Appendix B – Closed Actions

Recommendation (taken from Audit Report)	Risk Rating	Status	%	Management Progress Update December 2019 (Audit Committee January 2020)
Financial Systems – Payment Controls Assurance				
Review and refresh the existing documented policy framework across all areas of scope including Finance, Procurement and Payment policies, and Purchase Card user guidance. Produce system workflow documentation for key payment process and incorporate into documented policies to be shared across GMCA (noting that a number of these may change). Review BWO access rules based on system roles rather than individuals. Review and define key areas of responsibility across the finance functions to ensure these are properly defined and avoids duplication. Consider specific user training requirements across GMCA and responsibility for delivery of these.	Significant	Completed	100%	• Procure to Pay processes have been mapped with as is and potential improvement areas identified. • Ongoing training and procedural documentation has been developed for users. • Training provided for the Finance team and deputy systems administrators. • Approval limits and approvers have been updated to comply with the GMCA constitution. • Upgrade to BWO! which will address the P2P process changes and necessary updates.
Supplier (create and amend) approval should be within BWO as opposed to the current paper approval outside of the system. Ensure an adequate audit trail is captured in BWO for new and changes to supplier details that shows as a minimum, date of creation / amendment, who input, who approved, details input / changed which can be examined to see a full history of changes made to the supplier.	Significant	Completed	100%	The documenting of workflow and segregation of duties has been undertaken to ensure any changes made to the supplier master file have been checked. We have reviewed audit trails within BWO to ensure that the audit trail is sufficiently captured in BWO for new and changes to supplier details showing date of creation / amendment, who input, who approved, details input / changed. Monitoring of privileged access (super user access) to ensure system activity is monitored and standing access to privileges has taken place and necessary changes are underway. A report that monitors super user activity has been developed.

Appendix B – Closed Actions

Non-Order Payments - Define the payment types to be made through this payment route with a view to limiting the volume and value of payments processed via this method.	Significant	Completed	100%	This has been reviewed and processes amended to ensure payments are now made using purchase orders. Training has been delivered to facilitate this. Single payment instruction form designed. Evidence of compliance with contract procedure rules being determined for this process.
Payroll ITrent Application Audit				
Policies and procedures across all areas should be created and reviewed on an annual basis. These should be made available to all users with measures in place to ensure compliance, for example to ensure the new starter's process is followed.	Significant	Completed	100%	All actions are completed and ICT Security policies are drafted and being reviewed through appropriate governance
A formalised annual/six monthly review of the access of all users to confirm it is still appropriate is considered good practice.	Moderate	Completed	100%	All actions are completed
An access profile matrix should be created, clearly detailing each role and the corresponding access privileges.	Significant	Overdue	100%	All access levels have been reviewed with the access owners and rebuilt in the Electric theme
Business World On! Application Audit				
A regular governance meeting should take place to discuss the future of the application and any issues being faced by the business.	Significant	Completed	100%	User group has been set up to influence strategic direction of the system.
The conversations around the long and short term strategies for BWO should be formally captured as part of a strategy/roadmap which can be used to inform the wider organisation.	Moderate	Completed	100%	User group has been set up to influence strategic direction of the system, an overarching user group will be set up to oversee developments once the system is upgraded. Development log developed to capture potential areas for improvement.
Evaluate whether super users need access to privileged accounts at all times, and create a monitoring report to review super user activity within the application.	Significant	Completed	100%	There are no super users set up within the system. There are three System Admin roles within the system. Tracking of access reportable.
Information Security				
Identification of senior information security stakeholders, with clearly defined accountability for key activities (e.g. ensuring that staff complete mandatory information security training) should be established. A business impact analysis, whereby the critical services, processes and activities for each business area need to	Significant	Completed	100%	The Head of Information Governance/DPO is now in post. Senior information Asset owners have been identified at Head of Service level within the organisation. An Information Governance Team is in place and a business case for further investment in this area has been approved through the

Appendix B – Closed Actions

be clearly defined and subsequently reviewed, should be completed for all key services and departments. This should then be reviewed on a regular basis to ensure it remains relevant. Review the risk management framework to help ensure key cyber/information risks are included and formally accepted by the executive team. In addition, each risk should have controls associated with it that can be tested for operational effectiveness. The outcome of cyber/information security business assurance testing should be reported to the executive team on a monthly basis.				Strategic Integration Review programme to continue developing the organisation's maturity concerning information management. Cyber and information security position is reported to SMT on a monthly basis. Cyber and information risks are monitored by the Corporate Risk Management Group and recorded in the Corporate Risk Register.
GMCA should create, approve and implement the following policy documents as a minimum: • Information Security Policy • IT Acceptable Usage Policy • Cyber Incident Management	Significant	Completed	100%	Full ICT policy review has been undertaken, and overarching policies prepared for appropriate approvals. Overarching policy framework set with policies drafted awaiting approval.
Cyber incident management response should be formally tested at least annually, either as a “live” exercise or a desktop-based scenario. Cyber incident management should be incorporated into GMCA’s broader business continuity test plan.	Significant	Completed	100%	Process has been tested as a desktop exercise and in live incidents a number of times over the past 12 months
A mandatory information security training module should be established, incorporating GDPR, with a requirement that staff complete refresher training at least annually.	Significant	Completed	100%	Mandatory annual training in place and being monitored by SMT
Ensure that a process is defined to obtain assurances from all third parties responsible for providing IT related services (e.g. system development) that they operate a robust information security environment.	Significant	Completed	100%	Third party policy and process in place
GMCA should explore the possibility of enabling encrypted email as the default method of information transfer, potentially by enabling TLS rejection which would prevent	Significant	Completed	100%	TLS security on all email has been implemented, and there is an option of Egress for those needing greater levels of security. This has been communicated to all users.

Appendix B – Closed Actions

any unencrypted information from being sent in the first place.				
GMCA should conduct proactive threat monitoring, either by using existing threat intelligence tools or by conducting workstation/server reviews to identify security weaknesses that could allow a malicious user to escalate privileges. The review of build security should encompass areas such as system services, core security configurations, user accounts and permissions, password policies and auditing policies. This review might also extend to perform a full configuration review of the installed anti-virus/malware and internet browsers.	Significant	Completed	100%	Threat monitoring tools implemented and used actively to monitor potential threats
Establish a formal penetration-testing schedule, which extends beyond the GMCA's existing vulnerability management solution. Ensure penetration testing is carried out for all significant changes to the IT environment, including the introduction of new systems at least on an annual basis.	Significant	Completed	100%	Penetration test completed with minor adjustments actioned to improve security
Additional full-time resource should be made available to assist with the implementation of the planned information security activities	Significant	Completed	100%	ICT Security Manager role filled on a temporary basis. ICT Security Manager post re-sized to appropriate level and re-advertised.
Purchase cards				
The process for cancelling cards when staff leave the Authority was inconsistent and not formally linked to the corporate leaver's process. We reviewed a list of Cardholders with Procurement and a small number of users were identified who had left the Authority whose cards had not been cancelled.	Moderate	Completed	100%	The purchase card administrator receives the weekly HR report on new starters, movers and leavers, which will enable closer scrutiny, monitoring and improved management of p-cards.
There is no formal review of Cardholders to ensure their access to a purchase card and usage remains appropriate to business requirements. Our testing showed at least 30 cardholders that had not used their cards this financial year	Moderate	Completed	100%	All redundant cards now cancelled and the p-card administrator continues to monitor movers and leavers on a regular basis.

Appendix B – Closed Actions

A significant number of cardholder transactions from the previous financial year had received no approval within the system. Whilst these transactions were accrued for as part of the year end process they had not yet been appropriately accounted for in the financial ledger as this process is only completed when transactions are approved within the system.	Significant	Completed	100%	Unapproved spend which relates to 2017/18 posted to the correct cost centres by journal, likewise, where a previous cardholder has left the organisation.
Existing purchase card policy guidance provided insufficient advice over acceptable usage.	Moderate	Completed	100%	The new policy makes clear that p-cards must only be used when no corporate contract exists and a p-card is the only viable option. New online travel solution now in place to deal with business travel and accommodation and business trade accounts currently being arranged as alternatives to p-cards.
A significant proportion of transactions were not supported by a valid invoice or VAT receipt	Significant	Completed	100%	The uploading of receipts is mandatory in the new p-card policy and period end requirements are also made clear for card holders and line managers. Ongoing monitoring takes place on a monthly basis.
There was no clear timetable for month end checking, approval and reconciliation of all purchase card activity. There was a monthly reconciliation of the Barclaycard transaction list to the direct debit payment. However, there was no reconciliation to confirm all transactions had been correctly uploaded into Agresso BWO and posted in the financial ledger	Significant	Complete	100%	Each month a reconciliation is performed to match the Barclaycard transaction list to the direct debit and corrective action has been taken where necessary. Previous periods are being retrospectively reconciled via recently received statements from Barclaycard. The transaction lists from Barclaycard are accessed and uploaded to the suspense account on the 11th of the month and available on the system for approvers by 15th of the month.
VAT was not being claimed against any purchase card spend. Data, which would allow for the reclaiming of VAT for VAT enabled suppliers, is received from Barclaycard as part of the statement download. However this VAT information is not captured during the upload into Agresso BWO and consequently not reflected in the financial ledger or subsequent VAT claims	Moderate	Complete	100%	The ability to post transactions, separating the VAT value directly to the VAT control account has been investigated. Technical consultancy is required to address this, and in light of the small amounts of VAT that would be recovered, the implementation costs outweigh the benefits, and in the short term, the costs associated with this outweigh the claiming VAT back. Therefore, we have fixed the VAT code to zero VAT.

Appendix B – Closed Actions

Pot Hole Action Fund 2017/18				
To note the certification completed for 2017/18 and the outstanding certification requirements which we will aim to complete before 31 March 2019.	Not rated	Completed	100%	All actions implemented
Local Growth Fund 2017/18				
To note the significant underspend being reported to date. Any impact on future funding restrictions should be established as part of the annual conversation with DfT. GMCA Treasurer and GMCA Group Finance Lead to seek additional assurances from TfGM Finance and PMO in relation to the following: • Reconciliation of figures between GMCA, TfGM and Districts in terms of funding allocations, expenditure profiles and forecasted spend for LGF funding programme. • Any significant disparity between percentage scheme completion and costs claimed should be reviewed to ensure that any undue delays over cost claims are avoided. • To assess the risk associated with delays in scheme delivery timetables and any adverse impact on existing staffing capacity across GMCA and partner organisations. • To note the certification completed for 2017/18 and the major underspend being reported on the CCAG programme to date. • Confirming with DfT the current funding and spend position for CCAG2 and acknowledgement that this funding can continue to be spent beyond 31 March 2018 deadline without clawback. • Agreement with DfT of forecasted delivery completion dates and spending profiles for programme work streams • Assess any impact on future funding requirements and Government confidence as part of the annual conversation with DfT.	Significant	Completed	100%	All actions implemented. Regular monitoring and action taken where schemes are underspending. A paper has recently gone to the GMCA to approve new schemes for the Programme to ensure full spend is achieved. Work is now progressing against the CCAG plan; works will need to continue post March 19 to complete the programme. TfGM are in regular dialogue with DfT about progress, and the audit recommendations have been completed.

Appendix B – Closed Actions

To seek additional assurances from TfGM PMO in relation to the following; • Management and oversight of scheme delivery and reasons for significant programme delays. • Disparity over scheme completion and costs claimed, to ensure that any undue delays over cost claims are avoided. • Any necessity to build capacity within Districts and TfGM to avoid excessive delays in getting schemes underway.				
ICT Strategy, Governance and Programme Management				
Management should establish a stakeholder engagement strategy covering stakeholder analysis, planning, engagement channels and a communications plan. This would help ICT have a more robust process around prioritisation based on reliable data which in turn support the delivery of the GMCA wide objectives Also, management should define the responsibilities of each business area stakeholder regards engagement with ICT to ensure they are available to provide and coordinate input into strategy activities consistently and this should include documentation and supporting data to support articulation of each business area requirement.	Significant	Completed	100%	Quarterly engagement set up with wider CA. PfC manages workload through programme governance. Formal governance in place to capture business requirements and for it to be reviewed on a weekly basis by the service Prioritisation of projects agreed through Programme for Change and Digital Strategy Board leads
Management should seek to have the proposed new ICT Structure ratified at Board level as soon as possible so that clear roles and responsibilities can be implemented to oversee and support the delivery of ICT services.	Moderate	Completed	100%	Structure fully implemented in October 2019
Management should revisit the ICT governance methods / models developed and agreed and ensure that the current governance processes such as The Digital Strategy Board and ICT Operations Group align with the requirements set out within it.	Moderate	Completed	100%	ICT Operation Group set up with an initial meeting in Jan 2020
Culture and Social Impact Fund - Governance Audit				

Appendix B – Closed Actions

A formal quality assurance process should be developed and implemented to ensure consistency in assessments for future funding programmes		Minor	Completed	100%	Quality assurance process developed and used in appraisal of current funding round (Jan, 2020).