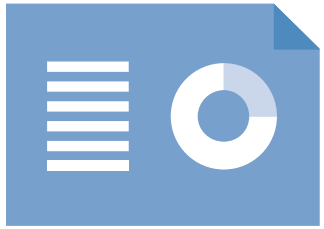
Hampshire Constabulary and Thames Valley Police

Data protection audit report

March 2021

Information Commissioner's Office

Executive summary



Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

Hampshire Constabulary and Thames Valley Police (HCTVP) have a collaboration agreement in place for their shared Information Governance functions. HCTVP agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 4 November 2020 with representatives of HCTVP to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and HCTVP with an independent assurance of the extent to which HCTVP, within the scope of this agreed audit, is complying with data protection legislation.

The scope areas covered by this audit are determined following a risk based analysis of HCTVP processing of personal data. The scope may take into account any data protection issues or risks which are specific to HCTVP, identified from ICO intelligence or HCTVP's own concerns, and/or any data protection issues or risks which affect their specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of HCTVP, the nature and extent of HCTVP processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to HCTVP.

It was agreed that the audit would focus on the following area(s):

Scope Area	Description
Governance and Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance with Part 3 of the DPA18 are in place and in operation throughout the organisation.
Information Risk Management	The organisation has applied a "privacy by design" approach. Information risks are managed throughout the organisation in a structured way so that management understands the business impact of personal data related risks and manages them effectively to assure the business of the organisation.
Personal Data Breach Management and Reporting	The extent to which the organisation has measures in place to detect, assess and respond to security breaches involving personal data, to record them appropriately and notify the supervisory authority and individuals where appropriate

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are normally a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

However, due to the outbreak of Covid -19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore HCTVP agreed to continue with the audit on a remote basis. A desk based review of selected policies and procedures and remote telephone interviews were conducted from 8 February 2021 to 11 February 2021. The ICO would like to thank HCTVP for its flexibility and commitment to the audit during difficult and challenging circumstances.

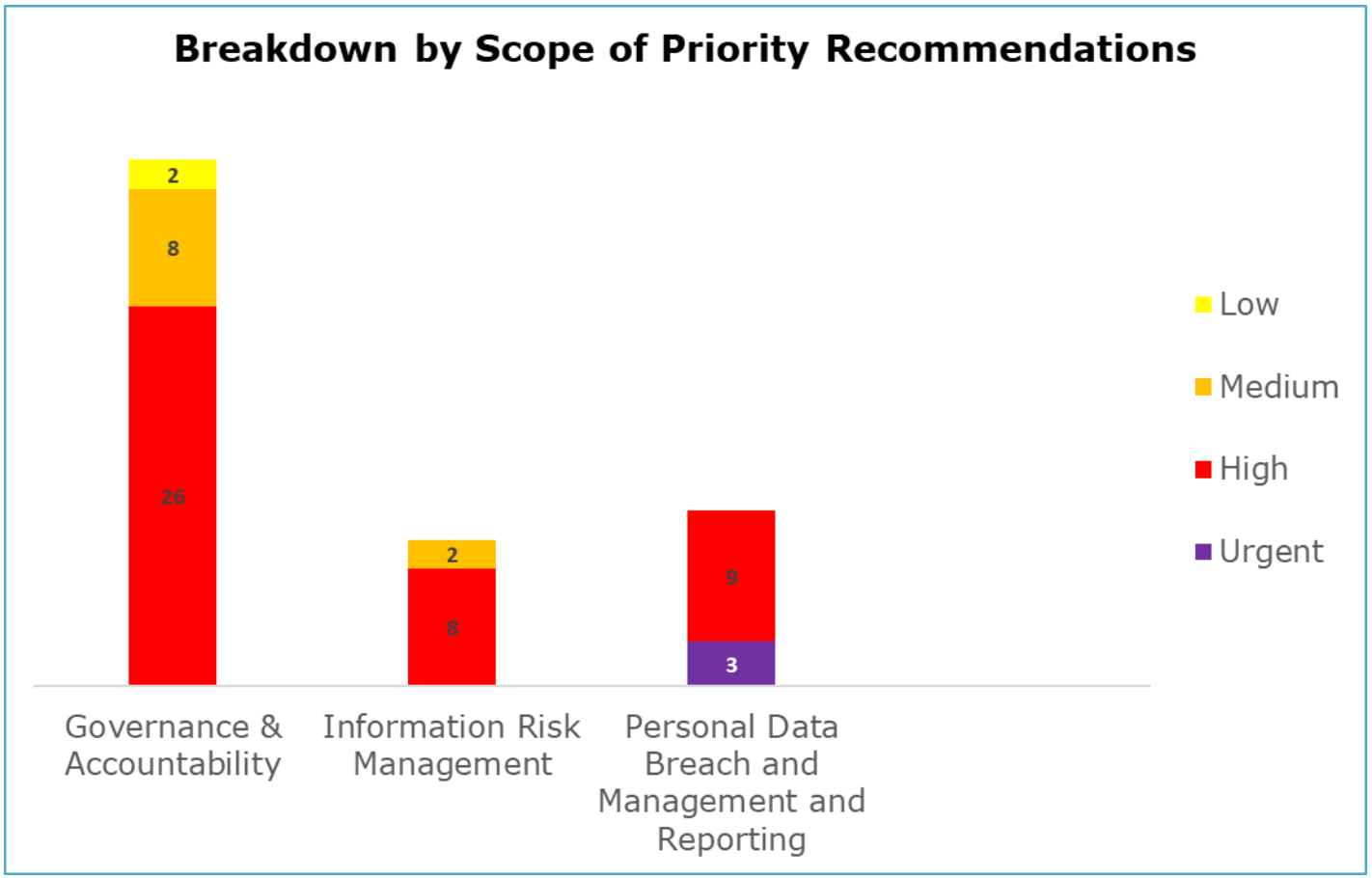
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist HCTVP in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. HCTVP's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary*

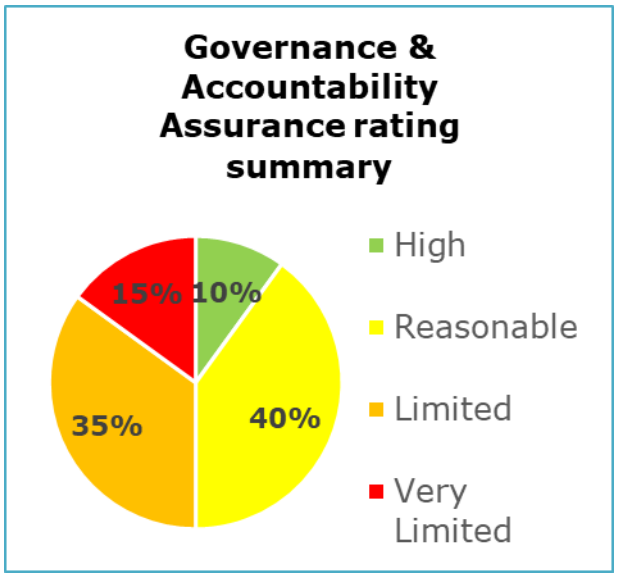
Audit Scope Area	Assurance Rating	Overall Opinion
Governance & Accountability	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Information Risk Management	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Personal Data Breach Management and Reporting	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

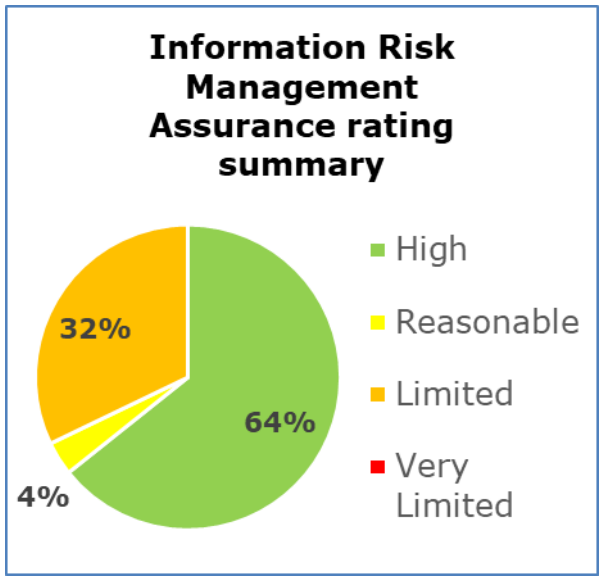
*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

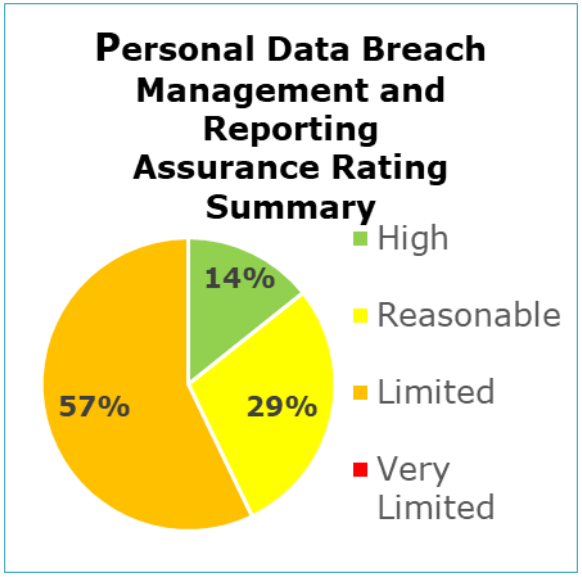
Priority Recommendations



Graphs and Charts







Areas for Improvement

The Logging of automated processing systems (any IT database) needs to be completed for all HCTVP systems to meet section 62 DPA18 requirements. The effectiveness of any processors logging systems should also be routinely checked.

Develop and make available to all staff sufficient and comprehensive procedural guidance that includes data protection, records management, information security and data sharing. This guidance should differentiate between personal data processed for general and law enforcement processing.

Review the Appropriate Policy Document to include more detail about the retention and erasure of sensitive personal data. The adherence to the retention period should be documented in HCTVPs Record of Processing Activities (ROPA).

Develop an Information Governance training plan and complete a Training Needs Analysis (TNA) for all staff, volunteers, agency staff and contractors to inform the training plan. A training needs analysis for staff with specific information risk management roles will identify gaps in understanding and enable development of further support or training. HCTVP should ensure that all staff receive sufficient training so they can recognise and respond appropriately to personal data breaches (PDBs).

An external audit plan should be developed and a regular programme of external audits implemented to provide additional assurance of HCTVP's compliance with data protection legislation.

Review all current contracts with joint data controllers and data processors and ensure appropriate contracts and agreements are in place. All contracts should be logged and routinely monitored to provide assurance that information risks are assessed and reported in line with the terms of the contract under the DPA18. This should be strengthened by due diligence checks which should be conducted before entering into and during the contract.

HCTVP has a general privacy notice on its website but there has been no review to ensure that sufficient privacy information is made available in all specific situations. There is therefore a risk that HCTVP are not complying with their obligations under section 44 of the DPA18 and that data subjects may not be aware of their rights and how their information is being processed.

The Data Protection Impact Assessment (DPIA) process should be referenced within the risk management policies and related procedures. DPIAs should be assigned a formal review date or an early review when a substantial change of the process occurs, to allow emerging risks to be identified and mitigating controls enabled. HCTVP should also instigate regular reviews of the implemented DPIA controls to assure they are proving effective.

A system of formal reporting should be introduced to enable complete oversight of all PDBs. HCTVP should continue with plans to ensure deletions can be made in breach logs. Minimisation methods and dip sampling checks should be introduced to ensure personal data in breach logs is reduced in line with the retention period. Policies and procedures should be streamlined via a dedicated PDB policy and a process should be established to notify affected individuals where a breach is likely to result in a high risk to their rights and freedoms.

Best Practice

The Joint Information Management Unit conducts a four monthly review of information assets with the data guardians. As well as identifying and mitigating information risks the review also highlights any up and coming new initiatives or project that may require a DPIA. This proactive horizon scanning is an excellent way of capturing projects involving the use of personal data at an early stage.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of HCTVP.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of HCTVP. The scope areas and controls covered by the audit have been tailored to HCTVP and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.