


APPENDIX 1

|  | | Corporate Governance and Assurance Policy | |
|---|--|--|------------|
| Creator | Author(s) | Gary Welch - Strategic Risk and Health and Safety Manager | |
| | Approved by | Audit Committee | |
| | Department | Risk and Assurance – All Directorates | |
| | Service area | Governance Policy & Information | |
| | Head of Service | Ann-Marie Johnstone - Head of Chief Executive's Department | |
| | Director | Chief Executive | |
| Date | Created | 06/10/2025 | |
| | Submitted | 17/03/2026 | |
| | Approved | 16/04/2026 | |
| | Updating Frequency | 3 Years | |
| Status | Version: 1 | | |
| Contributor(s) | Strategic Risk and Health and Safety Manager, Head of Chief Executive's Department, Head of Corporate Finance. | | |
| Subject | Corporate Governance and Assurance | | |
| Type | Policy | | |
| | Vital Record | | EIR |
| Coverage | Middlesbrough Council | | |
| Language | English | | |
| Document Control | | | |
| Version | Date | Revision History | Reviser |
| 1.0 | 17/03/2026 | Final agreed version | Gary Welch |
| | | | |
| | | | |
| | | | |
| Distribution List | | | |
| Version | Date | Name/Service area | Action |
| 1.0 | April 2026 | Internally via Intranet | Gary Welch |
| Contact: | Gary_welch@middlesbrough.gov.uk | | |

Summary

1. This policy outlines the Council's approach to ensuring that the corporate governance arrangements currently in place for all services are robust and being adhered to. This includes recognising cyber resilience and technical control assurance as integral elements of the Council's overall governance posture. Governance and Assurance Mapping (G&AM) provides a structured approach to identifying, managing, and assessing the level of assurance available across the Council, including assurance relating to cyber security controls. It is designed to support compliance with the Local Code of Corporate Governance. Application of the policy will also support development of the Council's Annual Governance Statement.
2. This policy will implement a governance mapping process which will drive the future assurance activity of both internal audit and the specialist functions that oversee corporate governance. This will result in improved targeting of areas where assurance levels are low and reduce the likelihood of duplications in assurance activity.

Context

3. This policy supports the Council's Local Code of Corporate Governance, Annual Governance Statement (AGS) and Risk Management and Opportunities Policy. It will contribute positively to the AGS as it will enable future AGSs to assess the effectiveness of internal controls and acknowledges Digital service dependency, cyber threat landscape, and reliance on cloud/SaaS systems.

Purpose

4. This policy aims to establish a structured and transparent approach to governance and assurance across the Council, in alignment with statutory obligations in the Accounts and Audit Regulations 2015, the Local Government Act 1999, and the Global Internal Audit Standards (GIAS) in the UK public sector. It supports the ethical delivery of public services by promoting selflessness, integrity, objectivity, accountability, openness, honesty, leadership and continuous improvement.
5. The policy is designed to provide an evidential base that will support completion of the Annual Governance Statement, delivery of the Council Plan priorities, and maintain a strong system of internal control. It outlines how assurance will be sourced, how risks will be monitored, and how internal audit and other corporate governance compliance activities will be shaped by governance assurance mapping whilst also ensuring the integrity, security, and availability of information systems and data assets.

Definitions

6. The following definitions will be used within the Policy:

| Term | Definition |
|-------------------------------------|---|
| Governance and Assurance Map (G&AM) | A map that assesses the level of assurance that a service area is compliant with the requirements of the Local Code of Corporate Governance. |
| Local Code of Corporate Governance | Sets out the principles, structures, and processes by which the council ensures accountability, transparency, integrity, and effective decision-making in delivering its objectives and serving the public. |
| Strategic Risk Areas | Risks aligned with the Council's long-term priorities (e.g. Council Plan) affecting core delivery |
| Corporate Risk Areas | Risks impacting internal controls, governance, and operational effectiveness |
| Level of Assurance | Level of confidence from internal or external sources that arrangements comply with the Local Code of Corporate Governance. |
| Internal Audit | Provides independent, objective assurance and advice to evaluate and improve the effectiveness of an organisation's risk management, control, and governance processes. |
| Integrated Assurance Framework | A structure combining governance, risk, and assurance for a holistic organisational view. |
| Annual Governance Statement (AGS) | A statutory report on governance and internal control effectiveness that forms part of the Council's Statement of Accounts. |
| Key Performance Indicators (KPIs) | Metrics used to assess internal audit performance and risk management effectiveness. |
| Assurance | Is the confidence, based on reliable evidence, that the Council's governance, risk management, and internal controls are effective and comply with statutory requirements and the Local Code of Corporate Governance. |
| Green Assurance Rating | Strong assurance. |
| Amber Assurance Rating | Moderate assurance with improvements. |
| Red Assurance Rating | Red means limited or no assurance with immediate improvements required. |
| Grey Assurance Rating | No assurance work completed to be able to give a judgement |
| Unplanned Audit Work | Audit tasks not in the original plan, triggered by emerging risks or issues. |
| National Fraud Initiative (NFI) | A UK-wide data matching exercise to detect and prevent public sector fraud. |

| | |
|--|---|
| Cyber Security Assurance | The process of providing confidence that cyber security controls, practices, and technologies are in place, effective, and operating as intended. |
| Information and Communications Technology (ICT) Controls | The safeguards, checks, and technical measures implemented within the Council's ICT environment to ensure the confidentiality, integrity, and availability of data and systems. |
| System Owner | The individual responsible for the overall governance, security, and performance of a specific system or application. |
| Digital Risk | The potential for loss, disruption, or harm arising from the Council's use of digital technologies, systems, and services. |
| Information Security | The discipline focused on protecting information, regardless of format from unauthorised access, disclosure, alteration, or destruction. |

Scope

7. This policy applies to the following:

| Group / Community | Description |
|---|--|
| Council Departments | All directorates and service areas responsible for delivering Council plan and statutory functions. |
| Chief Executive, Corporate Directors, Service Directors and Senior Officers | Key stakeholders involved in risk identification, assurance planning, and governance. |
| Internal Audit Team | Responsible for delivering the audit plan and providing independent, objective assurance. |
| Risk and Assurance Function | Leads the development and implementation of the Governance and Assurance Map |
| Audit Committee | Receives reports and monitors assurance and governance performance. |
| External Auditors / Inspectors | Provide independent assurance and contribute to the overall assurance framework. |
| ICT systems | Inclusive of infrastructure, cloud services, cyber controls, and Information Technology Service Management (ITSM) processes. |

Legislative and regulatory framework

8. This policy supports compliance with the Council's Local Code of Corporate Governance, which is based on the principles set out in the CIPFA/SOLACE Framework: Delivering Good Governance in Local Government (2016). It supports compliance with the following statutory and regulatory requirements:

- **Accounts and Audit Regulations 2015** - Requires local authorities to maintain an adequate and effective system of internal audit and to prepare an Annual Governance Statement.

- **Local Government Act 1999** - Imposes a duty of best value, requiring continuous improvement in the delivery of Council functions, including governance and risk management.
 - **Global Internal Audit Standards (UK Public Sector), 2025** - Provides mandatory standards for internal audit functions in public sector organisations, ensuring independence, objectivity, and quality assurance.
 - **CIPFA Guidance on Delivering Good Governance in Local Government** - Offers a framework for ensuring that governance arrangements are robust, transparent, and aligned with public sector values.
 - **Accounts and Audit (England) Regulations 2011, Regulation 4(3)** Requires authorities to conduct a review of the effectiveness of their governance framework.
 - **The Procurement Act 2023 and Public Contract Regulations 2015.**
9. This Governance and Assurance Policy is a key component of the Council's governance structure and supports the delivery of the Council Plan and the strategic priorities of the Mayor of Middlesbrough. It operates alongside and complements:
- **Council Plan** - The policy directly supports the delivery of strategic priorities by ensuring that risks are identified, managed, and assured in line with the Council's ambitions.
 - **Local Code of Corporate Governance** - Establishes the principles and practices of good governance across the Council.
 - **Annual Governance Statement (AGS)** - The policy contributes directly to the AGS by providing assurance on internal control and risk management.
 - **Risk Management and Opportunities Policy** - Provides the overarching framework for identifying and managing risks.
 - **Integrated Assurance Framework** - Ensures that assurance is sourced from multiple levels including service management, internal audit, and external bodies.
 - **Corporate Performance and Financial Management Policies** - The policy supports compliance with financial regulations, procurement standards, and performance monitoring.

Together, these policies form a hierarchy that ensures transparency, accountability, and continuous improvement in governance and service delivery.

Policy detail

10. This policy will be implemented through the Council's Governance and Assurance Map, which identifies key risk areas, sources of assurance, and planned audit activities. The policy guides the development of annual audit plans, risk registers, and governance assurance reporting protocols.

11. Specific Requirements

- Heads of Service must complete an annual self-assessment of their service in line with the Local Code of Corporate Governance.

- Corporate Governance leads must complete annual assessments of assurance they have in relation to each service area.
- All Council departments must maintain up-to-date risk registers aligned with strategic and operational objectives.
- The audit and work programmes of both Internal Audit and corporate governance leads will be shaped by the assurance map, with co-ordination where appropriate, respecting the remits of those roles.

12. The Council adopts the Three Lines Model as a framework for effective governance, risk management, and assurance. This model clarifies roles and responsibilities across the organisation and ensures that risk is managed consistently and transparently.

Overview

| Line | Role | Function |
|--------------------|--------------------------------------|--|
| First Line | Directorate / Operational Management | Owns and manages risks. Responsible for implementing controls and corrective actions. This line will provide a self-assessment of its compliance with the requirements of the Local Code of Corporate Governance. |
| Second Line | Risk Management and Compliance | Provides oversight, guidance, and support. Develops frameworks and monitors compliance. This line will provide an assessment of the level of assurance they have of compliance with the Local Code of Corporate Governance, as it relates to their discipline. |
| Third Line | Internal Audit | Provides independent assurance on governance, risk management, and internal controls, and assessing assurance against local code of corporate governance. |

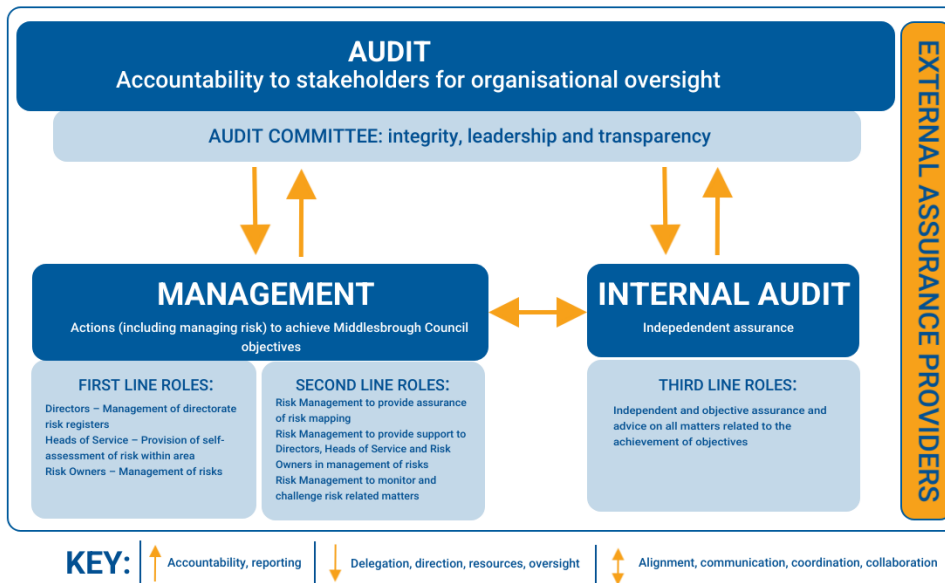
13. Moderation of Self-Assessments

Service self-assessments will be subject to review and challenge by the Risk and Health and Safety function, and relevant corporate governance leads to ensure consistency, proportionality, and objectivity.

14. Where necessary, self-assessments may be adjusted following review to reflect evidence, assurance activity, or audit findings, ensuring that assurance ratings provide a fair and accurate reflection of control effectiveness.

Implementation in Middlesbrough Council

Middlesbrough Council's Three Lines Model



First Line – Directorate / Operational Management self-assessment

- Who: Heads of Service, Service managers, team leaders, and frontline staff.
- Responsibilities:
 - Identify and manage risks within their service areas.
 - Maintain risk registers and implement controls.
 - Report issues and escalate concerns appropriately.
 - Heads of Service will complete self-assessments to provide an overview of their opinion in relation to compliance with the Local Code of Corporate Governance.
- Support: Training and guidance provided by Risk and Assurance.

Second Line – Governance and Assurance Functions

- Who: Assurance team and strategic leads for the following governance pillars:
 - Strategic Planning
 - Organisational governance
 - Financial governance
 - Risk management
 - Information governance
 - Performance management and data quality
 - Procurement and contract management
 - People management
 - Asset management
 - Programmes and project management
 - IT Governance
- Responsibilities:
 - Develop and maintain governance management frameworks and policies.

- Monitor risk exposure and control effectiveness.
- Support services with self-assessments and mitigation strategies.
- Provide an evidence-based view of assurance available for each service area.
- Support: Coordination of the Governance and Assurance Map and reporting to senior management.

Third Line – Internal Audit

- Who: Internal Audit team.
- Responsibilities:
 - Independently assess the adequacy and effectiveness of governance, risk management, and controls.
 - Deliver the annual audit plan and report findings to the Audit and Governance Committee.
 - Provide an annual assurance opinion on the council's governance, risk management and control.
 - Provide assurance for the Annual Governance Statement.

Benefits of the Model

- Clear accountability for governance and control.
- Improved coordination between assurance functions.
- Enhanced transparency and confidence in governance.
- Stronger basis for decision-making and resource allocation.
- Identification of areas of low or no assurance that can inform audit and compliance future focus.

Weaknesses in the Existing Approach

- Fragmented Assurance Sources, assurance is produced in many parts of the Council, but there is no single mechanism to bring these sources together.
 - Leads to duplication (two or more functions reviewing the same area).
 - Gaps occur where no assurance function takes ownership.
- Limited Visibility of Council Wide Assurance Levels, without a governance & assurance map, the Council cannot easily see:
 - which services have strong assurance,
 - which services have weak or no assurance,
 - where risks and controls are misaligned.This inhibits intelligent targeting of audit and assurance work.
- Inconsistent Self-Assessment and Oversight
- Assurance areas duplication of oversight while others do not have sufficient oversight.
- Self-assessments currently do not exist.
- Reliance on Annual, Not Continuous, Governance Insight
 - The AGS is retrospective and produced once a year. This means governance problems may only surface at year-end rather than being identified early for mitigation
- Siloed Work Programmes
 - Internal Audit, Risk, Information Governance, Procurement and other governance teams plan work independently, which can lead to:
 - overlapping scrutiny
 - missed emerging risks

- inefficient use of resources.
- Assurance Not Explicitly Linked to the Local Code of Corporate Governance
- Although all functions contribute to governance, there is no structured, auditable process showing how:
 - Controls, internal audit, governance leads, and risk registers collectively demonstrate compliance with each element of the Local Code of Corporate Governance.

Roles and Responsibilities

| | |
|---|--|
| The Mayor and Executive and Elected Members | Overall responsibility for effective management, including agreeing and adherence to the Council's governance and assurance mapping policy. |
| Chief Executive and Leadership Team | Lead, coordinate and champion effective management of the governance and assurance mapping policy ensuring that the Council fully complies with all legal and corporate governance requirements. |
| Senior Information Risk Owner (SIRO) | Responsible for the overall management of governance, information and policy within the Council, advising the Chief Executive, leadership management team and heads of service. Responsible for ensuring that the relevant specialists are present for governance mapping. |
| Governance and Information Manager | Manages the operational group of key officers within Complaints, Subject Access Requests (SAR) and Freedom of Information (FOI) Requests and Records Management. |
| Strategic Risk and Health and Safety Manager | Review and implement and corporately own the governance assurance map, completing the template for the self-assessment and ensuring all relevant heads of service submit the information provided. Responsible for reviewing and development of the governance and assurance mapping policy. |
| Data Protection Officer | Provide advice and guidance on data protection obligations and monitors compliance, Acts as the contact point for the ICO and data subjects and oversees DPIAs and maintains records of processing activities. |
| Corporate Governance leads | Corporate Governance Leads are responsible for providing second line assurance assessments within their areas of expertise, while Heads of Service retain ownership of risks and controls within their service areas. |
| Internal Audit | Internal Audit retains full independence and is responsible for providing objective assurance and an annual opinion on the effectiveness of governance, risk management, and internal control. |
| Heads of Service | Complete the self-assessment of their service area, support governance mapping by providing relevant information to the governance mapping team and ensuring that requests for information are actioned in a timely manner. |

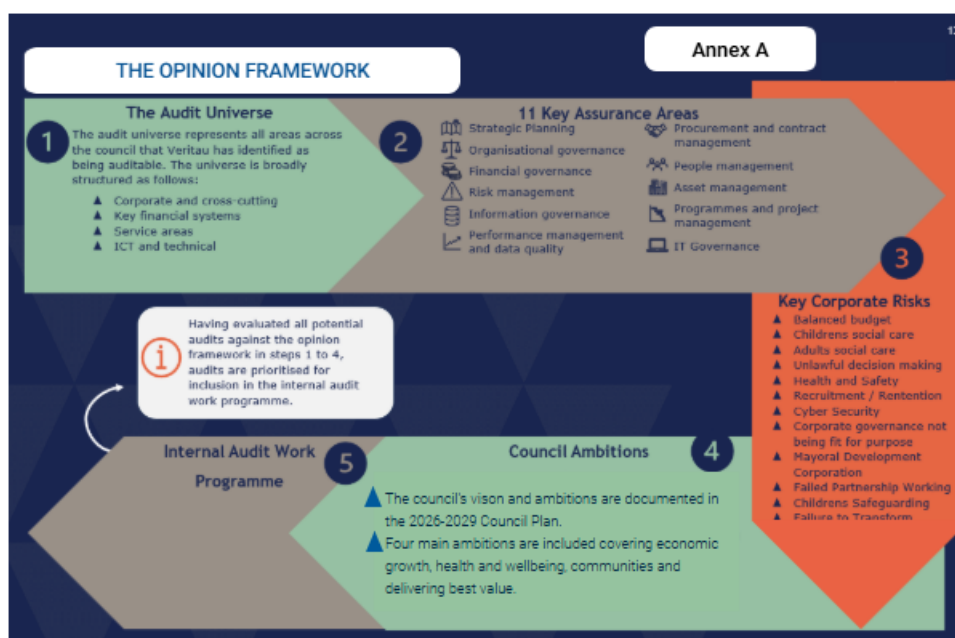
| | |
|----------------------|--|
| All employees | Understand the level of personal performance that is expected and deliver on this. Ensure data is entered accurately and in a timely manner. |
|----------------------|--|

Supporting policies, procedures, and standards

15. This policy operates within a broader governance framework and is supported by the following key documents and standards:

- Corporate Governance Framework
- Local Code of Corporate Governance (LCoCG) - Establishes principles of good governance and underpins all Council governance arrangements.
- Risk Management Framework
 - Risk Management and Opportunities Policy - Provides the overarching approach for identifying, assessing, and managing risks across the Council.
- Financial and Performance Management
 - Financial Regulations and Contract Procedure Rules - Ensure compliance with statutory financial controls and procurement standards.
 - Performance and Financial Management Policy and Framework Sets out how performance is monitored and reported to support strategic objectives.
 - Procurement Strategy and Contract Management Framework
 - The Procurement Act 2023 – Ensures compliance with procurement law when carrying out procurement processes compliantly
 - Social Value Act 2012 – Ensure compliance with the act in relation to Social Value consideration in procurement processes.
- Information Governance
 - Data Protection Policy - Ensures compliance with UK GDPR, Data Protection Act 2018, and the Data (Use and Access) Act 2025
 - Records Management Policy - Provides standards for maintaining accurate and secure records.
 - Corporate Performance Management Framework.
 - Project and Programme Management Framework.
 - Information Governance Framework, including Data Protection, Records Management, Cyber Security, FOI and SAR procedures.
- Audit and Assurance Standards
 - Global Internal Audit Standards (UK Public Sector) - Mandatory standards for internal audit independence, objectivity, and quality assurance.
 - Accounts and Audit Regulations 2015 - Statutory requirement for internal audit and Annual Governance Statement.
- Corporate Asset Management Plan
 - The Asset Management Strategy, highlighting the strategic context and factors that will influence change and translate organisational objectives into property objectives.

- The Asset Management Policy sets out the framework of rules, culture and behaviour that will ensure the consistent management and high performance of Council property assets.
- The Asset Management Action Plan – an action plan of activities and projects that deliver Council property objectives.
- Premises Security and Access Policy.
- Lockdown Procedure.
- Fraud and Ethical Standards
 - Anti-Fraud and Corruption Policy - Sets out measures to prevent, detect, and respond to fraud.
 - Whistleblowing Policy - Provides a safe mechanism for reporting concerns about wrongdoing.
- Health and Safety
 - Corporate Health and Safety Policy - Ensures compliance with health and safety legislation and promotes a safe working environment.
 - Counter Terrorism Plan.



The Opinion Framework

16. The Council's Opinion Framework provides a structured method for determining where assurance activity should be focused and how the annual internal audit opinion is formed. It brings together the full audit universe, key assurance areas, corporate risks, and strategic ambitions to ensure that assurance activity is targeted, proportionate, and aligned to both organisational risk and strategic priorities.
17. The framework begins with the Audit Universe, which represents all auditable areas across the Council, including corporate and crosscutting functions, key financial systems, service specific operations, and ICT and technical areas. These areas are then assessed against 11 Key Assurance Areas, which reflect the core governance disciplines required to meet the expectations of the Local Code of Corporate Governance, covering strategic planning, organisational

governance, financial and risk management, information governance, performance and data quality, procurement, asset management, people management, project and programme management, and IT governance.

18. The Opinion Framework also incorporates the Council's Key Corporate Risks, ensuring that assurance work is directly informed by major areas of strategic exposure, such as financial sustainability, safeguarding, governance effectiveness, cyber security, organisational resilience, and statutory compliance. By mapping each risk against the audit universe and assurance areas, the Council is able to identify the level of assurance available and areas where assurance is limited or absent.
19. These assessments are then considered alongside the Council's Ambitions, as set out within the Council Plan, ensuring that assurance activity supports delivery of the Council's priorities relating to economic growth, health and wellbeing, communities, and value for money.
20. Once all elements of the framework have been evaluated, potential audit areas are prioritised for inclusion in the Internal Audit Work Programme. This ensures that the annual programme is risk based, targeted, and reflective of both operational control needs and strategic objectives. The resulting audit work, along with wider governance assurance inputs, informs the Annual Governance Statement and underpins the Chief Internal Auditor's annual opinion on the effectiveness of governance, risk management, and internal control across the Council.

Information Governance Integration

21. Information Governance Assurance, including data protection, records management, information security, and data quality, is a core component of the Council's assurance framework.
22. The SIRO, Data Protection Officer, and Information Governance leads collectively provide Second Line assurance over information governance. Assurance roles are coordinated to avoid duplication and ensure that data protection, records management, cyber security, and information rights are fully represented within the Governance and Assurance Map.

Training and Support

23. Appropriate training, guidance, and support will be provided to officers involved in governance and assurance activities to ensure consistent understanding and application of this policy.
24. Targeted support will be made available to services where assurance ratings indicate weaknesses or where additional capability is required.

Monitoring and review arrangements

25. To ensure this policy remains effective and aligned with statutory and organisational requirements, the following monitoring and review processes will apply:

- Frequency of Review
 - The policy will be formally reviewed every three years or sooner if:
 - Significant changes occur in legislation, regulatory standards, or Council governance arrangements.
 - Emerging risks or audit findings indicate a need for revision.
- Responsible Roles
 - Strategic Risk and Health and Safety Manager - Leads the review process, coordinates updates, and ensures integration with the Governance and Assurance Map.
 - Head of Chief Executive's Department - Oversees compliance and approves proposed changes before submission to the Audit and Governance Committee.
 - Audit Committee - Provides oversight and endorses the revised policy for implementation.
- Monitoring and reporting
 - Annual Assurance Report.
 - Bi-Annual review by officer leads, with areas of significant concern escalated to the Audit Committee
 - Internal Audit progress report to the Audit Committee on delivery of the audit plan.
 - Annual Governance Statement (AGS) - The effectiveness of this policy will be assessed as part of the AGS process.

Evaluation

26. The effectiveness of this policy will be evaluated through a structured process to ensure continuous improvement and alignment with governance standards. The effectiveness of this policy will be assessed within the annual assurance report to committee which will include information on the following and improvements to:

- Number of areas with no assurance.
- Number of areas with low or limited assurance.
- Number of areas of concern.
- Number of substantial assurance internal audits.