Audit, Risk & Assurance Committee

Date	21 September 2018
Report title	General Data Protection Regulation (GDPR) Update
Accountable Chief Executive	Deborah Cadman, West Midlands Combined Authority email: deborah.cadman@wmca.org.uk tel: (0121) 214 7200
Accountable Employee	Gurmit Sangha , Data Protection & Information Sharing Officer email: gurmit.sangha@wmca.org.uk tel: (0121) 214 7301
Report has been considered by	

Recommendation(s) for action or decision:

The WMCA Audit, Risk & Assurance Committee is recommended to

(1) Consider and comment on this report.

1.0 Purpose

On 25 May 2018 the Data Protection Act 2018 came into force, introducing the General Data Protection Regulation (GDPR) into UK law. The purpose of this report is to provide an update on West Midlands Combined Authority (WMCA) meeting its responsibilities and compliance with the new legislation.

2.0 Background

Since September 2017 significant progress has been made by building on WMCA's commitment to the pre GDPR regime, and ensuring that the core elements of GDPR have been met and plans are in place to address ongoing requirements.

This report is intended to update the Committee on the work undertaken prior to GDPR going live, the approach going forward, and the work on addressing the recommendations from two reports commissioned by WMCA on GDPR.

3.0 Activity leading up to GDPR go live on 25 May 2018

The focus in the months before 25 May was to address the areas where WMCA processes personal data on a daylily basis as part of its operations. Some of the main areas of work were:

- All departments engaging with the Data Protection Officer (DPO) to establish the work required in their area to meet the new standard.
- All departments creating Information Asset Registers mapping out the data they hold, and how it flows through the WMCA.
- The DPO reviewed WMCA lawful grounds for processing data in light of the forthcoming changes to the law. Where required these were amended and the way in which data is collected, used or held changed.
- Data protection policies, procedures, and guidance were updated.
- Key data protection roles were introduced including a Senior Information Risk Owner (SIRO), and Information Asset Owners (IAO) for each department. Their responsibilities have been defined within the WMCA Information Assurance Framework and training provided to them.
- All Privacy Notices were redrafted to reflect the forthcoming legislation.
- Where required data subjects were contacted to explain the forthcoming changes.
- Standard WMCA contracts were amended to include the mandatory GDPR clauses.
- The process for amending existing WMCA contracts with data processors was commenced to reflect the new mandatory GDPR clauses.
- The GDPR concept of privacy by design was introduced. A Data Privacy Impact Assessment template with supporting guidance has been drafted and published to assist in the delivery of this concept.
- The seven data subject rights introduced by GDPR were highlighted across the WMCA. The process by which we will manage any data subject exercising such a right has been made clear both internally and externally. Teams have been advised on holding data in a manner which can support WMCA compliance.
- All staff were required to complete mandatory data protection and GDPR training.

- The role of DPO has been introduced, developed and highlighted across the organisation as a central point of contact for advice on data protection matters. The introduction of this role has seen an increase in advice being sought on data protection issues both at departmental level, and in relation to specific projects and programmes. The DPO has also taken responsibility for addressing any external queries raised by members of the public on data protection matters.

During May WMCA successfully moved from the Data Protection Act 1998 regime to the new GDPR (Data Protection Act 2018) regime, with no major concern.

However we recognise that GDPR compliance is not focused on a fixed point in time. Much of what the new legislation mandates will be an ongoing process. Since May 2018 WMCA has had in place a dedicated Data Protection Officer to lead on this work. It is also important to recognise that in many areas we, like all other organisations, will improve and develop as new concepts introduced by GDPR are embedded and developed. Examples include Data Privacy Impact Assessments, Information Asset Registers, training and development to increase staff data protection awareness.

4.0 WMCA approach to GDPR Compliance post go live on 25 May 2018

The expectation of the Information Commissioner (ICO) is that any organisation subject to an investigation must be able to evidence its commitment to meeting the GDPR standard, and the activity it has undertaken to address data protection. An organisation will be required to demonstrate this both strategically, and specifically within the area where any legislative breach may have occurred. With this in mind the immediate focus is in advancing the following now established areas:

- Clear and focused governance arrangements which provide control measures to protect data. Ensuring these are not only in place but understood.
- Organisational commitment to data protection that is cross-organisational, through all levels with everyone understanding their responsibilities.
- Creating a culture of transparency and accountability as to how we use personal data, both internally and externally.
- Understanding the information we hold, where it has come from, and who we share it with.
- Implementing accountability measures by:
  - Understanding our lawful basis to process the data we hold
  - Ensuring Privacy Notices are compliant,
  - Conducting Data Protection Impact Assessments to ensure “privacy by design” and
  - Ensuring our contracts with partner organisations are compliant with the GDPR standard.
- Ensuring appropriate security by making sure we have continual rigor in identifying, and taking appropriate steps to address security vulnerabilities and cyber risks.
- Training all that work at WMCA with regular and refresher training and awareness. Recognising that staff are our best defense against a breach of the legislation, but can also potentially be the greatest weakness.

Work is underway to create a central data protection portal within the WMCA intranet which will provide a central point available to all staff on data protection issues. This will not only aid awareness but also the management of GDPR compliance. Additionally to supplement the introduction of mandatory annual data protection training a programme of regular data protection awareness alerts will be introduced by October 2018.

A programme of internal data protection audits to provide monitoring and guidance for departments will also be introduced.

5.0 Internal Audit of Data Security Arrangements & externally commissioned GDPR Gap Analysis Report

To seek assurance that effective progress is being made towards compliance an internal audit of data security arrangements was completed in March 2018. This supplemented an external gap analysis review commissioned in December 2017, from which an action plan was developed. The work leading up to GDPR, and since its introduction has been underpinned by these documents.

We are nearing a position of completing the work required by the recommendations from these reports and seeking their closure. Those recommendations which remain open are now moving into the area of ongoing business as usual work we are required to undertake by the legislation.

Appendix A below provides an update on the 4 recommendations from the Internal Audit of Data Security Arrangements.

Appendix B below provides an update on the 37 action points from the externally commissioned GDPR Gap Analysis Report.

Completion of actions and "Signing off" for closure.

The action points form the Gap Analysis Report are to be signed off for closure by the Senior Information Risk Owner. Appendix A sets out the anticipated dates for their completion.

A meeting has been arranged with the Auditor to discuss closure of all recommendations from the Internal Audit. We anticipate being in a position to submit a report to the Audit Risk & Assurance Committee by 30 September 2018 recommending completion and closure of the report.

Appendix A: Internal Audit of Data Security Arrangements recommendations update September 2018

Action is imperative to ensure that the objectives for the area under review are met — Red			
No	**Recommendation**	**Update**	**Target date for closure**
2.1	A robust and suitably detailed action plan should be established to support the implementation of the actions and tasks required to achieve GDPR readiness and to ensure that the issues identified in the external review are appropriately, explicitly and fully addressed. Explicit implementation dates (with appropriate prioritisation) should be stated in the plan against each action and include a more detailed breakdown of medium to long term timescales where applicable. Until the Information Assurance Framework is fully operational, alternative action owners should be identified for each specific GDPR related action. Once established the GDPR action plan should be periodically reviewed, progress monitored and appropriately reported to the responsible officer and /or the Senior Information Risk Owner.	The GDPR compliance work stream has been formalised into a managed project with a project outline/proposal, project initiation document, and detailed implementation and action plan. The action plan was developed in conjunction with the externally commissioned GDPR Gap Analysis Report. The plan documents the action required to meet gaps in GDPR compliance, milestones, reviews, action owners, etc **Status:** Progress to be reviewed by Internal Auditor for closure.	12 November 2018 (Subject to ARAC approval)

Action is required to avoid exposure to significant risks in achieving objectives — **Amber**			
No	**Recommendation**	**Update**	**Target date for closure**

Action is required to avoid exposure to significant risks in achieving objectives **Amber**			
No	**Recommendation**	**Update**	**Target date for closure**
2.2	A review should be undertaken to ensure that appropriate policies are available to employees in the interim until such time that the Information Assurance Framework has been fully implemented. All redundant policies should be archived or removed. An organisational wide awareness programme should be undertaken to cover both GDPR readiness and development of the Insurance Assurance Framework and its underlying policies and procedures. This should extend from the WMCA Board to operational levels of the WMCA. A communications plan should be developed to support implementation of GDPR readiness and the Information Assurance Framework.	An Information Assurance Framework was established in January 2018 and work continues to imbed this within the WMCA. The following policies have been updated to incorporate the new provisions and published: • Data Protection Policy • Information Assurance and Information Security Management • Information Risk Management Policy • Information Risk Management Procedure • Information Security Acceptable Use Policy and Security Operating Procedures (SyOPs) • Information Security Classification Policy • Information Security Policy • Internet and Email Use Policy • Mobile Device Security Operating Procedures (SyOPs) • Data Subject Rights Guidance for Staff The HR induction programme now includes training and awareness of the above. The content of the above polices will feed onto the annual data protection awareness programme. **Status:** Progress to be reviewed by Internal Auditor for closure.	12 November 2018 (Subject to ARAC approval)
2.3	GDPR readiness activities should be formally established as a project supported by robust, specific and appropriate governance, roles and responsibilities, project management, risk management and reporting arrangements. The wider Information Assurance Framework implementation exercise should also be established ideally as a programme	The GDPR readiness programme was undertaken by the following officers; Cyber Security Specialist, appointed WMCA Lawyer, Data Protection Officer, Departmental Information Asset Owners, and a number of appointed officers within departments. The work has been enshrined within project management principles.	12 November 2018 (Subject to ARAC approval)

Action is required to avoid exposure to significant risks in achieving objectives **Amber**			
No	**Recommendation**	**Update**	**Target date for closure**
	under which specific projects or workstreams should be established, including GDPR readiness as a discrete project. A suitably resourced multi-disciplined programme / project team should be created with appropriate representation and supported by appropriate terms of reference, governance and reporting arrangements.	There has been regular reporting to the Senior Information Risk Owner (SIRO) and WMCA Audit, Risk & Assurance Committee Going forward an Information Assurance Group made up of the Senior Information Risk Owner, Information Asset Owners, the Data Protection Officer and Cyber Security Specialist has been established. The group will lead on the WMCA ongoing information assurance programme. **Status:** Progress to be reviewed by Internal Auditor for closure	
2.4	The role of the Data Protection Officer should be explicitly included in the Information Assurance Framework with associated responsibilities. Clarity within the action plan should be evidenced to ensure that any actions that would be undertaken by a Data Protection Officer have been clearly assigned to the Solicitor in the interim until the Data Protection Officer has been appointed.	The post of Data Protection Officer (DPO) has been created and the DPO has been in post since 1 May 2018. The position is incorporated within the Information Assurance Framework. The role is being embedded within the WMCA as a point of advice and guidance for teams, project managers and departments. The DPO leads on all GDPR and data protection compliance matters. **Status:** Progress to be reviewed by Internal Auditor for closure.	12 November 2018 (Subject to ARAC approval)

Appendix B: GDPR Gap Analysis Report action plan update September 2018

Recommendation	Priority	Update	Anticipated closure date
1. Governance			
1a) The board, executive team, and senior and functional managers have differing awareness of the GDPR's requirements and their implications for the authority. Everyone in top management needs to have the same level of awareness. This could be achieved through, for example, an in-house GDPR Foundation course (with exam at discretion). Individual roles and responsibilities should be added to job descriptions.	High	WMCA Information Assurance Framework, agreed at Leadership Team level, establishes executive and senior management roles and responsibilities and provides ToRs for the Senior Information Risk Owner (SIRO) and Information Asset Owners (IAO). The Framework also includes the requirement for mandatory annual GDPR and Information Security training and awareness for all users and at all levels. The first wave of this training has been completed. The option to tailor future training to meet roles and responsibilities is being explored. An ongoing organisational wide awareness programme is being developed to provide a foundation level understanding for all.	30 November 2018
1b) The board should receive regular updates on the progress towards closing the compliance gap. This should be part of the accountable director's role. The board does currently receive regular audit reports on DPA/GDPR compliance, so this should continue to be included in any future internal audit plan and reported regularly. The GDPR should also be included as a standard item on the agenda of board meetings.	High	The Information Assurance Framework establishes strategic internal information assurance review by the WMCA Information Assurance Group, chaired by the SIRO and core attended by all Information Asset Owners, DPO and Cyber Security Specialist. All information assurance projects and identified strategic risks are reported and managed at this level.	30 September 2018
2. Risk management			
2a) Although the authority has an information security policy (based on HMG's Information Assurance Standards) there is no formal process for the management of risks to data privacy. Privacy risk is on the board-level corporate risk register, but the board and the authority need to develop their understanding of the idea of risk to the rights and freedoms of natural persons, as distinct from risk to the authority. GDPR compliance and privacy both need to be reviewed on a regular basis by the board, which	High	An Information Risk Management Policy and Procedure, inclusive of SIROs risk appetite, in support of the Information Assurance Framework, is now in place. The policy includes mechanisms for the identification and management of "Impact on the Privacy of the Citizen" risk. The review and management of this risk is a function of the relevant Information Asset Owner,	30 September 2018

needs to determine – possibly by means of a half-day workshop – an appropriate and objectively expressed information risk appetite that can drive and inform the information risk assessment process.		operationally, and the SIRO with the Information Assurance Group strategically. The DPO supports and advices on the management and mitigation of privacy risk, and will hold an Information Risk Register. Reporting to the Information Assurance Group and SIRO has been put in place. Any organisationally critical risks will feed into WMCA risk registers.	
2b) WMCA should ensure the GDPR and privacy risk are considered in all relevant risk assessments. This should be defined in a documented risk assessment methodology to ensure application across all areas of the business.	High	As at 2a (above)	30 September 2018
2c) GDPR and privacy risk should be included in any control frameworks that set out risk controls and treatment.	High	As at 2a (above)	30 September 2018
3. GDPR project			
3a) WMCA has established only two members of a GDPR project team to ensure the authority has a coordinated strategy, systematically implemented, to achieve an acceptable level of GDPR compliance in the available time. This project team will need to be expanded, must set out a clear plan for achieving GDPR compliance by 25 May 2018 and will need training, external resources and clear top management support (via the accountable director).	High	The role of an autonomous DPO has been established and filled. The project team was expanded to include the Cyber Security Specialist, WMCA lawyer, DPO, Information Asset Owners, and appointed officers within departments. The Senior Information Risk Owner (Director of Finance) is the accountable Officer.	Closed
3b) WMCA could arrange for the relevant project personnel to attend a GDPR Practitioner course (which can be delivered in-house).	Medium	The appointed DPO holds a Data Protection Practitioner qualification, and has been leading the compliance programme since May 2018.	Closed
4. DPO			
4a) WMCA is processing personal data, including limited amounts that fall into the special categories of personal data (e.g. health data). As a public body, the authority is obliged to appoint a DPO in terms of Article 37.1(a) and has appointed its in-house solicitor as DPO designate. However, care should be taken before allocating any DPO role to an existing staff member	Very high	An autonomous DPO was recruited and started work in May 2018	Closed

to take account of the provisions of Article 38 of the GDPR regarding avoiding conflicts of interest. Selection of the DPO is urgent as the role is essential for key areas of the compliance project. The DPO role is set out in the GDPR and was discussed in detail during the gap analysis.			
4b) The DPO should report to the board regularly via the nominated director for oversight of GDPR compliance. This will ensure an appropriate level of input to senior management while securing independence for the DPO role (Article 38).	High	The DPO will provide reports to the Information Assurance Group which the Senior Information Risk Owner Chairs.	Closed
5. Roles and responsibilities			
5a) WMCA should implement an authority-wide GDPR awareness programme and make GDPR training a part of staff induction. Although the functional managers interviewed appeared to have a grasp of the basics of data protection, more specific GDPR-oriented training is required for management. Completion of the awareness training should be measured and reported to the board periodically. Employees should have data protection responsibility included in their job descriptions, particularly those with specific objectives such as information asset owners.	High	Information Assurance Framework establishes mandatory Data Protection and Information Security education and awareness to all users. This will take place annually and will be supplemented by privacy awareness initiatives during the course of each year. The first annual all staff training package has been completed. Bespoke training for identified post holders is being explored. The HR induction programme has been developed to include privacy training.	30 September 2018
5b) Aside from the compliance project team core members, WMCA currently has no specific roles for planning compliance with the GDPR (e.g. 'data champions'). The roles and responsibilities for delivering GDPR compliance, and for maintaining that compliance after the implementation date next year, need to be made clear.	High	The roles and responsibilities of Information Asset Owners have been established. The advantages of data champions within teams is recognised, and we will work to develop this concept.	31 December 2018
6. Scope of compliance			
6a) WMCA must determine its status with regard to all the personal data that it processes – i.e. as a data controller or as a data processor, as well as any data-sharing activity. Interviews identified most of the processes and databases that involve or store personal data, as well as issues and risks with these processes. Action points were identified during interviews.	High	Substantial work has been undertaken in establishing WMCA legal status in the individual areas where we process data. The DPO has advised departments, teams, and project managers across the WMCA ensuring the status is clearly understood. The corresponding GDPR issues have been addressed, including the amendment of	30 September 2018

These included specific areas of risk to data processed. Cross-border processing is a feature of the scope for WMCA.		contracts, sharing agreements, relationships with partner organisations, service level agreements, customer terms and conditions.	
6b) The scope of a PCF should include all personal data processed; services and support provided by WMCA staff and contractors; and all legal entities identified by WMCA, including any associated companies that are themselves data controllers/processors (e.g. Man Commercial Protection Ltd).	High	As at 6a (above)	30 September 2018
6c) WMCA should identify all third-party organisations, partners and entities (e.g. suppliers or processors) that might process and/or share data, and ensure this sharing is documented in the register of processing required by Article 30. Such documentation should be maintained (see 8h below).	High	As at 6a/b (above)	30 September 2018
6d) WMCA should perform a review of current contracts with data processors to ensure all relevant GDPR provisions have been included (Article 28). This should specifically include contracts with third parties providing Cloud storage or processing services.	High	As at 6a/b	30 September 2018
7. Process analysis			
7a) WMCA must review all processes to ensure each of the data processing principles is established for each process. Having a lawful basis for processing personal data is a key area of compliance. Interviews identified where processes may have issues and risks associated, such as the risk of retaining personal data for longer than is necessary for the purposes for which it was collected.	High	Departmental/Team Information Asset Registers have been drafted to address effective process analysis. As with many organisations this is a new concept and will be subject to review, development, and improvement.	31 December 2018
7b) WMCA must carry out a thorough check to ensure the lawful bases identified for processing in the Process Analysis worksheet provided are valid (Articles 6 and 9). The European Commission's model standard contractual clauses or other adequate protection must be in place in respect of the contracts governing all cross-border transfers of personal data out of the EEA (Articles 44–49).	High	As at 7a (above)	31 December 2018
7c) WMCA will need to address the delay in issuing fair processing/privacy notices to data subjects, e.g. staff at new customers providing their personal details to allow the new customer to be set up. Article 13 of the GDPR states that the notice must be provided "at the time personal data are obtained".	High	As at 7a (above)	31 December 2018

7d) The duty to serve an Article 14 notice (which informs data subjects about the processing of their personal data received from third parties) sets a particular challenge. To address this, WMCA will need to put in place a procedure so that when the personal data of individuals is received from a third party (e.g. a recruitment agency), the notice is sent to those data subjects.	High	As at 7a (above)	31 December 2018
8. PIMS – Personal Information Management System			
8a) WMCA must review its documentation to ensure the authority is able to manage and demonstrate compliance with the requirements of the GDPR. It was agreed that policy management could be improved. The importance of having an inventory of processing was stressed during interviews. IT Governance's EU GDPR Documentation Toolkit would assist WMCA in generating the suite of PIMS documentation that it requires.	High	The Information Assurance Framework 'sets the stage' for necessary GDPR compliance and a suit of policies has been drafted. The relevant documentation required by Article 30 of GDPR have all been completed. We are currently working on the future review process for these polices and the dissemination of this information across the WMCA	30 November 2018
8b) It is likely that a non-GDPR-compliant form of the prescribed Article 13 notice is currently provided to WMCA staff in the authority's standard employee contract. Fully compliant Article 13 privacy notices should be standardised and issued consistently whenever personal data is collected by the authority from the data subjects themselves, as detailed in 7c above. Consent cannot be relied upon as a condition for processing employees' personal data as the employer-employee relationship is not considered to be equal; an alternative lawful basis for processing employee information will be required and will need to be put in place with all employees before 25 May 2018.	High	All article 13 notices including internal HR notices have been redrafted by the DPO and are now in use. Consent is not relied upon as a ground for processing personal data and the DPO in conjunction with the HR department have revised the ground for processing such data. Article 13 notices have been built into the WMCA data transparency commitment.	Closed
8c) Article 14 notices on the collection of personal data from third parties are not currently issued. A consistent process to remedy this gap is needed as detailed in 7d above.	High	Article 14 notices are now in place Article 14 notices have been built into the WMCA data transparency commitment.	Closed
8d) The handling and obtaining of consent will change significantly with the introduction of the GDPR (Articles 6, 7 and 9). WMCA needs to modify its existing consent processes to comply with the Regulation, recognising that consent by default will be illegal and that the right to withdraw consent accompanies the granting of consent.	High	All grounds for processing personal data have been reviewed. On the advice of the DPO consent as a legal ground has been removed in a number of areas, and a more appropriate GDPR ground has been established.	Closed

		In the limited areas where the WMCA now relies on consent it has been reviewed to ensure GDPR compliance.	
8e) WMCA should introduce a data classification scheme to quickly identify documents or data containing personal and/or highly sensitive information. This will allow employees to handle this information appropriately.	High	WMCA has adopted the Government Security Classification (GSC). An Internal Classification policy has been written and published. GSC training is included within new starter/annual data protection and Information Security education and awareness programme.	Closed
8f) WMCA should implement a GDPR-compliant data retention policy, in writing, detailing retention periods and ensuring all personal data is anonymised or securely deleted as soon as it is no longer lawful to retain it.	High	An archive and retention project group has been established to find solutions in this area and establish a modern retention & archiving process. As part of this the current policy will be reviewed and amended.	31 December 2018
8g) WMCA should ensure its formal change management process includes provisions for DPIAs (see 8j below) to be completed whenever processing of personal data is introduced or modified.	High	Data Privacy Impact Assessments (DIPA) are now part of WMCA project management where it involves processing personal data. A DPIA template and supporting guidance has been published	31 December 2018
8h) WMCA should create and maintain a record of personal data processing activities (see 6c above) under its Article 30 responsibility.	High	As at Section 7	31 December 2018
8i) The process covering the handling of SARs should be updated to meet the GDPR's increased requirements in this regard (Article 15). Reporting should be set up to ensure the relevant SAR response times are met, and in respect of the other data subject rights referred to in 10 below. All areas of the authority should be made aware of this process.	High	The process has been updated both externally and internally to meet the GDPR standard.	Closed
8j) Article 35 contains the GDPR's requirements for when a DPIA must be undertaken. The format of any security assessments or privacy impact assessments already carried out by WMCA will need to be adjusted to meet the GDPR's requirements for DPIAs. The need for work on consistency with the GDPR is likely.	High	As at 8g (above)	31 December 2018
9. ISMS			
9a) WMCA stated that it is looking at obtaining ISO 27001 certification in the future. ISO 27001 certification demonstrates that technical and organisational measures are in place to ensure there is adequate security of personal data held in hard copy or electronic form, or processed through the authority's	Medium	Attaining ISO 27001 and CE+ is a WMCA IA objective This work is ongoing and being led by the WMCA Cyber Security Specialist	31 December 2018

systems. This includes a review of methodologies for testing security, and established cyber security certifications, standards and codes of practice. During the interviews we suggested that WMCA looks into adopting the BS 10012 standard, as it is specifically geared towards GDPR compliance. During the interviews information was provided on other relevant certifications, such as Cyber Essentials and Cyber Essentials Plus. These are being established as industry standards and some organisations are expressing a preference for them.			
9b) Encryption to the current recognised industry standard should be applied to all personal data at rest and in transit to ensure accidental data loss or data loss due to malicious activity, does not lead to disclosure. Where this is currently impossible because of the use of legacy software or systems, WMCA should develop and implement a plan to upgrade these systems to include encryption as soon as possible.	High	Data at rest and in transit encryption is a baseline standard of GSC (adopted by WMCA) is OFFICIAL information. Presuming all personal information will be at least OFFICIAL, this requirement is technically achieved.	31 December 2018
9d) WMCA should ensure employees are aware of the possibility to encrypt emails end to end and apply this to any emails containing personal data. Where this is currently impossible because suppliers/third parties do not support this, WMCA should continue to use a solution that provides secure file transfers for personal data (SFTP).	Medium	As at 9b. GSC allows a given handler to risk assess their processing of relevant data and apply baseline standards accordingly.	31 December 2018
9e) WMCA should ensure any policy concerning information security explicitly references the security of data subjects, as well as penetration/security testing.	Medium	As at 9b. Annual Penetration/Vulnerability testing of all relevant systems is conducted, as a BAU activity, by WMCA ICT.	Closed
9f) Logging and monitoring processes should be assessed to make sure access to personal data is logged and monitored to prevent abusive or excessive access, and to detect data breaches or cyber-attacks.	Medium	In accordance with the Information Security Policy, all users are afforded access as per their specific job role and relevancy. ACL are controlled through AD and application level authentication. Intrusion or cyber-attacks are monitored and prevented using robust anti-intrusion techniques and tools. Strictly speaking an auditing function is not currently employed across all relevant systems and assets. This forms part of the creation of an IAR and continuing service improvement.	30 November 2018

9g) WMCA's IT security roadmap should be reviewed to ensure the security of personal data/data subjects is considered, including by way of pseudonymisation or anonymisation.	Medium	Privacy by design is a consideration through the life cycle of all systems and information assets. The application, of these measures, in accordance with the draft IM Strategy, is the responsibility of the Information Asset Owners and all system users. The DPO is available for advice and guidance, and will be incorporated with the training and awareness programme.	Closed
10. Rights of data subjects			
10a) WMCA does not have a written SAR policy or procedure. WMCA needs processes that will allow it to both facilitate and respond to data subjects exercising any or all of their rights. During the interviews the importance of the enhanced rights of data subjects under the GDPR was repeatedly stressed.	Very high	We have externally published the process for data subjects: https://www.wmca.org.uk/freedom-of-information Internal Process is managed by DPO and the internal process is documented on the WMCA intranet	Closed
10b) WMCA should implement processes (automated, if possible) to ensure it can guarantee the rights of data subjects, especially the rights to rectification and erasure. Processes should also be put in place to handle requests pursuant to the right to be informed (see 8b and 8c above), and the rights to object, to erasure and to data portability.	High	All data subject rights are explained externally and how they can be exercised. Internally the DPO manages request to exercise a data subject right. The process is documented on the WMCA intranet. New or amended systems which process personal data are designed to aid the delivery of data subject rights.	Closed