**Agenda item:** 16

## Warwickshire Joint Audit and Standards Committee Report Summary

**Meeting Date: 23rd January, 2024**

**Subject: Information Assurance**

**Contact details: Stephen Russell**

**Purpose of the Report:**

The purpose of this report is to provide JASC with an update on the activity and priorities of the newly formed Information Assurance function

**Recommendation:**

It is recommend that JASC comment and note the contents of this report

**Background:**

Information Assurance (sometimes referred to as Information Governance) is a critical function for Warwickshire.

*P*olicing holds vast amounts of data for law enforcement and operational purposes, but how that data is used requires rigorous governance to ensure its retention and use is lawful, fair and proportionate and does not infringe on the rights and freedoms of individuals. The Information Assurance function has responsibility for information governance, records management and data protection.

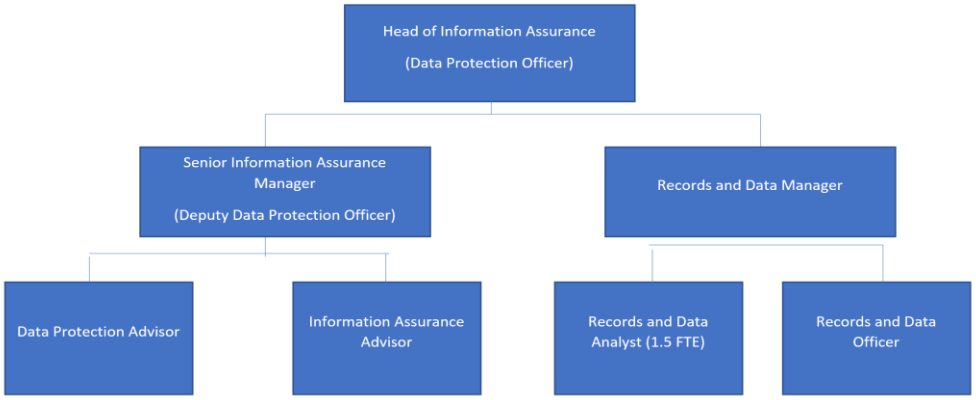
This report has been shared with the force Senior Information Risk Owner (DCC Franklin-Smith) and circulated to the force executive board.

**Executive summary**

The report introduces the new Information Assurance team in terms of structure, roles and key responsibilities. The report identifies the key priorities and areas of focus for the coming year and how we will approach achieving this.

**Introduction to the Information Assurance Team**

The Information Assurance (IA) function is a newly created team, reporting into the Data, Strategy & Technology Directorate.




Previously, roles such as the Data Protection Officer, were combined roles held by existing staff with full-time positions which created service delivery difficulties in terms of the workload demand.

The Force recognised this was not the correct functional model for information assurance and the implementation of the revised structure has allowed for the recruitment of specialised staff, with significant IA experience to lead a strategic and operational IA change programme.

The Head of IA joined the Force in July 2023 with the remaining IA posts identified above filled by 27th December 2023.This structure has meant that the team is centrally resourced with permanent Police staff, removed the need for contracted staff and the split role nature of the previous function.

The team is well represented with the Head of IA meeting with the SIRO (Senior Information Risk Owner/Deputy Chief Constable) on a monthly basis and there is also a direct line of escalation on matters requiring SIRO approval.

The Head of IA supports the Information Assurance Board, chaired by the SIRO, which meets quarterly and has recently made updates to the Terms of Reference, attendees and reporting format.

We are currently in the process of setting up a tactical Information Security Group to support and feed into the IAB (due Feb 2024).

The work of the team is measured and reflected at the IAB where each quarter reports on IA Training stats, Data Breach and ICO Reports, Records and Data Quality and the overall IA improvement plan are reported on.

The team leads project/process level oversight through its fortnightly Security & Risk Working Group and a weekly Information Security & Assurance checkpoint.

The Head of IA sits on the national Information Asset Owner (IAO) training board which is aiming to redesign the national training packages used to support IAOs.

They are also a member of a regional Police Data Protection Officer group, which includes Forces from across the Midlands, a regional information assurance group which includes representatives from Local Government, Health and Education, and is a member of NADPO (National Association of Data Protection Officers).

The Head of IA holds the following qualifications CIPP/E (Certified Information Privacy Professional/Europe), Certificate in Information Security Management Principles and ISEB Freedom of Information.

**Key Responsibilities**

The primary functions of Information Assurance within Warwickshire are to ensure that we meet our Data Protection obligations as set under the UKGDPR and Part 3 of the DPA 2018 (the measures that relate specifically to Law Enforcement Processing).

We ensure that records retention and management & data quality measures are specified, audited and we are moving towards implementation across our key systems. The team also undertakes information assurance risk reviews of projects/processes or system implementations to help us identify potential risks either legally, technically or contractually and to make suitable recommendations to help protect our information.

We work closely on this part with Digital Services and Cyber Security colleagues, as the technical experts and implementers of our key network and system security controls, and we are strengthening our links to procurement and the change process.

Please note that FOI, Subject Access Request and Disclosure sit within the Legal & Disclosure Function and are therefore separate to IA.

**Data Protection Controls**

Data Protection compliance requires an organisation to have undertaken foundational work to ensure it is meeting its basic requirements. In broad terms this means knowing what personal/special category data you have, where that data is within your estate, how much data you have, who has access to it, how long it should be kept for and that the data is appropriately protected by either technical or physical security measures.

As a newly formed team**,** there are several areas of improvement that have been identified by the Head of IA to ensure we can meet these fundamentals.

- The need to have comprehensive information asset registers across all teams and departments to map where our data is, and address some of the key points listed above.

- The legal requirement to produce a Record of Processing Activity (ROPA), which is a specified requirement under Article 30 of the UKGDPR and lists the lawful reasons for the data we process.

- Improvements in the visibility and understanding of what a data breach is, when and how they should be reported.

- Improvements to the Data Protection Impact Assessment (DPIA) process with further training and guidance. Under Article 35 of UKGDPR a DPIA is undertaken prior to starting any processing likely to result in a high risk to the rights and freedoms of data subjects. DPIAs are appropriate for IT and non-IT processing of personal data as it is about addressing the risk to the data subject not just a technology assessment.

- Stronger ties to our procurement process, to ensure that all suppliers/partners who access or process personal/special category or law enforcement data have the right checks in place, DPIAs are conducted when required, information assurance and cyber security risk assessments are conducted, contracts cover the necessary clauses and that reviews are undertaken throughout the lifecycle of the contract.

- Policy & Guidance revision, ensuring they are Force focussed and fit for purpose.

- Review of our e-learning packages and supplementing this with locally focussed and bespoke training.

The Head of IA has produced an approved report for the Information Assurance Board which outlines an action plan with timescales for delivery on each of the improvements for 24/25; understanding our information assets and the development of the ROPA will take priority with a delivery date of Q2 2024. DPIA improvement/full policy and procedure review by Q3 and the remaining priority improvement items will be in place by Q4 2024. These items will address the key gaps that were found through the internal audit work prior to the new Head starting and will aim to close this off fully by the end of 2024.

Compliance in meeting our action plan will be driven through quarterly update reporting to the IAB on progress. We will also have practical measures such as incident reporting metrics, training attendance as we rollout updated packages and via operational engagement through numbers of DPIAs/ISA we have coming through the service.

The team will in the longer term look to implement an audit programme internally whereby we review areas against their understanding and adherence to policies and processes, as we are building our foundations this is likely to be 2025.

**Information Security Controls**

Technical controls such as firewalls, Role Based Access, Access Management, Vulnerability and Patch Management all fall under the remit of DS, Cyber Security and our managed service partner Risual.

The role of the Information Assurance team in regard to information security is sometimes termed “the soft skills”. We issue out regular comms to the Force on key aspects of information security and assurance; reminders on how to stay safe online, understanding breach reporting, advice on working remotely.

Our work supports the technical controls we put in place, by creating an awareness of best practice and safer working practices and helps staff to know the role they play in keeping our information safe.

We support the completion of national compliance framework submissions such as our code of connection (CoCo) to the Public Services Network (PSN), the Police Digital Services

(PDS) SyAp (ongoing security assurance assessment framework), and our Airwave CoCo.

We coordinate regular workshops with DS and Cyber Security colleagues, ensure that actions are captured and complete the required documentation for submissions. This is very much a collaborative approach and we meet regularly with PDS to update on progress and seek feedback.

We support projects and new system reviews using an Information Risk and Review process (IRAR) which includes a comprehensive review of suppliers security documentation (security testing results, accreditations checks, security and data protection contract clause review) we ensure any risks identified are included in our IA risk register and are communicated to the IAO for their agreement.

Where risks are significant these may be escalated to the SIRO for oversight and approval, and these are formally presented and documented.

The team uses an Information Security Management System to host all review documentation, to track approvals and to provide an audit trail.

**Records Management**

The records management function has been a recent addition to the wider Information Assurance team, with the team formally reporting in to the Head of IA from mid November 2023. The active management of our information to make sure we are holding it in line with statutory or MoPI (Management of Police Information) guidelines is key to meeting our data protection obligations.

As we move forwards with the enhanced use of O365, with the potential to make greater use of Sharepoint/Teams and the apps available within the platform, applying consistent and automated retention will become a key control.

We retain a shared paper records store with West Mercia Police, and while this is working well, we need to consider if in the longer term Warwickshire may need to stand up its own provision.

**Role of the Data Protection Officer (DPO)**

The final piece of our Information Assurance function is the role of DPO, which sits with the Head of IA. This is statutory role, and the tasks are defined in Article 39 of the UKGDPR as:

- to inform and advise you and your employees about your obligations to comply with the UK GDPR and other data protection laws;
- to monitor compliance with the UK GDPR and other data protection laws, and with your data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting appropriate audits;
- to advise on, and to monitor, data protection impact assessments;
- to cooperate with the ICO; and
- to be the first point of contact for the ICO.

The role of DPO fits naturally with the Head of IA as it important that in carrying out the role the DPO is required to take into account the risk associated with the processing being undertaken and they must have an understanding of the nature, scope, context and purposes of the processing.

The DPO should prioritise and focus on the more risky activities, for example where special category data is being processed, or where the potential impact on individuals could be damaging, and provide risk-based advice to your organisation. The DPO cannot “tell” an organisation what it should do only offer advice and guidance and if the organisation decides not to follow the advice given by the DPO, it should be documented to demonstrate accountability. These processes are documented in our SIRO escalation process and our documentation trail within our ISMS.