Dear Councillor

CORPORATE GOVERNANCE COMMITTEE - WEDNESDAY, 27 APRIL 2022

I am now able to enclose for consideration at the above meeting the following reports that were unavailable when the agenda was printed.

Agenda Item
No.

4. **ANNUAL REPORT ON HDC COMPLIANCE WITH FREEDOM OF INFORMATION (FOI) & ENVIRONMENTAL INFORMATION REGULATIONS (EIR) ACTS** (Pages 3 - 16)

    To consider a report on requests for information received by the Council under the Freedom of Information and Environmental Information Regulations Acts and to highlight any issues encountered and actions to be taken to improve performance.

5. **INTERNAL AUDIT PLAN 2022/23 & INTERNAL AUDIT CHARTER** (Pages 17 - 40)

    To receive a report from the Internal Audit Manager outlining the Internal Audit Plan & Internal Audit Charter.

This page is intentionally left blank

3C Shared Services

HUNTINGDONSHIRE DISTRICT COUNCIL

Title/Subject Matter:	Annual report on HDC compliance with the Freedom of Information (FOIA) & Environmental Information Regulations (EIR) Acts
Meeting/Date:	27 April 2022
Executive Portfolio:	Executive Councillor for Corporate Services
Report by:	Information Governance Manager & Data Protection Officer
Ward(s) affected	All Ward(s)

EXECUTIVE SUMMARY:

The Information Governance Service for Huntingdonshire District Council (HDC) is currently provided by 3C ICT Shared Service hosted by Huntingdonshire District Council. This also serves South Cambridgeshire District Council and Cambridge City Council.

The Information Governance (IG) Team lead on:
- information requests under the Freedom of Information Act 2000, (FOIA) the Environmental Information Regulations (EIR) the Data Protection Act 2018 and the UK GDPR;
- data protection compliance advice; and
- information and records management advice.

The team is headed up by the Information Governance Manager who is also the Data Protection Officer for the three councils.

This is an annual report on the Council's compliance with the Freedom of Information Act 2000 and Environmental Information Regulations 2004.

This report also includes the Councils performance with regard to protecting personal data and covers the period Jan 2021 to Dec 2021.

The number of requests received by the Council in 2021 was 460; a decrease on the previous years total of 534 (a 14% reduction).

Recommendation(s):

Corporate Governance Committee is asked to note the contents of this report.

1. PURPOSE

1.1   The purpose of this report is to provide an update on Information Governance activity and performance during 2021 (January – December); hereby, highlight any issues encountered and actions to be undertaken to improve performance.

2. SCOPE

2.1   It provides:
   - An overview of the current arrangements in place to monitor the Information Governance at the Council.

   - An update on performance relating to:
      - Freedom of Information (FOI) Act / Environmental Information Regulations (EIR) Requests
      - Data Subject Rights Requests
      - Personal Data Breaches

3. BACKGROUND

3.1   Information is a vital asset and needs to be managed securely by the council. Appropriate policies, guidance, accountability and structures must be in place to manage the council's information legally, securely and effectively in order to minimise risk to the public and staff and to protect its finances and assets.

3.2   Information Governance describes the holistic approach to managing information by implementing processes, roles and metrics to transform information into business assets. This includes access to information, data quality, information management, information security and information sharing, all of which input into data protection compliance.

4. ORGANISATIONAL ARRANGEMENTS

4.1   In addition to the services details in the executive summary on page 1, the Information Governance Service work closely with 3C ICT on information security matters.

4.2 The IG Team consists of six members:

- The Data Protection Officer/Information Governance Manager (who will have been in post for 6 months at the time of this meeting) manages and oversees the service, and provides specialist advice on complex matters around data protection and information management for all three councils.
- The Deputy Data Protection Officer who provides cover and supports the team in the absence of the DPO and is also responsible for the information asset registers for the three councils and supports the information governance officers.
- Three Information Management Officers (one assigned ot each council) who support the Information Governance Officers with complex information requests and also provide advice and guidance to the councils internal departments on matters relating to data sharing, data protection impact assessment and personal data incident investigations.
- Two part time Information Governance Officers who manage incoming information requests and coordinate internal requests for support around personal data incidents/breaches, advice on data sharing and data protection impact assessments/contract reviews.

4.3 As this is a shared service, the Data Protection Officer (DPO) is the statutory DPO for all three authorities.

4.4 Updates on IG arrangements across Huntingdonshire District Council (HDC) are provided to the Information Governance Group (IGG). This Group is designed to facilitate the necessary engagement to ensure the relevant accountability of staff across the various services and to assist in driving any improvements required. It is chaired by the Senior Information Risk Owner (SIRO) and comprises of managers / heads of services across most service areas within the Council.

4.5 The Information Governance Group meets quarterly and last met in February 2022.

5.   DATA PROTECTION COMPLIANCE

5.1 As the DPO is new in post a report is in the final stages of completion around progress on data protection compliance against the previous plan and a health check across the information governance service and the three councils, in line with the ICO's compliance monitoring framework. The results of this report are due to be presented at the April/May board.

The initial findings from the review show that, whilst some procedures are in place, and required policies are in place, some of those in place are inconsistently applied/in need of review. Whilst clearly room for improvement exists, the position is not dissimilar to other local authorities, and the level of commitment to progress remains high and owned at the top of the organisation.

5.2   Improvements were required in the following areas:

Area	High Level Finding	Risk	Progress
Information Asset Registers / Flows	Although some Information Asset records were held by Service areas; we do not hold a central repository. These should be reviewed regularly to ensure information is accurate and held centrally.	The risk here is that there is no overview of our processes / systems which could result in delays to information requests; inappropriate controls being in place; no clear view on dependencies in terms of ICT systems when a change is made; etc.	Significant progress has been made in this action, with the IAR to be completed by July 2022. This will be centrally managed by the IG team to ensure quality of data.
Records of Processing (Article 30)	Although the Information Asset Register does collect most of the information required for Article 30; this is not held centrally; in addition to this, more information would be required on disclosures and transfers.	There is a risk that information is inappropriately being transferred (i.e. there may not be appropriate adequacy arrangements or appropriate technical safeguards in place)	Once the IAR task is completed a review of transfer arrangements for data will be undertaken, subject to resources.
Policies	Although there are some policies accessible on the Council's intranet pages, a number of these are out of date. To add to this, there are also additional IT Policies located within a repository (Protocol Policy) which is not	The risk is that staff are not aware of their obligations and therefore put the Council resources at risk.	Policies and procedures will be prioritised in order of importance and a complete set is anticipated to be in place across all three councils by the end of 2022, subject to resources.

Area	High Level Finding	Risk	Progress
	accessible to all staff as they are not published on the Intranet.		
Training Arrangements	The requirement by the ICO is that training is undertaken at least every two years. New starters are required to undertake e-learning as part of their induction process. For many existing staff, e-learning was undertaken in preparation for GDPR in 2018. This therefore means a number of staff will be coming up to the 2-year threshold for retraining. To date, there has been limited communication to enforce the requirement for refresher training for existing staff.	Although not in breach of the Act, by undertaking training every 2 years, this frequency is not in line with other partners in the public sector (e.g. NHS). This therefore creates a hurdle when signing up to Information Sharing Agreements.	Learning and Development are looking at the reporting functionality to allow greater understanding of take up of refresher training. The new DPO is meeting with HR representatives to review the existing training modules and look at service area engagement. Further actions are likely to result from this which will be reported to IGG in due course.
Information Sharing Arrangements	Although there are Information Sharing Agreements in place across the Council, there is no central register for this. There is no clear visibility if there are appropriate contracts / sharing agreements in place.	If a contract is not in place where data is being processed on behalf of the Council by a Data Processor; this is likely to be a breach of GDPR.	A log of information sharing arrangements where IG have been approached for input is now in place. Wider communication is required to ensure this is comprehensive and easily accessible. Additional actions will be required to ensure data sharing arrangements are

Area	High Level Finding	Risk	Progress
			communicated accordingly to relevant teams.
Incorporation of Privacy by Design in Projects	Data Privacy Impact Assessment (DPIAs) are completed; but it is unclear if this is always the case. DPIAs are currently treated as standalone documents to be completed at project initiation. Not all changes, go through a standard project process.	DPIAs may not be completed and therefore privacy risks may either not be identified / identified in a timely manner.	The new DPO is undertaking a review of the DPIA process and ensuring it is linked appropriately to ICT services requests for projects, software and other relevant areas; procurement processes; business transformation processes and all other relevant business areas. This will be in place by Aug 2022.

5.3 The actions to address the above will be factored into the ongoing IG forward plan 2022/23. It is likely that limited progress has been made with the previous plan due to a number of factors:

- Lack of consistency in the role of the DPO/IG manager; there have been 5 postholders in 5 years.
- Considerable volumes of reactive work around complaints from customers. (7 cases across two authorities, including one tribunal case, two ICO cases and several complaints).
- Limited resource required to deal with reactive and proactive work rather than definition between the two.

5.4 Updates to monitor the status and progress of the plan will be provided to the Council's Information Governance Group (IGG) on a quarterly basis.


6. PERFORMANCE UPDATE

### 6.1 FREEDOM OF INFORMATION / ENVIRONMENTAL REQUESTS

The public has the right of access to information held by the Council under the Freedom of Information Act. The Freedom of Information Act (FOIA) works alongside the Environmental Information Regulations (EIR).

6.2 Freedom of Information requests relate to requests for information that are not dealt with as part of the day-to-day business processes.

6.3 The 3C ICT Information Governance has implemented a shared request management system for handling information requests. Ownership of the response to these requests is placed on service areas by means of key responders and champions being designated and responsible for ensuring their service responds within the legal timeframe of 20 working days. An Information Governance Officer coordinates all formal requests and allocates specialist support from the Information Governance team where service areas require this.

6.4 The Council works to a target of 90% response compliance within 20 days (statutory requirement) as advised by the Information Commissioner. We achieved 81% in 2021 which is an improvement on the 77% of the previous year. Breakdown for each month in 2021 is provided below.
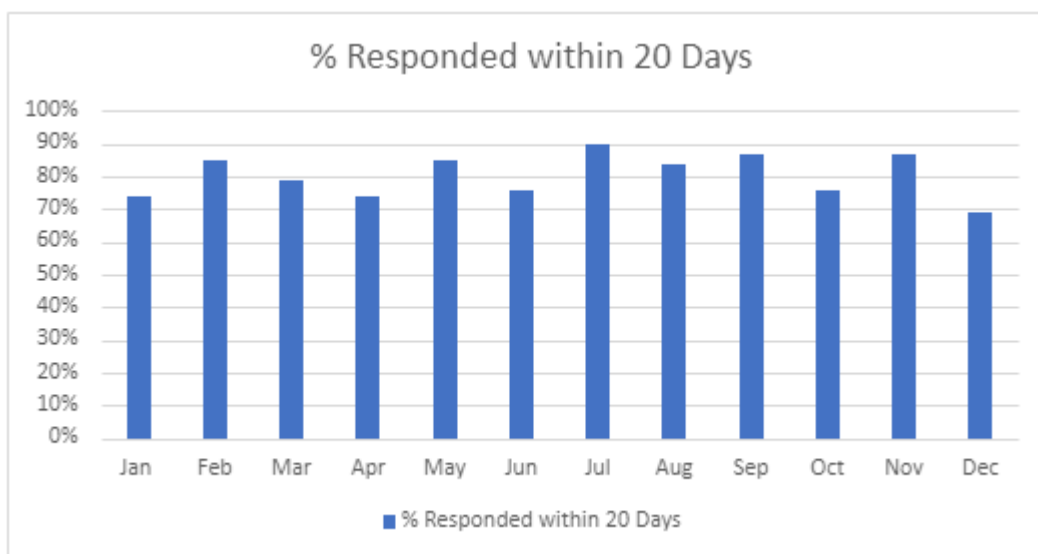

6.5 Reasons for this included service areas not being able to respond to requests for data on time due to priorities being diverted as a result of COVID-19.

6.6 The importance of responding to these on time and correctly is also being reinforced through the Information Governance Group Meetings.

6.7 For 2021 (Jan – Dec) the council received a total of 460 requests under FOI and EIR.
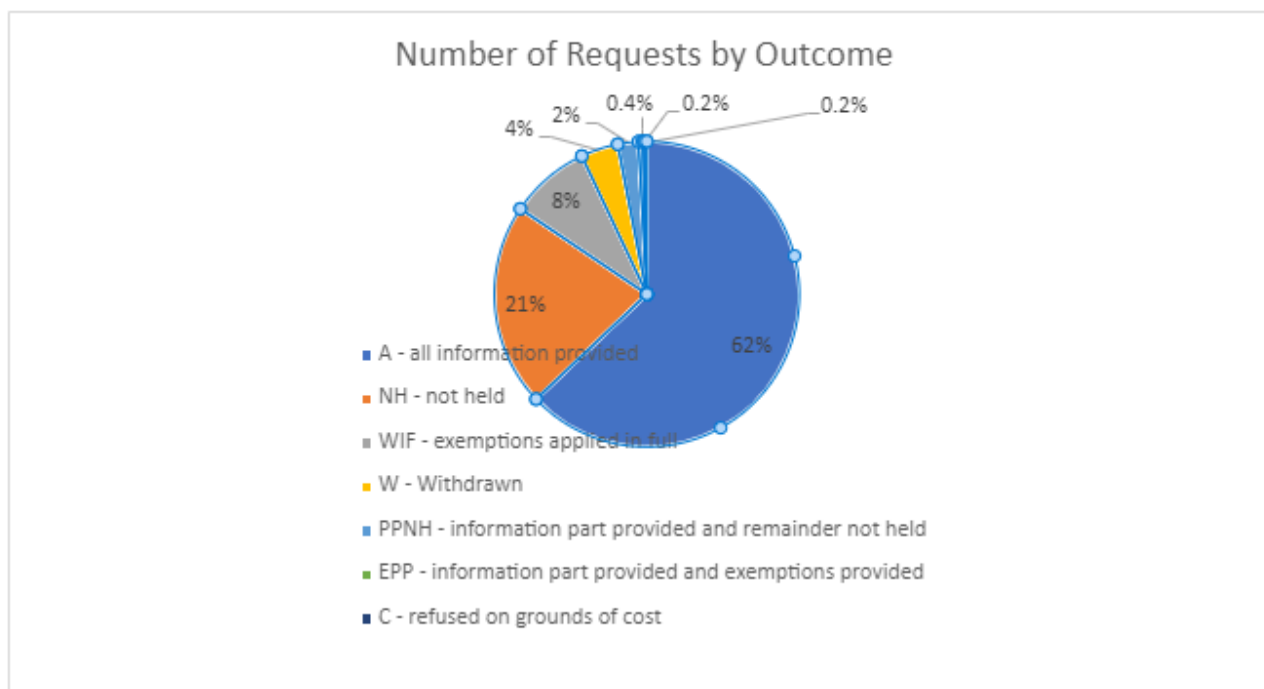
Volume of Requests Received Jan- Dec 21
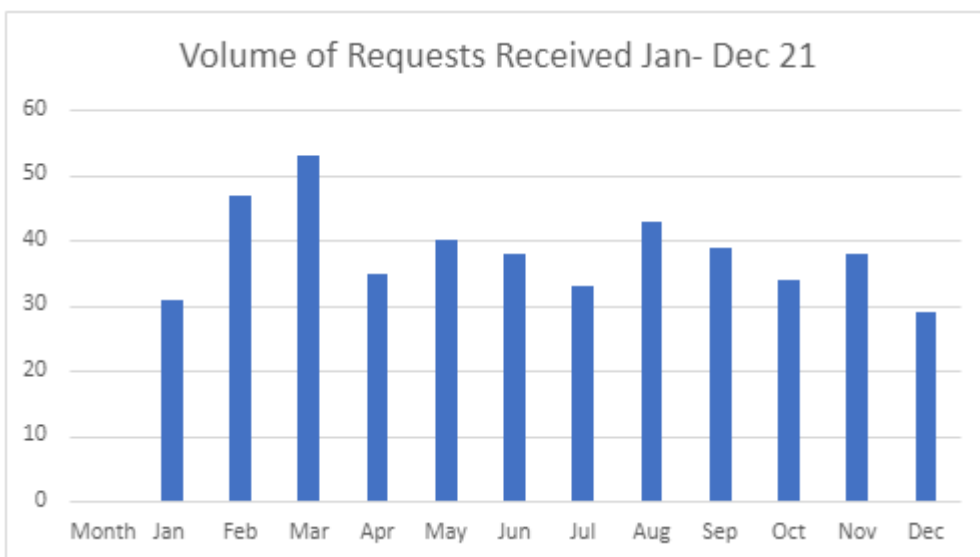
6.8   This represents a 14% decrease in the number of requests received in 2020. The graph below demonstrates the year on year trend in the number of FOI requests received since 2017.

Request Count by Year
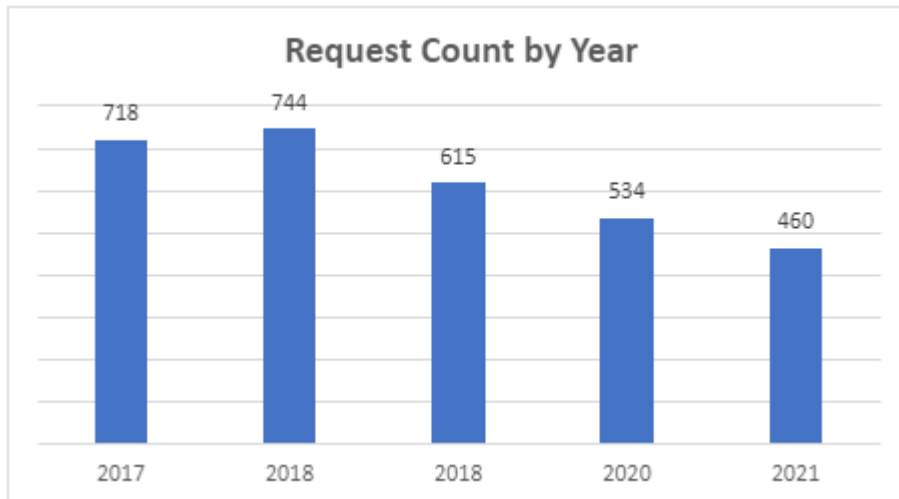
6.8.1   The Chief Operating Officer services and community services have received the most cases. This is also reflected in the volume of late requests (i.e. more requests mean less likely to hit target timescales).

Number of Cases per Service (Note: there maybe more than one service assigned to some cases)
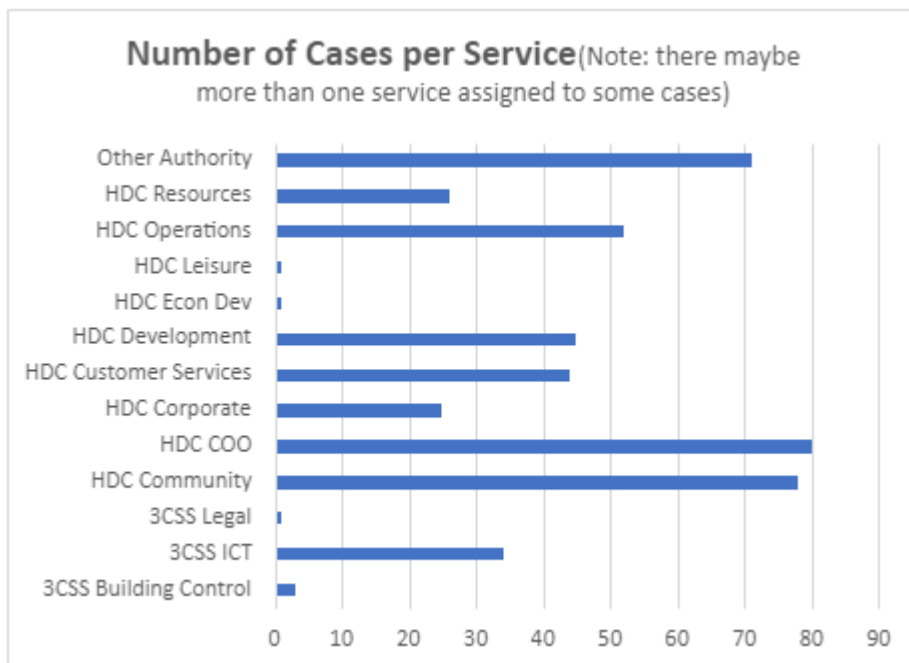
6.11 All the information was provided for the majority of requests. See breakdown of outcomes below.

Number of Requests by Outcome

- A - all information provided
- NH - not held
- WIF - exemptions applied in full
- W - Withdrawn
- PPNH - information part provided and remainder not held
- EPP - information part provided and exemptions provided
- C - refused on grounds of cost

6.12 The IG team continue efforts to support Services to increase this transparency offering via an Open Data Strategy.

6.13 The IG team continue to provide reports, which are shared with the Information Governance Group on a quarterly basis, to understand trends, and to help departments focus on what should be uploaded onto their publication scheme.

6.14 Requestors have the right to an 'internal review' of their case if they are not satisfied with the outcome or how the request was handled, before taking further action to the Information Commissioner's Office.

	Received
Internal Reviews / Complaints	4
ICO Investigations	6

Whilst there have been investigations by the regulator (ICO) these have resulted in no further action to date.

7. INDIVIDUAL DATA REQUESTS

7.1 The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulations (GDPR). Data protection is primarily concerned with personal data about individuals rather than general information.

7.2 The Information Governance Team coordinate requests relating to individuals rights such as right to request access to the personal data the Council holds, right to erasure, right to rectification as well as third party requests for personal data such as from the Police or to prevent or detect fraud.

7.3 Individual requests made during the year were as follows:

Other Requests	Received	Compliance with time frame
Subject Access Requests (SAR) (including Erasure Requests, etc.)	25	5 (+5 on hold)
SAR Complaints	1	0

7.4 Reasons for delays included:
- lack of awareness by service area officers around the ability to put requests on hold whilst awaiting identification or clarification;
- resources being diverted due to COVID.

The importance of prompt response and the need for training of all staff is also being reiterated through IGG, as well as additional training for Information Champions which will be rolled out in 2022/23 on a quarterly basis.

A review of the current Subject Rights request process is underway to ensure consistency and efficiency in handling these requests.

8. PERSONAL DATA BREACHES

8.1   The guidance on notification of data breaches under the Data Protection Act / GDPR is that where a breach incident is likely to result in high risk to the rights and freedoms of individuals, the Council must inform the ICO within 72 hours of becoming aware of the issue. If it's likely to result in high risk to rights and freedoms of individuals, the Council has a lawful duty to inform the individuals without undue delay.

8.2   As result, the IG team have established a framework to ensure that each reported incident is assessed for:

- The potential detriment and adverse effect to the data subject. This includes emotional distress and information about the private aspects of a person's life becoming known to others.

- The extent of detriment. Which could depend on the volume of the data and its sensitivity.

The assessment is carried out by the IG team when an incident is logged by a Service Area.

8.3   The IG Team have also developed a register to log incidents / near misses relating to personal data. This allows trends to be identified, with the view to establish if any specific training needs are required or if any actions are needed to enhance the current measures to prevent the likely reoccurrence.

8.4   **Performance Data – Data Breaches**
Although 17 incidents were reported in 2021 (Jan – Dec) only 1 of these met the threshold for reporting to the ICO. A breakdown of these is as follows:

Type of Incident (Category)	Number	Reported to ICO
Personal details inappropriately disclosed (e.g. via email/ shared/published on website)	16	1
Lost or stolen hardware	0	0
Technical Security failing	1	0
Total	17	1

8.5 In all instances, immediate steps were taken by officers to mitigate the incident, once known. Examples included contacting incorrect receiver of emails from the recipients of the email and those affected and removing documents from the Council's website.

8.6 A quarterly update on incidents is provided to the IGG to ensure visibility and ensure any improvements needed are discussed and followed through as appropriate. Where relevant learning from breaches/incidents/near misses is also shared across the three councils to minimise the risk of further occurrence.

9. TRAINING

9.1 To ensure organisational compliance with the law and relevant guidance relating to Information Governance (IG), all council staff and elected members must receive appropriate training.

9.2 A review of e-learning modules, and roll out of annual refresher is due in 2022, lead by the council's new DPO.

9.3 In addition to this, all new starters who manage confidential information are expected to undertake training on handling confidential information.

10. LOOKING FORWARD

10.1 Ensuring ongoing compliance with Data Protection Legislation (DPA 2018 and UK GDPR) has been the focus of the Information Governance team.

10.2 The Information Governance team will continue to work with Service areas to address gaps identified as part of the original gap analysis and subsequent

health check report (on Data Protection Compliance) and provide updates during the Information Governance Group meetings.

11. KEY IMPACTS/RISKS

11.1 The key impact of non-compliance with FOIA/EIR and the Data Protection Act along with GDPR is public scrutiny from the regulator.

11.2 Poor service or inadequate information management will lead to loss of trust from our customers. Inability to act in accordance with the Act and the Governments accountability and transparency directive will lead to reputational damage.

11.3 Furthermore, the right of access is bound with the Human Rights Act in respect of the right to privacy. Unlawful disclosure of personal information may lead to publicly enforced audit, warning, reprimand, corrective order and/or fine by the regulator.

12. WHAT ACTIONS WILL BE TAKEN

12.1 Compliance will Data Protection Legislation will continue to be monitored. Actions as identified in Section 5.3 will be undertaken. Updates will be provided via the Information Governance Group.

13. LINK TO THE LEADERSHIP DIRECTION

13.1 Supports the objective to become a customer focused organisation under the strategic priority of becoming a more efficient and effective Council.

14. CONSULTATION

14.1 None

15. LEGAL IMPLICATIONS

15.1 HDC must comply with the law concerning FOIA/EIR and UK GDPR/Data Protection Act 2018.

16. RESOURCE IMPLICATIONS

16.1 There are no direct resource implications arising from this report.

17. OTHER IMPLICATIONS

17.1 None

18. REASONS FOR THE RECOMMENDED DECISIONS

18.1 This paper updates Members on how requests under FOIA/EIR/DPA have been dealt with by HDC.

18.2 This report is for information purposes only.

19. LIST OF APPENDICES INCLUDED

19.1 None

20. BACKGROUND PAPERS

20.1 None

CONTACT OFFICER

Kirsty Squires
Information Governance Manager & Data Protection Officer (3C ICT)
Infogov@3csharedservices.org

Public
Key Decision – No

HUNTINGDONSHIRE DISTRICT COUNCIL

Title: Internal Audit Plan 2022/23

Meeting/Date: Corporate Governance Committee – 27 April
2022

Executive Portfolio: Executive Councillor for Corporate Services
Councillor David Keane

Report by: Internal Audit Manager

Wards affected: All wards

Executive Summary:

The Committee has responsibility under its terms of reference for ensuring
that the Council undertakes an effective internal audit to evaluate the
effectiveness of its risk management, control and governance processes
taking into account the Public Sector Internal Audit Standards (PSIAS).

The Plan, based on a list of assurance activities, has been prepared showing
areas where audit activity is planned. It shows audit activities which will
support an audit opinion covering:
   - key financial core systems
   - areas that form the basis of good governance
   - and operational audits which are risk-based and are subject to movement
     based on priority.

It is anticipated that as new risks emerge the Plan list can be adjusted to allow
for higher-priority reviews to be inserted. The Council's risk register is
undergoing an update and will feed in new risks for consideration.

In addition, the Internal Audit Charter, has been reviewed and is considered
still fit for purpose with only a change to one job title.

Recommendations
That the Corporate Governance Committee:
• reviews and approves the Internal Audit Plan
• agrees that changes can be made to the Internal Audit Plan following
  consultations between the Internal Audit Manager and S.151 officer and
  the Chairman of Corporate Governance Committee.
• Reviews and approves the Internal Audit Charter 2022.

1. PURPOSE OF THE REPORT

1.1 To recommend to the Committee that the Internal Audit (IA) Plan for 2022/23 be approved.

2. BACKGROUND

2.1 The Accounts and Audit Regulations 2015 require that the Council '…must undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account Public Sector Internal Audit Standards (PSIAS) or guidance'. The Council has adopted the PSIAS through the Committee's Terms of Reference.

2.2 The Council requires the Internal Audit Manager (IAM) to "establish risk-based plans to determine the priorities of internal audit activity, consistent with the organisations goals". The risk-based plan must also:

- take into account the requirement to produce an annual internal audit opinion;
- incorporate a strategic high-level statement of how the internal audit service will be delivered and developed and how it links to the Council's objectives and priorities;
- explain how internal audit's resource requirements have been assessed; and
- include the approach to using other sources of assurance and any work required to place reliance upon those other sources.

Furthermore, the IAM must review and adjust the plan as necessary, in responses to changes in risks, operations, programs, systems, and controls.

3. ANALYSIS

Available resources and evaluation

3.1 The planned internal audit staff resources for 2022/23 are intended to be:

    0.80 FTE: Internal Audit Manager
    0.44 FTE: Internal Auditor
    1.00 FTE: Trainee Internal Auditor
    0.27 FTE: Computer audit (externally contracted)

Resource time will be impacted by the following:
- Time spent within the Risk & Control Group
- Training and mentoring
- Unknown ad hoc work

3.2 Risk management was moved away from Internal Audit in 2019 to enhance the independence of Internal Audit from day-to-day business activity. Audit sits alongside, and as part of, the Risk & Control Group to support the risk management function and embed it into the Council's business operations.
After risk management has been fully embedded, then an Internal Audit review can be undertaken either by Audit (internal) or as a fully independent review commissioned

by our external IT internal audit contractor, who can also perform general non-IT reviews on our behalf. Once the Risk Register update has been completed, it will be used to influence and feed the Audit Plan to ensure that the reviews are both risk-based and support corporate objectives.

Internal Audit Plan

3.3   Annual internal audit plans have been prepared for many years based on an audit universe that contained details of all systems and significant processes, maintained and updated with risks recorded on the risk register. A significant amount of time is spent preparing the annual plan and scheduling audits across the year, only for the plan not to be fully delivered due to the need to advance, defer, add or remove audits throughout the year.

3.4   Moving to a more flexible and fully risk-based Audit process, planning resource days at the outset of the Audit Plan to any level of detail gives no real benefit nor assurance that the Plan is sound. For the last two years this methodology has been presented and agreed at Committee and this year's Audit Plan is presented in the same manner.

3.5   The Audit Plan for 2022/23 is attached at Appendix 1. It comprises three categories of audit activity:

- assurance activities in support of the annual Audit opinion.
- other assurance activities - for later consideration and inclusion in the Plan
- audit activities that need to be undertaken but do not support the audit opinion.

3.6   The plan has been prepared after considering the aims and outcomes of the Corporate Plan, the progress made in delivering the 2019/20 & 2020/21 annual governance statements, the requirement to review key financial and significant internal control systems and procedures. The Plan is designed to show audit activities that relate to: key financials, governance, finance, contracts, and operational areas, and shows alignment to the Council's new priorities.
Once the Council's risk register has been reviewed and updated the Audit Plan will need to be revisited to ensure it is in line with the significant risks identified. Corporate Governance Committee members and the Senior Leadership Team have also been asked for ideas or suggestions of areas that could be considered for inclusion in the plan.

Other sources of assurance

3.7   The PSIAS requires that the audit plan planning process takes into account other sources of assurance that will be available during the year. Managers have been requested to provide details of any planned independent reviews from which assurance could be obtained to avoid/minimise duplication of effort. It is intended that these external or third-party assurances will be captured and used to support the audit opinion.

4.   RISKS

4.1   Non-delivery of the internal audit plan, or not undertaking sufficient work across the Council's control environment (the framework of governance, risk management and

internal control) may affect the ability of the Internal Audit Manager to provide the Committee with a robust annual internal audit opinion.

4.2 The internal audit team is small and any reduction or diversion of resources (ie staff leaving, sickness, non-audit activities) would quickly have an impact on the deliverability of the audit plan.

5. LINK TO THE CORPORATE PLAN

5.1 The Internal Audit Service through the audit plan contributes to all the strategic themes and outcomes. Specifically, it supports the Senior Leadership Team by undertaking reviews that provide assurance that:
   - significant risks identified in the risk register are managed effectively
   - laws and regulations are being met,
   - business and financial processes and systems are managed effectively and
   - assets are safeguarded.

It also improves the performance of the Council by assessing current risks, considering emerging risks, identifying efficiency gains and process improvements.

6. RESOURCE IMPLICATIONS

6.1 The 2022/23 service budget supports the internal audit establishment detailed at 3.1.

6.2 It is essential that the internal audit plan is duly flexible. Therefore, it is considered that there should be appropriate delegation to the Director of Corporate Resources /S.151 officer *(Corporate Director of People in the interim until this new Director post is filled)* to permit such changes, in consultation with the Chairman of Corporate Governance Committee.

7. REASONS FOR THE RECOMMENDED DECISIONS

7.1 The Committee's terms of reference require it to approve the Internal Audit Plan.

8. LIST OF APPENDICES INCLUDED

Appendix 1 – 2022/23 Internal Audit Plan.
Appendix 2 – Draft Internal Audit Charter (v.2022)

BACKGROUND PAPERS
The Public Sector Internal Audit Standards

CONTACT OFFICER

Name/Job Title: Deborah Moss, Internal Audit Manager
Email: deborah.moss@huntingdonshire.gov.uk

Internal Audit & Assurance Plan
2022 - 2023

In delivering the Internal Audit (IA) Mission Statement -

to enhance and protect organisational value by providing risk-based and objective assurance, advice and insight and to specifically support the Council successfully achieve its vision and priorities as set out in the Corporate Plan -

it is important that IA engagements not only consider and review internal control, risk and governance issues but also:

remain future focused,
positively influence and contribute to service developments and initiatives
lead to a strengthening of the control environment, and
are performed in accordance with professional standards.

Remain future focused

Traditionally IA have reviewed how risks and objectives have been delivered in the past, rather than consider how they are to be managed going forward. The audit plan is future focused, considering the risks that lie ahead of the Council, and so allow IA to provide advice and insight that will help Corporate and Service Plan objectives be achieved. This is a step-change in approach and will take time to embed into the culture.

Corporate Governance Committee (CGC) members have also been contacted and asked for their thoughts on areas for inclusion in the plan. They will also be contacted during the year so their concerns continue to be heard.

Positively influence and contribute to service developments and initiatives

Due to the many challenges facing the Council, change remains a constant and all Services either have reviewed or will be reviewing how they deliver their services.

IA is able to add value at an early stage of service or transformational developments through contributing advice and assistance that influences how risks can be reduced through introducing appropriate controls. Providing assurance at an early stage will also allow IA to gain a fuller understanding as to how the changes proposed will assist in delivering service objectives and their consequential impact elsewhere across the Council. This approach should lead to a strengthening of the overall control environment and time will be made available in the audit plan for IA to undertake this type of advisory work. IA strives to be trusted advisor to senior management and the CGC. Contributing positively to service developments and initiatives is one way in which that trust can be gained.

Lead to a strengthening of the control environment

The results of IA work are communicated to Managers and Members via IA reports.
The IA Report template is designed so that issues identified are reported with greater clarity and impact. Remedial actions are agreed in collaboration with the client Service to provide a practical and workable solution that can be implemented by the Service.

Managers agree to implement actions that will strengthen the control environment and IA will continue to use the 4Action software to monitor and report upon their introduction. IA will undertake follow-up reviews on at least the red priority actions that managers have indicated as being fully introduced. The results of the follow-up work will be one of the factors that inform the annual IA opinion and time will be made available in the audit plan for follow-up reviews to be completed.

CGC will receive a summary update on the delivery of the audit plan agreed, be informed of any issues of concern and the progress being made with the implementation of agreed audit actions. Such a summary will allow the CGC to receive timely and relevant information and allow them to question IA whilst issues remain relevant.

Performed in accordance with professional standards.

The Public Sector Internal Audit Standards (PSIAS) require an external independent review of the IA service to be completed at least once every five years to confirm if the service is PSAIS-compliant. An external review was conducted in May 2014. A self-assessment was carried out internally by the IA team in 2018 and an action plan prepared, but another external review was not commissioned due to the need to concentrate efforts on delivery of the audit plan.

The Internal Audit Manager reviews the work performed by internal auditors at key stages throughout the audit process and evidences the checks they have performed. The IA service aims to act in conformance with the PSIAS.

Internal Audit Plan 2022/23

The Mission of Internal Audit articulates what internal audit aspires to accomplish within an organisation. *To enhance and protect organisational value by providing risk-based and objective assurance, advice and insight.*

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes. [Public Sector Internal Audit Standards' (PSIAS) Definition of Internal Auditing]

The following core principles articulate internal audit effectiveness; for an IA function to be considered effective, all Principles should be present and operating effectively:
- Demonstrates integrity.
- Demonstrates competence and due professional care.
- Is objective and free from undue influence (independent).
- Aligns with the strategies, objectives, and risks of the organisation.
- Is appropriately positioned and adequately resourced.
- Demonstrates quality and continuous improvement.
- Communicates effectively.
- Provides risk-based assurance.
- Is insightful, proactive, and future-focused.
- Promotes organisational improvement.

Internal Audit Planning

The Public Sector Internal Auditing Standards (PSIAS) state:

The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organisation's goals.
Interpretation: To develop the risk-based plan, the chief audit executive consults with senior management and the board and obtains an understanding of the organisation's strategies, key business objectives, associated risks and risk management processes. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organisation's business, risks, operations, programmes, systems, and controls.

> *Public sector requirement: The risk-based plan must take into account the requirement to produce an annual internal audit opinion and the assurance framework. It must incorporate or be linked to a strategic or high-level statement of how the internal audit service will be delivered and developed in accordance with the internal audit charter and how it links to the organisational objectives and priorities.*

2010.A1 The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.

2010.A2 The chief audit executive must identify and consider the expectations of senior management, the board and other stakeholders for internal audit opinions and other conclusions.

2010.C1 The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value and improve the organisation's operations. Accepted engagements must be included in the plan.

2020 Communication and Approval The chief audit executive must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations.

2030 Resource Management The chief audit executive must ensure that internal audit resources are appropriate, sufficient and effectively deployed to achieve the approved plan.

Interpretation: Appropriate refers to the mix of knowledge, skills and other competencies needed to perform the plan. Sufficient refers to the quantity of resources needed to accomplish the plan. Resources are effectively deployed when they are used in a way that optimises the achievement of the approved plan.

Public sector requirement: The risk-based plan must explain how internal audit's resource requirements have been assessed.
Where the chief audit executive believes that the level of agreed resources will impact adversely on the provision of the annual internal audit opinion, the consequences must be brought to the attention of the board.

Audit Plan 2022/23 – Assurance Activities that support the Annual Audit Opinion (Internal Control, Governance & Risk Mgt):

Area	Assurance sought	Type	Audit Type	HDC Corporate Priorities
Completion of 2021.22 Audit reviews				
The seven core financial systems below are usually audited on a continuous auditing basis every quarter. Frequency may now be adjusted based on previous assurance.				
Main Accounting System	*Are key financial controls still operating as they should be and are they still effective?*	Financial	Key Financial Controls	Good Basic Services
Creditors / Accounts Payable	*Are key financial controls still operating as they should be and are they still effective?*	Financial	Key Financial Controls	Good Basic Services
Debtors / Accounts Receivable	*Are key financial controls still operating as they should be and are they still effective?*	Financial	Key Financial Controls	Good Basic Services
Council Tax / NNDR	*Are key financial controls still operating as they should be and are they still effective?*	Financial	Key Financial Controls	Good Basic Services
Housing Benefits Creditors & Debtors	*Are key financial controls still operating as they should be and are they still effective?*	Financial	Key Financial Controls	Good Basic Services
Payroll	*what assurance in this process after staff change and new system introduced?*	Operational	Risk-based systems , cyclical scope	Good Basic Services

Social Value in Procurement	*Is social value embedded into our Procurement activities across Council?* *Is there adequate awareness to fulfil this?*	Contract	Risk-based systems	Good Basic Services Economy and Jobs
Information Governance: Information Security Training & Awareness ***(link to data breach procedure)***	*Are we ensuring all staff receive appropriate info security /DP training and is compliance and oversight in place?*	Governance	Risk-based systems	Good Basic Services
Planning /Development Mgt Control	*Are planning conditions appropriately managed?*	Operational	Risk-based systems	
Corporate Programme Delivery **(to include Recovery Programme)**	*Are our projects/project sponsors complying with the governance processes, to ensure projects are delivered? and are they working appropriately (including are they proportionate or not adjustment)*	Projects	Process assurance	Good Basic Services
KPI Planning results	*Are KPI results robustly and reliably calculated? (Time taken reporting, extensions to time limits.)*		Probity	Good Basic Services
Risk Management	*Is the Risk Management process in place and is it appropriate and working effectively?* *Is sufficient information presented to Corporate Governance Committee?*	Governance	Process assurance	Good Basic Services
Establishment Management (Staffing): **Scope to be decided from:** **- Starters and Leavers** **- Recruitment** **- Establishment control (ghost employees)**	*Is there control mechanism for checking that the finance for a post is secured before a recruitment begins?* *can we be sure that only our agreed establishment is paid (and assurance that this is regularly checked)?*	Operational	Risk-based systems	Good Basic Services

Managing Absence (follow up)	*Is sickness recording and monitoring now being carried out correctly and effectively, especially as now have new system?*	Operational	Follow-up	Good Basic Services
Small Works Contract (follow up)	*Have the actions been introduced and working effectively, any further action needed?*	Contract	Follow-up	Good Basic Services
New CIPFA Financial Management Code	*Is there key assurance in compliance with this Code - Financial control of budget setting, review, etc.; S.151 Action Plan.*	Financial	Compliance review	Financial Stability
Information Governance: Data Protection *[Dependent on findings from 100 day report?]*	*Is the Council data protection compliant across Services?* *Is training & awareness sufficient?*	Governance	Risk-based systems & Compliance	Good Basic Services
HMOs	*Do we maintain an appropriate register for HMOs as required by statute?*	Operational	Risk-based systems & Compliance	Good Basic Services
Procurement Cards	*Are cards used appropriately/economically and not to circumvent the controls mechanisms of the purchase ordering system?* *Was purchasing during lockdown and working from home still appropriate spending and adequately controlled?*	Financial	Probity & Compliance (lite-touch review)	Good Basic Services
Leisure	*Are our discounted memberships and their 'loss of income' providing value by incentivising people to join and creating retention value?* *Are the discounts based on sound business calculations, are they correctly applied and are they reviewed and monitored for compliance by the member?*	Operational	Risk-based systems	Good Basic Services Community and Health
Reserve Audits				

Facilities Management	*How are we commissioning work and letting our building security contracts?* *Are control mechanisms in place for ensuring building security for multi-occupancy sites?*	Operational	Risk-based systems	Good Basic Services
Shared Service cost allocation	*Ensuring that the costs of the shared services are appropriately allocated based on current use projections.*	Operational	Process Assurance	Good Basic Services

Shared Services:
Audit assurance activity for Services under the Shared Service Partnership is the responsibility of the hosting Authority. Any activity in this area will be shared and used in the Annual Opinion.

IT Audits:
These are yet to be decided but will be considered by all 3Cs Councils.

Follow- up reviews:
Where resources allow, every effort will be made to carry out follow up verification reviews on implemented actions. As a minimum this will cover those actions categorised as a 'red priority' or where a limited opinion was issued and all IT audit actions.

<u>**Other areas for consideration/inclusion in Plan**</u>:
- o Climate Change and Environment Strategy & our Plan
- o Remote working – impact, security and control
- o Staff Induction & Training
- o Leisure – corporate and other discounted memberships (linking to recovery, retention and future income proofing)
- o Leisure - Membership & Retention: the Customer Digital Journey
- o A Contract Review
- o Environmental Health/ Food
- o Printing Portal
- o Tree Maintenance

- o Scheme of Delegation
- o VAT
- o Modern Day Slavery (statement) (likely to become statutory requirement)
- o Legal – (contract costs and use of additional external provision)
- o Staff timekeeping & leave
- o Council Tax Support – increase in demand since lockdown began

Internal Audit activities that will not be used to support the annual audit opinion

Area	Area
Compliance Declarations	Annual declaration for DFG spend Compliance Declaration for govt grants on request
Audit Governance	Annual Audit Plan and risk assessment process review IA compliance with PSIAS – self assessment Quality assessment of audit work undertaken and file review (PSIAS) IA Charter Compliance with IIA Ethics policy
Assurance mapping	Assurance mapping of other sources of assurance (internal and external)
Whistleblowing & Fraud	Whistleblowing Policy and Guidance (review) Whistleblowing Log Advising on whistleblowing complaints received
Corporate Governance Committee	Reporting throughout the year on: IA Plan (for approval) – March/April CGC IA Service Interim Performance report (six monthly) IA Service Performance report (possibly including Annual Opinion) Implementation of Audit Actions – each CGC Annual Whistleblowing report

	Significant issues for inclusion in AGS – June CGC Progress reporting on any AGS significant issues – 6 months after. Annual Audit Opinion on internal control – June CGC
AGS	Governance issues included in the Council's AGS. Progress monitoring and reporting on all significant issues in AGS.
Governance	Internal Code of Governance - annual review; stated v actual? Attendance at Risk & Controls Group and Board Meetings Attendance at Information Governance Meetings Governance /assurance work on identified Council projects
IT audit contract	IT audit contract has expired and will be retendered in 2022.
Follow-up process & Management and monitoring of audit actions implementation	Review of our internal follow-up process and automation of reports from 4Action. Management of audit actions; reopening of actions found to be not fully implemented/compliant. 4Action outstanding actions reports to R&C Board and CGC.
Advice and assistance	By ad hoc requests from Services.
Consultancy & Projects work	By request from Services; acceptance will be dependent on resource and skills available.
National Fraud Initiative (NFI) work	Supporting the NFI initiative by assisting with investigation of matches found.
Training and Mentoring	Support for Trainee Auditor (both internal training and mentoring time and professional Auditing qualification)

Deborah Moss
Internal Audit Manager, March 2022

Internal Audit Charter

2022

INTERNAL AUDIT CHARTER *Effective March 2022*

The Council considers its Internal Audit Services to be a key component of its governance framework. This Charter provides a framework for the conduct of Internal Audit in Huntingdonshire District Council and has been approved by the Council's Corporate Governance Committee.

The key provisions of this Charter are set out below.

Internal Audit Service

The Council's internal audit service is an independent, objective assurance and consulting activity designed to add value and improve the Council's operations. It helps the Council accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

Independence & Objectivity

The internal audit service will remain free from interference by any element in the Council and its scope shall not be restricted in anyway. It shall be free to review the arrangements of any aspect of service delivery, finance or governance irrespective of whether those arrangements are provided directly or indirectly (via partnerships, contractually or any other business arrangement).

The objectivity, impartiality, integrity and conduct of all Internal Audit staff must be above reproach at all times.

Authority

Internal auditors are authorised to have full, free and unrestricted access to all services and functions, premises, assets, employees, elected members, suppliers and contractors, records and other documentation and information that the Internal Audit Manager considers necessary to enable the Internal Audit Service to meet its responsibilities. All employees are required to assist the internal audit activity in fulfilling its roles and responsibilities.

Confidentiality

All records, documentation and information accessed in the course of undertaking internal audit activities shall be used solely for the conduct of internal audit activities. The Internal Audit Manager and individual audit staff (including contractors and external service providers performing work on behalf of internal audit) are responsible and accountable for maintaining the confidentially of the information they receive during the course of their work.

Reporting

The Internal Audit Manager shall submit to the Corporate Governance Committee, no later than the date at which the Council's annual governance statement is approved, an annual report and formal audit opinion.

---

1. **Purpose of Internal Audit**

    The Internal Audit Service (IAS) has been established to:

    -   provide independent, objective assurance, advice and insight to the Council on its operations.

    -   enhance and protect value, by assisting management in improving the delivery of the Council's objectives and operations through evaluating, challenging and improving the effectiveness of risk management, control and governance processes.

2. **Mandatory Guidance**

    The IAS will govern itself by adhering to the Public Sector Internal Audit Standards (PSIAS)[1] as required by regulation 5 of the Accounts and Audit (England) Regulations 2015.

    Guidance issued and endorsed by the Relevant Internal Audit Standard Setters as applying to local government will also be adhered to along with the Council's relevant policies and procedures and the internal audit manual.

    Non-conformance with the PSIAS shall be reported to senior management and the Corporate Governance Committee.

3. **Relationship with Members & Senior Management**

    Corporate Governance Committee

    The Accounts & Audit (England) Regulations 2015 require the Council to "undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account public sector internal auditing standards or guidance".

    The Council has established a Corporate Governance Committee (CGC) and specifically delegated to it responsibility for "fulfilling the Board responsibilities of the PSIAS and ensuring effective internal audit is undertaken in accordance with the PSIAS"[2]   The internal audit service shall report functionally to the Corporate Governance Committee.

    The Internal Audit Manager (IAM) shall have:
    -   free and unrestricted access to the CGC and the right to attend all of its meetings, and
    -   the right to meet with the Chairman of the CGC and/or the relevant Cabinet Portfolio Holder to discuss any matters or concerns that have arisen from internal audit work.

---

[1] The PSIAS are based upon the Institute of Internal Auditors' mandatory guidance including the Definition of Internal Auditing, the Code of Ethics, and the *International Standards for the Professional Practice of Internal Auditing.*
[2] Extract from Committee's terms of reference approved by Council on 29 March 2017.

Senior Management

The Managing Director and the Corporate Director (People) and the Corporate Director (Place) fulfil the role of senior management as defined by the PSIAS. The Chief Financial Officer does not presently sit at Senior or Corporate Leadership Team – *this is under review.*

The Chief Financial Officer shall support the CGC by ensuring that there are effective arrangements[3] for the internal audit of the control environment.

The IAM shall:
- report administratively to the ~~Assistant Director of Corporate Services~~ Director of Corporate Resources; and
- have free and unrestricted access to senior management.

4. Independence & Objectivity

Independence is essential to the effectiveness of the internal audit service; so it will remain free from all conditions or interference that threaten the ability of internal auditors to carry out their responsibilities in an unbiased manner. This shall include, but not be limited to matters of audit selection, scope, procedure, frequency, timing or report content.

Internal auditors must exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. They must make a balanced assessment of all the relevant circumstances and not be unduly influenced by their own interests or by others in forming judgments.

Internal audit staff with real or perceived conflicts of interests must inform the IAM as soon as these issues become apparent so that appropriate safeguards can be put in place.

The IAM will confirm to the CGC annually, the organisational independence of the internal audit service. They shall also disclose to the CGC any interference and its related implications in determining the scope of internal auditing, performing work and/or communicating results.

Internal audit staff will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair their judgment. They shall also not assess specific operations for which they had responsibility in the previous 12 months.

5. Authority & Confidentiality

Internal auditors (including contractors and external service providers engaged to perform work on behalf of the IAM) shall have full, free and unrestricted access to all services and functions, premises, assets, employees, elected members, suppliers and contractors, records and other documentation and information that the IAM considers necessary to enable the IAS to meet its responsibilities. All employees and

---

[3] As outlined in the Cipfa publication "The Role of the CFO in public sector organisations".

members are required to assist the internal audit activity in fulfilling its roles and responsibilities.

All records, documentation and information accessed in the course of undertaking internal audit activities shall be used solely for that purpose. Individual internal auditors are responsible and accountable for maintaining the confidentially of the information they receive during the course of their work.

6. Internal Audit Management

The Council shall appoint an IAM who shall determine the priorities of, manage and deliver the internal audit service in accordance with this Charter.

The IAM shall:

- ensure they have a comprehensive understanding of the Council's systems, structures and operations so allowing the preparation of a risk-based audit plan each half year that is closely aligned to the need to provide assurance against the Council's strategic priorities, key business objectives and risks, as contained or identified within its Corporate Plan, Service Plans, risk register and framework of assurance.
- review and adjust the audit plan as necessary, in response to changes in the Council's risks, operations, programs, systems and controls.
- report annually the impact and consequence of any resource limitations to the CGC, who will then recommend to Cabinet whether or not to accept the consequence identified or seek an increase in internal audit resource.
- maintain a quality assurance and improvement programme to ensure that all audit work is completed to high standards and in accordance with the standards, practices and procedures as set out in the internal audit manual.
- undertake an annual review of the development and training needs of internal audit staff and arrange for appropriate training to be provided.
- put in place arrangements that ensure internal audit is notified of all suspected or detected instances of non-welfare fraud, corruption or impropriety and in conjunction with the Corporate Fraud Team Leader:
  - o promote a counter-fraud culture within the Authority
  - o determine the most appropriate method of investigating allegations.
- establish effective relationships with managers at all levels.

7. Role and responsibilities

Internal audit reviews shall examine and evaluate the adequacy and effectiveness of the Council's governance, risk management, and internal control processes. This shall be achieved via:

Assurance activities: *results of which will influence the opinion on the adequacy and effectiveness of the control environment.*

Risk based system audit reviews. The documentation, evaluation and testing of financial, operational and management information systems.

Thematic corporate reviews (potentially across all Services)

Risk Register specific risk

Information technology reviews. Specialist evaluation of hardware, software and the IT environment.

Fundamental financial systems. Reviews focusing on agreed key controls.

Follow up reviews focussing on revisiting an area or system previously found to have control weaknesses.

Light-touch agile reviews on areas where a full systems review may not be necessary. These do not preclude the review developing into a full system review.

Advisory activities: *results of which will contribute to the opinion on the adequacy and effectiveness of the control environment.*

Systems & processes. Control advice on new and developing systems.

Consulting services. Reviews at the request of management, that add value and improve governance, risk management and control processes and support management in their work.

Performance improvement. The economy, efficiency and effectiveness of business systems and processes.

Shared services

Where the Council provides 'shared services' to, or receives 'shared services' from other organisations, the IAM shall liaise with the other organisations IAS and agree the scope of the assurance that is to be provided or received and take account of that requirement when preparing the annual audit plan.

8. Reporting and Monitoring

Internal Audit Reports

At the conclusion of a review, a written report will be issued to the appropriate manager, that will
- include an overall assurance opinion, but not provide absolute assurance, on the adequacy of the governance, risk and control processes;
- identify inadequately addressed risks and non-effective control processes;
- detail agreed corrective action and timescales for implementation;
- identify issues of good practice

When corrective action has not been agreed, reporting will be escalated to a level consistent with the IAM's assessment of the risk.

The IAM shall regularly review and report to senior management, the progress made by managers in introducing the agreed corrective actions. Senior Management are responsible for ensuring that agreed corrective actions are introduced.

Reporting to the Corporate Governance Committee

The CGC will be provided with periodic updates on the work of the IAS. The updates shall cover significant findings and actions and provide information on the status of the agreed audit work plan. Amendments and revisions to the audit plan shall also be reported and agreed by the CGC.

Full copies of closed internal audit reports will be issued to CGC members on a quarterly basis.

The IAM shall present an annual report to the CGC that meets the requirements of the PSIAS. The annual report shall be timed to support the Council's annual statement of assurance on corporate governance and include an opinion on the overall adequacy and effectiveness of the control environment.

9. Quality and assurance programme

The IAM shall maintain a quality assurance and improvement programme that meets the requirements of the PSIAS. The results shall be reported to senior management and the CGC.

The IAM will arrange for an independent review of the efficiency and effectiveness of the internal audit service to be undertaken at least once every five years. The results of the review will be reported to senior management and the CGC.

Improvement plans arising from periodic reviews of internal audit shall be prepared as appropriate and reported to senior management and the CGC in the Internal Audit annual report.

10. Relationships with external audit and other assurance activities

Internal Audit will establish and maintain an open relationship with the external auditor and other assurance providers. Internal audit will plan its activity so that there is adequacy of audit coverage and to minimise duplication of assurance effort. However, the work of Internal Audit will not be driven by external audit's own priorities.

External audit will have full and free access to all internal audit strategies, plans, working papers and reports.

11. Review of the Charter

The IAM will review the Internal Audit Charter each year and report the outcome of that review to the CGC. Approval of the Charter shall be the responsibility of the CGC. This version was approved on the 27 April 2022.

Version: March 2022
Next review date: March 2023
Officer responsible for review: Internal Audit Manager
Approval: Corporate Governance Committee

This page is intentionally left blank