

Governance and Assurance Framework

Scottish Information Commissioner



Scottish Information
Commissioner

Contents

Introduction	1
Purpose	1
Statutory and Governance Context.....	1
Governance Principles	2
Accountability.....	2
Proportionality	2
Transparency	2
Assurance.....	2
Continuous Oversight	2
Governance Structure and Responsibilities	2
Commissioner	2
Senior Management Team.....	2
Heads of Department.....	3
Scheme of Delegation.....	3
Supporting Groups.....	3
Sources of Assurance	4
Management Assurance	4
Independent Assurance	4
Meeting and Oversight Arrangements	6
Monthly SMT Meetings	6
Mid-Year Assurance Review Meeting	7
Annual Assurance Review Meeting.....	7
Annual Data and Statutory Assurance Meeting.....	7
Exception Reporting and Escalation.....	8
Ad Hoc Meetings and Decisions Between Meetings	8
Review of the Framework.....	8
APPENDICES	10
Document control sheet.....	13

Introduction

1. The Scottish Information Commissioner (the Commissioner) is committed to maintaining effective governance arrangements that support accountability, sound decision-making, good stewardship of public resources and the achievement of organisational objectives. This Framework brings together the key governance and assurance arrangements through which the Commissioner obtains assurance regarding the effectiveness of the organisation's systems, controls, performance and compliance.

Purpose

2. This Framework sets out the governance, oversight and assurance arrangements through which the Commissioner obtains assurance regarding the effective stewardship, performance, compliance and control of the organisation.
3. The Framework establishes:
 - governance roles and responsibilities;
 - arrangements for decision-making and oversight;
 - sources of assurance available to the Commissioner;
 - arrangements for risk management and internal control;
 - mechanisms for escalation and exception reporting;
 - the annual assurance process supporting the Commissioner in their capacity as Accountable Officer.
4. The Framework reflects a proportionate approach to governance and assurance. It is based on the principle that assurance is achieved through effective management, clear accountability, appropriate scrutiny and timely escalation of significant matters, rather than through the routine production of large volumes of reports.

Statutory and Governance Context

5. The Commissioner is a public office holder appointed by His Majesty the King on the nomination of the Scottish Parliament and is responsible for enforcing and promoting Scotland's freedom of information legislation.
6. The Commissioner:
 - investigates applications and issues legally enforceable decisions;
 - promotes good practice among Scottish public authorities;
 - provides information and guidance regarding information rights.
7. Schedule 2 of the Freedom of Information (Scotland) Act 2002 (FOISA) requires the Scottish Parliamentary Corporate Body (SPCB) to designate an Accountable Officer for the organisation.
8. The Commissioner is currently designated as Accountable Officer.
9. As Accountable Officer, the Commissioner is personally responsible for:

- signing the annual accounts;
- ensuring the propriety and regularity of expenditure;
- ensuring resources are used economically, efficiently and effectively;
- maintaining an effective framework of governance, risk management and internal control.

Governance Principles

10. The organisation's governance arrangements are founded on the following principles:

Accountability

Responsibilities are clearly assigned and individuals are accountable for decisions and performance within their areas of responsibility.

Proportionality

Governance arrangements should be proportionate to the size, risk profile and statutory responsibilities of the organisation.

Transparency

Governance and decision-making processes should be documented appropriately, and information should be made publicly available wherever possible.

Assurance

The Commissioner must receive sufficient evidence to support confidence in the effectiveness of governance, risk management and control arrangements.

Continuous Oversight

Significant issues should be identified, discussed and addressed when they arise rather than waiting for a predetermined reporting cycle.

Governance Structure and Responsibilities

Commissioner

11. The Commissioner:
- provides strategic leadership;
 - acts as Accountable Officer;
 - approves significant organisational decisions;
 - receives assurance on governance, performance and control;
 - determines whether additional assurance or scrutiny is required.

Senior Management Team

12. The Senior Management Team (SMT) supports the Commissioner in exercising their statutory and accountabilities responsibilities.
13. The SMT is responsible for:

- organisational leadership;
- strategic and operational oversight;
- risk management;
- performance monitoring;
- resource management;
- decision making within delegated authority;
- ensuring effective governance and control arrangements operate across the organisation.

Heads of Department

14. Heads of Department are members of SMT and contribute collectively to the leadership, governance and strategic direction of the organisation. In their capacity as SMT members, they share responsibility for organisational oversight, decision-making, risk management and the provision of assurance to the Commissioner.
15. Within their individual areas of responsibility, Heads of Department are responsible for:
 - delivery of operational objectives;
 - management of resources;
 - maintaining effective controls;
 - managing risks within their areas;
 - escalating material issues; and
 - providing assurance to SMT and the Commissioner.
16. Heads of Department are expected to take an organisation wide perspective when acting as members of SMT, while maintaining accountability for the effective management and performance of their own service areas.

Scheme of Delegation

17. The Commissioner has established a Scheme of Delegation which sets out the authority delegated to SMT members and other authorised officers for decision making and the exercise of functions on behalf of the Commissioner.
18. All decisions must be made in accordance with the Scheme of Delegation and any associated policies, procedures and financial controls.
19. The Scheme of Delegation is maintained separately from this Framework and should be read alongside it.

Supporting Groups

20. The organisation may establish supporting groups, including short-life working groups, project groups and other forums, to support the delivery of business objectives and organisational development.

21. Such groups may be permanent or time-limited and may operate across teams or within individual business areas.
22. These groups do not replace the authority of the Commissioner or SMT. Accountability for decisions remains with the appropriately delegated officer in accordance with the Scheme of Delegation.

Sources of Assurance

23. The Commissioner obtains assurance from a range of sources.

Management Assurance

24. Day to day management activity provides the primary source of assurance through:
 - supervision and management oversight;
 - performance monitoring;
 - budget monitoring;
 - project and operational reviews;
 - risk management processes;
 - compliance monitoring.

Independent Assurance

25. Independent assurance is received through:
 - Internal Audit;
 - External Audit;
 - Advisory Audit Board;
 - Specialist professional advice commissioned where appropriate; and
 - Other independent scrutiny or assurance mechanisms as determined by the Commissioner.

Advisory Audit Board

26. The Advisory Audit Board provides independent advice and scrutiny on the effectiveness of the organisation's governance, risk management, internal control and financial stewardship arrangements. In doing so, it supports the Commissioner in obtaining assurance on key governance matters, audit findings, financial reporting and the implementation of agreed improvements.

Organisational Assurance Domains

27. Assurance is considered across the following areas:

Financial Stewardship

28. Including:
 - financial management;
 - budget control;

- procurement;
- fraud prevention;
- value for money;
- statutory financial reporting.

Workforce and Culture

29. Including:

- workforce planning;
- sickness absence;
- staff wellbeing;
- equality, diversity & inclusion;
- learning and development;
- performance management.

Information Governance

30. Including:

- information management;
- records management;
- data protection;
- information security;
- publication responsibilities.

Operational Performance

31. Including:

- investigations;
- enquiries;
- interventions;
- rights requests;
- service standards.

Risk and Control

32. Including:

- strategic risks;
- operational risks;
- business continuity;
- health and safety;

- effectiveness of internal controls.

Statutory Compliance

33. Including:

- Annual Report and Accounts;
- Public Services Reform reporting;
- Biodiversity reporting;
- British Sign Language reporting;
- other legislative obligations.

34. The Annual Report and Accounts will be prepared in accordance with applicable statutory requirements and relevant public sector financial reporting guidance, including the Government Financial Reporting Manual (FReM), where applicable.

35. The Annual Data and Statutory Assurance Meeting will provide the principal forum through which supporting assurances are reviewed prior to finalisation of the Annual Report and Accounts.

Meeting and Oversight Arrangements

36. Detailed agendas for governance and assurance meetings are set out in the appendices to this Framework. The agendas identify the routine governance, performance, risk, compliance and assurance matters to be considered and support a consistent approach to governance reporting and organisational oversight.

Monthly SMT Meetings

37. SMT meetings are the principal forum through which the Commissioner receives management information, exercises organisational oversight and takes strategic and operational decisions. Meetings support performance monitoring, risk management, resource management, coordination of activity and the escalation of significant issues.

38. SMT will normally meet monthly. The purpose of monthly meetings is to:

- oversee organisational performance;
- monitor delivery of priorities;
- consider emerging issues;
- review risks;
- make decisions;
- coordinate organisational activity.

39. Routine assurance reports will not normally be required. Monthly meetings will instead focus on:

- management information;
- dashboards;

- exception reports;
- decision papers;
- significant risks and issues.

Mid-Year Assurance Review Meeting

40. The Mid-Year Assurance Review is to consider the effectiveness of governance, risk management and internal control arrangements, identify emerging issues and determine whether any additional assurance or corrective action is required before the Annual Assurance Review
41. A formal Mid-Year Assurance Review will normally take place during the third quarter of the reporting year.
42. The purpose of the meeting is to:
 - review governance arrangements;
 - consider significant risks;
 - review progress against key objectives;
 - determine whether additional assurance, corrective action or follow-up review is required before the Annual Assurance Review Meeting.
43. The output from the review will be a summary of assurance, concerns identified and agreed actions.

Annual Assurance Review Meeting

44. A formal Annual Assurance Review Meeting will normally take place during the final quarter of the reporting year.
45. The purpose of the meeting is to review matters previously considered through the Mid-Year Assurance Review Meeting and provide assurance that identified issues, risks and actions have been appropriately managed.
46. The meeting will:
 - review actions arising from the Mid-Year Assurance Review Meeting;
 - consider progress against assurances provided at the mid-year review;
 - review emerging issues and risks identified during the year;
 - consider whether governance, risk management and internal control arrangements continue to operate effectively;
 - identify any matters requiring further review or escalation.

Annual Data and Statutory Assurance Meeting

47. A formal Annual Data and Statutory Assurance Meeting will normally take place following the end of the financial year and before finalisation of the Annual Report and Accounts.
48. The purpose of the meeting is to provide the Commissioner with assurance based upon year-end quantitative, financial and statutory reporting requirements.

49. The meeting will provide assurance supporting:
- preparation of the Annual Report and Accounts;
 - preparation of the Governance Statement;
 - statutory disclosures and reporting obligations;
 - financial stewardship and accountability requirements;
 - the Commissioner's responsibilities as Accountable Officer.

Exception Reporting and Escalation

50. The assurance cycle must not delay reporting or escalation of significant matters.

Ad Hoc Meetings and Decisions Between Meetings

51. The Senior Management Team may meet outside the planned meeting cycle where circumstances require urgent consideration of a matter, a significant issue arises, or a decision is needed before the next scheduled meeting. In addition, where appropriate, decisions may be taken by correspondence, including by email, provided that all SMT members have the opportunity to contribute to the discussion and the decision-making process. Any decisions taken at ad hoc meetings or by correspondence will be formally recorded and retained as part of the organisation's governance records
52. Material issues must be reported at the earliest opportunity and should not wait for the Mid-Year Assurance Review Meeting, the Annual Assurance Review Meeting or the Annual Data and Statutory Assurance Meeting.
53. Examples include:
- serious incidents;
 - personal data breaches;
 - fraud or suspected fraud;
 - significant legal risks;
 - substantial financial pressures;
 - major service failures;
 - significant reputational concerns;
 - material control weaknesses;
 - significant changes to strategic risks.
54. The Commissioner may require additional reporting, review or assurance activity where the significance of an issue warrants it.

Review of the Framework

55. The Commissioner will regularly review this Framework.
56. The review will consider:

- effectiveness of governance arrangements;
- effectiveness of assurance arrangements;
- adequacy of reporting and escalation mechanisms;
- findings from audits and external reviews;
- lessons learned from significant incidents and organisational experience.

57. Amendments to this Framework require the approval of the Commissioner.

APPENDICES

Scottish Information Commissioner

AGENDA – Monthly Senior Management Team Meeting (MSMTM)

Location:	
Date/Time:	

Item No.	Item	Lead	Paper / Verbal Update
1	Minutes and actions of previous meetings <ul style="list-style-type: none"> • Minutes for approval • Action List 	All	Paper Paper
2	Head of Business Support Update <ul style="list-style-type: none"> • Financial Summary • Sickness Absence • Rights Requests • Enquiries Service 	HOBS	Paper Verbal Verbal Verbal
3	Head of Policy & Information Update <ul style="list-style-type: none"> • British Sign Language Action Plan Review • Interventions Performance 	HOPI	Paper Verbal
4	Head of Enforcement Update <ul style="list-style-type: none"> • Investigations Performance 	HOE	Verbal
5	Senior Management Team Update <ul style="list-style-type: none"> • HR/Staffing • Risk Registers • Operational Plan check point 	SMT	Paper & Verbal
6	AOB		

Scottish Information Commissioner

AGENDA – SMT Mid-Year Assurance Review Meeting

Location:	
Date/Time:	

Item No.	Item	Lead	Paper / Verbal Update
1	Minutes and actions of previous meetings <ul style="list-style-type: none"> • Minutes for approval • Action List 	All	Paper Paper
2	Head of Business Support reporting <ul style="list-style-type: none"> • Performance and Development Framework / Annual Review and Development Scheme • Staff Training Summary • Health and Safety • Statement on Sustainable Growth • Equalities Monitoring – Staff 	HOBS	Paper Paper Paper Paper
3	Head of Policy & Information reporting <ul style="list-style-type: none"> • Publication Scheme • Policy and Information Team Assurance 	HOPI	Paper Paper
4	Head of Enforcement reporting <ul style="list-style-type: none"> • Quality Assurance Investigations • Quality Assurance Enquiries • GDPR Register of Personal Data Processing and Privacy Notice 	HOE	Paper Paper Paper
5	Senior Management Team update <ul style="list-style-type: none"> • Strategic Plan Check Point 	SMT	Verbal
6.	Additional substantive items		
7.	AOB		

Scottish Information Commissioner

AGENDA – SMT Annual Assurance Meeting

Location:	
Date/Time:	

Item No.	Item	Lead	Paper / Verbal Update
1	Minutes and actions of previous meetings <ul style="list-style-type: none"> • Minutes for approval • Action List • Updates from Mid-Year Assurance Review meeting 	Chair	Paper Paper Verbal
2	Head of Business Support reporting <ul style="list-style-type: none"> • Financial Outturn Report • Time Taken to Pay Suppliers • Report on Fraud • Sickness Absence • Workforce Trends • Records Management • Rights Requests • Service Standards – Complaints • Statements of Expenditure • Staff in Post 	HOBS	Paper Paper Paper Paper Paper Paper Paper Paper Paper
3	Head of Policy & Information reporting <ul style="list-style-type: none"> • Draft Annual Report and Accounts 	HOPI	Paper
4	Head of Enforcement reporting <ul style="list-style-type: none"> • Prescribed Persons (Reports on Disclosure of Information) Regulations 2017 • UK GDPR Register of Personal Data Processing and Privacy Notice and assurance that the register and privacy notice are up to date 	HOE	Paper Paper
5	AOB		

Document Information	
Full name of current version: Class, Title, Version No and Status. <i>E.g. C5 Key Documents Handbook v01 CURRENT ISSUE</i>	C1 Governance and Assurance Framework
VC Filed	255374
Type	Policy
Approver	SMT
Responsible Manager	HOBS
Date of next planned review	12/09/2029
Approval & Publication	
Approval Date (major version)	12/09/2026
For publication (Y/N)	Y
Date published	27/10/2026
Name of document in website file library	GovernanceAssuranceFramework
Corrections / Unplanned or Ad hoc reviews (see Summary of changes below for details)	
Date of last update	26/10/26

[illegible]

Scottish Information Commissioner

Kinburn Castle
Doubledykes Road
St Andrews, Fife
KY16 9DS

T: 01334 464610
E: enquiries@foi.scot
W: www.foi.scot

© Scottish Information Commissioner 2026

You may use and re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence v3.0. To view this licence, visit <http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/>