Appendix B – Closed Actions

Recommendation (taken from Audit Report)	Agreed Management Action	Risk Rating	Status	%	Management Progress Update August 2019 (Audit Committee October 2019)
Finance – Payment Controls Assurance					
System Documentation 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.	The recommended actions will be incorporated into the scope of service integration reviews for Finance and Procurement. A specific Action Plan will also be maintained.	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. This has been placed in the Learning Management System for users to access for training purposes. • Training has been provided for the Finance team and deputy systems administrators. • Approval limits and approvers have been updated to comply with the GMCA constitution for the 2 limit levels below £250k and above. • Upgrade to BWO! planned for September 2019 which will address the P2P process changes and necessary updates.
Supplier Masterfile Supplier (create and amend) approval should be within BWO as opposed to the current paper approval outside of the system.	The recommended actions will be incorporated into the scope of service integration reviews for Finance and Procurement. A specific Action Plan will also be maintained.	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

Appendix B – Closed Actions

Audit Trails: 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. Supplier Due Diligence: The role of the Procurement Team in the supplier create process should be reviewed and agreed. Once determined, an adequate audit trail of supplier create and amendments is in place, periodically this should be reviewed for any errors or erroneous entries.					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.
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. If one off salary or pension payments are to continue to be paid via this method then review and address any issues around (confidentiality / restricted access to payment details). Consider the approval levels for these payment types to ensure they are consistent with other payment streams and agreed delegated authority approval limits. Ideally these should be a minimum 2-way match requisitioner and	The recommended actions will be incorporated into the scope of service integration reviews for Finance and Procurement. A specific Action Plan will also be maintained.	Significant	Completed	100%	Most non-order payments are for canteen supplies, legal services, volunteers, honorariums and credit notes. We have worked with key users to ensure Purchase Order workflows are being used. Canteen supplies had a high volume of non-order payments. This has been reviewed and processes amended to ensure payments are now made using purchase orders. Training has been delivered where appropriate in order to facilitate this. Single payment instruction form designed. Evidence of compliance with contract procedure rules being determined for this process

Appendix B – Closed Actions

approver roles workflowed in BWO thus ensuring separation of duties is enforced. Ensure there is a single payment instruction form to record payment requests, rather than random free-form instructions to Exchequer Team. Given that these bypass workflow to Procurement Team for release, there should be a requirement to evidence compliance with procurement and competition rules where required.					
Payroll ITrent Application Audit					
Policies and procedures across all areas of the scope 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.	Process mapping session has begun work on this. Process maps plus guidance on key areas to be produced with regular review date, being picked up as part of Programme for Change work	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.	Access Role owners to be identified and meetings set up on a 6-month basis. Recertification processes to be established as core part of Digital Services and IG work on improving security.	Moderate	Completed	100%	All actions are completed

Appendix B – Closed Actions

Finance BWO Application Audit					
A regular governance meeting should take place to discuss the future of the application and any issues being faced by the business.	Business World On User Group to be set up with a clear Development Strategy and structured meetings.	Significant	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.
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.	This links closely to item above and a formalised structure to govern BWO is required to drive the development map for the system.	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.	Super Users to be set up with access requirements for usual role requirements plus an additional log in with separate password for Super User tasks only.	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					
Information Security Governance 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 be clearly defined and subsequently reviewed, should be completed for all key services and departments. This	Refine the initial plan for improving information security using the GDPR Working Group as the approval route for new policies and roles associated with better information management e.g. identification of Information Asset Owners and System Owners Deliver the priority policies by end Aug 2018. Participate in the planned Business Continuity Planning update and	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 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 through the Corporate Risk Management Group and recorded in the Corporate Risk Register.

Appendix B – Closed Actions

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.	exercise to test assumptions. Cyber/information security position to be reported to SMT on a monthly basis				
Policies and Procedures GMCA should create, approve and implement the following policy documents as a minimum: • Information Security Policy • IT Acceptable Usage Policy • Cyber Incident Management	ICT policies are being developed currently These policies will be approved through relevant governance groups.	Significant	Completed	100%	Full ICT policy review has been undertaken, and overarching policies prepared for appropriate approvals. Overarching policy framework set with 24 ICT security policies, 12 drafted for submission. August update: policies are drafted and awaiting approval.
Cyber Incident Management 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.	Draft document and process to be tested as a desktop exercise and used in a live incident or the CA's wider business continuity test	Significant	Completed	100%	Process has been tested as a desktop exercise and in live incidents a number of times over the past 12 months
Training, Communication and Awareness A mandatory information security training module should be established, incorporating GDPR, with a requirement	Ensure staff complete mandatory annual training as part of their access to GMCA systems.	Significant	Completed	100%	Mandatory annual training in place and being monitored by SMT

Appendix B – Closed Actions

that staff complete refresher training at least annually.					
Third Party Governance 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.	Develop a GMCA-wide policy and process that ensures that all third party ICT-related services operate a robust information security environment. Review existing arrangements to ensure that the highest risk third party arrangements are mitigated	Significant	Completed	100%	Third party policy and process in place
Information Sharing GMCA should explore the possibility of enabling encrypted email as the default method of information transfer, potentially by enabling TLS rejection which would prevent any unencrypted information from being sent in the first place.	Communications to all staff extending the use of Egress to those who need to communicate sensitive information/data	Significant	Completed	100%	TLS security on all email has been implemented, There is an option of Egress for those needing greater levels of security. This has been communicated to all users.
Threat Monitoring 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 etc. Consider a future business case to implement a Security Information and Event Management (SIEM).	The security around the WAN and LAN is going to be actively managed through a third party to a PSN standard. Develop a business case for an improved, proactive threat monitoring capability for consideration by senior management	Significant	Completed	100%	Threat monitoring tools implemented and used actively to monitor potential threats

Appendix B – Closed Actions

Ensure a well-defined audit log management and monitoring framework / strategy to ensure that there is a consistent approach for audit logging and monitoring cyber threats across the GMCA's IT environment.					
Penetration Testing 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.	Perform an external PEN test and repeat on an annual basis.	Significant	Completed	100%	Penetration test completed with minor adjustments actioned to improve security
Resource and Implementation Additional full-time resource should be made available to assist with the implementation of the planned information security activities	Deploy existing resources on the priority areas. Make the case for investment in additional resources to deliver other areas of work in an acceptable timeframe	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					
Leavers and Role Changes 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.	Requirements and process for dealing with leavers to be incorporated in to new p-card policy. Triggers to be introduced to enable procurement team to action changes immediately	Moderate	Completed	100%	The purchase card administrator is receiving the weekly HR report on new starters, movers and leavers, which will enable closer scrutiny, monitoring and improved management of p-cards.

Appendix B – Closed Actions

Cardholder Access 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	A number of p-cards have been identified for removal based on inactivity and/or low usage and will be actioned in line with revised policy.	Moderate	Completed	100%	All redundant cards now cancelled and the p-card administrator continues to monitor movers and leavers on a regular basis.
Unapproved Spend 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.	Process to be agreed and introduced to ensure all expenditure is posted to the financial ledger	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.
Analysis of spend Existing purchase card policy guidance provided insufficient advice over acceptable usage. Our analysis of purchase card expenditure for 2018/19 showed a high proportion of spend related to business travel, accommodation and subsistence costs which should normally be undertaken through the use of corporate contracts and the officer expenses process.	Revised p-card policy to provide clear guidance on acceptable and non-acceptable use of cards. Trade/business accounts to be explored and set up for relevant spend areas	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.

Appendix B – Closed Actions

Invoices and Receipts A significant proportion of transactions were not supported by a valid invoice or VAT receipt Our testing of 50 transactions found that: • Only 44% (22/50) of approved transactions had a valid receipt attached. • Invoices and receipts were not routinely uploaded onto Agresso BWO in accordance with the process Cost Centre Managers were continuing to approve transactions without valid receipts.	Retention and uploading of receipts/invoices to be made mandatory as part of revised policy with measures introduced for non-compliance with policy requirements.	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.
Month End Procedures and Reconciliation Timetable 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	Clear and consistent month end procedure and reconciliation to be introduced as part of revised p-card policy requirements	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.
Value Added Tax (VAT) VAT was not being claimed against any purchase card spend. Data, which would	System and process for recovering VAT on relevant transactions to be incorporated in to overall	Moderate	Complete	100%	The ability to post transactions, separating the VAT value directly to the VAT control account has been investigated.

Appendix B – Closed Actions

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	process review in line with revised policy.				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.
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.	Quarterly reports will be presented to Chief Executives Investment Group with details of both annual and cumulative actuals vs forecasts. Also as part of the BEIS quarterly monitoring each project will be RAG rated in terms of Deliverables, Finance and Reputation. b) Regular reconciliations with TfGM have already started to occur with further development particularly on district schemes planned before March 2019. c) Resource has also been factored in to provide monitoring support of the next phase of Skills Capital which has a forecast	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 being put into the Programme to ensure full spend is achieved.

Appendix B – Closed Actions

To assess the risk associated with delays in scheme delivery timetables and any adverse impact on existing staffing capacity across GMCA and partner organisations.	budget of £70m over the lifetime of the scheme.				
Cycle City Ambition Grant					
2017/18 To note the certification completed for 2017/18 and the major underspend being reported on the CCAG programme to date.	A general email to all CCAG delivering bodies has been issued by DfT confirming that due to the pioneering nature of this programme they understood that all schemes would not be delivered by the 31st March 2018 and asked for bodies to send through a progress monitoring survey which has been completed. There is no confirmation of new deadlines and DfT have also stated that they would not be looking to claw back any monies, however there was an expectation that all schemes would complete at a point in time.	Significant	Completed	100%	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.
2017/20 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.		Significant	Completed	100%	As above
2017/21 Agreement with DfT of forecasted delivery completion dates and spending profiles for programme work streams.		Significant	Completed	100%	As above
2017/23 To seek additional assurances from TfGM PMO in relation to the following;		Significant	Completed	100%	As above
2017/24 Management and oversight of scheme delivery and reasons for significant programme delays; in particular the Manchester Works package,		Significant	Completed	100%	As above

Appendix B – Closed Actions

2017/25 Disparity over scheme completion and costs claimed; to ensure that any undue delays over cost claims are avoided,		Significant	Completed	100%	As above
2017/26 Any necessity to build capacity within Districts and TfGM to avoid excessive delays in getting schemes underway.		Significant	Completed	100%	As above
Culture and Social Impact Fund - Governance Audit					
Management ensure that all payment conditions are fully met before payments are released		Significant	Completed	100%	Completed