

Appendix 5

| Audit | Finding Description | Priority | Action | Rec | Original Due Date | Owner | Current Due Date | Update Comments | Resolution |
|--------------------------------|---|----------|--|---|-------------------|---------------------|------------------|--|--------------|
| WLDC 2018/19 - Portfolio Board | <p>The Portfolio Board provides guidance, support and challenge to projects and programmes of work. It does this through review of summary reports. The reports provide a Red, Amber or Green (RAG) rating and a comment about the confidence the programme or project manager has on delivery.</p> <p>We found that the process for determining these ratings and confidence levels on delivery is through the author of the summary report discussing the project with the project lead, and taking their information from that verbal update.</p> <p>In essence this means that the Portfolio Board is placing some of its reliance on programme and project delivery on an estimation of risk and confidence and not on a set consistent process or system.</p> | Medium | Review of assessment process i.e. Performance and Programme Team confidence levels | A consistent process or system should be introduced to ensure there is assurance for the board that the information it receives is accurate. That the board is confident it has the right ratings and assurance from the summary reports on programme and project delivery. | 31.08.2018 | Darren Mellors | 31/10/18 | 6 month review of Senior Project Officer is due to be undertaken early October. This review will also ensure that documentation and procedures are fit-for-purpose. | Not Actioned |
| WLDC 2018/19 - Procurement | <p>The Council has a long-standing I.T. Software Maintenance contract, which is not recorded on the CMS or the Contract Register on the basis that its annual value falls below procurement thresholds.</p> <p>The contract has been continuously rolled over on an annual basis since its inception in 2003 (annual spend ~ £7,000). CPPR's state that the value of all contracts must be determined based on their expected lifetime value, or for open-ended contracts over a notional 4-year period; with those exceeding procurement thresholds being subject to more stringent procurement rules.</p> <p>No evidence has been provided to support the Council's rationale for continuing roll-forward with this supplier and that due process per the CPPR's is being followed, i.e. assurance that this contract is not an example of disaggregation to circumvent CPPR's.</p> | High | A review of rolling contracts, particularly ICT related, will be undertaken to identify the correct means by which they should be treated. | Identify and review rolling agreements to determine if compliant with CPPR's. | 31.07.2018 | James O'Shaughnessy | 31.12.2018 | Details of all ICT related contracts has been obtained, Currently reviewing to see if contracts are in place or rolling. This work forms part of the preparation for CRM/ERP procurement. Revised completion date of 31.12.2018. | Not Actioned |
| WLDC 2018/19 - PCI DSS | <p>The first step of PCI DSS is to accurately determine the scope of the environment. The scoping process includes identifying all system components that are located within or connected to the cardholder data environment. Scoping must occur at least annually, prior to the annual assessment. The Council therefore needs to identify all locations and flows of cardholder data, and identify all systems that are connected to or if compromised could impact the Card Data Environment (CDE).</p> <p>The original recommendation to document an annual scoping exercise has not been implemented.</p> <p>It may seem unnecessary to periodically confirm the points of entry to the Council for card data, and we acknowledge that there are compensating controls in that unauthorised devices attached to the network should not be able to consume</p> | Medium | The Council will ensure that as part of its scoping function a record of this is maintained and reference is made to the appropriate guidance. | <p>a) The Council should seek to ensure that it adequately documents all aspects of PCI DSS compliance.</p> <p>b) The Council continues to utilise the guidance within the full standard to help inform the PCI DSS compliance work it is required to undertake.</p> | 30.09.2018 | Cliff Dean | 14/12/18 | SAQ update has been completed - work on-going re documentation processes | Not Actioned |