Audit Objective To ensure that the administration of public money is protected against potential fraud and error.

Assurance Opinion

Most of the areas reviewed were found to be adequately controlled. Generally, risks are well managed, but some systems require the introduction or improvement of internal controls to ensure the achievement of objectives.

Number of Actions

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

Risks Reviewed

Risks Reviewed	Assessment
1. Grants are paid out to those that are not entitled because processes are not in place to prevent and detect fraud	Medium
2. Administrative staffing structures and capabilities do not protect against fraud	Low

Key Findings

The Council successfully delivered financial support to Small Business and Charities at short notice and without prescriptive and detailed guidance from Welsh Government. These payments supported the local employers in the continuation of their business at uncertain times of hardship.

A competent and capable Counter-Fraud Team undertook checks to identify potential errors and fraudulent cases. Significant pressure was placed on this team to process the grants quickly which resulted in other active fraud work being temporarily side-lined. In addition, financial checks on validity were undertaken by the Payments Team.

The risk of fraud and error was higher for the initial grant payments but reduced as the processes became more developed and embedded. This was a result of the implied need to ensure payments reached the business community without delay. The Council are recovering any overpayments.

Whilst the checking process was seen to be robust, the back-office system to support these checks was too simplistic to demonstrate the extent of the checking process and did not initially protect against duplicate payments. There was an absence of formal fraud reporting. In general, the division of duties protected against internal fraud.

The Council did not embrace the opportunity to use third party providers to undertake pre and post claim checking until too late into the award process. There was limited use of external intelligence around possible frauds

Audit Scope

The scope of the Audit looked at the following areas:

- Staffing structures and capabilities
- Administrative mechanisms used to collect and process data
- Pre and post payment claim checking
- Use of other forms of assurance
- Control to protect against internal fraud
- Performance reporting and fraud risks

Unrestricted

Full details of our audit testing are available upon request. Our audit assurance framework and definitions can be found here (www.swapaudit.co.uk/audit-framework-and-definitions)

Next Steps –

The Council, both the Senior Leadership Team and Audit Committee, should receive routine reports outlining the measures taken to protect against fraud, and the details of those cases of fraud and error detected so that they can gain assurance that appropriate controls are in place. This report should also indicate the recovery position of overpayments and fraud cases.

Appendix A	Findings & Action Plan

Finding	Action
A.1 Staffing arrangements and division of duties The Senior Manager Income & Awards was responsible for the overall management of the payment of the grants for both small businesses and charities. Staff within the Council's Corporate Anti-Fraud Team were responsible for the actual processing and checking of the claims. A sample of cases were checked internally for quality. The processing of claims was mostly carried out by the two Intelligence Officers within the team, with the Fraud Officer and Senior Investigator responsible for additional checking including duplication and control checks. Additional assistance was also provided by the Technical Manager from within the Income & Awards Team. The Senior Manager Income & Awards was responsible for downloading records at certain stages of the process and for moving processed claims onto the master payments spreadsheet. An Officer outside of the Corporate Anti-Fraud Team processed batches of payments to go to Creditors. The Council's Accounts Payable Team undertook final checks on the validity of bank account details. Telephone enquiries made by members of the public, including via the dedicated helpline, were dealt with by a separate team of staff and were not answered by the application processing team. As the grant process evolved updated information was routinely sent out to staff responsible for telephone enquiries via email from the Senior Manager Income & Awards. Processes were the same for both types of grants.	No action required

Priority		SWAP Reference	N/A
Responsible Officer	N/A		
Timescale	N/A		

Finding	Action
A2. Guidance & initial payment of Small Business grants Guidance and criteria for grant entitlement, for both small businesses and charities, produced by the Welsh Government was minimal. The Senior Manager (Income & Awards) stated although guidance from the Welsh Government was very basic, there was an emphasis from the Welsh Government to get grants paid to customers as soon as possible to avoid undue hardship. Regular weekly meetings were held with the Welsh Government and other local authorities were contacted to help establish best practice. The Senior Manager (Income & Awards) stated that it was a judgement call for each local authority as to how they would proceed with the processing of payments. The decision on processing was agreed by the Section 151 Officer. In order to make payments as swiftly as possible Powys County Council made 793 initial grant payments based on the conditions of the grant against the database and then an eligible list was extracted from the database of properties used for Non-Domestic Rate purposes. The database was maintained based on property information, including rateable values, provided by the Valuation Agency Office (VAO). Customers who received a grant payment at this stage, already had received a bill in the previous 12 month together with a bank account. Customers were advised by letter of the award and the conditions of the grant. It outlined that the letter was their acceptance of the grant and if a later issue around non eligibility was found, it would be reclaimed. Subsequently, the Council have stated that 97.7% of these initial grant payments were found to be accurate. 1.5% of Inaccuracies arose due to issues identified with the eligible list that reflected incorrect information within the original NDR property list. These Issues included: • Properties that had been split up that were not reflected on the list. • Grant due to a different member of the family. • Taxpayer not yet told PCC that moved into or out of a property. Taxpayers have a duty to tell PCC of any relevant changes, but for those entitled to the 100% Small Business Rate Relief, although they receive annual notification regarding NNDR from PCC, there may be a tendency not to keep the Council informed of changes.	No Action Required

Priority		SWAP Reference	
Responsible Officer	N/A		
Timescale	N/A		

Finding	Action

| **A3. 2nd Phase of payments** | No Action Required |

| **A3. *2nd Phase of payments***
 A letter was sent to those on the eligible list who had not previously been awarded a grant. Letters were sent to the business address and invited customers to complete an online form on the PCC website. To complete this form, customers needed their business rates account reference and the unique identifying code that appeared on the letter. Completed forms were downloaded and issued to the officers responsible for the assessment of the grant. | |

Priority	**N/A**	**SWAP Reference**	
Responsible Officer	N/A		
Timescale	N/A		

A4. *Eligibility and Fraud Checks*
Members of the Counter Fraud Team undertook the eligibility and fraud checks. The process they used had the following controls in place:

- The original eligible list formed the basis of initial eligibility.
- All applications were done through the on-line form
- Customers were marked off a master spreadsheet when they were paid. They were blocked off if ineligible or the claims are duplicate.
- I.D. and active business checks were undertaken.
- Some details of checks carried out are noted on a spreadsheet. However, the spreadsheet did not fully record the actual results of the check and who had undertaken those checks.
- Officers sought clarification by contacting customers; requesting confirmation in writing re any issue; looked at Civica for supporting documentation etc.
- Measures were in place to protect against any false internal claims.
- The Council responded to Anti-fraud bulletins

In general, as further tranches of grants were awarded, the checking process became more refined with assurance taken from the checking undertaken from previously awarded grants

The Accounts Payable Team did a cross check with the supplier database, to check if the Council had already paid the bank account. If we had a bank account set up as a permanent "supplier", the team checked the supplier matched the grant recipient and processed the payment against that supplier account. If the applicant was not set up as a supplier, the payment was made as a one-off payment. Any duplicates identified were not be paid, and the duplicates were then checked for validity.

Reports were sent to managers outlining the payments processed.

<An Action should be included by the Council to ensure that the audit trail of the checks undertaken is more transparent in their administration system.>

Priority	3	**SWAP Reference**	
Responsible Officer			
Timescale			

A5. Post Payment and Data Checking

Several digital solutions such as CiFAS, Spotlight and Experian were available for both pre and post payment checking that gather information from various sources to give indications about whether there are fraudulent indicators. However, the Council used Spotlight for grants to charities and for post payment Experian checks. It did not implement these opportunities to provide simple assurance until much later in the award process after most of the claims had been paid.

These simple digital checks would have been more effective if used in a pre-claim checking process for all grants awarded.

The level and success of post payment checking is still unclear.

The National Fraud Initiative (NFI) have released post payment data matches that identify potentially incorrect and fraudulent claims to the Council.

The data matching exercise identified potentially duplicate claims within Powys. It should be noted that these are not necessarily fraud or error but could be the result of misleading payment data. The Council are in the process of reviewing the matches to determine if they require further follow up work.

< Action required by the Council on the use of digital and pre and post payment systems to identify fraud>

Priority	2	SWAP Reference	
Responsible Officer			
Timescale			

A6. Overpayments and Fraud

On the 24th of September 2020, the Council had paid 4584 grants with a total value of £52, 842,610.

The following table was the overpayment position as at:

Overpayment Types	£'s	Cases
Duplicates	105,000	9
Ineligible	515,000	32
Repay	90,000	9
Fraud	40,000	4
Overpayments	**750,000**	**54**

The following commentary was provided on the above figures:

- Duplicate payments – are admin errors. So less than 1% of total payments.
- Ineligible – mean those with error by the customer and that were not entitled. These were found when doing intervention checks, checking data sources or assurance checks. Some were just error, but some could be fraud but there was not a high enough evidence threshold to say they were fraud.
- Repay – means people who wanted to give back their payment as they were eligible but didn't want it
- Fraud are ones where we have proved fraud from an evidence perspective.
- Recovery was 68%.

The auditors were provided with a more up to date position as of 20th October 2021 where it was stated that 58 cases of proven fraud were identified. More details around these cases has not been available for inclusion in the report.

The reporting of grants awarded and the position relating the potential fraud is inconsistent and informal. Improved fraud reporting would give greater transparency on the risks facing the Council.

< An action is required by the Council identifying how it can more effectively report on fraud performance and fraud risk in the covid grant process>

Priority	3	SWAP Reference	
Responsible Officer			
Timescale			

Covid Grants Fraud Risk Assessment

The following is a fraud risk assessment compiled by SWAP for covid grant administration based on the information gathered during the audit in Powys.

Ref	Risk	Control Measures identified by Audit	Residual Fraud Risk (after Mitigation)
B.1	A person/ business (i.e., name of undertaking) identified from the billing authority's records as the rate payer of a 'hereditament' located in Wales and eligible for a Covid Grant, who failed to notify the authority they had moved out, leaving the property unoccupied or rented by another business prior to the date of the commencement of the widespread national restrictions, applies and receives funding they are not entitled to.	The first tranche of grant payments was made directly to those persons identified in the Council's billing records as a rate payer of a 'hereditament' located in Powys. These payments were made without the expressed request of the bill payer but were processed automatically to reflect the urgent requirement to address the hardship of business during the lockdown. All further grants were process using the online application process sometimes with support over the telephone. The process collected data to allow the effective eligibility tests whilst undertaking checks to ensure entitlement. All grant recipients were aware of the eligibility criteria by directing them to the relevant and Local and National websites on the Application form. All businesses received a letter informing of the eligibility criteria and what to do to apply. The letter also advised the customer must tell the Council of a change It was expressed that any grant may be liable for recovery if obtained incorrectly or dishonestly.	Medium
B.2	A person/ business in administration, insolvent, subject to a striking off notice, or had ceased trading prior to the date of the commencement of the widespread national restrictions applies and receives Covid Grant funding they are not entitled to	Checks were made whether the business is in 'liquidation or dissolved' prior to grant payment. The Council checked the business' status on Companies House when approving the grant before payment. Where the business is flagged as 'in liquidation' or 'dissolved', the grant will be withheld. Some digital and post payment checks were added as the process evolved. The Counter fraud Team checked each application, though it is difficult to evidence the detail of those checks as the simplist results is recorded , but not a more detailed audit trail.	Low/ Medium
B.3	A person/ business not mandated to by the Government applies and receives Covid Grants funding they are not entitled to.	The application form, guidanceand web make it clear the eligibility criteria. The Council notified applicants by letter those all companies that were eligible to apply for the grant in the first tranche. Subsequent grants were processed either online.	Low/ Medium

		The Counter fraud Team checked each application, though it is difficult to evidence the robustness of those checks due to the recording rather than their rigour.	
B.4	An individual/ third party perhaps using open-source information (e.g., Companies House data, business website or linked in account) impersonates a person/ business eligible to receive Covid Grants funding they are not entitled to, and/ or redirects payment into their own bank account.	For those where there was no previous history of business operation, the Council requested that grant recipients complete an information/ data collection form via an online platform which includes entering their Billing Reference Number and a code sent by a letter. However,, this is not published information and if a business is unable to provide the billing reference. Additional information is requested in these cases. Third party bank verification services, such as Experian, Cifas, to identify any warning flags of possible account fraud were considered late in the awards process and were not done prepayment.	Medium
B.5	A person/ business hacks a genuine email account to facilitate mandate fraud funding they are not entitled to.	Some bank account checking was undertaken where possible.	Low /Medium
B.6	A person/ business sets up a fake website or phishing emails to harvest genuine applicant details and submit false applications to receive grant funding they are not entitled to.	Some Pre- payment checks on business validity were undertaken where possible Post Payment checks with third parties were added during the administration process.	Low /Medium
B.7	A person/ business resurrects a 'dormant' company, perhaps by changing director, to apply for and receive they are not entitled to.	Simple pre-payment checks on business validity were undertaken. Post Payment checks with third parties were added during the administration process.	Low/ Medium
B.8	A member of staff in the Local Authority with access to financial documents, systems and/ or payee standing data, falsely creates or diverts payments, perhaps in collusion with a third party, which leads to a financial gain/ benefit for the individual or another.	There is separation of duty between is information collection, processing, and payment. The Senior Manager (Income and Awards) was responsible for the information for all aspects of the process apart from making the actual payment. A Counter Fraud Team were responsible for the processing and the investigation process. Bank account Changes were made through a separate process under the control of the Accounts Payable Team/ independent person in Income and Awards.	Low/ Medium