SWAP
INTERNAL AUDIT SERVICES
Helping Organisations to Succeed

Cheltenham Borough Council

Report of Internal Audit Activity

September 2023

Internal Audit ▪ Risk ▪ Special Investigations ▪ Consultancy

Unrestricted

Contents

The contacts at SWAP in connection with this report are:

Lucy Cater
Assistant Director
Tel: 01285 623340
lucy.cater@swapaudit.co.uk

Jaina Mistry
Principal Auditor
Tel: 01285 623337
jaina.mistry@swapaudit.co.uk

- Contents:

Internal Audit Definitions

At the conclusion of audit assignment work each review is awarded a "Control Assurance Definition";

- **No**
- **Limited**
- **Reasonable**
- **Substantial**

●

Audit Framework Definitions

Control Assurance Definitions

No	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.
Limited	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
Reasonable	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Substantial	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.

Non-Opinion – In addition to our opinion based work we will provide consultancy services. The "advice" offered by Internal Audit in its consultancy role may include risk analysis and evaluation, developing potential solutions to problems and providing controls assurance. Consultancy services from Internal Audit offer management the added benefit of being delivered by people with a good understanding of the overall risk, control and governance concerns and priorities of the organisation.

Internal Audit Definitions

Recommendations are prioritised from 1 to 3 on how important they are to the service/area audited. These are not necessarily how important they are to the organisation at a corporate level.

Each audit covers key risks. For each audit a risk assessment is undertaken whereby with management risks for the review are assessed at the Corporate inherent level (the risk of exposure with no controls in place) and then once the audit is complete the Auditors assessment of the risk exposure at Corporate level after the control environment has been tested. All assessments are made against the risk appetite agreed by the SWAP Management Board.

- ## Audit Framework Definitions

Categorisation of Recommendations

When making recommendations to Management it is important that they know how important the recommendation is to their service. There should be a clear distinction between how we evaluate the risks identified for the service but scored at a corporate level and the priority assigned to the recommendation. No timeframes have been applied to each Priority as implementation will depend on several factors; however, the definitions imply the importance.

	Categorisation of Recommendations
Priority 1	Findings that are fundamental to the integrity of the service’s business processes and require the immediate attention of management.
Priority 2	Important findings that need to be resolved by management
Priority 3	Finding that requires attention.

Definitions of Risk

Risk	**Reporting Implications**
High	Issues that we consider need to be brought to the attention of both senior management and the Audit Committee.
Medium	Issues which should be addressed by management in their areas of responsibility.
Low	Issues of a minor nature or best practice where some improvement can be made.

Audit Plan Progress

Audit Type	Audit Area	Status	Opinion	No of Rec	Priority			Comments
					1	2	3	
Key Financial Control	Payroll	Final Report	High Substantial					Report Included
Key Financial Control	Treasury Management and Cashflow Forecasting	Final Report	High Substantial	0				Report Included
Governance	Business Continuity Management – Elections and Revenues and Benefits	Final Report	Medium Reasonable	2		2		Report included
Governance	Business Continuity Management – Corporate Reporting	Final Position Statement	N/A	-				Report Included
Governance	Freedom of Information	Draft Report						
Key Financial Control	Bank Reconciliation	Audit in Progress						
ICT	ICT Business Continuity Management	Audit In Progress						
Key Financial Control	Use of Waivers	Audit in Progress						
Operational	Grant Income	Brief Issued						
Governance	Projects – Lessons Learned	Brief Issued						
Governance	Transparency Data	Scoping						

SWAP
INTERNAL AUDIT SERVICES
Assuring – Improving – Protecting

SWAP work is completed to comply with the International Professional Practices Framework of the Institute of Internal Auditors, further guided by interpretation provided by the Public Sector Internal Audit Standards (PSIAS) and the CIPFA Local Government Application Note.

Audit Plan Progress

Audit Type	Audit Area	Status	Opinion	No of Rec	Priority			Comments
					1	2	3	
Operational	Accounts Payable – Qtly Review	In Progress						
Support	Business Grant Funding – Aged Debt	On-Going						Quarterly review of Business Grant Overpayment Aged Debts with Head of Service, Counter Fraud and Enforcement Unit for reporting to BEIS
Advisory	Procurement and Commissioning Group	On-Going						
Follow-Up	Follow-Up of Agreed Actions (not included in an audit above)	On Going						
Other Audit Involvement	Working with the Counter Fraud and Enforcement Unit	On Going						
Other Audit Involvement	Management of the IA Function and Client Support	On Going						
Other Audit Involvement	Contingency – Provision for New Work based on emerging risks							

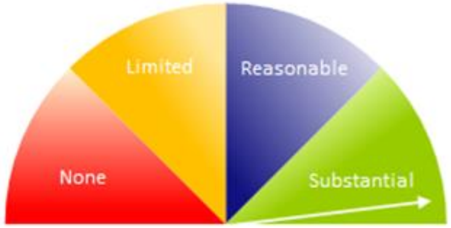
Summary of Audit Findings

The following are the Internal Audit reports, of each audit review finalised, since the last Committee update

Payroll – Final Report – June 2023

Audit Objective To provide assurance that the Payroll system is operated in accordance with agreed policy/procedure and with the Council/Clients Financial Rules.

Assurance Opinion



A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.

Number of Actions

Priority	Number
Priority 1	0
Priority 2	0
Priority 3	0
Total	**0**

Risks Reviewed	Assessment
Payroll is not processed accurately or on time which means inaccurate, or ghost payments are made resulting in financial losses and reputational damage.	Low

Key Findings

Processes have been adopted by the Payroll Team to ensure employees are paid promptly and accurately. Evidence demonstrated reconciliation, review and appropriate approval of payment files including variances, these processes ensure ghost accounts / payments are not created. Remaining leave entitlements are calculated and documented for final payments. Manual salary advances are rare but evidence of approval from Senior Management is documented when necessary. Evidence of recovery of advances and overpayments is available on the Finance system. 3rd party deduction testing did not identify errors. The Council's payroll suspense accounts balance at year end.

Audit Scope

This review includes testing accuracy of information for starters, leavers and contract variations, including name, NI, system status and hours.

An assessment of salary advances and overpayments, including recovery; and processes (including any workarounds) to ensure timely completion and accurate monthly payroll processing.

Deductions and payments for a selection of 3rd parties assessed for accuracy (HMRC not included as this was assessed in last year's audit).

Follow-up of previous agreed actions.

Other Relevant Information

Time analysis was conducted on the manual processes (workarounds) needed to ensure the payroll is processed correctly each month. We calculated that an estimate of 13%, of a Payroll Officer's time, is required for this as the system isn't able to produce a payroll without manual intervention. We are also aware that Payroll Officers only take leave once a payroll has been completed for a month. This can't be avoided without a significant financial investment for a new payroll system. Eliminating the manual workaround requirements would allow officers to concentrate on strategic and management tasks, including cleansing data on the system.

Testing on the accuracy of information identified minor administrative errors which required further assessment with Officers to confirm any impacts would not be of significant concern.

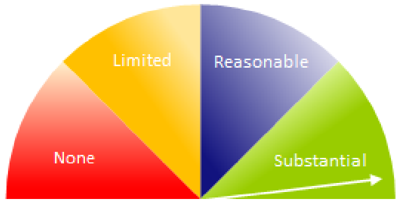
Outdated information identified on the Council's finance/spending webpages relating to pay. Officers should determine who has responsibility for this information as they will need to complete a request for a website update.

Treasury Management and Cashflow Forecasting – Final Report – August 2023

Audit Objective

To review Treasury Management & Cashflow forecasting processes are in accordance with agreed procedures and the Council's Investment and Treasury Management Strategies.

Assurance Opinion



A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.

Number of Actions

Priority	Number
Priority 1	0
Priority 2	0
Priority 3	0
Total	**0**

Risks Reviewed	Assessment
Inadequate cashflow forecasting may lead to poor decisions on investments and borrowing, resulting in financial loss to the Council.	Low

Key Findings

£ Cashflow forecasting has many dependencies and often relies on historical data from previous years which is uprated as necessary. All data is recorded within the Treasury Management system and is used for forecasting cashflow and is updated regularly from the relevant information sources such as the main financial management system.

Due to the return of the Treasury Management service to CBC during 2022, resource limitations meant that formal quarterly Treasury reconciliations were not completed. However, we are satisfied that the 2022/23 year end closedown reconciliation has been completed. Also, we can confirm that Treasury data is included in the Quarterly Budget Monitoring reports presented throughout 2022/23 and will also be included in the next report which is due in September 2023.

Treasury Management Strategies are approved. A Treasury Management Outturn report is presented to members each year as well as a mid-year progress report. Investments are made within the Investment Management Strategy guidelines.

Audit Scope

A review was completed in the following areas:

- Processes around cashflow forecasting to include roles and responsibilities.
- Accuracy, ongoing monitoring, and reporting of cashflow changes.
- Authority to determine and change investments in line with Council strategy.

We held discussions with the Treasury Accountant. And reviewed evidence provided to support discussions held.

Conclusion

Robust controls are operating within the areas reviewed in this audit. Roles and responsibilities are established and there is senior management oversite of Treasury Management activity.

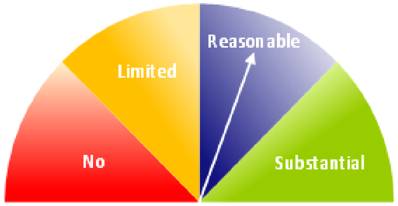
There were no issues or actions to raise.

Business Continuity Management (Elections and Revs and Bens) – Final Report – August 2023

Audit Objective

To ensure that the organisation has planned for and can maintain an agreed level of business continuity to priority services in the event of a critical ICT incident.

Assurance Opinion



There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.

Number of Actions

Priority	Number
Priority 1	0
Priority 2	2
Priority 3	0
Total	**2**

Risks Reviewed	Assessment
In the event of a major disruption to ICT availability, the over reliance on the ICT department to maintain corporate business continuity and a lack of preparedness by service areas may result in a loss of service continuity across the Organisation.	Medium

Key Findings

In both services tested, staff had no, or limited, offline access to copies of their departmental BCP. This could cause issues in the event of inaccessibility to the Council's ICT network or a national power outage.

Although the Service plans tested had been updated in the last 12 months, this was because of changes in staff/contact details. There was no evidence to suggest that Service BCP's were tested or updated annually on a routine basis, with a view to identifying new/emerging risks. There were no entries in the 'Training and Testing' section of the planning document.

There was no evidence of the use of version control for BCPs for either of the services tested.

Audit Scope

The following expected controls were reviewed for the Revenues & Benefits and Electoral Services:

- Completion and approval of Service Area Business Continuity Plans (BCP).
- Identification of critical business processes and their ICT dependencies within that service area and documentation within the BCP.
- Identification and documentation of mitigating factors or workarounds to ensure continuity of service during the loss of ICT availability.
- Identification of any differing requirements between Partner Councils (if applicable).
- BCP review and testing.

Other Relevant Information

Both services tested had commendable awareness and knowledge of the impact that an ICT outage would cause their service. Manual workarounds for business critical processes had been considered in applicable cases and mitigating actions documented.

We were notified post-audit, that the Elections Manager has now addressed the issue of offline access for her staff. We recognise that a training requirement exists for managers and officers involved in BCP issues (procedure, awareness, crisis management etc). This has been addressed in a Position Statement to be issued to CBC management. Similarly, we identified a need for greater support and clarity for Service Managers regarding their responsibilities in respect of business continuity. Again, this has been addressed within the Position Statement.

We acknowledge feedback from the services tested regarding greater ICT involvement in composing and updating their BCPs. These issues will be covered within the ICT Audit Plan.

Both services tested have been, or will shortly be, in contact with their Gloucester City Council counterparts to understand the issues they encountered before, during and after the ransomware attack in December 2021. This is an invaluable source of directly relevant information and experience and it's important that all Service Managers utilise this.

Business Continuity Management (Corporate) – Final Position Statement – July 2023

Audit Objective To ensure that the authority has planned for and can maintain, an agreed level of business continuity to priority services in the event of a critical ICT incident.

Introduction / Background

An audit for Business Continuity arrangements in the Revenues & Benefits Service and the Electoral Service was originally included in the agreed Audit Plan. Having reviewed and assessed the controls operating in both of these service areas we are pleased to provide a 'Reasonable' assurance opinion. However, during fieldwork, we identified several issues of a corporate nature which we would like to bring to the Council's attention.

In recent years, the types of threat to the Council's ICT systems have evolved, as evidenced by the ransomware attack on Gloucester City Council in December 2021 which had (and continues to have) a severe impact on their ability to continue to deliver services. Therefore, a programme of ICT audits have been planned with the Publica Chief Technical Officer, which will be reported to the Council in due course.

But it is equally as important to ensure that service areas have their own business continuity practices that can be enacted where ICT services are limited or non existent.

As a 'Value Added' piece of work, we have agreed with the Head of Corporate Projects to issue a Position Statement for consideration by the Director of Climate Change & Place Services who is the BCP (Business Continuity Planning) Corporate Lead.

Findings / Observations

1. *<u>Corporate and ICT Business Continuity Plans are not up to date.</u>*
   The Corporate Business Continuity Plan (CBCP) provided to us is headed January 2023 and shows it being revised in March 2023. However, this revised plan still contains out of date information. For example, it refers to SLT, GOSS HR, ICTSS (ICT Shared Service) and states relocating staff to the FoDDC council offices. This may not be the most appropriate place to relocate to given the current relationship with the Publica partner councils. Also, given that most officers are equipped to work remotely, should this not be the first approach?
   We acknowledge that work is ongoing to update corporate business continuity management provision.
   We are aware that the Publica ICT Service have reviewed their processes and audits of ICT Business Continuity and ICT Risk Management are currently being planned.
   The absence of up to date business continuity plans subjects CBC to greater risk if there is not a current co-ordinated corporate response in place. Consideration must be given to reviewing and updating the CBCP with relevant up to date information.

2. *<u>BCP Co-ordination and Support for Service Managers is lacking.</u>*
   The two Service Managers interviewed stated that there was insufficient guidance and support provided corporately in respect of business continuity planning and completion of the Business Continuity Plan (BCP) proforma. Previously the BCP required service managers to annually update and test their BCPs. But this is not stated in the updated CBC template. And so there was limited awareness of the need for annual updates and testing and neither manager spoken to knew whether their Service Continuity Plans, once submitted, were subject to any further scrutiny or sign-off. We searched the CBC intranet and found one post offering some guidance, but this was published in 2017 and the officers signposted for further information have both retired and left the Council some time ago.
   The lack of direction and potentially an unawareness of best practice by other service managers represents an area of weakness for CBC. If service managers are not kept updated then potentially efforts may be duplicated or processes may take longer to set up.

3. *Business Continuity Training / Communications / BCP Testing*
   The two Service managers advised that they had not received any recent business continuity training. Again review of the CBC intranet did not identify any relevant guidance or training courses. The Learning Management system may have suitable resources available.
   Furthermore, we reviewed the Business Continuity folder on the shared area, and although we accept work is ongoing, the last evidence of any BCP testing either corporately or at service level is from 2016. Failure to test BCPs, even if only a desktop exercise is undertaken, means that any weaknesses found will not be addressed and so business continuity risk increases.

4. *Operation Mighty Oak*
   We were advised that in March 2023, the Council took part in a national exercise, Operation Mightly Oak, which focussed on how to proceed in the event of a total power outage (i.e. zero access to IT systems), but the outcome or any points of note/learnings have not yet been communicated.
   It may be some time before information is cascaded nationally, and so CBC needs to incorporate their own findings within the current work to update the CBCP. As Business Continuity Plans should be live documents, updates should be completed each time there is a change.

Conclusion

We recognise the organisational changes that the Council has been undergoing may have contributed to Business Continuity Managment roles and responsibilities not being clearly allocated. But if there is no corporate approach and if processes are not defined and communicated then the ability to maintain service continuity will be severely hampered.

Since completing our fieldwork we note that a business continuity risk focussing on ICT failure has now been added to the Clearview system and another regarding ineffective business continuity plans. This is a good start to managing business continuity risks.

We have not proposed any formal actions, but suffice to say that business continuity is fundamental to the success of any organisation. Therefore robust processes and procedures must be in place, communicated to the whole organisation, and appropriate training provided. BCPs must be tested to ensure they are fit for purpose, and learnings from other organisations taken into account when considering the Councils' arrangements.