Report to:	MSMTM
Report by:	Helen Gardner-Swift, Head of Corporate Services (HOCS)
Meeting Date:	29 March 2022
Subject/ Title: (and VC no)	Internal Audit – UK GDPR Compliance (VC167401)
Attached Papers (title and VC no)	Internal Audit –UK GDPR Compliance Report (VC167072)

Purpose of report

1. The purpose of this Committee Report (CR) is to ask the Senior Management Team (SMT) to formally acknowledge receipt of the Internal Audit Report – UK GDPR Compliance and the recommended management action.

Recommendation and actions

2. I recommend the following:

   (i) the SMT formally acknowledge receipt of the Internal Audit Report – UK GDPR Compliance (the Report) and the findings set out in the Report

   (ii) the SMT note the Management Action set out in the Report

   (iii) this CR is published in full but the Report is not published for the reasons set out in paragraph 19.

Executive summary

3. Our internal auditor, Azets, reviewed the effectiveness of our UK GDPR Compliance and has submitted a Report to us.

4. The Report concludes that the Scottish Information Commissioner's (the Commissioner) procedures reflect good practice in a number of areas:

   - a Data Protection Policy and Handbook is in place which covers all the expected areas under the UK GDPR as well as staff procedures for Data Subjects Access Requests (DSARs), Data Protection Impact Assessments (DPIAs) and data incident reporting.

   - a Personal Data Processing Spreadsheet is in place which includes a record of the data assets held by the Scottish Information Commissioner. The spreadsheet details information about each asset, including how it is processed, the purpose for collection, where it is held, the retention period and whether it contains special category data.

   - there is regular monitoring of subject access requests (SARs) via quarterly Committee Reports. These report that within the first three quarters of 2021-22, 100% of SARs received were processed within one calendar month.

- templates are in place for both a pre-Data Protection Impact Assessment (DPIA) checklist and a DPIA. The Commissioner has completed DPIAs and also reviewed completed DPIAs.

- There is extensive mandatory training for all staff on data protection leading practices. There is also regular awareness raising activities which focus on reducing the risk of data protection incidents.

5. The internal audit did not identify any high-risk, significant or reportable weaknesses.

6. One area for improvement has been identified which, in the view of the internal auditor, if addressed, would strengthen the Commissioner's control framework and there is a related recommended management action.

7. The area for improvement relates to the review of the Data Protection Safeguards Policy. This policy was due to be reviewed by October 2021. The Responsible Manager for the policy is the Head of Enforcement (HOE) and the HOCS. The SMT agreed last year that the policy would be reviewed after the draft DPIA relating to Section 65 and Regulation 19 allegations had been finalised as this is relevant in the consideration of the review. The draft DPIA is being considered at present by the GDPR Working party. Unfortunately, the DCS in the policy was not updated to reflect the SMT's decision and the review date amended accordingly.

8. The Management Action is to review and update (as required) the Data Protection Safeguards Policy. The action owner is the HOE and myself, the HOCS, and the action due date is 31 May 2022.

Risk impact

9. The risk of not having in place and monitoring effective and robust governance arrangements, is mitigated by the maintenance and implementation of an internal audit plan and the engagement of an internal auditor or an appropriate expert to carry out the planned audits.

10. The Commissioner's reputation and, also, public confidence in the Commissioner, could be undermined if the Commissioner fails to meet UK GDPR duties and responsibilities and does not have effective and robust UK GDPR and data protection policies in place.

11. Carrying out an internal audit mitigates against strategic and operational risks of not complying with UK GDPR duties and responsibilities and provides assurance that there are effective policies and procedures in place.

Equalities impact

12. There is no direct equalities impact arising from the report.

Privacy impact

13. There are no direct privacy implications arising from this report.

Resources impact

14. The internal audits to be carried out in each financial year are reflected within the annual Operational Plan so that the resources impact is taken into account.

Operational/ strategic plan impact

15. The internal audits for each financial year take account of strategic risks and are reflected within the annual Operational Plan.

Records management impact (including any key documents actions)

16. None.

Consultation and Communication

17. The draft internal audit report was circulated to the SMT for factual comment and agreement of the proposed Management Action.

18. MSMTM minute.

Publication

19. This CR can be published in full but the Report is withheld on the basis that the exemption(s) in Sections 30(b)(ii) of the Freedom of Information (Scotland) Act 2002 would apply if a request were, at this stage, to be made for the information.