APPENDIX C

LIMITED / NO ASSURANCE AUDIT REPORTS

The **EXECUTIVE SUMMARY** is provided for those reports produced in the year which had lower assurance ratings. The following reports are included for 2022 / 2023:

- NNDR
- PCI Compliance
- Business Continuity
- Mayors Charities

It should be noted that were audits are in progress or awaiting agreement of the draft report, should they also not mean minimum standards then those Executive Summaries will be provided to Audit Committee later in the year.

NATIONAL NON-DOMESTIC RATES

Introduction

National Non-Domestic Rates, or business rates, are collected by PCC from occupants of non-domestic properties in Peterborough to contribute towards the cost of providing local services. Under the business rates retention arrangements introduced by central government, PCC keep a proportion of the business rates paid locally. This provides an incentive for PCC to work with local businesses to create a favourable local environment for growth so the Authority benefits from business rates revenues. NNDR income, together with council tax revenue, support grants provided by the Government and other income, is used to pay for PCC services.

Payment of business rate bills is automatically set on a 10-monthly cycle. However, ratepayers can elect to pay via 12 monthly instalments. The NNDR billing and payments operation has been outsourced to Serco, although PCC remain responsible for overseeing and managing the service provided by Serco.

PCC is responsible for overseeing the calculation of business rates based on multiplying the rateable value of properties by the appropriate non-domestic multiplier. There are two multipliers; the national non-domestic rating multiplier and the small business non-domestic rating multiplier. Central government sets the multipliers for each financial year which is based on the previous year multiplier adjusted to reflect the Consumer Price Index (CPI) inflation figure for the September prior to the billing year.

The rateable value of each applicable non-domestic property is set by the Valuation Office Agency (VOA), an agency of HMRC. This broadly represents the yearly rent the property could have been let for on the open market on a particular date specified in legislation. The Valuation Office Agency may alter valuations if circumstances change, and ratepayers and other interested parties may challenge property valuations directly with the VOA.

Depending on individual circumstances, ratepayers may be eligible for business rates relief. There are a range of available reliefs based on government policy and specific qualifying criteria, for example; small business rates relief, charity and community amateur sports club relief, unoccupied property rate relief, transitional and retail rate relief.

Objectives and Scope

The purpose of the audit is to assess the adequacy and effectiveness of NNDR process to ensure that business rates revenue due to the Council is maximised, reducing the need to write off uncollected debt.

The review will assess NNDR process, including:

- Adequacy and effectiveness of processes and controls in place for accurate and timely billing and collection of NNDR payments due, including best practise;
- Serco adherence with PCC contractual NNDR processing requirements, and the adequacy of Council process for monitoring Serco Key Performance Indicators (KPI);
- Adequacy and accuracy of NNDR management information and reports provided to PCC, including performance indicators that demonstrate KPI achievement;
- Effectiveness of the process for reconciling VOA schedules and NNDR records;
- Compliance with NNDR regulations and the effectiveness of Serco technical check processes;
- Process for managing business notifications about business property use and ownership changes;

- Process for applying rates relief and confirming eligibility;
- Process for collecting NNDR payments and the effectiveness of PCC oversight; and
- Process for refunding credit balances when properties are vacated.

Main Findings

- NNDR services provided by Serco are subject to two key performance indicators; collection and arrears rates. There is an opportunity to enhance PCC oversight of NNDR operations by expanding performance indicator reporting allowing formal scrutiny by PCC at monthly service review meetings.
- The process for reconciling VOA valuation records with PCC records is not documented, and there are currently eight NNDR account reconciling anomalies which are being addressed by Serco.
- The process for authorising discretionary rates relief authorisation is not documented and PCC does not have adequate oversight of all discretionary reliefs applied.
- NNDR debt recovery procedures are not documented and debts over 10 years old amount to £136K covering 136 NNDR accounts. A debtor account cleansing exercise is currently underway, and we recommend that aged debt and debt recovery progress be formally monitored as part of the monthly Serco service review meeting.
- NNDR credit accounts amount to £1.1M (Q4, Jan-Mar 22) covering 433 property accounts. Credit account review and refund processing should be performed more frequently, and we recommend that this is formally monitored as part of the monthly Serco service review meeting.

Conclusion and Opinion

A key mechanism for monitoring NNDR activity and performance is the Shared Transactional Service & PCC Liaison Meeting held monthly between Serco and PCC. There is an opportunity to further utilise this review process by supplementing KPI reporting with additional performance reporting which will allow PCC management greater oversight and opportunity to scrutinise NNDR processing.

The service contract signed by PCC and Serco in 2011 indicates that the PCC Compliance team should undertake a series of checks of Revenue & Benefits services including a series of NNDR activity reviews. The PCC Compliance team no longer exists and PCC do not perform compliance checks of Serco Revenue & Benefits processing. This further demonstrates the importance of enhancing oversight at the monthly Shared Transactional Service & PCC Liaison Meeting.

Not all key NNDR procedures are documented and there is evidence that long-standing NNDR debts need addressing. Action to review and process credit account refunds should also be undertaken more frequently.

The audit opinion is of limited assurance.

PCI COMPLIANCE

Introduction

The Payment Card Industry Security Standards Council (PCI SSC), set up by the major payment brands (such as Visa, MasterCard, Amex etc), have a number of different sets of security standards to cover the entire card-processing eco-system. The intention behind these standards is to protect cardholders' payment card data. Merchants (i.e. organisations that accept payment by debit / credit card), or service providers acting on their behalf, that are entities who store, process or transmit debit or credit card information must comply with Payment Card Industry Data Security Standards (PCI DSS). The latest version of PCI DSS Quick Reference Guide says:

> *"The global acceleration of cashless transactions puts payment system in the crosshairs of criminals looking for easy money, Payment account data is the Number One attraction – 84 percent of data breach caseloads entailed payment card data according to Verizon. They all seek the simplest path to steal payment account data used by payment cards and related electronic payment systems. As a payment system stakeholder, your company is on the front line of a high stakes battle for keeping payment data safe from theft and exploitation. Occasional lax security enables criminals to easily steal and use personal consumer finan cial information from payment transactions and processing systems."*

PCI DSS has 12 headline requirements to comply with. These are mostly around security of the IT environment, but they also cover physical access to data, and organisational policies. Failure to comply with PCI DSS can lead to significant reputational damage and fines. It should be noted that fines can be imposed for continuing failure to meet the required standards and are not dependent on having had a data breach. Each merchant's expected PCI compliance regime is determined by the types of cards accepted, and which financial institutions (e.g. bank, or credit card company) process those transactions. Those financial institutions are known as acquirers (or acquiring banks). Each merchant is expected to have an annual assessment against the standards. This is either an external assessment undertaken by a Qualified Security Assessor (QSA) leading to a Report on Compliance, or completion of a Self-Assessment Questionnaire (SAQ), as directed by the relevant acquirer or payment brand. The results must be submitted to the acquirer, along with a separate document called an Attestation of Compliance.

The Council began its PCI compliance journey as far back as 2007, engaging a QSA in the early days to provide consultancy over how to implement PCI standards as necessary. Internal Audit has undertaken three previous reviews of corporate PCI compliance, in 2008, 2009 and late 2017. The last of those, a desktop review that took place during the Cash Office closure project, found that:

- There was no officer within the Council with overall responsibility for PCI compliance.
- SAQs were reportedly being completed and submitted in relation to the Call Centre and Cash Office environments operated by Serco on the Council's behalf. It is believed these were completed by Serco's central ICT service in Birmingham
- Card payments made to PCC online by were being taken by Capita on the Council's behalf and were considered out of scope for PCC's PCI compliance, since PCC did not store, process or transmit any card data from those transactions. Capita were declaring being level 1 PCI compliant on their payment website.
- No corporate assessments of PCI compliance were being undertaken. However, several outlying Council teams were processing card transactions either in person, or via phone call, and therefore the Council should have been having annual corporate assessment against the standards.

PCI compliance was identified as an amber risk in the Customer & Digital Services risk register rated as an amber risk. It was selected for audit in the 2022/23 Audit Plan.

Objectives and Scope

The purpose of the review was to assess the adequacy and effectiveness of PCC management controls that ensure PCC payment card processes comply with PCI Data Security Standards.

The scope covered:

- Internal and external assessment of technical and operational PCI DSS compliance
- Identification and action to address data vulnerabilities
- Timely and accurate reporting of assessment and remediation results
- Compliance oversight by PCC management across the estate including outsourced services provided by Serco and Peterborough Limited.

This audit was conducted in accordance with proper audit practices, which are set out in the Public Sector Internal Audit Standards (PSIAS). The audit was planned and performed so as to obtain all relevant information and sufficient evidence to express an opinion.

Main Findings

- There was no clear overall owner of PCI compliance, and PCI compliance is not overseen by the Cambridgeshire & Peterborough Information Management Board, or Cyber Security Board despite being about protection of cardholder data and PCI requirements mainly relating to IT environments.
- The Council continue use a number of third parties to collect payment by debit, credit or procurement card on the Council's behalf, and therefore most card transactions won't be the Council's direct responsibility under PCI, although there will be an implied indirect responsibility to ensure that contractors handling payments for the Council are themselves PCI compliant.
- Cash Office was closed. SAQs have stopped being completed in relation to the Call Centre (which is still operated by Serco), and this seems likely to be linked to the cessation of the ICT managed contract in 2020. It is understood that security of Call Centre card transactions has improved, as call handlers tend not to receive payment card details to manually enter to the Capita system. Instead customers enter their card details into the Capita system via their phones' keypads. Those transactions will be out-of-scope. A few Call Centre transactions have to be taken manually by call handlers, so those will remain in scope for PCC.
- ICT provide the IT service to Peterborough Limited and complete the IT parts of Peterborough Limited's SAQs on an annual basis. It is understood that Peterborough Limited provide self-assessment on the non-IT aspects of compliance.
- Some of the previously identified Council teams who processed card payments have now ceased taking card payments, and instead channel these requests via the Call Centre or online. Bereavement Services and Register Office continue to process card payments and have confirmed they are not asked about card security arrangements. It has also been confirmed that Gladstone Park Community Centre accept card payments. It is not known whether there any other teams processing card payments. No one is completing corporate assessments against PCI, although this remains a requirement.

Conclusion and Opinion

The Council does not appear to have ever been truly compliant with PCI DSS because it has failed to identify that some of the card transactions taken are in-scope due to the nature of how and where

they are taken, and as a result have failed to undertake, or be subject to, an appropriate corporate assessment, and to provide its acquirer with the required attestation of compliance. Lack of day-to-day ownership of PCI seems never to have been resolved and appears to be a significant factor in the lack of corporate approach. It is vital that a lead officer within the Council is identified to co-ordinate corporate assessments against the standards, ascertaining that any required remedial work is carried out in a timely manner, and provision of appropriate guidance.

The vast majority of the Council's transactions will be out of scope for PCI because the payment is taken directly by a third party on the Council's behalf, entirely outside of the PCC environment (e.g. online transactions via Capita), so most of the risk is transferred. Even if the taking of card payments is contracted out, there may be some access to card data via back office systems, so contracted out payments should still be considered within a corporate assessment to explain why they are out of scope for the Council, what access if any the Council has to card data, and whether third parties taking card payments on behalf of the Council are PCI-compliant (and whether this is a contractual requirement) either as a complete entity, or just in relation to service provided to the Council.

The lack of corporate PCI assessment doesn't necessarily mean that all or most card transactions are insecure, and there is further mitigation in some of regular pieces of work that are carried out, such as:

- ICT assisting Peterborough Limited self-assess against the entire IT environment (including segmentation for Peterborough Limited), and this work would likely be relevant to the Council's own corporate assessment
- Quarterly penetration testing conducted by a QSA on behalf of Barclays against the full Council IT environment. Although the reports identify the customer as Peterborough Limited, the findings will refer to the Council too.
- Undertaking of other IT assessments of the Council's data security environment (e.g. Public Sector Networks, IT Health Checks, "IG for NHS") that cover similar controls, although these won't correspond exactly to PCI.

It is important that all teams / services that take payments directly and indirectly are identified, and their security arrangements assessed, where relevant to PCI, to allow demonstration that the whole Council has been considered. Security arrangements will include physical or environmental security, training and guidance. For example, secure storage and disposal of card receipts; whether transactions are, or can be, performed where card details can be seen or heard; and whether payment-taking officers are given training or guidance on security of card transactions. Where security arrangements are found not to be compliant with PCI, these will need to be rectified in a reasonable timescale, and this may require allocation of a budget to allow this (e.g. purchase of appropriate software or additional system licences). Consideration could be given to getting advice from an accredted QSA where this might be helpful.

The audit opinion is Limited Assurance.

BUSINESS CONTINUITY

Introduction

Internal Audit undertook a review of the Council's Business Continuity arrangements from a strategic business position as part of the 2019 / 20 Internal Audit plan. An action plan was produced and agreed in January 2021, following the impact of the pandemic. Progress against the observations made in January 2021 was reviewed during January 2022, where it was found that several action points have remained outstanding due to the extreme impacts of Covid along with staff shortages affecting implementation. These outstanding areas have been previously reported and were due to be subject to further review in July 2022. Following recent discussions with the Head of Emergency Planning, action implementation dates have now been further delayed due to a staff resignation until early November 2022 to allow for recruitment.

In light of the findings made during the above review, Internal Audit extended the review to assess departmental business continuity arrangements as part of the 2021 / 22 Internal Audit plan, in order to provide an overall opinion on Business Continuity.

Observations

Departmental Business Continuity Plans

The Guidance for Managers: Business Continuity and PCC Business Continuity Policy (dated February 2021) both clearly state the responsibilities for all parties regarding business continuity arrangements. Elements detailed within these documents relating to the issues highlighted as part of this review are detailed below.

Managers are required to liaise with the Emergency Planning team, ensure completion of relevant documentation and subsequent Business Continuity Plan on an annual basis for all services they are responsible for. This subsequently feeds into the Annual Governance Statement as a declaration that all services have up to date Business Continuity Plans.
The Emergency Planning Team's role is to maintain policy and templates. They provide a supportive role ensuring completion of templates by departments, offering an assistance, guidance and advisory service, along with annual review of all documentation. They have responsibility for tracking and monitoring plans across the Council using the Business Continuity Tracker.

The Business Continuity Tracker maintained by the Emergency Planning Team to record information regarding Responsible Officers and annual review of Business Continuity Plans and related documentation is not currently an up to date record. The last update was January 2021, and due to the Covid pandemic and staff shortages there has also been limited ongoing correspondence with departments. The Emergency Planning Manager has highlighted this on the Risk Register for the department and this issue has been raised in the earlier reviews mentioned above. An update on progress will be sought by Internal Audit in November 2022.

During the course of this review the Business Continuity Tracker was used to select a sample of PCC departments in order to assess the extent to which Business Continuity had been addressed in the absence of the Emergency Planning Team performing their co – ordination and support role.
The sample selected represented departments who had a plan recorded on the tracker to assess the up to date position, and also those departments without records on the tracker to assess whether plans had been developed and implemented. The results showed that:-

- 25% were not available

- 50% were out of date
- 25% had been updated in a timely manner

Those that had expired were all dated late 2019 and early 2020, and therefore due for review at the time the tracker was being updated during January 2021. Although managers are responsible for the production of Business Continuity Plans ensuring they are fit for purpose, the impact of Covid 19 and staff absence within the Emergency Planning Team has resulted in plans that have not been maintained appropriately as their annual review acts as a reminder for managers. This demonstrates that departments are relying on the central function to prompt review and update.

Provision of training where appropriate for those officers with business continuity responsibilities may assist in maintenance of plans. This has already been reported within the Business Continuity review and will be subject to subsequent follow up. The Emergency Planning team plan to highlight new guidance available once annual meetings with departmental responsible officers are re – instated to offer advice and guidance as part of the update of the review tracker.

The PCC Business Continuity Policy states that the owners of Business Continuity Plans should exercise plans biennially to ensure their accuracy, and that the Emergency Planning team can assist with this. The sample selected showed that 38% had informally tested their Business Continuity Plans as a result of the pandemic.

Risk Registers

The Civil Contingencies Act 2004 requires Category 1 responders (this includes Peterborough City Council) to maintain plans to ensure that they can continue to exercise their functions in the event of an emergency so far as is reasonably practicable. Therefore, it is essential that the Council can maintain its business processes. Business continuity planning is a key process to ensure that in the event of disruption PCC's activities and services can be recovered and resume.
In light of the importance placed on business continuity, inclusion in all risk registers would seem prudent.
Current Risk Registers show that many PCC departments make reference to emergency planning and business continuity, however it would be pertinent to make it a standing item so that it is always considered when assessing risks.

Conclusion & Opinion

There is currently limited support and guidance provided to departments from the Emergency Planning team regarding business continuity planning. This was initially due to the impacts of Covid and more recently staff shortages. This is being addressed within the ongoing Internal Audit review, and the EP Team are endeavouring to implement actions by November 2022.
The EP manager has also added two relevant issues to the Customer & Digital Services risk register as follows to highlight the operational difficulties presently being experienced:-

- There is a risk that the under resourcing in the Emergency Planning Team due to vacancy and budget constraints results in insufficient staff to test plans and audit plans across both councils.
- There is a risk that the BC plans have not been reviewed in the last 2 years which could mean they are significantly out of date based on new ways of working and use of technology. These need to be reviewed in light of new ways of working and team structures.

However, it is the responsibility of managers to ensure there are up to date Business Continuity Plans in place within their departments. It appears departmental reliance has been placed on the central

team, and currently plans are not up to date. The ownership of responsibilities therefore needs to be reclarified to Managers. It is appreciated that due to the nature of the pandemic all teams will have had to adjust their ways of working, so many business continuity options are likely to have been tested as a result. This should assist the process in updating out of date plans and ensuring they are fit for purpose.

The audit opinion is Limited Assurance. This takes into account the outstanding recommendations made during the initial Council's Business Continuity arrangements review, delays in implementation as detailed within the introduction and limited documented plans evident within departments.

MAYORS CHARITIES

Introduction

The role of Mayor of Peterborough is subject to election every May. It is longstanding convention that each Mayor nominates three local charities to raise money for throughout their term of office. This is done via the Mayor of Peterborough's Charity Fund (MPCF). Each mayor brings together a small team of volunteers to run MPCF during their term of office, with support from officers provided by Peterborough City Council. MPCF raises money through holding events, such as the annual Mayor's Ball, or from receiving minor donations. After the end of the mayoral year, the net proceeds are shared out between the nominated charities. MPCF was registered as a charity in 2015 and is regulated by the Charity Commission. Under charity law, gross annual income determines the accounting and reporting requirements and whether external scrutiny of accounts is required. For 2021-22, the Mayor nominated Supporting Peterborough Veterans, Family Voice and The Light Project as their three nominated charities.

Internal Audit have been reviewing MPCF accounts and providing advice since 2018 after the Executive & Members Services Manager became MPCF's Treasurer. During an earlier review, it was identified that the MPCF's Constitution, which uses a Charity Commission template, did not reflect how MPCF works in practice, and that it was not consistent with the Memorandum of Understanding (MoU) template used annually to detail the agreed roles of MPCF, the Council and the nominated charities. Significant work was undertaken by Legal Services in 2021 to address this.

Objectives and Scope

Early examination of the Accounts Workbook for 2021-22 found that the annual gross income fell beneath the threshold at which formal detailed external scrutiny of accounts was required. The purpose of the audit was to therefore to provide assurance that accounts have been kept appropriately, that the disbursements made to the nominated charities for 2021-22 reflected the net proceeds raised, and to gauge progress of implementation of agreed actions from previous reviews.

The scope covered:

- MPCF's accounts for 2021-22.
- Outstanding recommendations and agreed actions from previous reviews of MPCF.
- Provision of advice where required.

This audit was conducted in accordance with proper audit practices, which are set out in the Public Sector Internal Audit Standards (PSIAS). The audit was planned and performed so as to obtain all relevant information and sufficient evidence to express an opinion.

Main Findings

- Internal Audit were able to confirm that the net proceeds total for disbursement to the nominated charities was correct, based on the records and explanations available. It is understood the nominated charities have been paid their shares of the proceeds.
- The original MPCF Constitution contains no ownership of, or responsibility for, MPCF by the Council, and thus the Council appears to have no power over MPCF in its current form. As the MPCF title strongly suggests significant link to the Council, there would be risk to the Council's reputation if anything went seriously wrong. The revised MPCF Constitution attempts to address this and was presented to those at the MPCF meeting of 15.7.21. To take effect, the revised Constitution needed a simple majority of MPCF members to pass a resolution agreeing

its adoption. However as each Mayor's set of volunteers is replaced informally at the end of the mayoral year, there appears not to be any official membership. Minutes of MPCF meetings record no resolution approving the revised Constitution. Charity Commission were provided with a copy but have not yet accepted it as the MPCF's new governing document.

- Since Internal Audit started examining MPCF accounts in 2018, the level of income has dwindled from £95k in 2016-17 to £19k in 2021-22. The Covid pandemic, restricting ability to hold events, has undoubtedly affected the amount of income achieved in the past three years, but significant decline was noticeable between 2016 and 2019. The Council provides a significant support to MPCF, and it is questionable whether the levels of income achieved in the couple of years before the pandemic justify MPCF as a standalone charity.
- It is understood that significant donations totalling around £20k have been received in 2022-23 from the Mayor (funded from their Mayoral Allowance) and from a local Solicitors practice. If significant donations are accepted, MPCF's annual income is inflated, causing additional work for MPCF (as a registered charity) though in reality it is the Council, in terms of officer time and greater responsibilities when certain income thresholds are reached. There can also be delays in paying the intended recipients. Where significant donations are offered, the donors should be encouraged to donate directly to the charities or good causes of their choosing as this is a quicker, more efficient way of providing them with the money, and avoids adding to the administration Council officers will undertake.

Conclusion and Opinion

The general approach of MPCF in replacing its participants almost en masse at the end of each mayoral year is not the approach expected in Charity Commission's charity constitution template, and there is a lack of understanding of what the MPCF Constitution actually requires. It is not helped that the key 'governance expert' role of Secretary is not a permanent appointment and is instead filled by annual election from mayoral invitees, potentially leading to loss of knowledge and experience. We have concluded that the Dec 15 version of the MPCF Constitution remains in force. Membership and Trusteeship of MPCF, and its Constitution must be resolved as a matter of priority.

We note that there are lots of local authorities who have their own equivalents of MPCF as registered charities, with varying income levels. However, some local authorities seem to run their charity element through main Council accounts, with a limited programme of Civic Office administered fundraising, thus not needing a separate registered charity. In light of MPCF's relatively small annual pre-Covid income, and that most income from events comes from Civic Office run events, careful consideration should be given to the purpose and future of MPCF and whether a more appropriate 'delivery model' can be found. The findings from the review are explained in more detail in the main body of the report, along with recommendations to address them, although these are mainly predicated on the current model remaining in place.

The audit opinion is Limited Assurance.

This page is intentionally left blank