MOPAC | MAYOR OF LONDON OFFICE FOR POLICING AND CRIME

METROPOLITAN POLICE

MPS-MOPAC JOINT AUDIT PANEL
4 October 2021

Digital Asset Management Procurement Review Update

Report by: The Chief of Corporate Services

Report Summary

Overall Summary of the Purpose of the Report
This report provides an update on progress delivering recommendations from the DARA audit report, 'Digital Asset Management Procurement Review'. This includes an update on information assurance and security, governance, procurement and commercial services.

The report provides an update on plans for future procurement and summarises progress towards the actions commissioned by the Chief of Corporate Services.

Recommendations

The Audit Panel is recommended to note the report.

This report has interdependencies with the Commercial Services Audit Panel report.

1. Introduction and context

1.1. In August 2020, recommendations from the DARA audit report, 'Digital Asset Management Procurement Review', were presented to the MPS. This followed concerns about the Box tool and resulted in a report containing 30 recommendations.

1.2. This paper outlines progress since the DARA audit and provides an update on the MPS's plans for future procurement of a Digital Asset Management (DAMs) solution.

1.3. As previously noted at Audit Panel, the MPS receives, creates and stores large volumes of data in a wide variety of formats. The MPS needs a digital asset management platform to store its data and ensure that documents and media can be shared both internally and externally with trusted partners.

1.4. Box is recognised as the market leader for external collaboration and is currently used in the MPS for information management and sharing. It is an important tool in the MPS' management of data, with 48,000 internal users, 8,000 external users, a large amount of data storage and integration with other MPS tools.

1.5. Since the DARA review, there have been significant changes to the MPS operating environment, including strengthened governance and controls alongside new leadership and internal capabilities. We believe that the changes that have taken place ensure that we have adequate controls and systems in place to make ethical and legal decisions.

2. Progress on delivery of DARA recommendations

2.1. The Appendix provides a full summary of progress delivering recommendations. This shows that we have now completed over 80% of the recommendations. The remaining 'in progress' recommendations are regarding procurement and commercial services. We have a clear plan in place to deliver these changes and the recommendations, but acknowledge that embedding the aspirations of the ambitious Commercial Blueprint are significant and will take further time to be delivered effectively. Progress is outlined in more detail in the Commercial Services Audit Panel report.

Information assurance and security

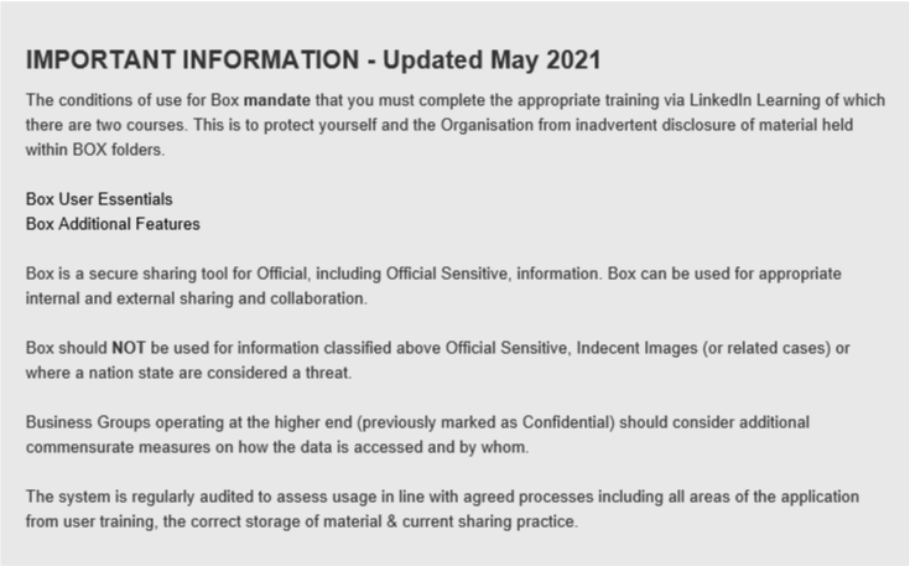
2.2. The DARA audit identified a number of information assurance and security concerns surrounding the MPS use of Box. Following this, Robin Wilkinson, Chief of Corporate Services, requested a comprehensive review of Box compliance with data protection responsibilities in the MPS. This found no fundamental security or data processing concerns with the use of Box. It did identify the need for improved governance to ensure users comply with published security guidance. This has now been incorporated into the revised IRAR.

2.3. There were a number of security issues raised in the DARA audit that the MPS has since been able to clarify. Firstly, the report identified that data may be held in the USA whilst awaiting encryption. DP and Box have now clarified that, whilst this was the case in the pilot and early stages, all encryption is now done in the EEA, so the data is not processed in the USA. Some MetData (e.g. file size, last accessed data) is still processed in the USA, but this is deemed to be low risk and does not include any content from the documents stored.

2.4. The DARA audit raised the fact that Box hold the encryption keys, not the MPS, which could pose a risk to the security of the data. It is correct that Box hold the encryption keys despite the fact that the MPS originally purchased the option to manage them in-house. However, there is no precedent for the MPS holding encryption keys for Cloud-based SaaS services. For the MPS to hold the encryption keys for Box would have added significant additional costs and would have severely limited the 3rd party sharing functionality, which is a critical requirement for the DAMs solution. The NPCC National Enabling Programme established the principle of suppliers holding encryption keys for Office 365 and this is also the case for evidence.com (BWV storage). The MPS is content that allowing Box to hold the encryption keys is acceptable and any risk is mitigated through appropriate vetting of Box employees.

2.5. The DARA audit identified that the MPS did not have a completed DPIA when Box was initially rolled out in the MPS. This has been refreshed and approved by the CIO and DPO. This DPIA has been shared with DARA.

2.6. The DARA audit highlighted the need to refresh the IRAR. This has subsequently been updated and approved, and includes updates to Data Classification and a new file structure to give owners greater control over file sharing. Following sign-off of the IRAR, new guidance has been issued to clarify the use of Box for Official Sensitive information. This is shown on the landing page for all users accessing Box. Training is also available via LinkedIn Learning.



IMPORTANT INFORMATION - Updated May 2021

The conditions of use for Box **mandate** that you must complete the appropriate training via LinkedIn Learning of which there are two courses. This is to protect yourself and the Organisation from inadvertent disclosure of material held within BOX folders.

Box User Essentials
Box Additional Features

Box is a secure sharing tool for Official, including Official Sensitive, information. Box can be used for appropriate internal and external sharing and collaboration.

Box should **NOT** be used for information classified above Official Sensitive, Indecent Images (or related cases) or where a nation state are considered a threat.

Business Groups operating at the higher end (previously marked as Confidential) should consider additional commensurate measures on how the data is accessed and by whom.

The system is regularly audited to assess usage in line with agreed processes including all areas of the application from user training, the correct storage of material & current sharing practice.

Governance and decision making

2.7. Significant progress has been made on the use of internal controls and governance surrounding decision-making.

- Several improvements have been made to the functioning of Management Board meetings. These meetings are chaired by either the Commissioner, Deputy Commissioner or Chief of Corporate Services and encourage debate. There is now improved alignment between Board decisions, supported by the strategic secretariat.
- A Director-level meeting has been introduced to strengthen assurance surrounding investment decisions, before submission to the Portfolio and Investment Board (PIB). There is now increased senior accountability for control over decision-making, as this meeting is chaired by the Director of Finance and attended by the Director of Legal, Commercial, Strategy and Governance, Transformation and DAC Corporate Services. Additionally, the Chief Finance Officer from MOPAC is now invited to these meetings.
- Work has begun with MOPAC to revise the Scheme of Delegation ensure governance and decision-making is aligned to the risk, scale and complexity of decisions.
- A Data Board has been introduced to provide oversight, assurance and appropriate governance of key risks and opportunities for collection, storage and use of data.
- Work is progressing to improve the MPS approach to change, following an independent stocktake by Mary Calam, which identified 32 recommendations. All the recommendations were accepted by the MPS Management Board and vary in scale, complexity and resourcing requirements to deliver effectively. Corporate Services are carefully working through the necessary process and capability required over the longer-term.

Procurement and Commercial Services

2.8. The MPS Commercial Services function is progressing through considerable change to increase commercial capability, including people, processes and technology. The new Commercial Blueprint and subsequent operating model became operational in 2020.

Plans for future procurement

2.9. The Box contract is due to expire in July 2021, following a one-year extension agreed by Management Board. To oversee and assure the procurement of this capability, the MPS set up a Box Procurement Oversight Group, chaired by the Chief of Corporate Services. In 2020, the Procurement Oversight Group commissioned an independent market review.

2.10. The MPS is currently in procurement phase to conduct discovery work for a solution. This is being conducted through the Solution Provider Framework

(SPF). This procurement includes both design of a solution and implementation. The MPS have currently conducted initial supplier engagement, agreed a high level scope and will now proceed to sign off a high level plan, requirements and route to market.

3. Progress on actions commissioned by the Chief of Corporate Services

3.1. In addition to the recommendations made by DARA, the Chief of Corporate Services requested specific actions be taken forward:

- The Chief of Corporate Services requested a briefing for all senior leaders in the Met on procurement and commercial activity. The scope of these sessions has now been expanded and will cover procurement, governance and assurance. These sessions will be mandatory and begun in June.
- In December 2020, the Chief of Corporate Services asked an independent Met Director, Bidisha Kondal, to undertake a separate review on whether concerns with the overarching question being could the multiple concerns identified in an audit linked to the procurement of DAM occur again, through the review of current corporate controls in relevant Met enabling Departments.
- Respond to concerns about internal behaviours. This has been managed internally.

4. Equality and Diversity Impact

No equality and diversity implications are noted.

5. Financial Implications

No financial implications are noted.

6. Legal Implications

No legal implications are noted.

7. Risk Implications

No additional risk implications are noted.

8. Contact Details

Report author: Robin Wilkinson, Chief of Corporate Services

9. Appendices and Background Papers

Appendix 1 – Full recommendation list, status update

Appendix 1 – Full recommendation list, status update

Rec. No.	Recommendation	MPS Update – October 2021
Digital Asset Management – Strategic Approach and Box Evaluation		
1	Clarify and agree the Met's strategic approach and service requirements for Digital Asset Management and in particular for digital evidence management.	**Complete:** Accenture review of MPS DAMs requirements now completed. Review identified that Box does not meet all the MPS's digital media evidence requirements, such as CCTV. Evidence.com now used as the primary tool for sharing digital media evidence with law enforcement and CJ partners. Box remains the MPS DAMs solution for documents & third-party sharing. Discovery exercise with Microsoft currently in procurement phase.
2	Conduct independent evaluation of the Box solution: • Evaluate the realisation of anticipated benefits/savings against the initial Business Justification. • Assess the effectiveness of implementation of solution to meet identified needs. • Determine any DAM requirements not being met by current solution in consultation with Subject Matter Experts • Full cost of implementation of solution to date • Capture and evaluate user experience • Review pricing model for Box contract - clarify contract price and terms and functionality purchased. • Report to DMPC/MOPAC (as previously agreed)	As above. Findings of Accenture review were presented to DMPC in March as part of the business case requesting a new contract award with Box. Contract awarded on a one-year basis, enabling MPS to explore feasibility of a Microsoft DAMS solution in the future.
3	Future procurement: • Determine and document DAM requirements to support future procurement activity • Conduct market engagement to determine market position • Assess viability of other potential solutions in the market and/or the Met under existing contracts • Plan and agree procurement strategic approach • Follow approved procurement process lead by Commercial	As above.
Box Security Risk Assessment and Information Governance		

Rec. No.	Recommendation	MPS Update – October 2021
4	Complete a revised IRAR (and/or consider completion of independent ITHC check) for Box and ensure the following is specifically addressed: • Define and agree Met's security requirements for a DAM solution and risk assess against them. • Define national guidelines that apply to use of Box, including; HMG, NPRIMT, Cloud Principles and assess the Met's position in terms of compliance using the Box solution. • Determine and be explicit on the status of Box for the Met's use of 'Official' and Official Sensitive in line with national guidelines • Confirm the classification of data that can be held on Box. • Re-assess the risk position, in particular for geographical location of processing data, management of encryption. • Determine and assess any data protection and GDPR implications associated with the use of Box. • ISO and DPO to assure and sign off the IRAR. • Review controls for restricting use of Box, including process for assuring compliance.	**Complete:** The IRAR has now been updated. This was supported by Data Board in November 2020 and signed off by the SIRO in February. Actions are now ongoing.
5	Complete the Data Protection Impact Assessment for Box for the consideration of SIRO and Data Board and confirm compliance with Data Protection and GDPR legislation: Ensure DPIAs cover all use of Box – ensure they accurately reflect the position in transfer/processing of data outside the UK/EEA and assurance is given to ICO as appropriate, including Gangs Matrix.	**Complete**: The DPIA has been completed and signed by the CIO and DPO.
6	Communicate to users the completion of the risk assessment and DPIA and assure users Box can be used in line with agreed parameters (once confirmed following IRAR).	**Complete –** updated DPIA and IRAR signed off. New splash screen implemented and training available on LinkedIn Learning. Folder structure & ownership improved to improve security. This includes designating folders as internal, partners and public to reduce risk of data breaches.
Proof of Concept – Governance		
7	Clearly define the Met's strategic approach and policy on engaging suppliers to test a Proof of Concept.	**Complete:** New policy and approach has now been agreed by Management Board. Policy shared with MOPAC and DARA on September 8th.

Rec. No.	Recommendation	MPS Update – October 2021
8	Define governance arrangements supporting a Proof of Concept to include; accountability for key decisions, programme/project management, reporting to appropriate governance forum/board, level of oversight required based on proportionality of risk/potential impact.	As above
9	Define Met processes/protocols to support the agreed strategic approach to Proof of Concept trials, to include; • Definition of Business Need and setting scope • Clear definition and appropriate allocation roles for all involved in the process e.g. Programme/Project Leads, Business leads, Commercial Services and Technical and Security leads. • Protocols for engaging with suppliers • Selection of suppliers with due regard for fairness to potential competitors throughout • Agreeing standards terms and documentation between MPS and supplier to govern the Proof of Concept • Defining procurement approach in line with appropriate rules and regulations • Maintaining transparency and adequate records throughout the process.	As above
10	Outline standards for conduct, evaluation and reporting outcomes of Proof of Concept Trials.	As above
11	Ensure Proof of Concept trial does not exceed the approved trial period – formal decision is taken to proceed in line with procurement and project management.	As above
Security and Information Governance and Assurance		
12	Debate and determine Met's strategic approach to the use of the 'Cloud' based solutions setting security requirements and standards in line with national standards/guidance – define Met's risk appetite.	**Complete:** MPS has a cloud-first approach, as articulated in the Digital Strategy. The Technology team has developed a set of standard non-functional requirements for technology procurement.
13	Clearly define the Met's security requirements in testing and purchasing new technology, including stipulating 'live' data is not to be used in Proof of Concept trials. Any differing views on the standards	**Complete:** MPS has improved controls on use of live data for testing. All requests must be submitted to DPO for approval. An information security group will be established, as a sub-group to Data Board.

Rec. No.	Recommendation	MPS Update – October 2021
	of security to be applied within the Met when procuring/implementing IT solutions are considered and debated and an agreed position reached. The agreed standards are consistently applied across the organisation.	
14	Roles and Responsibilities – define, roles and responsibilities for setting, assessing and assuring security requirements, ensure appropriate consultation with key stakeholders and subject matter experts and appropriate level of segregation/independence.	As per 13
15	Ensure independence and increase status of the Met's Information Security Officer and Data Protection lead, develop direct reporting line to the SIRO/Chair of Data Board.	**Complete:** The Data Protection Officer is a member of Data Board. Information Security Officer reports to DPO and attends Data Board when required.
16	The strategic approach to conducting Data Protection Impact Assessments to meet the requirements of the legislation is agreed and DPIAs are completed and independently assured at an appropriate stage in line with the agreed approach.	**Complete:** The approach to conducting DPIAs has been refined following the creation of the Data Office. This is overseen by Data Board.
MOPAC Governance		
17	Ensure papers are appropriately signed-off and assured before submitted to IAM in line with approved approach.	**Complete:** A new Director level governance group is focused on appropriate sign-off and assurance prior to submission to MOPAC.
18	Recommendations to the DMPC supporting key decisions are explicit and appropriately reflect what is required.	**Complete:** MPS continue work with MOPAC to ensure that appropriate clarity is provided
19	Minutes of IAM appropriately capture discussions supporting key decisions made.	**Complete:** MOPAC author IAM minutes and distribute to MPS as appropriate
20	Key requirements set in approving a decision at PIB and/or IAM are properly captured and referred to in taking any future decisions (in this instance there was a requirement of evaluation of the pilot and market engagement that did not take place).	**Complete:** For 2021, renewed focus from PIB Chair in clarity of PIB minutes. As above in relation to IAM. MPS capture and act upon learning from investment decisions.
Procurement and Commercial Services		
21	Implement Commercial Blueprint model addressing: • Roles and responsibilities for Commercial activity – business and Commercial • Status of the Commercial Function • Capacity and Capability of Professional Procurement support	**In progress:** As stated in the Commercial Services update to Audit Panel for October and in the Audit Report on Commercial Services, work continues to address each of these areas.

Rec. No.	Recommendation	MPS Update – October 2021
	• Compliance with approved process • Appropriate sign off in line with Contract Regs and approved process • Streamline business processes, maintain appropriate records - supported by effective IT system	
Digital Marketplace – Strategic Approach, Governance and Protocols		
22	Agree and define the Met strategic approach to procuring via the Digital Marketplace and/or similar frameworks.	**In progress:** As stated in Commercial Services update to Audit Panel for October, this is being included in the Commercial Services Handbook following agreement with Digital Policing and DARA.
23	Establish protocols/procedures governing the use of the Digital Marketplace/frameworks in support of the agreed strategic approach, ensuring published guidance is consistently applied to ensure integrity of process and compliance with public procurement regulations, including; • Maintenance of a sufficient audit trail and documentation • Conduct of Market Engagement • Documentation of requirements • Consultation with technical specialists, service users, security experts, risk specialists • Documentation of criteria • Evidence of assessment of suppliers • Retention of all correspondence with suppliers • Application of the 'Buying Fairly Guide' to preserve the integrity of the process and meet standards laid down in procurement regulations.	As above
24	Regulate the use of the Digital Marketplace/frameworks, recording and authorising registered users, defining the respective roles of the Business and Commercial Services in the process.	As above
25	Maintain protocols for engaging with the market and suppliers – Commercial Services to lead.	**In progress**: Work continues to build and strengthen our relationships with our suppliers and markets. Whilst we have highlighted previously the efforts on SRM which continue, we are now looking at better equipping both Commercial and non-Commercial staff through best-in-class training in areas such as negotiation.
Decision Making Governance		

Rec. No.	Recommendation	MPS Update – October 2021
26	Establish effective corporate governance standards that are applied equally, consistently and transparently across the Met, including within Digital Policing – Management Board members are seen as advocates for good governance	**Complete:** Management Board have committed to effective governance and significant changes have been made to strengthen assurance. A stronger assurance framework has been introduced for all investment decisions (PIB Level 2 meetings). There have been a number of improvements to Management Board meetings. These meetings all have a standing chair and Alignment between Board decisions and considerations is the responsibility of the Director of Strategy and Governance, supported by the strategic secretariat.
27	Increase transparency in taking key decisions, ensuring an appropriate level of consultation and communication with key stakeholders impacted by decisions.	**Complete:** PIB Chair encourages and expects open debate both in advance and at key meetings. The director level meeting prior to PIB also considers appropriate consultation and communication.
28	Encourage a culture of openness in governance forums that supports appropriate challenge and debate and allows key concerns and differing views to be raised and heard in a respectful environment.	As above
29	Clearly articulate risk appetite, assessment of risk and acceptance of risk in taking key investment decisions.	**Complete:** Risk considerations, including risk appetite, feature highly in our key investment decisions as evidenced by PIB discussions. Management Board agendas are tied to the risk register and Board meets as Risk & Assurance Board quarterly.
30	Supporting processes for PIB; • Review the process for signing-off papers/business cases submitted to PIB in support of key investment decisions i.e. ensure appropriate officers sign off in line with responsibilities/accountabilities clearly articulated on the sign off form. • Papers in approved format and contain complete information – rejected if standards are not met/key information missing. • Recommendations in papers to PIB supporting key decisions are explicit and appropriately reflect what is required in line with its defined role. • Minutes appropriately capture discussions, including any objections/challenge supporting key decisions made.	**Complete:** Supporting processes for PIB have been significantly strengthened. There is an ambition for continuous improvement going forward, including working through the governance pilot.

Rec. No.	Recommendation	MPS Update – October 2021
	• Key requirements set in approving a decision at PIB and/or IAM are properly captured and referred to in taking any future decisions (in this instance there was a requirement of evaluation of the pilot and market engagement that did not take place).	