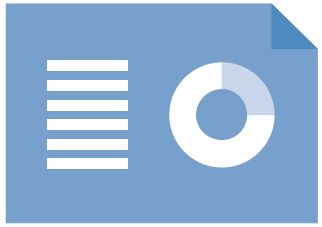
Her Majesty's Revenue and Customs (HMRC)

Data protection audit report

August 2019

ico.
Information Commissioner's Office

Executive summary



Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the General Data Protection Regulation (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.

The Information Commissioner served HMRC with an Enforcement Notice, on 09 May 2019, following an investigation into its use of voice authentication for customer verification. The Enforcement Notice required HMRC, within 28 days of the date of the Notice, to:

- Delete all of the biometric data held under the Voice ID system for which it does not have explicit consent.
- Require its suppliers who operate, manage or are involved in the Voice ID system to delete all the biometric data they process under the Voice ID system for which it does not have explicit consent.

In the course of the investigation, which resulted in the serving of this Enforcement Notice, the Information Commissioner identified concerns in relation to the governance and information risk arrangements in place at HMRC which ought to have prevented the Voice ID system from being utilised in a non-compliant way.

An audit was therefore proposed to provide assurance that these concerns had been addressed and that the risks of similar issues recurring had been adequately reduced.

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

Scope Area	Description
Governance & Accountability	Without robust governance and accountability processes for evaluating the effectiveness of information governance policies and procedures there is a risk that personal data may not be processes in compliance with the regulations resulting in regulatory action and/or reputational damage.
Information Risk Assessment (DPIA) & Management	Without effective processes in place to identify, assess and manage personal data related risks and facilitate a "privacy by design" approach, the organisation may fail to identify the business impact of information risk and meet individuals' expectations of privacy. This may result in regulatory action, reputational damage to the organisation and damage or distress to the individuals who are the subject of the data.

It was also agreed that the audit would serve to review the steps that HMRC had taken to comply with the requirements of the Enforcement Notice.

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

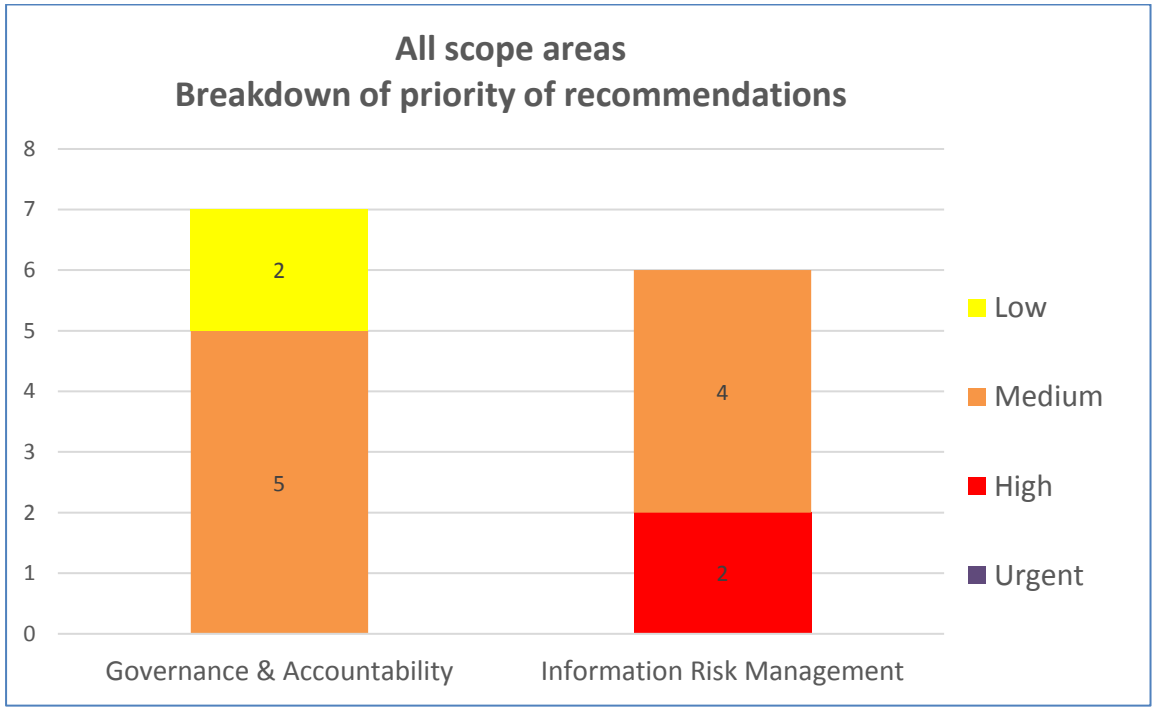
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist HMRC in implementing the recommendations each has been assigned a priority rating based upon the risks that they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

Audit Summary

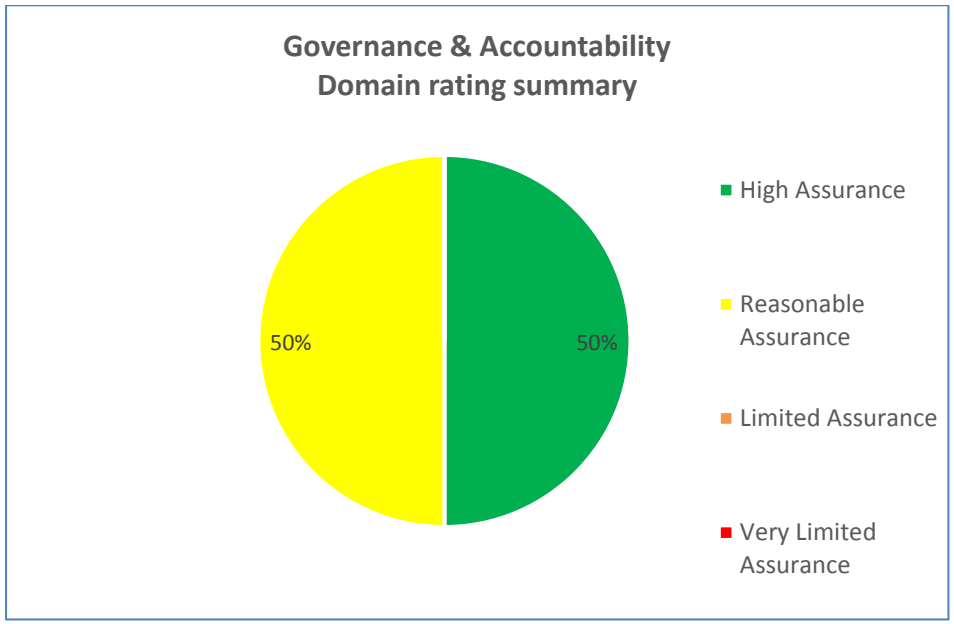
Audit Scope Area	Assurance Rating	Overall opinion
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Information Risk Assessment (DPIA) and 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.

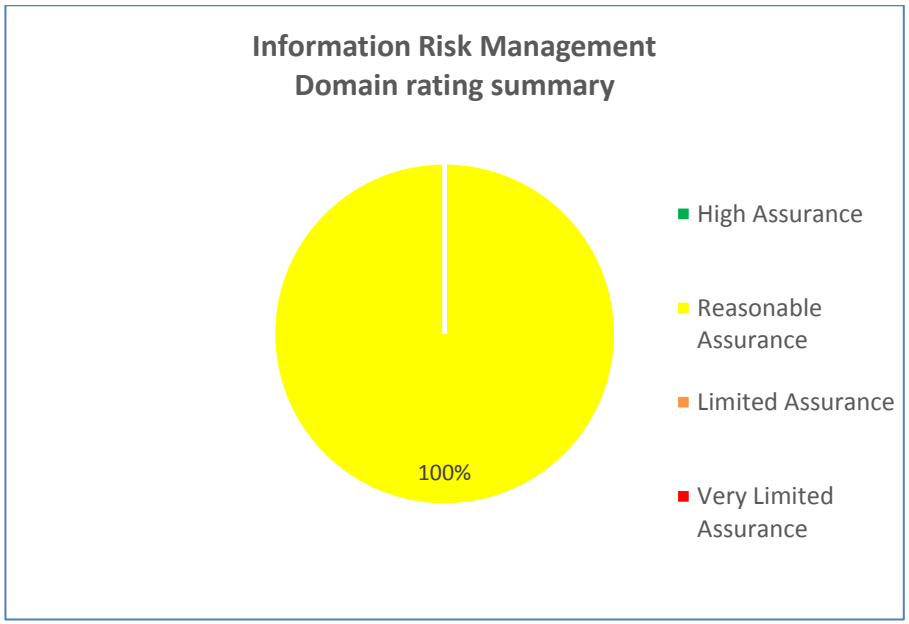
The ICO were satisfied with the approach taken by HMRC to meet the requirements of the Enforcement Notice of 9th May 2019. The project was well-managed with sufficient oversight and monitoring provided by senior management. While we did not conduct forensic testing of HMRC systems we are satisfied that HMRC, and their contractors, have undertaken sufficient monitoring and verification checks to ensure that all relevant data has been deleted in line with the requirements of the notice.

Priority Recommendations



Graphs and Charts





Areas for Improvement

Governance & Accountability

HMRC has developed an internal audit programme in relation to information governance and data protection. The programme will be owned by the Office of the Data Protection Officer (oDPO), utilising a combination of self-assessment questionnaires and full audit engagements, and is intended to provide oversight of data protection and assurance to senior management.

This audit programme is due to be piloted and rolled-out in the coming months. The oDPO will need to keep the programme under review, once it is piloted and rolled out, to ensure that the controls are appropriate and that the programme operates effectively and provides the Data Protection Officer (DPO) and HMRC with adequate assurance.

Information Risk Assessment (DPIA) and Management

Information risks are generally managed in a structured way; however, there are still risks in relation to ensuring that information risks are identified and addressed in a timely manner through the Data Protection Impact Assessment (DPIA) process. As this is a relatively new process HMRC need to monitor the situation to ensure that DPIAs are completed where required and that the DPO has the necessary oversight of and input into projects that are likely to involve high risk processing.

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 HMRC.

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 HMRC. The scope areas and controls covered by the audit have been tailored to HMRC and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.