surplus of £1.340m which, based on current guidance, will be recovered by central government. It should be noted that the Council was only able to pay to those businesses that met the government's grant criteria and therefore there was no other alternative way of utilising this funding. The government's initial allocation to Bury was greater than anticipated and initially it was envisaged that c.£3m would be repaid. The Council however worked to ensure that the grant was maximised as much as possible. Representations were made as part of Greater Manchester for surplus funds to be retained however this was not accepted. A summary of the grants paid are set out in table 4 below. Some grants originally paid have since been withdrawn following further checks and reconciliation

Table 4

Covid Business Grants	
Number of Grants Paid Out	3,715
Total Paid (£M)	41.58
Grant Available (£M)	-42.92
Surplus (To be repaid) (£M)	-1.34

3.9.4 In late summer 2020 the government announced new grants called the Locals Restrictions Grants (LRSG) and the Additional Restrictions Grant (ARG). The LRSG is made up of multiple grants and eligibility is subject to government criteria. The ARG is available for discretionary payments to business including those not eligible for the LRSG. A summary of the Covid grants supporting business is set out in Table 5 below.

Table 5

		Bury Council Allocation				
Description	**Calculation Per Business**	**2020/21 (£M)**	**2021/22 (£M)**	**Total (£M)**	**Spent / Committed (£M)**	**Uncommitted (£M)**
Business Rates Grants	The council was responsible for administering the scheme until it closed at the end of September 2020. It should be noted that the Council is only able to pay to those businesses that met the government's grant criteria and therefore there is no other alternative way of utilising this funding.	42.92	0.000	42.920	41.580	1.340
Local Restrictions Support Grant for Businesses legally required to close during a national lockdown (Addendum & Sector)	Payments cover 28 day periods. Based on RV: RV of £15,000 or under a payment of £1,334 RV of £15,000-less than £51,000 a payment of £2,000 RV of £51,000 or over a payment of £3,000	8.358	0.000	8.358	6.881	1.477
Local Restrictions Support Grant for Businesses that remain open but who are severely impacted by the restrictions.	Payments cover 28 day periods. Based on RV: • RV of £15,000 or under: up to £934 • RV of £15,000-£51,000: up to £1,400 • RV of £51,000+: up to £2,100	1.653	0.000	1.653	1.983	-0.330

Description	Calculation Per Business	Bury Council Allocation 2020/21 (£M)	2021/22 (£M)	Total (£M)	Spent / Committed (£M)	Uncommitted (£M)
Local Restrictions Support Grant for Businesses legally required to close during a national lockdown during the period 16 Feb – 31 March	Payments cover 28 day periods. Based on RV: • RV of £15,000 or under: up to £2,096 • RV of £15,000-£51,000: up to £3,143 • RV of £51,000+: up to £4,714	5.062	0.000	5.062	3.534	1.528
Christmas Support Payment – For wet-led pubs closed during December 2020.	One-off payment of £1000 per pub. Application deadline 31/1/21 Payments are being made in advance of 31 January as applications are received.	0.083	0.000	0.083	0.087	-0.004
National Lockdown Top-Up Grant Jan-Feb 2021	Additional to other grants. Based on RV, 6 week payment: • RV of £15,000 or under: £4000 • RV of £15,000-£51,000: £6,000 • RV of £51,000+: £9,000	9.036	0.000	9.036	6.772	2.264
Additional Restrictions Grant (ARG)	Allocations made on a population basis in November 2020 and January 2021. GM agreed 2 overarching principles for ARG: 1. Businesses badly affected by restrictions, but not receiving other grant support. 2. Businesses important for the economy, e.g. because they drive footfall, are a major employer, or part of supply chains.	5.738	0.000	5.738	5.738	0.000
Additional Restrictions Grant (ARG) - Top Up	The ARG Top-Up grant was allocated on a per-business calculation. This allocation was paid directly to Bury Council. ARG distribution was flexed to meet local needs and reflected allocation made by Bury Council Business Rates Team. The fund are required to be defrayed by March 31st 2022.	1.383	0.000	1.383	0.562	0.821

		Bury Council Allocation					
Description	**Calculation Per Business**	**2020/21 (£M)**	**2021/22 (£M)**	**Total (£M)**	**Spent / Committed (£M)**	**Uncommitted (£M)**	
New Burdens 1 for the administration of the business rates grants.	Formulaic allocation to all Local Authorities with billing responsibilities.	0.170	0.000	0.170	0.000	0.170	Note 1
New Burdens 2 – Administration of Retail, Leisure and Hospitality Grants		0.076	0.000	0.076	0.000	0.076	
New Burdens 3 - for the administration of the business rates grants.		0.228	0.000	0.228	0.000	0.228	
Restart Grant	One off payment made to eligible businesses in the non-essential retail sector of up to £6,000 and to eligible businesses in the hospitality, accommodation, leisure. personal care and gym sectors of up to £18,000	9.282	0.000	9.282	9.206	0.076	
Total		83.989	0	83.989	76.343	7.646	

Note 1 - Although no costs have currently been charged to, the Covid funding to support the administration of the new burdens grants temporary staffing resource have been brought in to support the Revenues and Benefits team and their costs need to be recharged.

3.9.5 All grant schemes, with the exception of the Additional Restrictions Grant (ARG) have now closed and all payments made. The Council are now working with the government around reconciliation of the grants paid out and at the end of reconciliation any uncommitted amounts will be returned to the Government. The government over-estimated the amount of grant awards and provided money in advance to Councils to aid cash flow.

3.9.6 Business Rates Officers carried out a number of take up campaigns, worked closely with colleagues in the Council and external partners to maximise take up of the grants in the allotted periods for accepting applications. Officers also worked closely with the governments Business, Energy, and Industrial Strategy (BEIS) team at the time to look at potential barriers to business claiming and a national take up publicity.

3.9.7 Cabinet received a report on 24 March 2021 setting out new phases and eligibility for the Additional Restrictions Grant to speed up the allocation of the grant.

4.0 Transparency and Governance

4.1 The Department for Business, Energy and Industrial Strategy (BEIS) and the Ministry of Housing, Communities and Local Government (MHCLG) are committed to transparency and governance, as consequence returns are being submitted on a weekly/monthly basis. At the same time the Council is also utilising its fraud assurance framework and must comply with set criteria to minimise fraudulent clams. Bury is complying fully with the requirements set by the Government including data sharing and more detailed analysis and checks. Updates are being provided to the Council's Audit Committee to provide assurances on the controls in place and any findings that emerge.

5. Recommendations

Cabinet is asked to:

1. Note the totality of the grants received from the government in response to the Covid-19 pandemic.
2. Note the progress to date with regards to expending/committing the Grant Support in Response to Covid
3. Note the responses to the questions tabled at the at the previous Overview and Scrutiny Committee.

Community impact / Contribution to the Bury 2030 Strategy

Delivery of the Bury 2030 strategy is dependent on resources being available. The delivery of the strategy may be impacted by changes in funding and spending.

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
The information set out in the report forms part of the Council's financial monitoring process. Covid has had a significant impact on the council's financial position and of residents and businesses across the Borough.	The speed at which the grants have been paid has supporting local businesses and individuals who are severely impacted by the Covid pandemic. Monitoring of the grants ensures that the Council's financial position is fully understood and can be reported to cabinet on a regular basis.

Consultation:

There are no consultation requirements arising from this report.

Legal Implications:

This report updates Members on the covid grants spend across 2020- 21 and 2021 – 22, the section 151 officer has confirmed that all returns requested by government have been completed.

Financial Implications:

The financial implications are set out in the report.

Report Author and Contact Details:

Sam Evans

(S151 Officer)

Background papers:

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

Term	Meaning

Appendix 1

Funding Type	Grant/Funding	Description	2020/21	2021/22	Total	Spent /Committed	Uncommitted
COVID-19 Un-ringfenced Tranche Funding	First Tranche	Un-ringfenced support for the Council to meet additional costs and loss of income as a result of COVID-19.	5.364	5.330	10.694	10.694	0.000
	Second Tranche		5.253	0.000	5.253	5.253	0.000
	Third Tranche		1.699	0.000	1.699	1.699	0.000
	Fourth Tranche		3.324	0.000	3.324	3.324	0.000
Sub Total			15.640	5.330	20.970	20.970	0.000
Contain Outbreak Management Fund (COMF)	Test and Trace Service Support Grant	Provides funding to local authorities in England to help reduce the spread of coronavirus and support local public health.	1.080	0.000	1.080	1.080	0.000
	Additional Surge Funding		5.307	1.376	6.682	6.682	0.000
Sub Total			6.387	1.376	7.763	7.763	0.000
Infection Control Support To Providers	ASC Infection Control Fund (including Rapid Testing)	Supports adult social care providers, including those with whom the local authority does not have a contract, to reduce the rate of COVID-19 transmission in and between care homes and support wider workforce resilience.	4.922	3.487	8.408	8.408	0.000
Sub Total			4.922	3.487	8.408	8.408	0.000

Funding Type	Grant/Funding	Description	2020/21	2021/22	Total	Spent /Committed	Uncommitted
Other Government Funding for Local Authorities	ASC Workforce Capacity Fund	Supports local authorities and social care providers to maintain safe staffing levels	0.408	0.000	0.408	0.408	0.000
	Clinically Extremely Vulnerable Support Funding	Funding to provide support to those clinically extremely vulnerable	0.689	0.000	0.689	0.689	0.000
	Community Champions Fund	Funding to expand work to support those most at risk from COVID-19 and boost vaccine take up.	0.467	0.000	0.467	0.467	0.000
	Compliance and Enforcement Grant	Funding to support communities to prevent, manage and contain outbreaks of COVID-19.	0.104	0.000	0.104	0.104	0.000
	Welcome Back Fund (formerly Reopening High Streets Fund)	To support the safe return to high streets and help build back better from the pandemic	0.169	0.169	0.338	0.338	0.000
	Provisional Rough Sleeping Emergency Funding	Support people who are sleeping rough and in accommodation where it was difficult to self-isolate were safely accommodated	0.002	0.000	0.002	0.002	0.000

Funding Type	Grant/Funding	Description	2020/21	2021/22	Total	Spent /Committed	Uncommitted
	Next Steps Accommodation Programme	Safeguard people who were taken safely from the streets with a planned transition to more sustainable interim accommodation options	0.081	0.000	0.081	0.081	0.000
	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)	0.000	0.097	0.097	0.097	0.000
	National Leisure Recovery Fund	Support eligible public sector leisure centres to reopen to the public	0.004	0.000	0.004	0.004	0.000
Sub Total			1.925	0.266	2.191	2.191	0.000
Welfare	Local Council Tax Support Scheme	Provide help for people on low incomes with their Council Tax bill.	0.000	2.081	2.081	2.081	0.000
Sub Total			0.000	2.081	2.081	2.081	0.000
Hospital Discharge Programme	Hospital Discharge Programme	Support to cover some of the cost of post-discharge recovery and support services,	5.100	3.348	8.448	8.448	0.000

Funding Type	Grant/Funding	Description	2020/21	2021/22	Total	Spent /Committed	Uncommitted
		rehabilitation and reablement care following discharge from hospital					
Sub Total			5.100	3.348	8.448	8.448	0.000
Schools	Wellbeing for Education Grant	Non-ringfenced grant to better equip education settings to support wellbeing and psychological recovery as they return to full time education.	0.030	0.000	0.030	0.030	0.000
	Covid catch-Up Premium	Additional funding to help children catch up on lost learning and reach expected curriculum levels during the 2020/21 academic year.	2.367	0.000	2.367	2.367	0.000
	Covid Exceptional Cost Re-Imbursement Scheme	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	2.645	0.000	2.645	2.645	0.000

Funding Type	Grant/Funding	Description	2020/21	2021/22	Total	Spent /Committed	Uncommitted
		scrutiny and validation.					
	Holiday Activities and Food Programme 2020/21	To support free school meals and activity over Easter	0.073	0.000	0.073	0.073	0.000
	Covid Mass Testing funding for schools	To Support testing within Schools	0.098	0.271	0.369	0.369	0.000
	Covid Summer School Funding for Schools	To Support Summer School Costs	0.000	0.722	0.722	0.722	0.000
	Covid Workforce Fund for Schools	Funding to support schools facing significant staff absences and financial pressures with the costs of staff cover	0.000	0.014	0.014	0.014	0.000
	Covid Free School Meals Additional Costs - Schools	To support free school meals	0.000	0.100	0.100	0.100	0.000
Sub Total			5.213	1.107	6.320	6.320	0.000
Welfare	Hardship Relief Fund	Specific to 2020/21 whereby all working age claimants eligible for the Local Council tax Support Scheme have received a £150 reduction in their council tax bill.	1.880	0.000	1.880	1.880	0.000

Funding Type	Grant/Funding	Description	2020/21	2021/22	Total	Spent /Committed	Uncommitted
	DEFRA Food and Essentials Hardship Grant	Specific to 2020/21 awhereby £0.140m targeted as a food offer for the Borough and the remaining £0.089m was added to the Council's Welfare Scheme, the criteria for which was expanded to provide support for those suffering hardship as result of isolation but who did not qualify for the government's scheme.	0.229	0.000	0.229	0.229	0.000
	Self-Isolation Grant	Grant payments to eligible claimants who are self-isolating	0.171	0.000	0.171	0.171	0.000
	Self Isolation Grant Top Up		0.124	0.000	0.124	0.124	0.000
	Self Isolation Grant Top Up February 21		0.160	0.000	0.160	0.160	0.000
	Self Isolation Grant Top Up March, April		0.000	0.362	0.362	0.362	0.000
	Self Isolation Grant Top Up May, June, July		0.000	0.228	0.228	0.228	0.000
	Self Isolation Grant Top Up August, September		0.000	0.091	0.091	0.091	0.000
	COVID Winter Grant scheme	To support families/vulnerable households	0.619	0.000	0.619	0.619	0.000
			0.000	0.215	0.215	0.215	0.000
			0.000	0.145	0.145	0.145	0.000

Funding Type	Grant/Funding	Description	2020/21	2021/22	Total	Spent /Committed	Uncommitted
		particularly with food, energy and water bills . Also used to cover free school meal vouchers over the holidays.	0.000	0.582	0.582	0.582	0.000
	Household support fund Oct '21 - 31 March22	To support families/vulnerable households particularly with food, energy and water bills . Also used to cover free school meal vouchers over the holidays.	0.000	1.534	1.534	1.534	0.000
Sub Total			3.183	3.157	6.340	6.340	0.000
Loss of Income	Loss of Income (Sales, Fees and Charges)	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.	4.897	0.541	5.438	5.438	0.000
Sub Total			4.897	0.541	5.438	5.438	0
Support To Business	Business Rates Grants	Grant payments of £10k and £25k to eligible business and funding for a	42.92	0.000	42.920	41.580	1.340

Funding Type	Grant/Funding	Description	2020/21	2021/22	Total	Spent /Committed	Uncommitted
		discretionary scheme.					
	Local Restrictions Support Grant (Closed)	Funding to support businesses legally required to close.	8.358	0.000	8.358	6.881	1.477
	Local Restrictions Support Grant (Open)	Funding to support businesses that remain open but who are severely impacted by the restrictions.	1.653	0.000	1.653	1.983	-0.330
	Christmas Support Payment	Funding to support wet-led pubs where tier 3 restrictions imposed	0.083	0.000	0.083	0.087	-0.004
	National Lockdown Top-Up Grant Jan-Feb 2021	One-off top-up grant for retail, hospitality and leisure businesses closed in national lockdown Jan-Feb 2021	9.036	0.000	9.036	6.772	2.264
	Additional Restrictions Grant (ARG)	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.	5.738	0.000	5.738	5.738	0.000

Funding Type	Grant/Funding	Description	2020/21	2021/22	Total	Spent /Committed	Uncommitted
	Additional Restrictions Grant (ARG) - Top Up	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.	1.383	0.000	1.383	0.562	0.821
	New Burdens 1 for the administration of the business rates grants.	New costs to support the administration of grants to businesses and increase in welfare and benefit claimants.	0.170	0.000	0.170	0.000	0.170
	New Burdens 2 – Administration of Retail, Leisure and Hospitality Grants	New costs to support the administration of grants to businesses and increase in welfare and benefit claimants.	0.076	0.000	0.076	0.000	0.076
	New Burdens 3	New costs to support the administration of grants to businesses and increase in welfare and benefit claimants.	0.228	0.000	0.228	0.000	0.228
	Restart Grant	One off payment made to eligible businesses in the non-essential retail sector of up to £6,000 and to eligible	9.282	0.000	9.282	9.206	0.076

Funding Type	Grant/Funding	Description	2020/21	2021/22	Total	Spent /Committed	Uncommitted
		businesses in the hospitality, accommodation, leisure. personal care and gym sectors of up to £18,000					
	LRSG allocation 16 February – 31 March - Closed payment	Funding to support businesses legally required to close.	5.062	0.000	5.062	3.534	1.528
Sub Total			83.989	0	83.989	76.343	7.646
Grand Total			131.256	20.693	151.949	144.303	7.646

Agenda Item 9

Classification Open	Item No.

Meeting:	Audit Committee
Meeting date:	25th November 2021
Title of report:	Internal Audit Progress Report – 1st April 2021 to 8th November 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:

- Twenty-five reports have been issued to Members since the beginning of the financial year, fifteen of which have been issued since the Committee last met in September 2021.
- Of the fifteen reports issued since September 2021, six reports with a Limited assurance have been issued. A total of seven reports with Limited Assurance have been issued during the year to date. These reports will need to be considered within the Annual Governance Statement produced at the end of the financial year 2021/22.
- The original audit plan produced for 2021/22 is to be revised to take account of staffing changes which have occurred since April 2021 and to adjust for Management requests for audit work to be undertaken.

Recommendation(s)

That:

- Members note this report and the work undertaken by Internal Audit.
- Members note and approve the changes to the Annual Audit Plan for 2021/22.
- Members delegate any further required changes to the Audit plan for 2021/22 to the Councils S151 officer and the Audit Committee Chair

Key Considerations

1. Background

1.1 This report outlines the work undertaken by Internal Audit between 1st April 2021 to 8th November 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 second report of the 2021/22 financial year covering the period from 1st April 2021 to 8th November 2021 which includes 31 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.

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

Childrens Services

- Recruitment of staff within schools
- Recruitment of School Governors
- Complaint's process

The original plan is shown at appendix 1, the proposed changes to be made to the plan are: -

Directorate	Topic	Indicative Days	Reason for adjustment to plan
Delete the following provisions (50days): -			
Corporate Core	Complaints	15 days	Change review to be undertaken in Childrens Services to respond to request for review from client.
Corporate Core	Recruitment	15 days	Change review to be undertaken in Childrens Services to respond to request for review from client.
Corporate Core	Establishment budget and Alignment with HR records	5 days	Delete as HR and Finance Teams are working on this issue. Audit advice is being requested as and when required.

Corporate Finance	I-Trent - Payroll – Additional hours / overtime payments	15 days	Defer to 22/23, allow i-trent self serve to be introduced. Advice is being provided as and when required
Add / increase the following provisions (50days): -			
Childrens Services	Complaints	10 days	Request from client
Operations – Waste Management Service	Complaints	10 days	Request from Audit Committee
Childrens Services	Recruitment of Staff within Schools	15 days	Request from client
Staff Training		15 days	Member of staff has commenced CPFA

- The audit request regarding Recruitment of School Governors will be carried forward to the 2022/23 annual audit plan.

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 Audit clients.

Audits completed and Reports Issued.

2.2.1 The last report to Audit Committee in September 2021 detailed 10 audit reports which had been issued since the beginning of the financial year. Since the last Audit Committee, a further 15 audit reports have been finalised and issued. These are detailed in Table 1 below, which also shows the corresponding number of agreed actions and overall level of assurance provided for each of those audits.

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).

Additionally, four reports for Six Town Housing have also been finalised and issued within Six Town Housing. These reports will be circulated to Audit Committee after they have been through the Governance Process within Six Town Housing. Details of the subjects covered are reflected in Table 1 below.

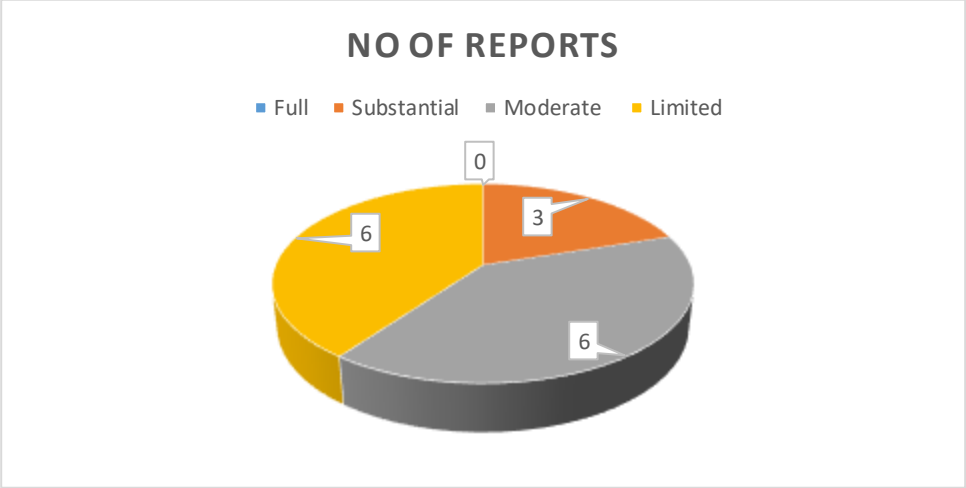
Table 1: Final Reports Issued

Audit	Number of agreed actions and priority				Level of Assurance
	Fundamental	Significant	Merits Attention	Total	
Health and Safety	2	12	1	15	Limited
Members Discretionary Budgets	2	2	0	4	Limited
Creditors Key Controls	1	5	0	6	Limited *
Debtors Key Controls	3	2	2	7	Limited *
Cash and Bank Key Controls	1	3	0	4	Limited
Main Accounting Key Controls	1	6	2	9	Limited *
Grounds Maintenance - Procurement	0	4	1	5	Moderate
Council tax Key Controls	0	6	6	12	Moderate
Housing Benefits and Council Tax Support Key Controls	0	2	0	2	Moderate
National Non Domestic Rates (NNDR)Key Controls	0	5	1	6	Moderate
Housing Employment and New Opportunities (HEN)- Accommodation Team – Petty Cash	0	6	0	6	Moderate
Payroll Key Controls	0	7	6	13	Moderate

Treasury Management	0	1	2	3	Substantial
Mobile Phones	0	1	2	3	Substantial
GM Supporting Families Programme	0	2	0	2	Substantial
STH Fraud and Business Controls	To be informed (TBI)	TBI	TBI	TBI	TBI
STH Procurement Repairs and Maintenance	TBI	TBI	TBI	TBI	TBI
STH Payroll	TBI	TBI	TBI	TBI	TBI
STH Data Quality	TBI	TBI	TBI	TBI	TBI
Total	8	66	23	97	

- Three of the fundamental recommendations in the key control audits marked * are for the same issue.

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 2 for explanations of the different levels of assurance).

Actions are classified over the categories of Fundamental, Significant and Merits Attention. (See appendix 2 for explanations of the different levels of priority).

Where a fundamental recommendation is made, this leads to a Limited Assurance of the area under review.

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 two audits still being finalised from the 2020/21 plan. There has been some difficulty in obtaining information during these reviews, however all the information has now been provided and the reports are now being prepared. The 2021 plan is now being delivered.

Audits which are currently taking place are: -

2020/21

- Six Town Housing Disabled Facilities Adaptations
- Estates Property Management

2021/22

- Six Town Housing Rents Key Controls
- Petty Cash Choices for Living Well Team
- Housing Development Program
- Complaints (Childrens Services)
- Residential Payments
- Leisure Services – Income Review
- Six Town Housing - Electrical Safety
- Six Town Housing – Fire Safety
- Taxi Licences
- Six Town Housing – No Access
- Highways Maintenance
- Contract Register

It was reported at September Committee that a review was being undertaken within Six Town Housing, Arrears Prevention. At the request of Six Town Housing this review has been deferred and is to be undertaken in 2022/23.

2.3.2 Assurance work – Draft reports

- Persona Payroll

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. There are no issues to bring to the attention of Audit Committee at this time.

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 have been 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 a low level of sickness reported in the team for the current financial year. Adjustments to the annual plan have not needed to be made for sickness periods incurred to date.

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 level of training included in the annual plan has been amended and this report requests permission to increase the Training provision in the plan by 15 days. Whilst this is not the full provision for the course, items in the plan have been slightly flexed to accommodate the training provision. The situation will continue to be monitored as the year progresses.

A team member was 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 continue to be monitored as the year progresses.

As the Audit Committee is not scheduled to meet until March 2022, Members are asked to delegate that any further adjustments to be made to the 2021/22 plan before the end of the financial year will be agreed between the S151 officer and the Chair of the Audit Committee.

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.

The audit team are currently involved in the investigations regarding two whistleblowing incidents. Details of the investigations are not included in this report as to do so may reveal 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) and could potentially jeopardise any resulting disciplinary or criminal proceedings if these are required. It should be noted however that these investigations are still ongoing.

2.6.4 Collaboration

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

- Contract Audit 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.

School funds

The annual accounts for three 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:

The Council must have a sound system of internal control which facilitates the effective exercise of its functions, including risk management. This is both a legal requirement and a requirement of the Financial Regulations set out in the Council's Constitution. This report provides information on the work of the Council's Internal Audit Service, in ensuring compliance.

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
HEN	Housing Employment and New Opportunities
NNDR	National Non Domestic Rates

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			Deferred to QTR 4 to accommodate other work brought forward.
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	15	QTR4			Propose to use this budget for the review requested by Childrens Services and defer Corporate Core review until 22/23

			4 an appropriate division of duties is enforced by the system.					
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	QTR3			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			Final reports have been issued.

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			Propose to delete the review as the process is being addressed by HR and Payroll Teams and audit advice is being given as and when required
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			Poropsed that this is deferred to 2022/23
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			Deferred to quarter 4 to take account of audit of 2020/21 accounts
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 Families (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			Final report issued

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			Deferred to QTR 3 - 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	15	QTR3			

			benchmarking processes are in place and review.					
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	QTR2/3			Audit ongoing

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	15	QTR3			

			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.					
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	Review of highways maintenance – work programmes, allocation of works and subsequent monitoring, and costs	20	QTR3			Engagement letter sent to client

		claims to be made against the Council which may incur significant financial penalties.						
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	QTR3			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	10	QTR2/3			Audit review ongoing

			work in the UK and hold the appropriate driving licence.					
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	QTR3			Planning underway, engagement letter being prepared.
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	QTR3			

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	QTR2/3			Audit ongoing

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		Advice is being given as and when requested.
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	15	TBA	N/A		

			revised write off procedures when they have been updated.					
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 undertaken in two areas as requested by Management Accountancy Team. Issues have been identified, one report (HEN Accommodation Team) has been presented to Audit Committee

								(November 2021) the second, Killelea, Choices for Living Well, is being finalised and will be presented to Audit Committee March 2022.
			TOTAL	552				

OTHER COMMITMENTS		
Activity	***Indicative Days***	***Comments***
Completion of audits commenced during 2020/21: **Health and Safety** **GDPR** **Pooled Budgets**	25	Indicative days were set too low • Final Audit reports now issued for: • GDPR • Pooled Budgets • Budget Setting and Monitoring in Schools

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**		• Purchase Cards • Car Allowances • Adoption • Integrated Equipment Store • Pupil Premium • Members Allowances • Health and Safety • Members Delegated Funds (Discretionary Budgets) • Operations Procurement • Mobile Phones
External Traded Services - -perform audits of School Fund and Out of School Club accounts	10	Three 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	Work has commenced to undertake follow up reviews.
Contingency for GMCA Collaboration / reactive GM assurance work	5	

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.
Provisions for annual leave / training / sickness	243	Indicative days to be increased from 243 to 258 as member now commenced CPFA studies. Team member seconded to P1 service to support COVID 19 pandemic. No adjustment has been made to date (November 2021) to reflect this.
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)

Appendix 1

This page is intentionally left blank

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

Document is Restricted

This page is intentionally left blank

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

Document is Restricted

This page is intentionally left blank

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

Document is Restricted

This page is intentionally left blank

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

Document is Restricted

This page is intentionally left blank

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

Document is Restricted

This page is intentionally left blank

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

Document is Restricted

This page is intentionally left blank

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

Document is Restricted

This page is intentionally left blank