Joint Audit & Scrutiny Panel

27 October 2020

Mazars GDPR Audit Update

Mazars GDPR Audit – December 2018 and March 2020 revisit report

- As part of the Internal Audit Plan for 2018/19 for the OPCC and Nottinghamshire Police, Mazars undertook an audit of the controls and processes in place in respect of the response to General Data Protection Regulation (GDPR) legislation.
- The aim of the audit was to establish the level of GDPR processes and procedures in place within the Force post the implementation date of May 25th, 2018 and where applicable include testing from areas within the Force.
- The outcome of the audit identified a ‘Limited Assurance‘ level and seven areas of risk that required improvement.
- In October 2019 a revisit was arranged and the audit report provided in March 2020. The outcome from the revisit identified improvements in all of the risk areas resulting in a ‘Satisfactory Assurance’ level.
- The next slides provide some brief details on the original risks and the current position

Risks & Current Position

December 2018 – Limited Assurance	Revisit Report – March 2020 – Satisfactory assurance
GDPR Gap Analysis & Action Plan: **Risk: There is no formal plan to achieve compliance or the resource available to implement resulting in non-compliance with key aspects of GDPR**	Information Management Strategy agreed at Information Management Board & published Information Management Unit priority areas have been clearly identified and a fuller plan will be implemented once the unit is up to full establishment.
Subject Access Request Resources **Risk: The organisation has insufficient resources to manage the demand for disclosures and may be at risk of not achieving the statutory time limit**	An increase of 3 full time staff for the Information Request Team was approved as part of the IMU business case and additional staff took up their posts in December 2019
Information Asset Register **Risk: The organisation does not have a full view of what and where data is stored and its purpose leading to potential data protection breaches.**	The initial first round of IAO visits has been completed and updated Information Asset registers prepared for each department. We are now working with the A & E department in linking these registers with the retention schedule to assist IAO's with putting in place regular review, retention & disposal processes as part of Op Archive

Risks & Current Position

December 2018 – Limited Assurance	Revisit Report – March 2020 – Satisfactory assurance
Deputy Data Protection Officer/Key Knowledge **Risk: Key knowledge is lost should team members leave.**	Two nominated deputies are now in place, Information Request Team Leader & Information Security & Compliance Team Leader and The Deputy DPO role is now defined in the relevant Job Description. The agreed IMU restructure currently being implemented should also reduce reliance and risk on key single points of knowledge in key areas such as DP and Information Security.
Records Management **Risk: Potential to breach retention policies and not fully understand records held.**	A decision was taken to return approx. 12000 boxes in off-site storage to an internal facility within the Force and the processes required to manage these assets is being reviewed as part of Op Archive. This work is ongoing.
Training **Risk: Staff not effectively trained and aware of their obligations.**	The NCALT Managing Information Training package was relaunched on the 18th September 2019, mandated for officers and staff with two separate packages depending on role. Completion is being monitored and Heads of Department have been notified of their team's compliance rates.
Regional Data Protection Meetings **Risk: Highlighted by Lincolnshire Police as this audit was approached on a regional basis. Group discussions do not meet terms of reference or provide an effective forum.**	Nottinghamshire Police has continued to attend the regional DP meetings and the scope and nature of the meetings has been subject to review. There are also regional meetings in place for Information Security Officers, Compliance Auditors, FOI Officers & Records Management Officers