Summary of Audit Findings

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

Data Breaches / Protection – Final Report – March 2026

Audit Objective	To conduct a follow up audit in order to provide assurance that when Data Breaches occur, they are reported/actioned as per agreed policy/protocols.

Executive Summary

Assurance Opinion	Management Actions		Organisational Risk Assessment	Low
The review confirmed a sound system of governance, risk management and control, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.	Priority 1	0	Our audit work includes areas that we consider have a low organisational risk and potential impact.	
	Priority 2	0		
	Priority 3	0		
	Total	0		

Key Conclusions

The updated Data Breach Policy and the new toolkit provide clear definitions of data breaches and near misses and reporting procedures for staff. The Data Breach Toolkit also includes practical resources comprehensive guidance, templates, and training materials to support the Compliance and Information Governance team in managing data breaches effectively. Reporting requirements to the ICO are well-defined, and the triggers for escalation are appropriately established.

Based on the fieldwork undertaken, the new Data Breach Register is operating effectively as a central system for recording and managing breach cases. It integrates well with the reporting process, ensuring that all required information is captured consistently and accurately. The Data Breach Toolkit also supports robust and comprehensive breach reporting. Its alignment with the reporting form ensures that essential information is gathered at the point of submission. The high level of data completeness within the register indicates that the toolkit is being used appropriately and is enabling accurate record-keeping. Overall, the toolkit provides a structured and reliable framework for managing data breaches.

Audit Scope

The audit included a review of the data breach process arrangements in place, including, but not limited to, a review of the following areas:

- Policies and process for reporting/responding to a data breach
- Training provision for service areas
- The data breach register
- Data breach statistics
- Data breach communications.

Other Relevant Information

Overall significant progress has been made since the previous audit, in particular with the development of the Data Breach Toolkit. Ongoing development and refinement of the toolkit and policies will support this work even further. The updated Data Breach Policy is in the process of being rolled out across the councils at the time of reporting. The Reporting Data Breach Policy is in the process of being removed from the councils' websites as this is considered to no longer be relevant due to data breaches being included in the main Data Protection Policy available to the public.

It was noted as part of the audit that the Information Security Standards policy and the Acceptable Use policies are out of date. Furthermore, we have been advised that the Data Protection Policy is in the process of being updated to ensure it is in line with the new Data Breach process. We have not raised these as actions as we have been advised that they do not fall within the remit of the Compliance and Information Governance Team. We have informally advised ICT of these findings.

A staff survey was undertaken as part of this audit. The responses from this indicate broadly positive views across policies, training, reporting and communication relating to data breaches. Those responding to the survey generally stated that policies are accessible and comprehensive, training is adequate, breaches are being reported, and that remedial action is taken. There were a couple of comments in the survey, which we suggest are considered by the Compliance and Information Governance team: one requesting additional or more tailored training, and another regarding increasing the visibility of breach-related communications. One of the final comments from the survey was to say, "I have always found the data team supportive and approachable". A summary of the survey results has been provided to Management for information and to inform future activity.

Bank Reconciliations – Final Report – March 2026

Audit Objective To provide assurance that core financial processes are operated in accordance with agreed policy/procedure and with the Financial Rules.

Executive Summary

Assurance Opinion

The review confirmed a sound system of governance, risk management and control, with internal controls operating effectively and being consistently applied to support the achievement of objectives.

Management Actions

Priority 1	0
Priority 2	0
Priority 3	1
Total	1

Organisational Risk Assessment

Low

Our audit work includes areas that we consider have a low organisational risk and potential impact.

Key Conclusions

At the time of audit work (December 2025) there were several outstanding entries in the Council's suspense account, with the oldest unresolved item from 2021. The Publica Casual Business Partner Accountant is working to clear historic balances.

Items in suspense should not be held over several years with no resolution. Suspense account entries including historical balances are being resolved.

We can confirm the monthly bank reconciliation is being completed in a timely manner, it is appropriately authorised and it is in accordance with the financial rules (except for the clearing of the suspense account discussed above).

Audit Scope

The following areas were reviewed:

- Suspense account monitoring processes.
- Frequency and accuracy of bank account reconciliations.
- Authorisation process for bank account reconciliations.
- Implementation of previously agreed actions.

The period reviewed was April – December 2025.

Other Relevant Information

The Publica Interim Head of Finance advised (November 2025) she is working on a Business World project with Publica IT Officers to match and move repeat payments which go into the suspense account because of incorrect reference numbers.

Accounts Payable (Continuous Analysis) – Final Report – March 2026

Audit Objective	To identify potential duplicate payments. To summarise and present any such payments to the Accounts Payable (AP) team for remedial action.

Executive Summary

Assurance Opinion

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

Management Actions

Priority 1	0
Priority 2	0
Priority 3	0
Total	0

Organisational Risk Assessment Low

Our audit work includes areas that we consider have a low organisational risk and potential impact.

Key Conclusions

Accounts Payable (AP) use Business World to process payments on behalf of partner organisations and Councils. We used BW to generate AP reports capturing payments to suppliers between 1st April 2025 and 30th September 2025.

A total of 90,160 lines of transactional data was analysed. We cleansed the data and applied conditional formatting to highlight potential duplicate transactions. These transactions were inspected to establish whether mitigating circumstances could be identified (e.g. credit note). 3 suspected duplicates with a potential overpayment value of £622.06 were forwarded to the AP team for further investigation. This represents <0.001% of the total payments analysed.

At the time of writing this report, all potential duplicates for 2025/26 Q1&2 have been resolved. However, AP are managing 1 unresolved payment totalling £126 from 2024/25. We will continue to monitor this through to resolution.

Audit Scope

Our review covers Q1 and Q2 of the 2025/26 Financial Year. We check for potential duplicate payments at Councils and organisations hosted on Business World.

Findings have been summarised and reported to the Accounts Payable team, for further review and remedial action where necessary.

Next Steps

AP continue to work with officers and suppliers to rectify the unresolved duplicate transaction. Potential duplicates for Q3 2025/26 have been forwarded to AP for further investigation.