

# Agency Board meeting

## 24 June 2025

# Annual Assurance Report 2024-2025

### Purpose:

### The purpose of this paper is to provide information on areas of corporate governance to give the Agency Board assurance that they are being managed well.

### Recommendations:

We recommend that the Agency Board **discuss** and **note** the content of this report and consider whether there are any further areas of assurance they would like added to this report going forward.

Author: Alanna Sloan, Assurance and Risk Manager

Corporate Leadership Team Sponsor**:** Kirsty-Louise Campbell, Chief Officer Governance, Performance and Engagement

Date: 13 June 2025

## 1. Introduction

1.1. This is the first annual assurance report which pulls together some of the previous standalone reports, such as the Annual Certificate of Assurance, the Standards Report, the Corporate Governance and Best Value Assessment and the quarterly Assurance Reports for the Audit, Risk and Assurance Committee. It also covers some areas which were not previously reported on but where additional assurance would be welcomed by the Agency Board including information governance and cyber resilience.

1.2. This report covers the reporting period 1 April 2024 to 31 March 2025. The areas covered in this first annual report are Business Resilience; Complaints; Cyber Resilience; Data Protection; Health and Safety; Information Governance; Fraud Bribery and Corruption and Whistleblowing.

1.3. Further sections may be added over time to cover areas of assurance that are requested by the Agency Board, Corporate Leadership Team or Audit, Risk and Assurance Committee.

## 2. Overview

2.1. We are in the early stages of developing a new assurance map for SEPA now that the Assurance and Risk Manager started on 28th April 2025. The assurance map is a tool that will demonstrate the sources and types of evidence that exist across the organisation to provide oversight on governance, risk and control. A gap analysis can then take place to ensure there is coverage where assurance is needed with little or no duplication.

2.2. Whilst a good risk management framework and positive risk culture will assist the organisation to identify and assess risk, the assurance map will aim to provide comfort that good governance exists and can be evidenced.

2.3. We have used the standard three lines of assurance model (also known as the three lines of defence model) to demonstrate the different levels of assurance we can provide for each of the areas identified in the section above. The three lines of assurance are:

**1st line of assurance**: management assurance from “front line” or business operational areas. For example, policies, procedures, colleagues training followed or delivered by colleagues across the organisation.

**2nd line of assurance**: Oversight of management activity, separate from those responsible for delivery, but not independent of the organisation’s management chain. This includes access to internal experts’ advice; risk management; Senior Management and Corporate Leadership Team.

**3rd line of assurance**: Independent and objective assurance, including the role of internal audit and other external bodies. This includes internal audit; external audit; other external verification, such as UKAS accreditation, external experts input or peer review, and external consultation.

For each of the lines of assurance, we have given examples of what we already have in place.

2.4. The Standards Report and an update on ongoing legal action will also be included in this report as sections 3 and 4.

## 3. Standards Report

3.1. The Audit, Risk and Assurance Committee was given delegated responsibility for dealing with matters involving standards of conduct in public life. This includes acting as a source of reference for the Standards Officer and dealing with any concerns raised about the conduct of Agency Board members. There were no instances of misconduct requiring formal investigation during the period of this report and routine advice has been provided as required.

3.2. The Standards Commission provided training for Board members on advice notes in March 2025. Standards Commission updates are routinely added to the Resource Centre in Diligent Boards for all Board members to access.

## 4. Ongoing Legal Action

4.1. Quarterly updates are provided, for oversight and awareness, to the Audit, Risk and Assurance Committee on significant ongoing legal actions and the papers are made available to the full board on Diligent Boards.

## 5. Annual Assurance

5.1**.** The areas covered in this first annual report are Business Resilience; Complaints; Cyber Resilience; Data Protection; Health and Safety; Information Governance; Fraud Bribery and Corruption and Whistleblowing.

#### 5.2. Business Resilience

##### 5.2.1. 1st Line of Assurance

SEPA has a Business Continuity Policy in place which has been approved by the Corporate Leadership Team. There are Business Continuity plans in place for each office as well as Functional Business Continuity Plans and Business Impact Analyses.

We have a Training and Exercising programme in place which includes: a resilience module on our learning and development platform, Incident Response Officer training to all response colleagues in SEPA; delivery of specialist training including Crisis Management training for senior managers; an annual Corporate Leadership Team exercise; quarterly exercises and workshops across a range of subjects and Learn after Lunch sessions.

We have developed a comprehensive Resilience Handbook, and several contingency plans and guides have also been developed to support colleagues.

##### 5.2.2. 2nd Line of Assurance

SEPA has an annual resilience exercise which is attended by the Corporate Leadership Team and has Emergency Management Team arrangements in place. The Resilience Team conducts Lessons Identified reviews (debriefs) after each incident, event or exercise of note.

SEPA report on the number of up-to-date business continuity plans and number of security breaches in the [Corporate Performance report](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fbeta.sepa.scot%2Fmedia%2Fbg0cgmrn%2F250212-quarter-3-corporate-performance-report-final.docx&wdOrigin=BROWSELINK) which is presented quarterly to the Corporate Leadership Team and Agency Board.

##### 5.2.3. 3rd Line of Assurance

As SEPA is delivering services critical to Scotland, much of the work of the Resilience Team is managed through Local and Regional Resilience Partnerships, facilitated by the Scottish Government, where all the work is peer reviewed. SEPA is represented on all the Resilience Partnerships including the Scottish Resilience Partnership.

SEPA participate in multi-agency exercises and workshops including statutory exercises under Control of Major Accident Hazards (COMAH), Radiation Emergency Preparedness and Public Information Regulations (REPPIR), Pipelines and Harbours legislation as well as risk-based planning work including, for example, on a National Power Outage.

#### 5.3. Complaints

##### 5.3.1. 1st Line of Assurance

We have a [SEPA Complaints Handling Procedure](https://beta.sepa.scot/about-sepa/how-we-work/complaints-handling-procedure/) in place. This has been approved by the Scottish Public Service Ombudsman (SPSO) and is fully endorsed by the Corporate Leadership Team and the Agency Board.

The Complaints Handling Procedure is available to all colleagues via the intranet and there is a training module for all colleagues, available on the SEPA learning and development platform.

Oversight of the day-to-day process is provided by the Complaints Team, who conduct a weekly review of complaints including numbers received; cases closed or resolved and whether that was within SPSO timescales.

##### 5.3.2. 2nd Line of Assurance

We report quarterly to the Corporate Leadership Team and Audit, Risk and Assurance Committee on our complaints handling performance statistics, outcomes and lessons learned via the Quarterly Assurance Report.

We also provided a weekly update on statistics to Governance, Risk and Resilience Management Team and conduct a monthly review of lessons learned and remedial actions.

We reported on complaint response timescales via our Key Performance Indicator: percentage of customer complaints responded to within statutory timescales, in the 2024 –2025 Corporate Performance report which is presented quarterly to the Corporate Leadership Team and Agency Board.

##### 5.3.3. 3rd Line of Assurance

External oversight is provided by the SPSO through the review of cases referred by unsatisfied customers. They also provide bespoke guidance on handling cases when requested.

Our internal auditors, BDO, conducted an audit of our complaints handling process in May/June 2024 where we were assessed as having a substantial level of assurance on design of controls, and moderate effectiveness of controls.

##### 5.3.4. 2024 – 2025 Update

SEPA’s target over the 2024 – 2025 reporting period was to respond to 85% of complaints within the timescales that are set out in the Complaints Handling Procedure. SEPA responded to 92% of Stage 1 complaints and to 87% of Stage 2 complaints within the target timescales. Therefore, the cumulative target for the reporting year was achieved.

**Stage 1 Complaint Overview**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Withdrawn | Not Upheld | Resolved | Partially Upheld | Upheld | **Total** |
| Q1 | 0 | 4 | 2 | 3 | 1 | **10** |
| Q2 | 0 | 2 | 1 | 0 | 2 | **5** |
| Q3 | 0 | 5 | 0 | 0 | 0 | **5** |
| Q4 | 0 | 4 | 1 | 0 | 0 | **5** |

**Stage 2 Complaint Overview**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Withdrawn | Not Upheld | Resolved | Partially Upheld | Upheld | **Total** |
| Q1 | 0 | 3 | 0 | 1 | 0 | **4** |
| Q2 | 1 | 0 | 0 | 1 | 1 | **3** |
| Q3 | 0 | 2 | 0 | 2 | 0 | **4** |
| Q4 | 0 | 3 | 0 | 1 | 0 | **4** |

The Stage 2 complaint which was upheld, concerned the time taken by SEPA to determine an application for a Water Use Licence.

Partially upheld complaints included SEPA failing to provide the customer with a clear explanation of the regulatory processes around waste shipment; SEPA providing a late response to the Scottish Government Planning and Environmental Appeals Division from information relating to an appeal against a local authority planning decision; SEPA charging a customer for the issue of a septic tank registration document when one was already in existence from a predecessor body; SEPA failing to provide clear advice about the statutory timescale to which SEPA adheres to for updating the Flood Maps and for SEPA failing to correctly follow their Complaints Handling Procedure on one occasion.

In all Stage 2 upheld and partially upheld cases, SEPA issued an apology to the customer.

### 5.4. Cyber Resilience

##### 5.4.1. 1st Line of Assurance

We have an IT Acceptable Use Policy (AUP) in place which sets out basic guidance and expectations on all users.

Mandatory cyber training is in place for all colleagues, and this is renewed and updated annually, and each colleague must complete the updated pack within set timescales. We have a set of processes and procedures in place which provide a framework for systems and security.

We run regular exercises to improve awareness and identify where targeted training may be required.

We have a Disaster Recovery Plan and Business Continuity Plans in place across the organisation which identify the key systems that should be prioritised for support and recovery.

We have weekly security meetings to review the week’s activity and identify lessons learned to prepare for the next week.

##### 5.4.2. 2nd Line of Assurance

We have an Information Technology Security Officer (ITSO) which is a nominated role responsible for reviewing and mitigating internal and external cyber risks. The ITSO maintains regular contact with Data Protection Officer (DPO) and Information Manager to cover crossovers between technical security and data governance.

We have two main oversight groups in place who meet regularly:

* Security incident group – investigate security incidents and provides recommendations on actions to reduce or eliminate future risks.
* Change and Control Board – Review changes to our systems and ensures security controls are in place before changes are made.

We have a comprehensive suite of security tools in place which monitor our systems and block malicious activity in a zero-trust environment. These tools also monitor communications to protect against phishing attacks and data egress.

##### 5.4.3. 3rd Line of Assurance

We have Cyber Essentials Plus accreditation which is a UK and Scottish Government backed audit to ensure a baseline of technical controls. This is renewed annually.

We have a Security Operation Centre (SOC) in place which is run by third party specialists and provides 24/7 monitoring of our environment, highlights possible incidents and take immediate action where appropriate. We receive regular vulnerability report from SOC on current vulnerabilities rated against current real-world threats.

We have a programme of penetration testing completed by security specialists in which they test public facing services against known attack vectors. We can also request these ad hoc and changes to services are tested before release.

In addition, we utilise External Technical Reviews which are provided by support specialists advising us on best practice on current and upcoming technologies.

We also have contracts with external contractors who provide external advice and technical assurance.

### 5.5. Data Protection

##### 5.5.1. 1st Line of Assurance

We have a Data Protection Policy in place, which lays out the framework for all colleagues to ensure the appropriate use of personal data in line with the law.

The Data Protection Team provide advice and assurance relating to the processing of personal data by SEPA to ensure we meet the obligations laid out in the UK GDPR and the Data Protection Act 2018.

Key tasks include:

* Advice and assurance during the preparation of Data Protection Impact Assessments / Notifications of Processing to support the Data Protection by Design and Default approach.
* Ensuring key documentation and policies are in place.
* SEPA’s privacy notice.
* Responding to requests made by data subjects (articles 13 – 22 UK GDPR).
* Investigation of personal data breaches.
* Handling of Data Protection complaints.

Colleagues are required to report security incidents to the Security Incident Response Group. Incidents are categorised and investigated by the most appropriate investigator.

##### 5.5.2. 2nd Line of Assurance

SEPA has a Data Protection Officer (DPO), as required by Article 37 of the UK GDPR.

SEPA maintains an expanded Register of Processing Activities (RoPA), including the statutory fields as required by Article 30 of the UK GDPR. The Register includes details of processes for both Part 2: General Processing and Part 3: Law Enforcement Processing. The processes are documented in Data Protection Impact Assessments/Notifications of Processing that are assured by the Data Protection Officer and owned by the Information Asset Owner (IAO) for the process.

The DPO is a member of the Security Incident Response Group and leads on the handling of personal data breaches. Where required, the DPO formally reports personal data breaches to the Information Commissioner’s Office (ICO) and is the designated contact between SEPA and regulator during any subsequent investigation.

SEPA has a Key Performance Indicator (KPI) for personal data breaches reported to the ICO. This KPI is currently reported weekly to the Governance, Risk and Resilience Leadership Team and the Governance, Performance and Engagement Portfolio Leadership Team. It is reported quarterly to the Corporate Leadership Team and the Board via the Corporate Performance Report.

##### 5.5.3. 3rd Line of Assurance

SEPA is regulated by the ICO for data protection matters. SEPA is required to pay an annual data protection fee to the ICO.

##### 5.5.4. 2024 – 2025 Update

During the reporting year, no personal data breaches reported to the Security Incident Response Group (SIRG) met the criteria to be reported to the Information Commissioner.

### 5.6. Health and Safety

##### 5.6.1. 1st Line of Assurance

We have a suite of Health and Safety policies and procedures in place which include our overarching Health and Safety Policy which sets out our Statement of Intent, Roles and Responsibilities, and Arrangements for Health and Safety at SEPA. Supporting health and safety policies and guidance specific to key pieces of legislation continue to be developed, to support portfolio management teams ensure compliance and implementation of safe working practices during work tasking. To further support this, we also have a Health and Safety Handbook which details the practical implementation of the main Health and Safety Policy. We have various contracts in place to support colleagues including Occupational Health and our Employee Assistance Programme.

We conduct risk assessments, site specific safety audits and audits of high hazard activities to ensure compliance, with a forward plan of further development through 2025-26 on these activities.

We also have a range of Health and Safety training modules available on our learning and development platform as well as portfolio specific on-site training activities identified via risk assessment for higher risk operational employees in the field.

##### 5.6.2. 2nd Line of Assurance

We have a small team of competent Health and Safety professionals who are members of the Institute of Occupational Safety and Health (IOSH) and are available to provide bespoke, risk-based advice to colleagues. This is currently backed up via external expertise from a third-party provider who are on hand to provide any other advice to the health and safety team as required.

Following a reset of health and safety governance and performance internally throughout 2024, an audit was commissioned by the People, Workspaces & Development Portfolio to further understand risks and opportunities. The third-party provider conducted a review in November 2024, visiting multiple field-based locations and offices, and gathering detailed insight from different leaders and managers in 1:1 interviews.

A series of recommendations were made, and although SEPA does not hold ISO45001, the audit scope to this widely recognised ISO H&S standard (ISO45001 is an international standard that specifies requirements for an Occupational Health and Safety (OH&S) Management System) was agreed as a basis for benchmarking and identification of any gaps in health and safety management and supporting systems. Where recommendations identified higher risks areas for improvement, these were prioritised and work continues on a risk-based approach to address these.

The agency recognised that the Health and Safety Team was requiring further resource and planned to appoint a new Head of Health and Safety in early 2025-26 to support continuous improvement and assurance around health and safety management.

We have a National Health and Safety Committee whose role is to promote an effective health, safety and welfare framework within the organisation in consultation with our colleagues and has representation from Trade Union colleagues.

There are two Health and Safety related KPIs included in the Corporate Performance Report which is produced quarterly for the Corporate Leadership Team and Agency Board.

We also provide regular updates on Health and Safety statistics to the Corporate Leadership Team and National Health and Safety Committee.

We have a Health and Safety Senior Leaders group which meets regularly.

##### 5.6.3. 3rd Line of Assurance

We have had several internal audits of Health and Safety related topics in recent years:

* Health and safety (2019).
* Health and safety training (2020).
* Violence and aggression audit (2022).
* Compliance with health and safety legislation (2023).

We have an internal audit of Health and Safety scheduled for quarter 3 of the 2025-2026 financial year.

We continue to have access to external expertise from our third-party provider.

##### 5.6.4. 2024 – 2025 Update

In 2024, a performance baseline was introduced for the number of near miss reports and hazards spotted. The target was to increase the number of reports for these in the 2024-2025 reporting period.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Baseline Figure (taken from annual reporting period 2023-2024)** | **Figures from Annual Reporting Period 2024 - 2025** | **Percentage Increase in Reporting** |
| **Near misses reported** | 14 | 63 | 78% |
| **Hazards spotted** | 16 | 67 | 76% |

The marked increase in the reporting of near misses and hazards, was helped by the message of support and encouragement which was released by our Chief Executive, Nicole Paterson in November 2024 to all colleagues regarding the importance of Health and Safety at SEPA, as well as promotional work carried out by the Health & Safety Team.

Importantly, none of these incidents required reporting under RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013).

This trend reflects a more open and proactive reporting culture, where employees feel confident reporting hazards spotted, near misses and other incidents. This is a positive sign that health and safety awareness is improving, allowing us to address issues early and continue to prevent more serious incidents from occurring.

This is being helped with continual incremental improvements of the incident reporting system and supporting processes, to make it easier for employees to access and report incidents, allowing quicker responsive support and investigation tracking from the Health & Safety Team, this continues into 2025-26.

### 5.7. Information Governance

##### 5.7.1. 1st Line of Assurance

We have an Information Framework which sets out our commitment to achieving high standards in Information Management. The Framework identifies the key roles, responsibilities, principles and policies to help us deliver our commitments, our duties as a public authority and compliance with information legislation. The framework is supported by several key policies and tools which are reviewed and updated periodically.

We have a Records Management Plan which was agreed by the Keeper of the Records of Scotland. It sets out the actions we will deliver and the future developments we will work towards to demonstrate our compliance with the Public Records (Scotland) Act 2011.

Information Asset Owners appoint Information Champions to help them manage their information. We have established an Information Champions network which meets monthly to keep up-to-date and exchange knowledge and learning.

SEPA’s Access to Information service monitors and manages our performance for compliance with statutory time limits set in the Freedom of Information (Scotland) Act 2002 and Environmental Information (Scotland) Regulations 2004.

##### 5.7.2. 2nd Line of Assurance

We have key expert roles to support good information governance and security, these are: Senior Information Risk Officer; Information Asset Owners; Information Manager; Data Protection Officer; and Information Technology Security Officer.

We complete an annual certificate of assurance to Scottish Government which includes sections on information management and security, access to information, and data protection. Our Senior Information Risk Owner (SIRO) provides accountability and assurance to the Accountable Officer (AO) on these. Each Information Asset Owner provides assurance to the SIRO for the information they are responsible for.

SEPA has a Key Performance Indicator for responding to Access to Information requests within statutory time limits. It is currently reported weekly to the Governance, Risk and Resilience Leadership Team and the Governance, Performance and Engagement Portfolio Leadership Team. It is reported quarterly to the Corporate Leadership Team and the Board via the Corporate Performance Report.

##### 5.7.3. 3rd Line of Assurance

Following the approval of our Records Management Plan by the Keeper of the Records of Scotland we will be keeping all Elements of the Plan under review and will submit annual updates to the National Records of Scotland in line with their Annual Progress Update Review process. We anticipate that SEPA will receive an invitation to submit a progress update in November 2025. SEPA’s Access to Information service was audited in 2023-2024.

Along with all other Scottish public bodies, SEPA must submit quarterly performance information to the Scottish Information Commissioner. The Scottish Information Commissioner reviews the reported performance and decides whether to take enforcement action to improve performance. Following his intervention in 2021, SEPA’s performance has improved to consistently achieve his Good or Excellent performance category.

When someone is unhappy with the way SEPA has handled their request and subsequent formal review, they have the right to appeal to the Scottish Information Commissioner who will investigate how we dealt with their request and decide if we need to carry out any further actions to resolve the request.

##### 5.7.4. 2024 - 2025 Update

SEPA received a total of 1,939 requests during the reporting period for Access to Information.

|  |  |  |
| --- | --- | --- |
|  | **Freedom of Information Requests** | **Environmental Information Requests** |
| Q1 | 10 | 434 |
| Q2 | 16 | 549 |
| Q3 | 11 | 447 |
| Q4 | 15 | 457 |
| **Total** | **52** | **1,887** |

Overall, in 2024-2025, we received 1,887 requests for environmental information compared to 1,623 in 2022-2023, an increase of 16%.

SEPA’s mean annual performance during this reporting period for responding to Access to Information requests was 95%.

### 5.8. Fraud, Bribery and Corruption

##### 5.8.1. 1st Line of Assurance

We have an Anti-fraud, Bribery and Corruption Policy in place, as required by Standing Financial Instruction (SFI) 19. We have a Conduct and Capability Procedure and Code of Conduct for colleagues which covers fraud, bribery and corruption.

All colleagues’ communication ‘when things go wrong’ highlighted the need to look out for and report suspected incidents of fraud, bribery and corruption (June 2024).

We have a central repository to record and manage all reported incidents.

We have a dedicated email address and inbox for Fraud, Bribery and Corruption.

##### 5.8.2. 2nd Line of Assurance

We have a Fraud Response Group (FRG) which leads on the response to any allegations made of Fraud Bribery or Corruption. The FRG is chaired by the Chief Officer Governance, Performance and Engagement and members include Chief Officer Finance, Modernisation and Digital; Head of Governance, Risk and Resilience; Head of People, Recruitment and Reward; Head of Corporate Legal and Leadership Support.

##### 5.8.3. 3rd Line of Assurance

Financial processes are being audited as part of the internal audit plan for 2025-2026 this will include expenses and credit card expenditure.

External Audit look at any allegations of fraud, bribery and corruption as part of the Annual Report and Accounts.

We participate in the National Fraud Initiative Annual Certificate of Assurance to Scottish Government including an update on fraud, bribery and corruption.

##### 5.8.4. 2024 – 2025 Update

There were 6 cases of suspected fraud in the reporting year. These were all reported to and managed by SEPA’s Fraud Response Group.

### 5.9. Whistleblowing

##### 5.9.1. 1st Line of Assurance

We have an internal Whistleblowing Policy and procedures for colleagues**.**

We also have an [External whistle blowing policy](https://beta.sepa.scot/about-sepa/how-we-work/complaints-handling-procedure/whistleblowing/whistleblowing-report/) - SEPA is designated as a prescribed person for whistleblowing and workers can contact SEPA about matters in relation to acts or omissions which have an actual or potential impact on the environment, or the management or regulation of the environment, including those relating to flood warning systems and pollution.

Whistleblowing is also referred to in the Anti-fraud, Bribery and Corruption Policy; the Complaints Handing Procedure; the Code of Conduct for colleagues; the Procurement Policy; the Board governance official documents; governance framework; ‘when things go wrong’ which was an all-colleagues communication on Fraud, Bribery and Corruption; and the ‘Speaking up about concerns’ page on SEPA’s intranet.

We have a confidential phoneline for internal and external whistleblowing which is managed by our third-party Safecall.

We have a dedicated email address and inbox for internal and external whistleblowing reports.

##### 5.8.2. 2nd Line of Assurance

We have a dedicated Whistleblowing Team consisting of the Head of Corporate Legal and Leadership Support; Head of Governance, Risk and Resilience; and the Business Support Officer for Governance.

We also have dedicated contacts from the Corporate Leadership Team: Chief Officer Governance, Performance and Engagement; Chief Operating Officer Data, Evidence and Innovation; and the Chief Officer Finance, Modernisation and Digital.

In addition, we have three dedicated contacts from the Agency Board: Craig Hume; Harpreet Kohli; and Lorraine McMillan.

##### 5.8.3. 3rd Line of Assurance

We report on Whistleblowing annually to Parliament.

Our last internal audit of Whistleblowing was completed in 2020.

We complete an Annual Certificate of Assurance to Scottish Government which includes an update on whistleblowing.

##### 5.8.4. 2024 – 2025 Update

SEPA received 36 external disclosures which were initially identified as whistleblowing via its dedicated Whistleblowing Team and the SEPA Contact Centre.

Following an initial assessment, it was determined that 7 of these disclosures did not meet the standard of a qualifying disclosure. Therefore, there were 29 disclosures within this reporting period that fell within SEPA’s remit and which we considered as qualifying disclosures.

Training is now being provided to Board members periodically on whistleblowing.

There were no internal disclosures of whistleblowing.

## 6. Recommendations

6.1. Agency Board **discuss and note** the content of this report and consider whether there are any further areas of assurance they would like added to this report going forward.

END

<Report date here (month, year)>