



THE CHIEF CONSTABLE OF CLEVELAND

Data Protection

FINAL Internal Audit Report: 6.24/25

29 January 2025

This report is solely for the use of the persons to whom it is addressed.

To the fullest extent permitted by law, RSM UK Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party.

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING



OUTCOME OVERVIEW

Background:

As part of the approved internal audit plan for 2024/25, we have undertaken a review of the Force's data protection framework and approach to compliance with the UK General Data Protection Regulation (GDPR) in relation to the use of personal data and Part 3 of the Data Protection Act 2018 (DPA 2018) in relation to the processing of personal data for preventing, investigating, detecting and prosecuting crimes.

Both the UK GDPR and the supporting Data Protection Act 2018 place an emphasis on organisations, in this case the Force, to implement a framework by which individual's data is held securely, is only used for the purposes specified and data subject rights can be adhered to. The Information Commissioner's Office (ICO) is responsible for regulating data protection and ensuring organisations adhere to the aforementioned laws.

The Force has an Information Management Team in place that includes information governance and information security as part of the wider team. The Head of Information Management who was also the Data Protection Officer (DPO) has left the Force and this position remains vacant. The Information Governance Manager and Deputy DPO is currently undertaking the DPO role on an interim basis. There is a Head of Digital and Data Technology who the teams currently report to and the team is currently being reviewed with the expectation that the structure will change going forward. The changes will include a DPO and Deputy.

The GDPR Data Protection Auditor completes a review of the information within the Register of Processing Activities (RoPa) for every area each calendar year and the Information Asset Register is updated to ensure that the details are still relevant and accurate.

This is an agreed upon procedures assignment delivered at the request of management and the Joint Audit Committee. This report does not provide a level of assurance / internal audit opinion.

Headline findings:

Our review identified the following issues resulting in **two medium priority management actions**:

Training

- GDPR training is delivered to all staff on induction. All staff are also required to undertake a bi-annual data protection eLearning course as a refresher or to inform them of any changes that have taken place. On review of the eLearning dashboard it was clear that this training has not been undertaken by all staff as the training completion rates are 72.5% for operational staff and 57.7% for non-operational staff. If staff have not undertaken up to date GDPR training there is increased risk of the correct processes not being undertaken in relation to data protection including the security of data and reporting when a breach occurs. **(Medium)**

Role of the data protection officer

- The Force does not currently have a formally appointed DPO as the previous DPO left and has not yet been replaced. The role is currently being covered by the Deputy DPO with the help of the Information Security Manager when needed. The interim arrangements have not been formally documented. As the Deputy DPO is undertaking the role there is no deputy in place and therefore limited resource is available. **(Medium)**

We noted the following controls to be adequately designed and operating effectively:

Data ownership and roles and responsibilities

- The Force has a number of approved and up to date policies and procedures in place in relation to data protection, information governance and information security. All these documents are available on the intranet for staff and a number are available to members of the public on the internet. The policies include the roles and responsibilities in relation to data protection including the information asset owners.

Business processes and data discovery

- The Force has an Information Asset Register and a RoPa that are reviewed and updated at least once per calendar year. Details of systems and areas data is stored is documented within these along with other information required by the ICO including but not limited to whether personal data is held, how data is processed and shared (where applicable), including the security measures in place, the purpose of processing, whether consent is needed and if not the lawful reason for holding the data. The Information Management team attend Change Board meetings to identify whether any new projects require a Data Protection Impact Assessment to be undertaken.

Individuals' rights

- Information on individuals' rights is available on the Force website, along with the Privacy Notice. There is also information in relation to freedom of information and subject access requests on the website. We reviewed a sample of freedom of information and subject access requests and on all occasions the correct process had been followed. We also reviewed the response time compliance figures for both Subject Access Requests (SAR) and Freedom of Information (Fol) requests and on both occasions the Force had just met the 90% requirement. We acknowledged that this has improved throughout the year and will require the same amount of resource as currently in place to maintain this.

Consent

- The Force has undertaken a large amount of work on consent since the previous audit which identified a number of areas of improvement. A consent guidance document has been produced and this is available on the Intranet for all staff members to access. The Information Governance Manager has also had meetings with each area to discuss consent and to determine whether consent is needed on all occasions. The RoPa has also been updated to include a question to determine whether consent is required or whether there is another lawful reason for the data being required.

Data breaches

- The Force has a detailed Information Security Incident response plan which includes data breaches. Breaches are then recorded in a system called Flatfish and this includes details of how the breach was investigated, actions taken and lessons learnt.

Good practice

- The Data Protection Auditor meets with all areas within the calendar year to talk through data protection and the RoPA. We identified that as a result of these discussions there were improvements made in processing data. There were also occasions where additional data processing was identified, which may not have been picked up if the Information Asset Owners had completed the annual review without the input of the Data Protection (DP) Auditor. This also makes the DP Auditor more approachable and staff will not hesitate to ask questions if they are unsure of anything.

SUMMARY OF ACTIONS FOR MANAGEMENT

The action priorities are defined as:

High

Immediate management attention is necessary.

Medium

Timely management attention is necessary.

Low

There is scope for enhancing control or improving efficiency.

Ref	Action for management	Priority	Responsible Owner	Date
1	The Force will investigate the most effective ways to make staff aware of the bi-annual training and improve completion rates. Non completion of training will be monitored and chased to ensure that all staff complete the required training.	Medium	Information Governance Manager	30 September 2025
2	The Force will recruit and employ a permanent DPO with detailed roles and responsibilities. There will also be a Deputy DPO in place to ensure there is enough resource to cover all roles and responsibilities required of a DPO.	Medium	Head of Digital Data and Technology	31 July 2025

Detailed Findings and Actions

02



DETAILED FINDINGS AND ACTIONS

The results of our testing are set out below.

Area: Awareness – all staff

Control	The Force provides training to all new members of staff in order to provide them with knowledge of data protection requirements. There is also an eLearning package that must be completed by all existing staff bi-annually.	Controls complied with	x
----------------	---	-------------------------------	---

Findings summary Through discussion and review of the Data Protection and Information Governance Training Matrix, we established that GDPR training is provided in a number of ways. All new staff and officers are provided with training as part of their induction programme. We obtained and reviewed the induction training slides and these detailed the key members of staff to contact in relation to data protection, what data protection is, details on processing data, principles, myths, breaches and consequences, records management and various aspects of information security.

There has also been additional 'Protecting our Information' training which covers areas similar to the induction training.

In addition to the in person training, there is also a GDPR eLearning module that all staff are required to undertake on a bi-annual basis.

We reviewed the eLearning dashboard which contains data for all employees to determine whether staff had undertaken the training required and it was evident from the statistics that there are a large number of staff that are not up to date with the mandatory training. For example the MI training completions are 72.5% for operational staff and 57.7% for non-operational staff. Levels of mandatory training non compliance are reported within the Governance structure as part of the Data Protection reports.

If staff have not undertaken up to date GDPR training, there is increased risk of the correct processes not being undertaken in relation to data protection including the security of data and reporting when a breach occurs.

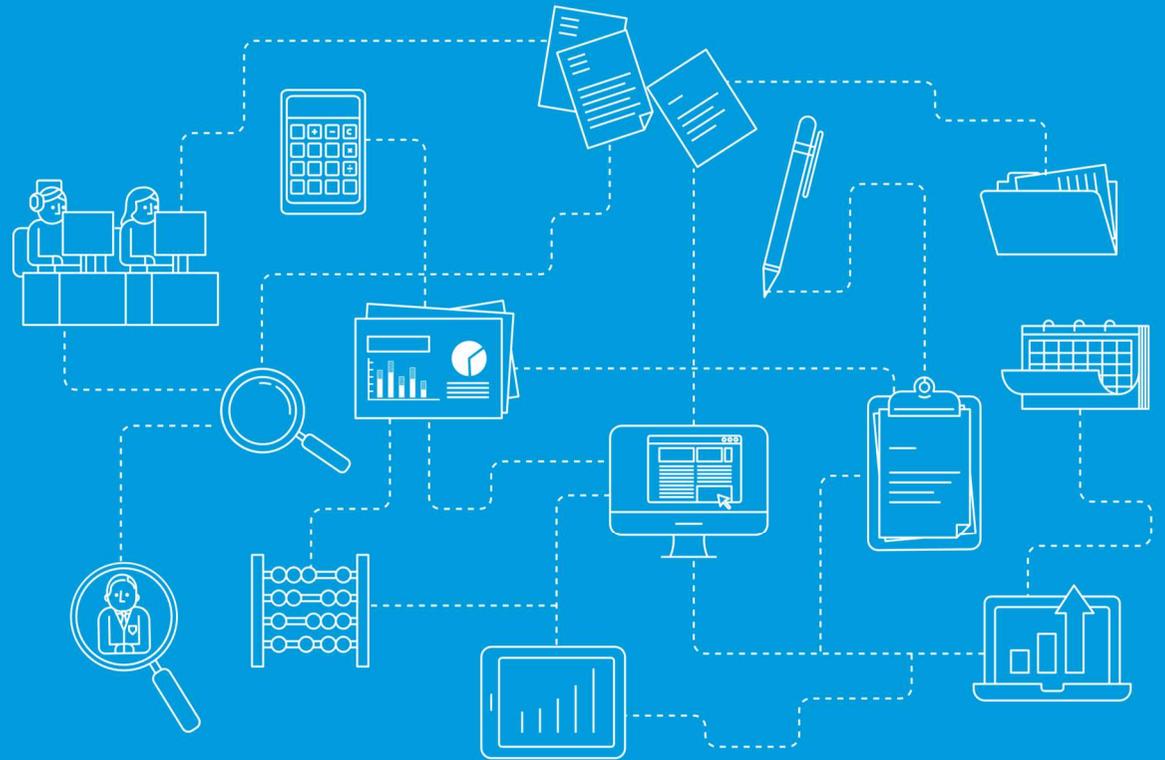
Management action 1	The Force will investigate the most effective ways to make staff aware of the bi-annual training and improve completion rates. Non completion of training will be monitored and chased to ensure that all staff complete the required training.	Responsible Owner: Information Governance Manager	Date: 30 September 2025	Priority: Medium
----------------------------	---	---	-----------------------------------	----------------------------

Area: Data Protection Officer - role, priority and resource

Control	<p>Partially missing control</p> <p>There is a formally appointed DPO at the Force. The DPO is afforded sufficient resources to perform their required tasks.</p> <p>The acting DPO and Information Security Manager have monthly meetings with the SIRO (Senior Information Risk Officer).</p>	<p>Controls complied with x</p>
Findings summary	<p>Through discussion and review of the organisational structure we identified that there is currently no dedicated DPO in place. The previous DPO has left the Force and not yet been replaced. We also identified that the department is undergoing a review with the likelihood of restructure so the DPO may not be a like for like replacement. At the time of the audit, the proposed new structure had not been finalised so we were unable to confirm where the DPO would fit in.</p> <p>The Information Governance Manager is currently undertaking the DPO role as an interim measure along with the Information Security Manager. The Information Governance Manager is the Deputy DPO as part of their permanent role so whilst they are undertaking the DPO role there is currently no deputy. Without a DPO and a Deputy DPO there may not be sufficient resource to undertake all tasks especially in the absence of the Information Governance Manager as there is no assigned deputy.</p> <p>Through discussion with the Information Governance and Information Security Manager we established that both have regular one to ones with the Senior Information Risk Officer to discuss any Data Protection issues.</p>	
Management action 2	<p>The Force will recruit and employ a permanent DPO with detailed roles and responsibilities.</p> <p>There will also be a Deputy DPO in place to ensure there is enough resource to cover all roles and responsibilities required of a DPO.</p>	<p>Responsible Owner: Head of Digital Data and Technology</p> <p>Date: 31 July 2025</p> <p>Priority: Medium</p>

Appendices

03



APPENDIX A: CATEGORISATION OF FINDINGS

Categorisation of internal audit findings

Low

There is scope for enhancing control or improving efficiency.

Medium

Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media.

High

Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

The following table highlights the number and categories of management actions made as a result of this audit.

Area	Non-compliance with controls*	Agreed actions		
		Low	Medium	High
Data Protection	2 (11)	0	2	0
Total		0	2	0

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area

Debrief held 6 January (last information received)
Draft report issued 10 January 2025
Responses received 29 January 2025
Final report issued 29 January 2025

Internal audit contacts Dan Harris, Head of Internal Audit
Phil Church, Associate Director
Lucy Sheridan, Senior Consultant

Client sponsor Director of Finance and Assets, Chief Constable
Information Security Manager
Data Protection Officer
Head of Digital Data and Technology

Distribution Director of Finance and Assets, Chief Constable
Information Security Manager
Data Protection Officer
Head of Digital Data and Technology

We are committed to delivering an excellent client experience every time we work with you. If you have any comments or suggestions on the quality of our service and would be happy to complete a short feedback questionnaire, please contact your RSM client manager or email admin.south.rm@rsmuk.com.

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of **The Chief Constable of Cleveland**, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM UK Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM UK Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.
RSM UK Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.