Report to the Chair and Members of the Audit Committee
12th September 2022

Executive Officer: **Lisa Theaker, ACC, Temp SIRO**
Presenting: **Susan Haider, Head of Information Management and Data Protection Officer**

Status: For Information

Information Management Update

1. Purpose

1.1 The purpose of this report is to provide the Audit Committee with continued assurances that Cleveland Police has implemented the necessary technical, physical, personnel and procedural security controls to protect its information and satisfy national Information Assurance (IA) requirements that are pertinent to government and policing. This report will also provide assurances around compliance with data protection legislation and areas of risk. A high-level summary of information assurance activities performed so far in 2022 is detailed below.

2. Recommendations

2.1 It is recommended that Members note the content of the report and take assurance that the appropriate information security controls are in place.

3. Information Assurance Governance

3.1 The force continues with a governance framework including specialist IA roles: Senior Information Risk Owner (SIRO), Information Asset Owners (IAOs), Information Security Manager (ISM), Records Manager and Data Protection Officer (DPO is also the Head of the Information Management Unit).

The SIRO is temporarily ACC Lisa Theaker. The strategic risks remain

i. loss/disclosure of paper documents;
ii. inappropriate disclosure electronically (e.g., email, social media);
iii. availability of critical computer systems;
iv. loss/disclosure of removable media; and
v. physical security of sites.

3.2 The GDPR Auditor and Deputy ISO continues to review existing and new workflows across the organisation, providing additional detail information in relation to information risks. The IT Security Officer (ITSO) continues to work closely with ICT, in particular on matters relating to IT health checks and liaising with the National Monitoring Centre.

3.3 The baseline e-learning training for all officers and staff remains "Managing Information" (operation and non-operational) and "Government security classification". Monitoring compliance of e-learning packages remains a concern

and area of focus, although new dashboards on the force's intranet are assisting with mitigating this. All IAOs are still expected to complete the "Protecting Information" level 2 course and are encouraged to consider the level 3 course and "Data Protection Foundation" course.

3.4 The remodelled Information Assurance Board continues to be effective, negating the need for a separate Information Asset Owners Board, the IAO Board has been formally dissolved to prevent duplication of governance with the Information Assurance Board. Performance indicators on compliance with information rights, personal data breaches and data protection compliance matters, feature as a standing agenda item.

3.5 Several areas of work consume significant amounts of staff resource:

i. M365 is part of the National Enabling Programme and uses Microsoft's public cloud capability. The force is beyond the technical pilot stage, but without full rollout. The continuing changes in the cloud platform and the need to exploit the business benefits of this environment are particularly demanding.

ii. Education and preventative work continue and expand. Infosec staff are engaged with training teams and induction days to provide input to both PCDA officers and new staff. Along with the Digital Services staff, infosec visit business areas to assist in identifying ways to improve business processes (e.g., reducing the need for removable media).

iii. Multiple audits have required infosec staff. This includes the UKAS audit for the forensic services, and internal audit in relation to cyber security (which was generally positive).

3.6 Security incidents continue to be recorded, assessed and reviewed by the ISM. Whether personal information is involved, the DPO makes an assessment in relation to notifying the Information Commissioner's Office. Critical incidents are handled by "gold" groups. Some statistics are provided in the table in the appendix.

4. Compliance

4.1 The Force is a registered Data Controller with the Information Commissioner's Office and is responsible for ensuring compliance with the UK GDPR and the Data Protection Act (2018) through the duties and responsibilities of the Data Protection Officer.

4.2 Remediation from the 2021 IT Security Health Check (ITSHC aka ITHC) remains incomplete due to ICT resource. As a direct result, the various Code of Connection approvals have all expired. We anticipate resubmission for these approvals by the end of August 2022. This issue was raised as a risk for the force's corporate risk register. Planning for the 2022 ITHC has commenced.

4.5 The Head of Information Management and DPO has completed the ICO Self-assessment toolkit on accountability, which has identified areas of compliance, partial compliance and non-compliance with the ICO's 338 expectations of data controllers. A plan is being developed to work through the area of partial and non-compliance based on risk.

4.6 A new role of Information Governance Manager has been established and currently going through recruitment. This role will progress a lot of the work identified in the ICO's toolkit, along with addressing work identified in paragraph below.

4.7 Work is underway to refocus the activities of Information Asset Owners to identify where we use Data Processors and need data processing contracts, where we need information sharing agreements and where we need to review privacy notices, so that we can understand the scale of the problem and prioritise work based on risk. Progress and risk will be reported into the Information Assurance Board.

4.8 An Information Management and Data Protection Policy, along with an Appropriate Policy Document to safeguard the processing of sensitive personal data (a legal requirement) have been drafted and are going through the consultation process.

4.9 Work is underway within Records Management to initiate pre-requisite work to prepare for the Niche eRRD (electronic retention, review and deletion) module. This is a significant piece of work that is likely to take 3-4 years and spans across many parts of the organisation, ensuring processes and data are in shape for the eRRD tool to be effective. The eRRD tool will not only allow Cleveland Police to comply with MoPI within Niche, but this also allows us to manage the RRD of records held outside of Niche, who retention period are linked to the Niche record.

4.10 The Records Manager is also working on the implementation of a 2 year retention policy to Cleveland Police's email content, following approval already given. The implementation will include providing users with a 12 month countdown to the change, and instructions on how to manage emails requiring a longer retention period (by exception). This will reduce the risk of processing personal data for longer than is necessary.

5. Implications

5.1 Finance

There could be some financial implications if we were to receive fines from the ICO in relation to non-compliance with data protection legislation. Individuals could also raise civil claims as a result of Cleveland Police incurring a breach with their data.

5.2 Diversity and Equal Opportunities

There are no diversity or equal opportunity implications arising from the content of this report.

5.3 Human Rights Act

There are no Human Rights Act implications arising from the content of this report.

5.4 Sustainability

There are no sustainability implications arising from this report.

5.5 Risk

The risk of reputational harm or a breach of operational security arising from Airwave radio management has been added to the corporate risk management system.

5.6 A risk relating to reputational harm and/or potential breaches of security and/or adverse findings from regulators was added in relation to ITHC and ICT resource.

5.7 There are risks associated with non-compliance with data protection legislation including records management that may result in ICO enforcement action (including audit, being served improvement notices, recommendations and fines). We are at risk of civil claims being received in relation to handling of personal data. There is a risk of reputational damage and public confidence in the handling and management of personal data. This risk has been added to the risk register.

Susan Haider
Head of Information Management and Data Protection Officer
12th September 2022

Appendix: Incident statistics

An incident can be in multiple incident types (e.g., Disclosure due to Data Quality)

Incident type	8 Sep **2018** -7 Sep **2019**	8 Sep **2019** -7 Sep **2020**	8 Sep **2020** -26 Aug 2**021**	27 Aug **2021** – 18 **Aug 2022**
Accidental damage/destruction	2	0	1	0
Asset misuse	0	1		3
Breach policy	-	-	7	3
Breach procedure	1	1	0	2
Cybersecurity	5	6	6	11
Cybersecurity - other party	-	-	5	4
Data quality	-	-	-	15
Disclosure (see next table)	29	33	58	61
Disclosure - other party	-	-	1	5
Failure/misconfiguration	-	-	2	6
Fault	0	1	0	0
Intruder	5	1	1	0
Loss of availability	-	-	-	11
Lost Airwave	1	9	5	16
Lost BWV	1	4	2	0
Lost ID card	26	25	20	0
Lost SIM card	1	0	0	0
Lost equipment	0	1	0	0
Lost item	2	0	0	0
Lost keys	1	0	0	0
Lost media	2	4	1	4
Lost mobile phone/device	6	10	15	15
Lost paper	3	5	2	7
Lost police equipment/uniform	5	1	3	2
Lost token	1	0	0	0
Lost warrant card	0	0	0	0
Lost/found Airwave	3	5	0	0
Lost/found BWV	1	0	0	0
Lost/found ID card	8	12	7	10
Lost/found keys	1	0	1	1
Lost/found laptop	0	1	1	6
Lost/found media	-	-	2	4
Lost/found mobile phone/device	2	6	3	12
Lost/found paper	2	3	6	8
Physical security	9	10	9	16
Post	0	1	0	0
Stolen Airwave				0
Stolen BWV	0	1	0	0
Stolen ID card	0	1	1	0
Stolen item	-	-	-	1
Stolen laptop	0	1	0	0
Stolen mobile phone/device	-	-	-	2
Stolen police equipment/uniform	-	-	1	1
Suspicious incident	1	0	1	5
Unconfirmed	0	1	1	0
Unknown	0	0	0	0
Vetting	2	0	0	0
Non-incidents (cancellations, duplicates, tests)	10	5	1	6
Total	130	149	175	308

Involves personal data	-	-	9 (part year)	73

Disclosure categorisation – an incident can be in multiple categories

Email	11	Internal	7
Email_misaddressing	4	Partner agency	15
MS Teams (new category)	0	External	25
Social media (new category)	0		
Paper	16		
Phone	3		
Verbal	2		