AUDIT COMMITTEE

15 September 2022

7.00 pm

Rooms 201 and 202, Annexe, Town Hall, Watford

Contact
Laura MacMillan
democraticservices@watford.gov.uk
01923 278306

For information about attending meetings please visit the council's website.

Publication date: 7 September 2022

Committee Membership

Councillor M Hofman (Chair)
Councillor M Devonish (Vice-Chair)
Councillors K Clarke-Taylor, L Nembhard and M Turmaine

Agenda

Part A - Open to the Public

1. **Apologies for Absence/Committee Membership**

2. **Disclosure of Interests (if any)**

3. **Minutes**

   The minutes of the meeting held on 28 July 2022 to be submitted and signed.

4. **RIPA Update** (Pages 3 - 36)

   Report of the Group Head of Democracy and Governance

5. **Statement of Accounts Update** (Pages 37 - 41)

   Report of the Head of Finance

6. **External Auditor update**

   The committee to receive a presentation.

7. **Shared Internal Audit Services (SIAS) Annual Report 2021/22** (Pages 42 - 54)

   Report of the Shared Internal Audit Service

8. **Shared Internal Audit Service Progress report 2022/23** (Pages 55 - 84)

   Report of the Shared Internal Audit Service

Part A

Report to: **Audit Committee**

Date of meeting: **Thursday, 15 September 2022**

Report author: **Group Head of Democracy and Governance**

Title: **RIPA Update**

1.0 Summary

1.1 This Committee is responsible for oversight of the council's use of the Regulation of Investigatory Powers Act (RIPA).

1.2 To note that since the last report in March 2019 the council has not requested any authorisations under the Act.

2.0 Risks

2.1

Nature of risk	**Consequence**	**Suggested Control Measures**	**Response** (treat, tolerate, terminate or transfer)	**Risk Rating** (combination of severity and likelihood)
Officers fail to apply for RIPA authorisation as required by the Act	The evidence collected using directed surveillance will be inadmissible and could result in a failure to convict	Officers are trained in RIPA	treat	2

3.0 Recommendations

3.1 The Committee notes that no RIPA authorisations have been made for the financial years 2019/20, 2020/21 and 2021/22.

Further information:
Carol Chen
carol.chen@watford.gov.uk
Tel: 01923 278350

4.0 **Detailed proposal**

4.1 This Committee oversees the council's use of RIPA. Since the restrictions imposed on councils on the use of RIPA by the Protection of Freedoms Act, which limited the ability to undertake directed surveillance to offences where the penalty was six months or more imprisonment or selling alcohol or tobacco to children, and the need to get approval from a magistrate where it was applicable, the council mow rarely uses the powers.

4.2 Since the last report to this Committee in March 2019 no authorisations have been requested.

4.3 RIPA training was undertaken by officers who are able to grant authorisations under the RIPA policy in July 2021.

4.4 The RIPA policy has been regularly reviewed since 2019 and the changes to the senior management structure have been reflected in title changes to authorising officers. A copy of the policy is attached as appendix 1 for information.

5.0 **Implications**

5.1 **Financial**

5.1.1 The Shared Director of Finance comments that there are no financial implications in this report

5.2 **Legal Issues** (Monitoring Officer)

5.2.1 The Group Head of Democracy and Governance comments that there are no legal implications in this report

5.3 **Equalities, Human Rights and Data Protection**

5.3.1 It is a requirement of considering any application for authorisation under RIPA to have regard to the human rights of those likely to be subject of the surveillance as well as any one indirectly affected and any collateral intrusion.

Appendices

- Appendix 1 RIPA Policy 2022

Background papers

No papers were used in the preparation of this report.

CORPORATE POLICY & PROCEDURES DOCUMENT FOR COVERT SURVEILLANCE AND THE USE OF COVERT HUMAN INTELLIGENCE SOURCES

AUTHOR: CAROL CHEN, GROUP HEAD OF DEMOCRACY AND GOVERNANCE, EXT 8350

FIRST PUBLISHED: 2010

REVIEWED 2011

REVIEWED AND UPDATED NOVEMBER 2012

REVIEWED AND UPDATED MARCH 2014

REVIEWED AND UPDATED SEPTEMBER 2014

REVIEWED AND UPDATED MARCH 2016

REVIEWED AND UPDATED MARCH 2018.

REVIEWED AND UPDATED MAY 2018

REVIEWED AND UPDATED JULY 2018

REVIEWED AND UPDATED OCTOBER 2018

REVIEWED AND UPDATED NOVEMBER 2018

REVIEWED AND UPDATED FEBRUARY 2020

REVIEWED AND UPDATED MARCH 2021

REVIEWED AND UPDATED JANUARY 2022

CONTENTS PAGE

NB:
The Regulation of Investigatory Powers Act 2000 ('RIPA') refers to 'Designated Officers'. For ease of understanding and application within Watford Borough Council, this Corporate Policy & Procedures Document refers to 'Authorising Officers'. Furthermore, such Officers can only act under RIPA if they have been duly certified by the Council's Group Head of Democracy and Governance. For the avoidance of doubt, therefore, all references to duly certified Authorising Officers refer to 'Designated Officers' under RIPA.

A. Introduction and Key Messages

1. This Corporate Policy & Procedures Document is based upon the requirements of The Regulation of Investigatory Powers Act 2000 ('RIPA'), The Protection of Freedoms Act 2012 and Codes of Practice issued by the Home Office pursuant to Section 71 of RIPA. The authoritative position on RIPA is, of course, the Act itself, regulations and the Home Office's Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources. Any officer who is unsure about any aspect of this document should contact, at the earliest possible opportunity, the Council's Group Head of Democracy and Governance, for advice and assistance. The Codes of Practice and guidance can be downloaded from the Home Office web site.

2. This document and the related forms can be found on the Council's Intranet.

3. The Council will maintain, and the Group Head of Democracy and Governance will check, the Corporate Register of all RIPA authorisations, reviews, renewals, cancellations and rejections. It is the responsibility of the relevant Authorising Officer, however, to place all RIPA authorisations, reviews, renewals, cancellations and rejections on the Corporate Register within 1 week of the relevant authorisation, review, renewal, cancellation or rejection.

4. Officers who undertake surveillance or who manage CHIS's and Authorising Officers have the responsibility of reporting to the Group Head of Democracy and Governance any situations where direct surveillance or CHIS activity has been undertaken without having obtained the appropriate authority/warrant within one working day of the event having been brought to their attention. It will be the responsibility of the Group Head of Democracy and Governance to investigate and to report the matter to the Investigatory Powers Commissioner no later than 10 working days from the date the event occurred.

5. RIPA, the Protections of Freedoms Act Regulations, the Codes of Practice and this document are important for the effective and efficient operation of the Council's actions with regard to covert surveillance and Covert Human Intelligence Sources. This document will, therefore, be kept under review by the Group Head of Democracy and Governance. Authorising Officers must bring any suggestions for continuous improvement of this document to the attention of the Group Head of Democracy and Governance at the earliest possible opportunity.

6. If you are in any doubt on RIPA, the Codes of Practice, this document or the related legislative provisions, please consult the Group Head of Democracy and Governance.

7. Local Authorities investigating criminal offences have powers to gain access to communications data – that is, information held by telecommunications or postal

service providers about the use of their services by persons who are the subject of criminal investigations. In using such powers, officers must always have regard to the Home Office Guidance –Acquisition and Disclosure of Communication Data Code. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf .The Council belongs to NAFN who will obtain such communications data on the provision of appropriate authorisation.

8. The Council has had regard to the Codes of practice produced by the Home Office in preparing this guidance. If any doubt arises, the Home Office Code of practice should be consulted.
CHIS and Covert Surveillance Codes of Practice:
https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

In addition further guidance in respect of the judicial approval process and the crime threshold has been issued by the Home Office:-
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

Furthermore the Investigatory Powers Commissioners procedures guidance can be found on the shared network under Regulation of Investigatory Powers Act. This guidance is available to all those who need to access in order to apply for and to grant authorisations for covert activities. It is also available to those who have oversight or other management responsibilities associated with the use of covert tactics. This document MUST NOT be published on the internet or through any other type of publicly available media.

B. Borough Council Policy Statement

1. The Council takes seriously its statutory responsibilities under the Regulation of Investigatory Powers Act 2000, and will at all times act in accordance with the law, and take necessary and proportionate action in these types of enforcement matters involving the use of covert surveillance. In that regard, the Group Head of Democracy and Governance, is duly authorised by the Council's Leadership Board as the Council's 'Senior Responsible Officer' with responsibility to keep this document up to date and to amend, delete, add or substitute relevant provisions, as necessary.

C. General Information on RIPA

1. The Human Rights Act 1998 (which incorporated the European Convention on Human Rights into UK law) requires the Council, and organisations working on its behalf, to respect the private and family life of the citizen, his/her home and his/her correspondence.

2. This is not an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council, as a Relevant Public Authority under RIPA, may interfere in the citizen's right to privacy mentioned above, if such interference is: -

   (a) **in accordance with the law;**

   (a) **necessary** (as defined in this document); **and**

   (b) **proportionate** (as defined in this document).

3. Local authorities can only authorise the use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment **or** are related to the underage sale of alcohol and tobacco or nicotine inhaling products.
   Local authorities **cannot** authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment.
   Local authorities are no longer able to orally authorise the use of RIPA techniques.
   All authorisations must be made in writing and require JP (Magistrates) approval.
   (See chapter 4 para 4.42 to 4.47 of the Home Office Covert Surveillance and Property Interference Revised Code of Practice, August 2018).

   Directed surveillance is covert surveillance that is not intrusive and is carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person (other than by way of an immediate response to events or circumstances such that it is not reasonably practicable to seek authorisation under RIPA). *(See chapter E below).*
   Local authorities can only use RIPA in relation to their 'core functions' i.e, the 'specific public functions' undertaken by a particular authority in contrast to the 'ordinary functions' undertaken by all authorities (e.g. employment issues). *(See chapter E, section 15, below).*

   The internet may be used for intelligence gathering and/or as a surveillance tool. Local authority officers covertly conducting online monitoring or investigations (including Social Media) for the purpose of a specific investigation or operation which is likely to result in the obtaining of private information about a person or group need to consider if authorisation for directed surveillance under RIPA is required, if RIPA applies.
   (See chapter E, section 11, below, this includes details of when CHIS authorisation may be needed for online activity)

4. RIPA provides a statutory mechanism for authorising **covert surveillance** and the use of a **'covert human intelligence source' ('CHIS').** A CHIS is a person used by the Council to establish or maintain a personal or other relationship with another person for the covert purpose of obtaining information (e.g. undercover agents). RIPA seeks to ensure that any interference with an individual's right under the Human Rights Act 1998 is **necessary** and **proportionate**. In doing so, RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

5. Directly employed Council staff and external agencies working for the Council are covered by RIPA for the time they are working for the Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Council's behalf must be properly authorised by one of the Council's designated Authorising Officers. Authorising Officers are those whose posts appear in **Appendix 1** to this document and, duly added to or substituted by the Group Head of Democracy and Governance.

6. If the correct RIPA procedures are not followed, evidence may be disallowed by the courts, the matter must be reported by the Group Head of Democracy and Governance to the Investigatory Powers Commissioner, a complaint of maladministration could be made to the Local Government and Social Care Ombudsman, and/or the Council could be ordered to pay compensation. Such action would, of course, harm the reputation of the Council and will, undoubtedly, be the subject of adverse press and media interest. It is essential, therefore, that all Council staff involved with RIPA comply with this document and any further guidance that may be issued, from time to time, by the Group Head of Democracy and Governance.

7. A flowchart of the procedures to be followed appears at **Appendix 2**.

8. **Necessity and proportionality**

   8.1 The authorising officer must believe that the surveillance activities which are being authorised are **necessary for the purpose of preventing or detecting crime, and that the offence being investigated is one either punishable by at least 6 months imprisonment or one related to the underage sale of alcohol, tobacco or nicotine inhaling products.** This is the only statutory ground available for local authorities for the use of covert surveillance. The authorising officer must also believe that the surveillance activities are **proportionate** to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the person who is the subject of the operation (or any other person who may be affected) against the need for the surveillance in investigative and operational terms.

   8.2 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate.

8.3 The following elements of proportionality should therefore be considered:

- Balancing the size and scope of the proposed activity and the potential intrusion into the subject's personal life against the gravity and extent of the perceived crime or offence;

- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Considering whether the activity is an appropriate use of RIPA and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;

- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not used

9. **Collateral intrusion**

Before authorising applications for directed surveillance, the authorising officer should also take into account the risk of obtaining private information about persons who are not the subjects of the surveillance (members of the subject's family for example). This is referred to as collateral intrusion. All applications should include an assessment of the risk of collateral intrusion and details of any measures taken to limit this. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance. The authorising officer must therefore consider fully the proportionality of the proposed actions.

10. **Magistrates Approval**

Before any authorisation for directed surveillance can be implemented the authorising officer must obtain the approval of a Justice of the Peace.

D. What RIPA Does and Does Not Do

1. **RIPA does**:

- Require prior authorisation, from the Council's authorising officer and Magistrate's Court, of directed surveillance.

- Prohibit the Council from carrying out intrusive surveillance.

- Require authorisation of the conduct and use of a CHIS

- Require safeguards for the conduct and use of a CHIS.

2. **RIPA does not**:

- Prejudice or dis-apply any existing powers available to the Council to obtain information by any means not involving conduct that may be authorised under RIPA. For example, it does not affect the Council's current powers to obtain information via the DVLA or to get information from the Land Registry as to the ownership of a property.

3. If the authorising officer or any applicant is in any doubt, s/he should ask the Group Head of Democracy and Governance BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

E. Types of Surveillance

1. **'Surveillance'** includes:

- Monitoring, observing or listening to persons, their movements, conversations, or other activities or communications, including online and social media activities.
- Recording any information obtained in the course of authorised surveillance.
- Surveillance, by or with, the assistance of appropriate and approved surveillance device(s).

Surveillance can be overt or covert.

2. **Overt Surveillance**

Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, Officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. the Park Rangers patrolling the Parks).

3. Similarly, surveillance will be overt if the subject has been told it will happen e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the owner/proprietor to check that the conditions are being met.

4. **Covert Surveillance**

Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place. (Section 26(9)(a) of RIPA).

5. RIPA regulates directed surveillance, intrusive surveillance (the Council cannot carry out **intrusive surveillance**) and the use of Covert Human Intelligence Sources (CHIS).

6. **Directed Surveillance**

Directed Surveillance is surveillance which: -

- is covert; and
- is not intrusive surveillance (see definition below – **the Council must not carry out any intrusive surveillance**);
- is not carried out in an immediate response to events which would otherwise make seeking authorisation under RIPA unreasonable, e.g. spotting something suspicious and continuing to observe it; and
- it is undertaken for the purpose of a **specific investigation** or operation in a manner **likely to obtain private information** about an individual (whether or not that person is specifically targeted for purposes of an investigation). (*Section 26(10) of RIPA).*

7. **Private information**

The 2000 Act states that private information includes any information relating to a person's private or family life. As a result, private information is capable of including any aspect of a person's private or personal relationship with others, such as family and professional or business relationships. Information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public. Non-private data will also include the attributes of inanimate objects such as the class to which a cargo ship belongs.

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable

expectation of privacy even though acting in public and where a record is being made by the Council of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites. See section 11 below for further guidance about the use of the internet as a surveillance tool.

Example: *Two people holding a conversation on the street or in a bus may have a reasonable expectation of privacy over the contents of that conversation, even though they are associating in public. The contents of such a conversation should therefore still be considered as private information. A directed surveillance authorisation would therefore be appropriate for the Council to record or listen to the conversation as part of a specific investigation or operation.*

Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance authorisation may be considered appropriate.

Example: *Council officers wish to drive past a café for the purposes of obtaining a photograph of the exterior. Reconnaissance of this nature is not likely to require a directed surveillance authorisation as no private information about any person is likely to be obtained or recorded. However, if the Council wished to repeat the exercise, for example to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person and a directed surveillance authorisation would be required.*

Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that s/he comes into contact, or associates, with.
Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate.

8. Similarly, although overt town centre CCTV cameras do not normally require authorisation, if a particular camera is being used for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others. *(Also see section 16 below).*

9. **Confidential information**

Special consideration must be given to authorisations that involve confidential personal information. Where such material has been acquired and retained, the matter should be reported to the Group Head of Democracy and Governance so that s/he can inform the Investigatory Powers Commissioner's Office (IPCO) or Inspector during his next inspection and the material made available to him if requested.

Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

Examples include consultations between a health professional and a patient, or information from a patient's medical records.

10. For the avoidance of doubt, only those Officers designated and certified to be 'Authorising Officers' and identified in Appendix 1 for the purpose of RIPA can authorise an application for 'Directed Surveillance' if, and only if, the RIPA authorisation procedures detailed in this document are followed.

Only the Chief Executive can authorise applications for covert surveillance when knowledge of confidential information is likely to be acquired.

11. **Online covert activity**

11.1 The growth of the internet, and the extent of the information that is now available online, presents new opportunities for Local Authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that Local Authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist council officers in identifying when such authorisations may be appropriate.

11.2 The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of

private information about a person or group, an authorisation for directed surveillance should be considered.
Where a person acting on behalf of the Council is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed *(paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).*

11.3 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where the Council has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

11.4 As set out in paragraph 11.5 below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

11.5 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by the Council of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

11.6 Whether the Council interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is

unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where the Council is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online. *(See section 7 above)*.

Example 1: *A council officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.*

Example 2: *A council officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)*

Example 3: *The Council undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.*

11.7 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance in section 7 above);
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;

- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

11.8 Internet searches carried out by a third party on behalf of the Council, or with the use of a search tool, may still require a directed surveillance authorisation.

Example: *Researchers within a local authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by local authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.*

12. **Intrusive Surveillance**

This is when it: -

- is covert;
- relates to anything taking place on residential premises or in any private vehicle;
- and, involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

Residential premises includes any part of premises which are being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation. It includes hotel accommodation. However, common areas to which a

person has access in connection with their use or occupation of accommodation are excluded from the definition of residential premises.

Examples of common areas of residential premises which are excluded would include:

- a communal stairway in a block of flats;
- a hotel reception area or dining room;
- the front garden or driveway of premises readily visible to the public.

A private vehicle is any vehicle which is used primarily for the private purposes of the person who owns it or a person otherwise having the right to use it. This includes, for example, a company car, owned by a leasing company and used for business and pleasure by the employee of a company.

Local authorities are not allowed to carry out intrusive surveillance and therefore no Council officer can authorise a covert surveillance operation if it involves intrusive surveillance as defined above.

13. **Where authorisation is not required**

Some surveillance activity does not constitute directed surveillance under RIPA and no directed surveillance authorisation can be obtained for such activity. Such activity includes:

- covert surveillance by way of an immediate response to events;
- covert surveillance as part of general observation activities;
- covert surveillance not relating to the statutory grounds specified by RIPA;
- overt use of CCTV
- certain other specific situations (see point 17 below).

14. **Immediate response**

Covert surveillance that is likely to reveal private information about a person but is carried out by way of an immediate response to events such that it is not reasonably practicable to obtain an authorisation under RIPA.

Example: *An authorisation would not be required where Council officers conceal themselves in order to observe an incident that they happen to come across where a person appears to be in the act of illegally dumping waste.*

15. **General observation activities**

The general observation duties of Council officers do not require authorisation under the 2000 Act, whether covert or overt. Such general observation duties frequently form part of the legislative functions of the Council, as opposed to the pre-planned surveillance of a specific person or group of people. General observation duties may include monitoring of publicly accessible areas of the internet in circumstances where it is not part of a specific investigation or operation.

Example 1: *Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A trained employee or person engaged by the Council is deployed to act as a juvenile in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of the Act, that the Council may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment and is not authorised as a CHIS, or an adult is observing, consideration should be given to granting a directed surveillance authorisation.*

Example 2: *Local authority officers attend a car boot sale where it is suspected that counterfeit goods are being sold, but they are not carrying out surveillance of particular individuals and their intention is, through reactive policing, to identify and tackle offenders. Again this is part of the general duties of the Council and the obtaining of private information is unlikely. A directed surveillance authorisation need not be sought.*

16. **Not related to the prevention or detection of crime punishable by 6 months imprisonment or more or related to the underage sale of alcohol, tobacco or nicotine inhaling products.**

In the case of local authorities directed surveillance can only be authorised under RIPA if it is for the purpose of preventing or detecting crime where the offence is punishable by a term of imprisonment of 6 months or more or where it is related to the underage sale of alcohol or tobacco. Covert surveillance for any other general purposes should be conducted under other relevant legislation. A local authority can only use RIPA in relation to its 'core functions' i.e, the 'specific public functions' undertaken by a particular authority in contrast to the 'ordinary functions' undertaken by all authorities (e.g. employment issues).

Example: *A Council employee is off work due, he claims, to an injury sustained at work for which he is suing the Council. The employee's manager suspects the employee is exaggerating the seriousness of their injury and that they are, in fact, fit enough to come*

to work. The manager wishes to place the employee under covert surveillance outside of his normal work environment to establish that he is indeed fit for work and to gather evidence for disciplinary proceedings against the employee for deceiving the Council. Such surveillance, even though likely to result in obtaining private information, does not constitute directed surveillance under RIPA as it does not relate to the Council's core functions. It relates instead to the carrying out of its employment functions which are common to all authorities In order to undertake surveillance of this nature the Council would need to satisfy itself that it would not be contravening the GDPR and Data Protection Act 2018 and the Council's own employment policies.

17. **CCTV**

The use of overt CCTV cameras by the council does not normally require an authorisation under RIPA. Members of the public should be made aware that such systems are in use. For example, by virtue of cameras or signage being clearly visible, through the provision of information and by undertaking consultation. Guidance on their operation is provided in the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 ("the 2012 Act") and overseen by the Surveillance Camera Commissioner. The council should also be aware of the relevant Information Commissioner's code ("In the Picture – A Data Protection Code of Practice for Surveillance Cameras and Personal Information").

The Surveillance Camera code has relevance to overt surveillance camera systems (as defined at s 29(6) of the 2012 Act) and which are operated in public places by the Council. The 2012 Act places a statutory responsibility upon the Council, to have regard to the provisions of the Surveillance Camera code, where surveillance is conducted overtly by means of a surveillance camera system in a public place in England and Wales.

The Surveillance Camera code sets out a framework of good practice that includes existing legal obligations, including the processing of personal data under the Data Protection Act 2018 and the councils duty to adhere to the Human Rights Act 1998.

Example: *Overt surveillance equipment, such as town centre CCTV systems, is used to gather information as part of a reactive operation (e.g. to identify individuals who have committed criminal damage after the event). Such use does not amount to covert surveillance as the equipment was overt and not subject to any covert targeting. Use in these circumstances would not require a directed surveillance authorisation.*

However, where overt CCTV or other overt surveillance cameras are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people, a directed surveillance authorisation should be considered. Such covert surveillance is likely to result in the obtaining of

private information about a person (namely, a record of their movements and activities) and therefore falls properly within the definition of directed surveillance. The use of the CCTV or other overt surveillance cameras in these circumstances goes beyond their intended use for the general prevention or detection of crime and protection of the public.

Example: *A local police team receive information that an individual suspected of committing thefts from motor vehicles is known to be in a town centre area. A decision is taken to use the town centre CCTV system to conduct surveillance against that individual, such that he remains unaware that there may be any specific interest in him. This targeted, covert use of the overt town centre CCTV system to monitor and/or record that individual's movements should be considered for authorisation as directed surveillance.*

18. **Specific situations where authorisation is not available**

There are a number of specific situations which do not require an authorisation under RIPA. The specific situations most relevant to the Council are –

- the overt or covert recording of an interview with a member of the public where it is made clear that the interview is entirely voluntary and that the interviewer is a Council officer. In such circumstances, whether the recording equipment is overt or covert, the member of the public knows that they are being interviewed by a Council Officer and that information gleaned through the interview has passed into the possession of the council;

- the covert recording of suspected noise nuisance where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear. In the latter circumstance, the perpetrator would normally be regarded as having forfeited any claim to privacy.

19. ***Examples of different types of Surveillance***

Type of Surveillance	**Examples**

Overt	- Police Officer on patrol - Signposted Town Centre CCTV cameras (in normal use) - Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. - Most test purchases (where the officer behaves no differently from a normal member of the public).
Covert but not requiring prior authorisation	- CCTV cameras providing general traffic, crime or public safety information.
Directed (this is also covert) must be RIPA authorised. This includes relevant online covert activity.	- Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit; where the offence they are investigating is punishable by a term of imprisonment of 6 months or more. - Test purchases where the officer has a hidden camera or other recording device to record information which might include information about the private life of a shop-owner, e.g. where s/he is suspected of selling alcohol or tobacco to underage customers.
Intrusive – **Council cannot do this!**	- Planting a listening or other device (bug) in a person's home or in their private vehicle.

F. Conduct and Use of a Covert Human Intelligence Source (CHIS)

Who is a CHIS?

1. Someone who establishes or maintains a personal or other relationship for the covert purpose of helping the covert use of the relationship to obtain information. **In normal circumstances the Council will not consider the conduct or use a CHIS. If consideration is given to the conduct or use of a CHIS the Group Head of Democracy and Governance must be consulted first. The Council may seek the assistance of the Police to manage the CHIS**

2. The Council is not required by RIPA to seek or obtain an authorisation just because one is available (see section 80 of RIPA). The use or conduct of a CHIS, however, can be a particularly intrusive and high risk covert technique, requiring dedicated and sufficient resources, oversight and management. Authorisation is therefore advisable where the Council intends to task someone to act as a CHIS, or where it is believed an individual is

acting in that capacity and it is intended to obtain information from them accordingly. The Council must ensure that all use or conduct is:

- necessary and proportionate to the intelligence dividend that it seeks to achieve;
- in compliance with relevant Articles of the European Convention on Human Rights (ECHR), particularly Articles 6 and 8.

3. RIPA does not apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information.

4. Watford BC does not normally ask informants to gather information on the Councils behalf as this may result in the informant forming a relationship with a subject; which could result in the informant becoming a CHIS.

What must be authorised?

5. The conduct or use of a CHIS requires prior authorisation.

- **Conduct** of a CHIS = Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information.

- **Use** of a CHIS = Actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

6. **If a CHIS is used the RIPA procedures, detailed in this document, must be followed, including obtaining the approval of a Justice of the Peace.**
7. **Council Officers, and authorising officers, need to be clear that Online covert activity may also require the conduct and use of a CHIS. *(See chapter E, section 11, para 11.2).***

Juvenile Sources

8. Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 year olds). On no occasion can a child under 16 years of age be authorised to give information against his or her parents.

Only the Chief Executive or, in his or her absence, the Director of Finance or Monitoring Officer can authorise the use of Juvenile Sources, again such authorisation must be approved by a Justice of the Peace.

Vulnerable Individuals

9. A 'vulnerable individual' is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take

care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.

10. A vulnerable individual will only be authorised to act as a source in the most exceptional of circumstances.

Only the Chief Executive or, in his or her absence, the Director of Finance or Monitoring Officer can authorise the use of vulnerable individuals, again such authorisation must be approved by a Justice of the Peace.

Test Purchases

11. Carrying out test purchases will not (as highlighted above) require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

12. By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products) will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and also directed surveillance.

Anti-social behaviour activities (e.g. noise, violence, etc)

13. Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

14. Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to record if the noisemaker is warned (preferably in writing) that this will occur if the level of noise continues.

G. Authorising Officer Responsibilities

1. The Group Head of Democracy and Governance will ensure that sufficient numbers of Authorising Officers are duly certified under this policy.

2. It will be the responsibility of Authorising Officers who have been duly certified to ensure their relevant members of staff are suitably trained as 'Applicants' so as to avoid common mistakes appearing on forms for RIPA authorisations.

3. Authorising Officers will also ensure that staff who report to them are familiar with this policy and that they do not undertake or carry out any form of surveillance without first complying with the requirements of this document.
4. Authorising Officers must also pay particular attention to any health and safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should an Authorising Officer approve any RIPA application unless, and until s/he is satisfied that a proper risk assessment has been carried out and the health and safety of Council employees/agents are suitably addressed and/or risks minimised, so far as is possible. If an Authorising Officer is in any doubt, s/he should obtain prior guidance on the same from his/her manager, the Council's Corporate Health & Safety Adviser or the Group Head of Democracy and Governance.

5. Authorising Officers must obtain authorisation from a Justice of the Peace (Magistrate) before any Directed Surveillance, or the conduct or use of a CHIS, can be undertaken.

H. Authorisation Procedures

1. Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation. **Appendix 2** provides a flow chart of process from application consideration to recording of information.

Authorising Officers

2. Forms can only be signed by the Authorising Officers set out in **Appendix 1**.

Only the Chief Executive or, in his or her absence, the Director of Finance or Monitoring Officer can authorise an application for directed surveillance when confidential information is likely to be acquired.

Appendix 1 will be kept up to date by the Group Head of Democracy and Governance, and added to as needs require. If a Chief Officer wishes to add, delete or substitute a post, s/he must refer such request to the Group Head of Democracy and Governance for consideration, as necessary. The Group Head of Democracy and Governance is authorised to add, delete or substitute posts listed in **Appendix 1**.

3. Authorisations under RIPA are separate from delegated authority to act under the Council's Constitution. RIPA authorisations are for specific investigations only, and must be renewed or cancelled once the specific surveillance is complete or about to expire. **The authorisations do <u>not</u> lapse with time!**

4. The Group Head of Democracy and Governance will monitor applications recorded on the central register

<u>Application Forms</u>

5. Only the approved RIPA forms named in this document, and found on the Council's intranet, must be used. Any other forms will be rejected by the Authorising Officer.

6. **<u>Directed Surveillance and use of Covert Human Intelligence forms – See Appendix 3</u>**

Form RIP 1	**Application** for Authority for Directed Surveillance
Form RIP 2	**Renewal** of Directed Surveillance Authority
Form RIP 3	**Cancellation** of Directed Surveillance
Form RIP 4	**Review** of Directed Surveillance
Form RIP 5	**Application** for use of Covert Human Intelligence Source
Form RIP 6	**Renewal** of authorisation for use of Covert Human Intelligence Source
Form RIP 7	**Cancellation** of Covert Human Intelligence Source
Form RIP 8	**Review** of use of Covert Human Intelligence Source

<u>Grounds for Authorisation</u>

7. Directed Surveillance (form RIP 1) can be authorised by the Council only on the following ground: -

- To prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment **or** are related to the underage sale of alcohol and tobacco or nicotine inhaling products.

<u>Assessing the Application Form</u>

8. Before an Authorising Officer signs a Form, **s/he must**: -

(a) Have due regard for RIPA, the Home Office Codes of Practice, the Human Rights Act 1998, this Policy and any other guidance issued, from time to time, by the Group Head of Democracy and Governance on such matters;

(b) Satisfy his/herself that the RIPA authorisation is: -

(i) **in accordance with the law**;

(ii) **necessary** in the circumstances of the particular case on the grounds mentioned above; **and**

(iii) **proportionate** to what it seeks to achieve.

(c) 'Proportionate' means the Authorising Officer must believe that intruding upon someone's privacy through surveillance is proportionate to the desired outcome taking into account the size of the problem as against the breach of privacy

In assessing whether or not the proposed surveillance is proportionate, the Authorising Officer must be satisfied that the application form demonstrates that every other reasonable means of gathering the information has been considered and explains why the alternative means considered would not be likely to achieve the desired outcome. The Authorising Officer must also be satisfied that the proposed method of surveillance is the least intrusive.

The proportionality test is explained in more detail in Section C paragraph 8.

The Authorising Officer must in each case follow the "five Ws" (i.e, who, what, where, when and why) incorporated into the forms to make clear what is being authorised. They must also explain how and why they are satisfied that the proposed action is both **necessary** and **proportionate**. It is not enough simply to state that it is so – the reasons **why** it is so must be given.

Every question on the application form must be dealt with fully, following the prompts which are now incorporated in the forms.

(d) Take into account the risk of accidental intrusion into the privacy of persons other than the specified subject of the surveillance (**Collateral Intrusion**). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion and the matter may be an aspect of determining proportionality;

(e) Set a date for review of the authorisation and enter it on the Central Register. The Authorising Officer is responsible for ensuring that key dates are adhered to.

(f) Allocate a Unique Reference Number (URN) for the application as follows: -. Year / Service / Number of Application.

(g) Seek approval to the authorisation from a Justice of the Peace (Magistrate).

(h) Ensure that any RIPA Service Register is duly completed, and that a copy of the RIPA Forms (and any review/cancellation of the same) are recorded on the Corporate Central Register, **within 1 week of the relevant authorisation, review, renewal, cancellation or rejection**.

Additional Safeguards when Authorising a CHIS

9. When authorising the conduct or use of a CHIS, the Authorising Officer **must also: -**

(a) be satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved;

(b) be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS and this must address health and safety issues and any risk to the CHIS arising should their role in the investigation be revealed through a risk assessment;

(c) consider the likely degree of intrusion of all those potentially affected;

(d) consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and

(e) ensure **records** containing particulars are not available except on a need to know basis.

(f) **The requirements of s29(5) RIPA and the Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI:2000/2725) must be considered and applied when authorising the use of a CHIS. Contact the Group Head of Democracy and Governance for advice on the requirements if required.**

Duration

10. The authorisation **must be reviewed in the time stated (which can be any time stated in the application) and cancelled** once it is no longer needed. The 'authorisation' to carry out/conduct the surveillance lasts for a maximum of 3 months (from authorisation) for Directed Surveillance and 12 months (from authorisation) for a CHIS (or 4 months for a juvenile CHIS). However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the 'authorisation' is 'spent'. In other words, **the Forms do not expire and remain 'live' until cancelled!** The forms must be reviewed and/or cancelled (once they are no longer required)!

11. Authorisations can be renewed in writing when the maximum period has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred. The Authorising Officer must still be satisfied that the surveillance is still necessary and proportionate.

12. A renewal must be approved by a Justice of the Peace in the same way as an original application.

I. Working With / Through Other Agencies

1. When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and the forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

2. When some other agency (e.g. Police, HMRC, Home Office, etc): -

   (a) wish to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes, s/he must obtain a copy of that agency's RIPA authorisation for the record (a copy of which must be passed to the Group Head of Democracy and Governance for the Central Register) and/or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources;

   (b) wish to use the Council's premises for their own RIPA action, the officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the Council's co-operation in the agent's RIPA operation. In such cases, however, the Council's own RIPA forms should not be used as the Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.

3. In terms of 2(a), if the Police or other Agency wish to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the Police or other Agency before any Council resources are made available for the proposed use.

4. **If in doubt, please consult with the Group Head of Democracy and Governance at the earliest opportunity.**

J. Record Management

1. **The Council must keep a detailed record of all authorisations, renewals, cancellations rejections, and errors and a Central Register of all Authorisation Forms will be maintained and will be monitored by the Group Head of Democracy and Governance.**

2. **Records Maintained**

The following documents must be retained by the each Authorising Officer for such purposes.

- a copy of the forms together with any supplementary documentation and notification of the approval given by the Authorising Officer and warrant obtained from the Magistrate; To include the date the authorisation and warrant granted and the name and job title of the authorising officer. A brief description of the investigation and the names of those being surveilled if known
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation and warrant obtained from the Magistrate, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the Authorising Officer;
- Date authorisation cancelled
- Date of any refusal to grant and authorisation.
- Any errors (i.e. failures to obtain an authorisation when one was required)
- the Unique Reference Number for the authorisation (URN).

3. Each form will have a URN. The Authorising Officer will issue the relevant URN to Applicants. The cross-referencing of each URN takes place within the forms for inspection purposes. Rejected forms will also have URN's.

Central Register maintained by the Monitoring Officer

4. Authorising Officers must place details of each application on the Central Register, within 1 week of the authorisation, review, renewal, cancellation or rejection. The Group Head

of Democracy and Governance will monitor the same and give appropriate guidance, from time to time, or amend this document, as necessary.

5. The Council will retain records for a period of at least five years from the ending of the authorisation. The Investigatory Powers Commissioner (IPC) can inspect the Council's policies and procedures, and individual authorisations.

6. Any errors, that is, failures to obtain authorisation when an authorisation should have been obtained, need to be notified to the Group Head of Democracy and Governance within one working day of it becoming apparent that an error has been made. They should also be logged on the central register. The Group Head of Democracy and Governance will investigate and will no later than 10 working days after the error having become apparent will notify the Investigatory Powers Commissioner.

7. The Group Head of Democracy and Governance will undertake a regular review of all errors and provide advice and guidance on how to avoid continuing occurrences.

Retention and Destruction of Evidence

8. Where evidence gathered from surveillance could be relevant to future or pending court proceedings, it should be retained in accordance with established disclosure requirements for a suitable period, commensurate to any subsequent review. Particular attention should be paid to the Criminal Procedure and Investigations Act 1996 which requires evidence gathered in criminal investigations to be recorded and retained.

9. All private information obtained during the course of a directed surveillance should be maintained securely and only be made available to officers entitled to view it in order to undertake their investigation, or for the purposes of conducting criminal proceedings. Officers handling private information should familiarize themselves with Home Office codes of practice on the handling of such information;
See chapter 9 of the Covert Surveillance and Property Interference Code of Practice, and chapter 8 of the Covert Human Intelligence Sources Code of Practice.
https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

K. Concluding Remarks of the Group Head of Democracy and Governance

1. Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure set out in RIPA and this document, may be that the action (and the evidence obtained) will be held to be unlawful by the Courts pursuant to Section 6 of the Human Rights Act 1998.

2. Obtaining an authorisation under RIPA and following this document, will ensure, therefore, that the action is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.

3. Authorising Officers must exercise their minds every time they are asked to sign a form. They must never sign or rubber stamp forms without thinking about their personal and the Council's responsibilities.

4. Any boxes not needed on the form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the same. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and the form retained for future inspections.

5. For further advice and assistance on RIPA, please contact the Council's Group Head of Democracy and Governance (who is also the Council's Monitoring Officer). The Group Head of Democracy and Governance also acts as Senior Responsible Officer (SRO)

Appendix 1 – List of Authorising Officer Posts

Officer	Service area
Chief Executive; (only where confidential information is likely to be acquired, or where it is proposed to use juveniles or vulnerable persons as covert human intelligence sources)	**All**
Director Of Finance;	**All**
Monitoring Officer;	**All**
Head of Finance;	**All**
Fraud Manager Shared Services	**All**
Executive Head Strategy & Initiatives (Sustainability and Culture)	**Community Protection**
Associate Director Housing and Wellbeing	**Community Protection**
Business Compliance Officer	**Community Protection**
Community Protection Manager	**Community Protection**

IMPORTANT NOTES

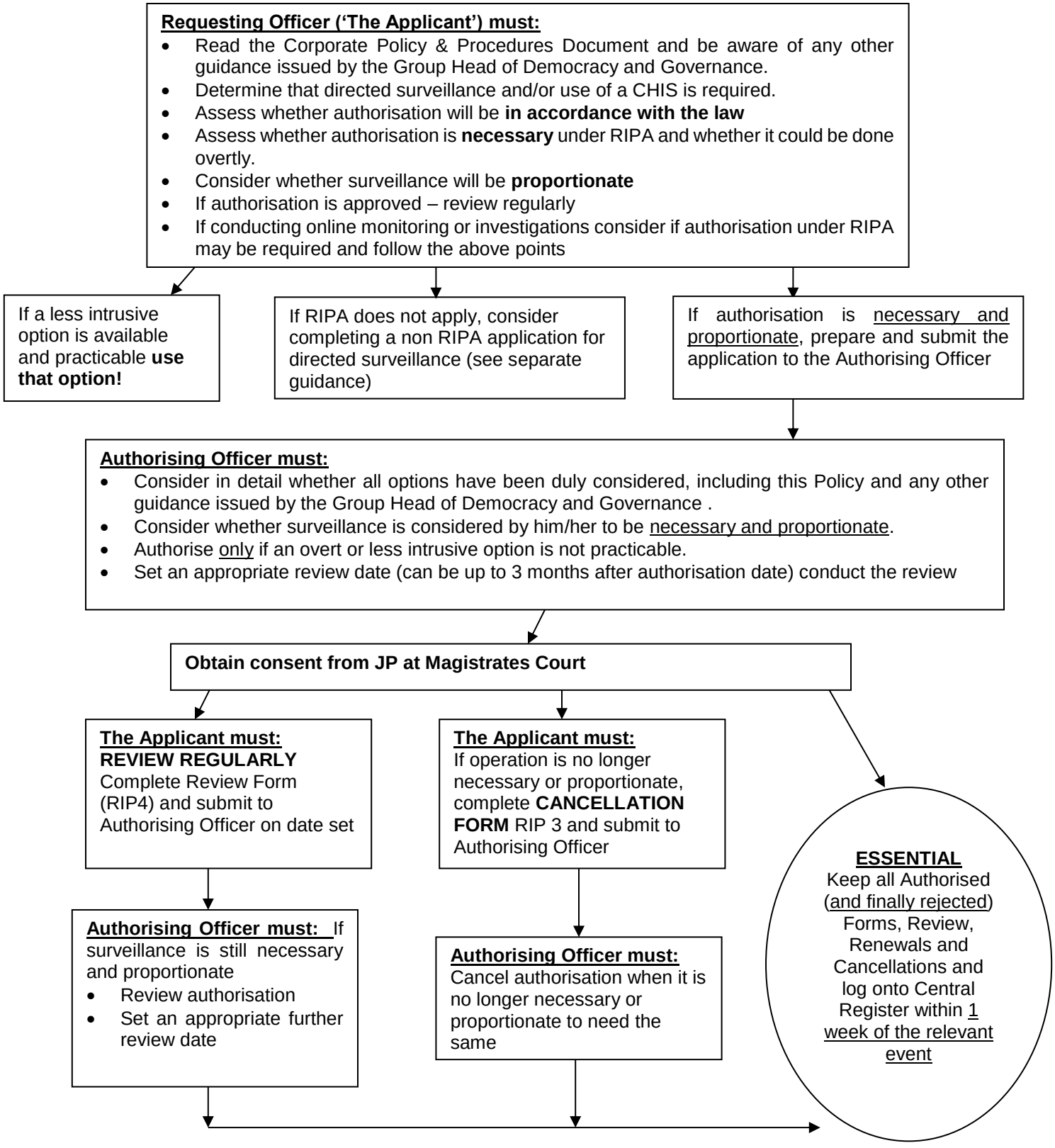
A. Only the Chief Executive and in her absence the Director of Finance or Monitoring Officer is authorised to sign forms relating to Juvenile Sources and Vulnerable Individuals (see paragraph F).

B. If a Chief Officer wishes to add, delete or substitute a post, s/he must refer such request to the Group Head of Democracy and Governance for consideration, as necessary.

C. If in doubt, ask the Group Head of Democracy and Governance BEFORE any directed surveillance and/or CHIS is authorised, renewed, rejected or cancelled.

APPENDIX 2

RIPA APPLICATION FOR COVERT DIRECTED SURVEILLANCE (or use of a CHIS) FLOW CHART



NB: If in doubt, ask the Group Head of Democracy and Governance BEFORE any directed surveillance, and/or CHIS, application is authorised, renewed, cancelled or rejected.

Part A

Report to: **Audit Committee**

Date of meeting: **Thursday, 15 September 2022**

Report author: **Head of Finance**

Title: **Statement of Accounts Update**

1.0 Summary

1.1 This report sets out the latest position for the external audit of the Statement of Accounts for 2019/20, 2020/21 and 2021/22.

2.0 Risks

2.1

Nature of risk	**Consequence**	**Suggested Control Measures**	**Response** (treat, tolerate, terminate or transfer)	**Risk Rating** (combination of severity and likelihood)
The Council's Statement of Accounts are not approved and audited within the statutory timeframe	Failure to comply with statutory timeline impacts on audit opinion	Proactive liaison with the external audit team	Tolerate	4
Changes to accounting policies are not properly reflected in the Statement of Accounts	Material mis-statement or qualification	Review accounting policies annually. Maintain awareness of future changes	Treat	4

Changes to accounting policies have an impact on the revenue budget or capital programme.	Impact on reserves, especially where not identified at budget setting.	Maintain awareness of future changes	Tolerate	6

3.0 **Recommendations**

3.1 To note the latest timetable for completion of the external audit of the statement of accounts for 2019/20, 2020/21 and 2021/22.

Further information:
Hannah Doney
hannah.doney@threerivers.gov.uk

Report approved by:
Alison Scott, Shared Director of Finance

4.0 **Detailed proposal**

4.1 **Statement of Accounts 2019/20**

4.1.1 Officers continue to work with the external auditors, Ernst Young (EY), to progress the outstanding issue in relation to accounting for infrastructure assets. It is expected that the accounts can be signed off by the end of September 2022 subject to completion and review of the final amended draft and following the conclusion of an internal review process within EY.

4.2 **Statement of Accounts 2020/21**

4.2.1 The audit of the Statement of Accounts 2020/21 commenced on 4 July 2022. An update from EY on progress towards concluding the audit is elsewhere on the agenda.

4.2.2 There are two key areas where the Council is reliant on external experts to provide further information in order for EY to conclude their work in these areas. These are:

- Pension Fund Valuation – information required from the Actuary
- Investment Property Valuation – information required from the external valuer

4.2.3 Work will continue to progress the 2020/21 audit during September with the anticipation that it can conclude shortly after the signing of the 2019/20 accounts.

4.2.4 At this stage there have been no significant issues raised with Officers by EY arising from the 2020/21 audit with the majority of agreed changes reflecting findings that have rolled forward from the 2019/20 audit. This is because the original 2020/21 draft accounts, authorised for issue on 31 July 2021, were prepared in advance of concluding the response to the 2019/20 audit findings.

4.3 **Statement of Accounts 2021/22**

4.3.1 The draft Statement of Accounts 2021/22 was authorised for issue by the Director of Finance and published on the Council's website on 31 July 2022 in line with the statutory timeframe. The period of public inspection ran from 1 August to 12 September 2022.

4.3.2 The brought forward balances and comparator figures for 2020/21 will be updated in the draft 2021/22 accounts following the conclusion of the 2020/21 audit. As previously reported to the Committee, the audit of the 2021/22 accounts is expected to commence in January 2023.

4.3.3 Analysis published by Room 151, an online news service, found that only 69% of local authorities met the deadline of 31 July to publish draft accounts with the figure falling to 63% amongst lower tier authorities. This compares to 77% for all authorities and 72% for lower tier authorities for the 2020/21 draft accounts. The fall in compliance reflects continuing challenges across the sector as a result of audit delays and resourcing issues. This is likely to have a knock on impact on compliance with the statutory deadline for the publication of audited accounts by 30 November.

4.4 **Appointment of External Auditors for 2023/24 onwards**

4.4.1 On 24 January 2022, Council agreed to opt into the national procurement for external audit services for the five year period beginning on 1 April 2023, led by Public Sector Audit Appointments Limited (PSAA).

4.4.2 The PSAA issued the invitation to tender on 7 April 2022 and audit firms had until 11 July 2022 to submit responses.

4.4.3 On 24 August 2022 the PSAA confirmed that this process has secured 96.5% of the capacity required to enable auditor appointments to all bodies that have opted into the PSAA's national scheme. A rapid supplementary procurement for four small-sized Lots was launched on 25 August 2022 to secure the remaining capacity needed with an invitation issued to nine registered suppliers that completed pre-qualification checks earlier in the process.

4.4.4 A full statement about the outcome of the procurement is expected in September following the conclusion of the supplementary procurement.

5.0 Implications

5.1 Financial

5.1.1 The Shared Director of Finance comments that there are no direct financial implications arising from this report.

5.2 Legal Issues (Monitoring Officer)

5.2.1 The Group Head of Democracy and Governance comments that the Accounts and Audit Regulations 2015 require councils to undertake an annual review of their governance. The Regulations require that an Annual Governance Statement, prepared to fulfil this requirement, should form part of the Council's Statement of Accounts.

5.3 Equalities, Human Rights and Data Protection

5.3.1 Under s149 (1) of the Equality Act the council must have due regard, in the exercise of its functions, to the need to –

- eliminate discrimination, harassment, victimisation and any other conduct prohibited by the Act
- advance equality of opportunity between persons who share relevant protected characteristics and persons who do not share them
- foster good relations between persons who share relevant protected characteristics and persons who do not share them.

Having had regard to the council's obligations under s149, it is considered that there are no equalities or human rights implications.

5.4 Staffing

5.4.1 There are no staffing implications arising from this report.

5.5 Accommodation

5.5.1 There are no accommodation implications arising from this report.

5.6 Community Safety/Crime and Disorder

5.6.1 There are no community safety/crime and disorder implications arising from this report.

5.7 **Sustainability**

5.7.1 There are no sustainability implications arising from this report.

Background Papers

Statement of Accounts and Annual Governance Statement 2021/22 report to Audit Committee 28 July 2022

Appendices

None

SIAS

Shared Internal Audit Service

Hertfordshire in Partnership

Shared Internal Audit Service

Annual Report

2021/22

Annual Report Contents

Introduction

Welcome to the Shared Internal Audit Service (SIAS) Annual Report for 2021/22.

I recently enjoyed the festivities and celebrations of the Platinum Jubilee weekend, and while investing a little time on my wellbeing and some of the more joyous aspects of life, I was struck by the thought that SIAS was entering its second decade at the heart of internal audit in Hertfordshire. While a long way from emulating the Queen's longevity and achievements, SIAS has certainly experienced its fair share of successes and challenges.

Reading my introduction to last year's Annual Report, I was struck with an acute sense of déjà vu that my paragraphs on the Covid-19 pandemic could so easily be replicated, certainly in the early to mid-part of the year anyway. My wife was stranded abroad for six weeks as the Omicron variant struck, travel restrictions were hastily imposed, and eventually ended up enduring a stay in a quarantine hotel. My young son and I got a whole heap of quality time together! It was most certainly another year defined by the pandemic and our local government partners ongoing response to it, along with mounting challenges posed by multiple strategic migration crises.

In many ways though, we did get back some semblance of normalcy, as children returned to school, fans returned to sports venues, and shops and restaurants reopened. From an internal audit perspective, it meant continuing to improve on remote auditing and evolving flexible and hybrid working practices, managing a team that was often not meeting face to face and maintaining sound relationships with our partners and their teams from afar. I still did not get to enjoy the in-person company and camaraderie of the team and other colleagues as much as I had hoped but look forward to this in the coming year.

Professionally, we opened ourselves up to scrutiny as part of our five yearly external quality assessment in terms of the Public Sector Internal Audit Standards (PSIAS). We not only sort the required opinion on our conformance with the PSIAS but bravely grasped the opportunity to have a 'proper look under the hood' of our service. It is not often that the auditors are thoroughly audited, but I am extremely proud of the team that the assessors concluded that we "are a well-regarded internal audit partnership, delivering professional and quality services to its partner organisations". We developed a comprehensive action plan to address issues identified and have made significant progress in implementing and embedding recommendations that will ensure that we are suitably equipped to meet the challenges of the future.

SIAS also said a sad farewell to team members departing during the year, some as part of an organisational change process, and others to well-earned retirement, or career opportunities elsewhere. All are thanked for their achievements and contribution to the service and will be greatly missed. Departures offer the opportunity for new beginnings, and we welcomed two new trainee auditors, who have settled wonderfully well into the service. Congratulations are also extended to team members for their deserved promotions.

For further highlights and reflections, I invite you to delve into the Annual Report itself. As ever, I enjoy the engagement, dialogue and feedback the report fosters.

Chris Wood - Head of Assurance

June 2022

SIAS
Shared Internal Audit Service
Hertfordshire in Partnership

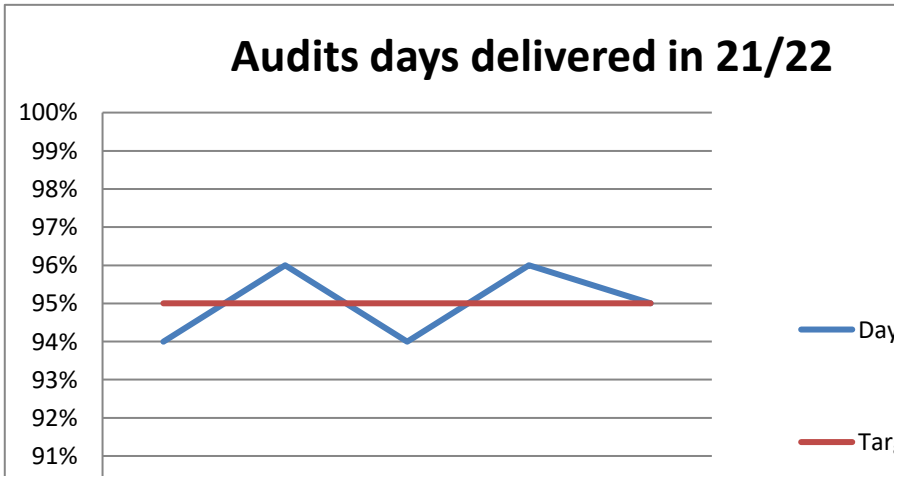
Levels of delivery

2021/22 presented a number of challenges to SIAS in relation to delivering audit plans, with our Partners continuing to progress their response and recovery activities in relation to COVID-19, the emergence of new external pressures arising from political conflict and the EU Transition and the Service undertaking an organisational change process to adapt to the changing commissions from our Partners.

Despite such challenges, SIAS managed to meet the 95% target for delivering days commissioned by clients, with a final outturn of 95%. Whilst our delivery of audit reviews to draft report stage by the close of the year fell 1% short of the target of 95%, we believe the end of year outcomes pay testament to the hard work and resilience of the SIAS Team.

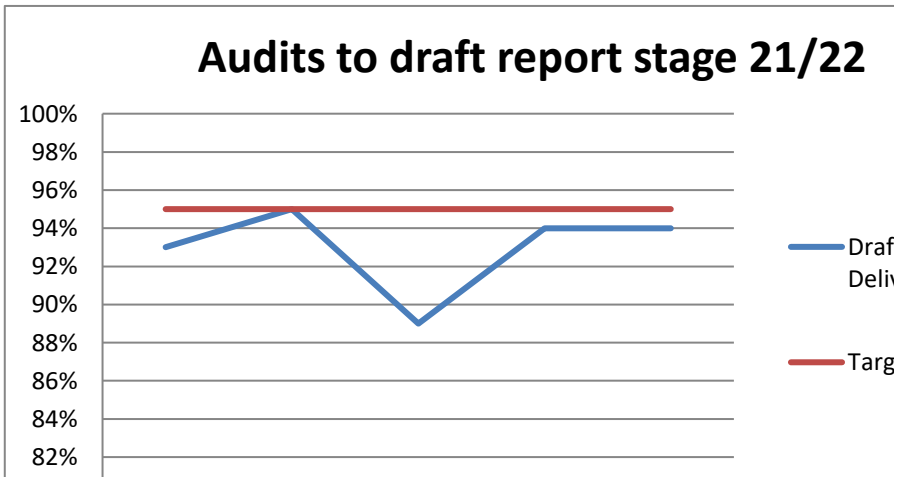
With our key objective being to complete enough work to allow an annual assurance opinion to be provided for each SIAS Partner, we are pleased to report that this was achieved.

Figure 1: Percentage of audits days delivered



Despite the challenges of 2021/22, we delivered our billable days target and achieved within 1% of our 95% project target…

Figure 2: Percentage of audits to draft stage



Shared learning - the power of partnership

Shared learning happens through the dialogue we have with others. It has long been part of the vision of our Board that the service acts to facilitate the sharing of learning across its partners. A shared learning culture, both formal and informal, is embedded through our team, our sister services within Assurance and across our partners and opportunities abound to promote issues big and small.

Shared learning happens through the dialogue we have with others…

We continued to use our networks with bodies such as the Chartered Institute of Internal Auditors (CIIA) Local Authority Chief Auditors Network (LACAN) and Home Counties Chief Internal Auditors Group (HCCIAG) to ensure that we remained in touch with the challenges facing the audit profession and those being faced by the organisations that they provide assurance to. This ensured that we could build robust audit plans for 2022/23 and share emerging risks and opportunities.

We also scoped for a future SIAS joint audit (covering all Partners) on Environmental Enforcement, which has been approved by the SIAS Board. This is seen as an opportunity for all Partners to benchmark their approach to the balance between preventative, educational and enforcement activities and how these have supported the achievement of strategic aims.

During 2021/22, our staff, partners and Audit Committee members have continued to support our cycle of continuous development with helpful challenges and comments, these being particularly critical in a time that presents an opportunity to re-look at all aspects of the delivery of the Service post pandemic.

Managing the challenges of auditing in a changing environment

We worked with Partners to ensure our audit work during the year considered the impact of the pandemic on key objectives, and internal control and governance frameworks.

As we entered 2021/22, the Covid-19 pandemic brought opportunities for our Partners (and indeed SIAS) to review their working arrangements, with many adopting a hybrid working approach. The above required changes in the way we conducted audits, with consideration given to the use of data analysis, process mapping and continuous assurance activities to support our more traditional systems and compliance-based audits.

In respect of our audit plans, we worked with our partners to ensure our audit work during the year considered the impact of the pandemic on key objectives, and internal control and governance frameworks. We also provided assurance to several of our partners on the appropriate use of grant funding that they received in relation to COVID-19 response and recovery activities, providing the required certifications for key returns.

In relation to audit delivery, we continued to embrace the use of mobile technology to adapt to hybrid working, both within SIAS and across our Partners.

Whilst 2021/22 proved to be a challenging year, we achieved our key goal of completing a programme of work for all our partners to support an annual opinion

on the robustness of internal control arrangements. This is a fantastic achievement for the Service, given that some other Local Authority Internal Audit Services continued to have difficulties in delivering their full work programmes during 2021/22.

Developing our people and processes

SIAS is committed to providing an exemplar service to its partners and clients that successfully blends cost effectiveness, resilience and quality.

During 2021/22, our required Public Sector Internal Audit Standards (PSIAS) External Quality Assessment was undertaken. As part of this, we took the opportunity to ask the assessors to go beyond the required remit of compliance with the PSIAS and seek to suggest other opportunities and good practice that would assist Service Development. The assessors duly provided several useful areas for consideration and many we have taken forward within our action plan in response to the assessment. We have also ensured that any specific recommendations to support conformance with requirements of the PSIAS have been completed, allowing us to self-assess as “generally conforms”, the highest rating under the PSIAS.

At the core of our service are our team members, and we continue to develop a core learning and coaching offering for all members of staff, with this being rolled out during 2022/23.

At the core of our service are our team members, and we continue to develop a core learning and coaching offering for all members of staff, with this being rolled out during 2022/23. We have also continued to support staff in their personal development, whether this is through the sponsoring of professional training, enrolment on apprenticeships or in one case a secondment.

Despite the challenges of holding a recruitment drive during the pandemic, we were pleased to appoint two new trainees to the team and provide internal promotions to three of our internal staff members. Following the completion of an organisational change process during 2021/22, we are fully committed to a ‘grow your own strategy’, seeking to develop our staff to allow them to progress within the team and the audit profession.

We continue to review how we obtain and disseminate learning from our quality review processes is used to support the development of our staff, seeking feedback from team members to support this process.

A continued hot topic for the audit profession is data analytics, with organisations seeing increasing digitalisation of their operations. We have trialled data analytics within several of our audits during 2021/22, and this has provided us with the opportunity to undertake whole population testing and provide improved assurance on the management of risk and controls.

First class customer service

To monitor our effectiveness and improve our service, at the end of each assignment we request the completion of a short satisfaction survey. We have been given and have acted upon invaluable improvement ideas, and we are proud of the fact that in 2021/22 we have received 95% satisfactory or higher feedback rating from our customers.

Some of the comments that accompany the formal scoring document are shown below:

- "The service was very thorough and good. The auditor was friendly and competent and understanding of wanting to not take up too much of the teams time, whilst ensuring she had all she needed to complete the audit."
- "Good, focused audit, that took a strategic view."
- "Excellent service, audit was very well planned and very constructive."
- "I am happy as ever with the service from SIAS - they are helpful and approachable and carry out a professional service."
- "Auditor was very approachable and was willing to work within timescales that worked for our service. Recommendations have been noted and will strive to implement them as best possible and as soon as practical."
- "The auditor managed to get to grips with everything really quickly regarding Modernisation Programme governance and processes. He was professional, patient and explained what he needed clearly. I found him easy to work with, he would ask open questions and would listen to responses. In return he helped me understand and see what it is we need to improve, with respectful debates where we may not have fully agreed."
- "Working with SIAS has once again been a very useful exercise as it helped the team to tighten up on processes and provided a lessons-learnt exercise to improve further."
- "The audit was undertaken in a professional manner and time taken to understand the processes and issues. This has resulted in useful recommendations for future developments."
- "Under the circumstances and due to covid restrictions the audit was carried out virtually. Although collating the information initially took additional office time, the whole process was managed effectively, and we were extremely happy with the process and outcome."

"the Auditor….was professional, patient and explained what he needed clearly. I found him easy to work with, he would ask open questions and would listen to responses. In return he helped me understand and see what it is we need to improve, with respectful debates where we may not have fully agreed"

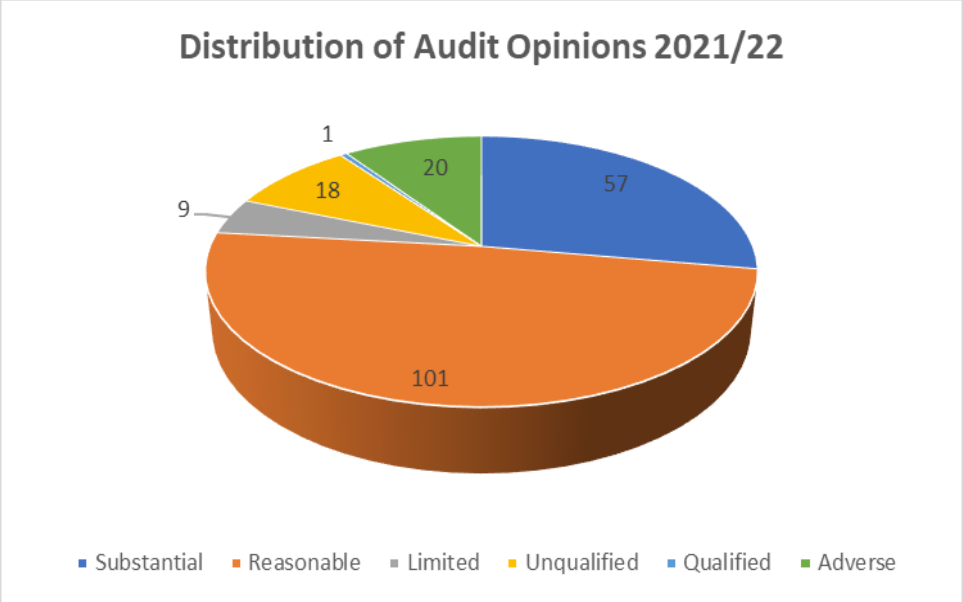
Performance - outcomes

SIAS completed 248 assurance and other projects to draft or final report stage, giving the assurance opinions and recommendations detailed in the charts below.

For those pieces which resulted in a formal assurance opinion, the distribution of opinions is set out in figure 3 below:

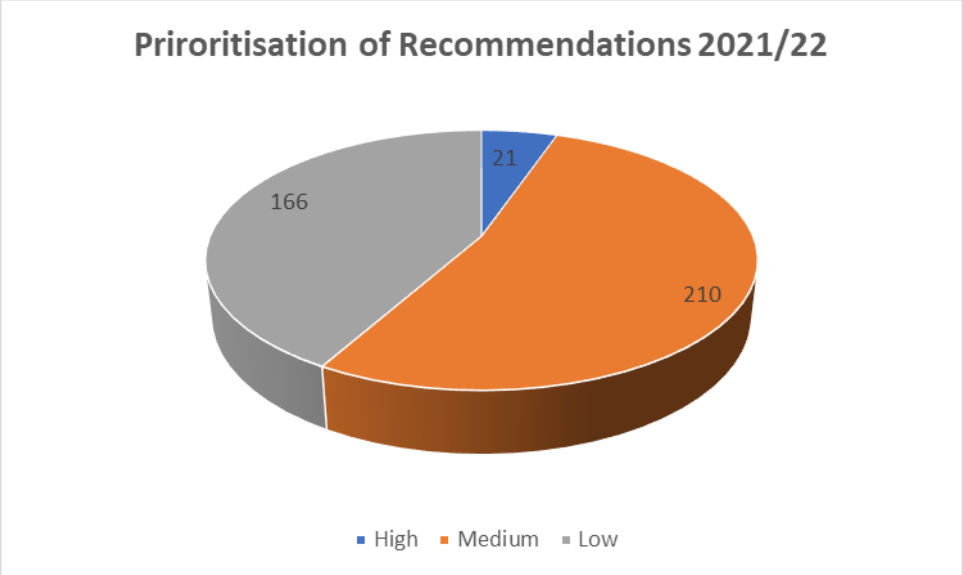
Figure 3: Distribution of Audit Opinions 2021/22

248 assurance and other projects identifying 397 recommendations



For those audits where recommendations were required and were graded, the priority ratings are set out in figure 4 below:

Figure 4: Prioritisation of Recommendations 2021/22



Performance indicators

The overall business performance of SIAS is monitored by the SIAS Board by means of a balanced scorecard which provides a range of measures by which progress can be evaluated.

The overall performance of SIAS against our key performance indicators is reported below.

Table 1: SIAS Business Performance

Indicator	Target	Actual as at 31 March 2021	Actual as at 31 March 2022
Progress against plan: actual days delivered as a percentage of planned days.	95%	96%	95%
Progress against plan: audits issued in draft by 31 March	95%	94%	94%
Client satisfaction	100% client satisfaction questionnaires returned at 'satisfactory overall' level or above	95%	95%

Financial performance of SIAS

SIAS began operating on a fully traded basis in 2012/13.

Appendix A sets out the summary financial position at 31 March 2022. Prudent financial management has allowed the service to build a reasonable reserve over the last few years, with the intention of smoothing the impact of any unforeseen events on trading performance in future years or investing in projects that support the delivery, growth or development of the service.

The costs of the SIAS organisational change during the year were absorbed by the trading reserve.

Future developments

embed new ways of working… ensuring that we work with other audit teams to share and develop best practice…

From a training, development and professional practice perspective, we will continue to support those members of our service that are striving to attain professional qualifications. For all staff, we are also rolling out a more comprehensive learning and development offering, this focused on a team-based training programme for the 2022/23 financial year to compliment individual training and development plans. The plan will be created based on feedback from the Team, our knowledge of new and emerging risks and the outcomes of our quality assessment reviews on completed audits. The above will also ensure that as a team we continue to network regularly following our move to hybrid working.

During 2022/23, we will be undertaking the re-procurement of our External Partner contract, currently held by BDO. This is a key undertaking for the Service as it is a critical part of ensuring that we have access to additional specialist skills and resilience to deliver our Partner audit plans.

We are also progressing the re-procurement of our existing Audit Management Software, where the current support for the existing in-house system ends in 2023.

From a workforce perspective, we are continuing to progress recruitment activities to fill existing vacant positions, in what is an exceptionally challenging recruitment market.

Finally, during 2022/23 we will continue to work with our colleagues across audit networks to support the development of our knowledge and approach to making the most effective use of data analytics within our assurance activities.

Our board members

The SIAS Board provides strategic direction and oversight for the partnership, bringing a wealth of local government experience and insight to our operation.

In 2021/22, our Board members were as follows:

Name	Title	Partner
Clare Fletcher	Strategic Director (CFO)	Stevenage Borough Council
Matthew Bunyon	Head of Finance and Business Services	Hertsmere Borough Council
Steven Pilsworth	Director of Finance	Hertfordshire County Council
Ian Couper	Service Director (Resources)	North Hertfordshire District Council
Richard Baker	Executive Director (Finance and Transformation)	Welwyn Hatfield Borough Council
Steven Linnett	Head of Strategic Finance and Property	East Herts Council
Alison Scott	Director of Finance	Watford Borough Council and Three Rivers District Council
Chris Wood	Head of Assurance	SIAS

Appendix A: SIAS Trading Account 2021/22

SIAS cost centre: budget against outturn 2021/22

	Budget £	Outturn £
Employee Costs	995,822	904,071
Organisational Change Costs	-	149,523
Partner / Consultancy Costs	101,040	186,510
Transport (Travel)	3,000	754
Supplies	24,183	14,683
Office Accommodation Cost	17,005	17,005
Total expenditure	1,141,071	1,272,546
Income	-1,121,411	-1,132,095
Net (surplus) / deficit	19,639	140,451

2021/22 Definitions of Assurance and Recommendation Priority Levels

Assurance Level		Definition
Substantial		A sound system of governance, risk management and control exist, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable		There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited		Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No		Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control are inadequate to effectively manage risks to the achievement of objectives in the area audited.
Priority Level		**Definition**
Corporate	**Critical**	Audit findings which, in the present state, represent a serious risk to the organisation as a whole, i.e. reputation, financial resources and / or compliance with regulations. Management action to implement the appropriate controls is required immediately.
Service	**High**	Audit findings indicate a serious weakness or breakdown in control environment, which, if untreated by management intervention, is highly likely to put achievement of core service objectives at risk. Remedial action is required urgently.
	Medium	Audit findings which, if not treated by appropriate management action, are likely to put achievement of some of the core service objectives at risk. Remedial action is required in a timely manner.
	Low / Advisory	Audit findings indicate opportunities to implement good or best practice, which, if adopted, will enhance the control environment. The appropriate solution should be implemented as soon as is practically possible.

Watford Borough Council
Audit Committee Progress Report
15 September 2022

Recommendation

Members are recommended to:

- Note the Internal Audit Progress Report for the period to 2 September 2022
- Approve amendments to the Audit Plan as at 2 September 2022
- Agree the change to the implementation date for four recommendations (paragraph 2.6) for the reasons set out in Appendix C
- Agree removal of implemented audit recommendations set out in Appendix C
- Note the implementation status of high priority recommendations

Contents

1. Introduction and Background

Purpose of Report

1.1 This report details:

a) Progress made by the Shared Internal Audit Service (SIAS) in delivering the Council's Annual Internal Audit Plan for 2022/23 as at 2 September 2022.
b) Proposed amendments to the approved 2022/23 Internal Annual Audit Plan.
c) Implementation status of all outstanding previously agreed internal audit recommendations from 2018/19 onwards.
d) An update on performance management information at 2 September 2022.

Background

1.2 The work of internal audit is required to be reported to a Member Body so that the Council has an opportunity to review and monitor an essential component of corporate governance and gain assurance that its internal audit provision is fulfilling its statutory obligations. It is considered good practice that progress reports also include proposed amendments to the agreed annual audit plan.

1.3 The 2022/23 Annual Audit Plan was approved by Audit Committee on 10 March 2022.

1.4 The Audit Committee receives periodic updates on progress against the Annual Audit Plan from SIAS, the most recent of which was brought to this Committee on 28 July 2022.

2. Audit Plan Update

Delivery of Audit Plan and Key Audit Findings

2.1 As at 2September 2022, 27% of the 2022/23 Audit Plan days had been delivered for the combined WBC and Shared Services audit plans (excludes 'To Be Allocated' days). Appendix A provides a status update on each individual deliverable within the audit plan.

2.2 The following 2021/22 final report has been issued since July 2022 Audit Committee:

Audit Title	Date of Issue	Assurance Level	Number and Priority of Recommendations
Operational Buildings Compliance	July 2022	Limited	Four high Three medium

2.3 The following 2022/23 reports have been finalised since July Audit Committee:

Audit Title	Date of Issue	Assurance Level	Number and Priority of Recommendations
Contain Outbreak Management Fund (COMF) Grant	July 2022	Unqualified	N/A

Status of Audit Recommendations

2.4 Audit Committee Members will be aware that a Final Audit Report is issued when it has been agreed by management and includes an agreement to implement the recommendations made. It is SIAS's responsibility to bring to Members' attention the implementation status of all audit recommendations. It is the responsibility of officers to implement recommendations by the agreed date.

2.5 The table below summarises progress in implementation of all outstanding internal audit recommendations as at 2 September 2022, with full details in Appendix C**:**

Year	Recommendations made No.	Implemented	Not yet due	Outstanding & request made for extended time or no update received	Percentage implemented %
2018/19	30	29	0	1	97%
2020/21	28	26	1	1	93%
2021/22	37	20	7	10	54%

2.6 Since 28 July 2022 Audit Committee, extension to implementation dates have been requested by action owners for four recommendations as follows:

a) Two from the 2021/22 Procurement Cards audit, with a revised target date of 26 September 2022 to accomplish the last part of an action substantially completed.
b) Four from the 2021/22 Operational Buildings Compliance audit, with a revised target date of 30 September 2022 or 7 October 2022.

2.7 Since 28 July 2022 Audit Committee, no update has been received and / or request made for a revised target date in respect of the following seven recommendations:

a) One recommendation from the 2018/19 Benefits audit (previous revised target date 31 August 2022.
b) One recommendation from the 2020/21 Debtors audit (previous revised target date 31 December 2022).
c) One recommendation from the 2021/22 NDR audit (target date 31 March 2022).
d) One recommendation from the 2021/22 Council Tax audit (target date 31 August 2022.

e) Two recommendations from the 2021/22 Benefits audit (target date 31 July 2022).

2.8 Four new high priority recommendations have been made within the period since the last update report, these relating to the audit of Operational Buildings Compliance. Further details of these recommendations and their implementation status is provided within Appendix C of this update report. By way of summary, two of these high priority recommendations are deemed to have been implemented, one has a request for an extension to the implementation date (30 September 2022) and one has surpassed its target date, but no request has been made for an extended implementation date.

2.9 The four high priority recommendations relate to the following:

a) Generation of a remedial log which should include RAG-rated remedial actions raised from risk assessments with an assigned person and deadline to ensure they are monitored and completed within timescales. Evidence of timely completion of recommended actions should be retained alongside the remedial log.
b) Scheduling of electrical installation inspections for the five buildings with EICs outstanding and obtaining these as the CAM Team did not receive certification from the previous contractor.
c) Production of management reports which include progress against key performance indicators (KPI) on compliance rates and numbers of outstanding remedial actions to the Leadership Board.
d) Formally completing the building related outstanding actions from the most recent HCC health and safety audit within a suitable timescale.

2.10 Internal Audit have been advised that an action log and reporting mechanism is in place to ensure a robust and timely response to the Operational Building Compliance audit. The delivery of the action plan is being reported to the Council's Corporate Management Board every fortnight and is deemed a corporate priority.

Proposed Audit Plan Amendments

2.11 The original approved Shared Services 2022/23 Audit Plan included an allocation of 30 days for audits within the Finance Service. Following a meeting with the Head of Finance and agreement with the Director of Finance the following audits have been agreed for use of this time and are brought to the attention of the Committee:

- Fixed Asset Register – review of the completeness of the records on the finance system, including how valuations are determined (10 days).
- Financial Reconciliations – review of the robustness of key financial account reconciliations including ownership, frequency and sign-off (12 days).
- Treasury – review of compliance against the Prudential Code, including the Treasury Management Practices (8 days).

Performance Management

2.12 To help the Committee assess the current situation in terms of progress against the projects in the 2022/23 Audit Plan, we have provided an analysis of agreed

start dates at Appendix B. These dates have been agreed with management and resources allocated.

2.13 Annual performance indicators and associated targets were approved by the SIAS Board in March 2022. Actual performance for Watford Borough Council against the targets that can be monitored for 2022/23 is shown in the table below.

Performance Indicator	Annual Target	Profiled Target to 2 September 2022	Actual to 2 September 2022
1. Internal Audit Annual Plan Report – approved by March Audit Committee or the first meeting of the financial year should a March committee not meet	Yes	N/A	Yes
2. Annual Internal Audit Plan Delivery – the percentage of the Annual Internal Audit Plan delivered (excludes unused contingency days)	95%	32% (72 / 227.5 days)	27% (62.5 / 227.5 days)
3. Project Delivery – the number of projects delivered to draft report stage against projects in the approved Annual Internal Audit Plan	95%	21% (4 out of 19 projects to draft)	16% (3 out of 19 projects to draft)
4. Client Satisfaction* – percentage of client satisfaction questionnaires returned at 'satisfactory overall' level (minimum of 39/65 overall)	95%	100%	100% (based on two received)
5. Chief Audit Executive's Annual Assurance Opinion and Report – presented at the first Audit Committee meeting of the financial year	Yes	N/A	Yes

APPENDIX A - PROGRESS AGAINST THE 2022/23 AUDIT PLAN AT 2 SEPTEMBER 2022

2022/23 SIAS Audit Plan

AUDITABLE AREA	LEVEL OF ASSURANCE	RECS				AUDIT PLAN DAYS	LEAD AUDITOR ASSIGNED	BILLABLE DAYS COMPLETED	STATUS/COMMENT
		C	H	M	L				
Key Financial Systems									
Council Tax (shared services plan)						10	SIAS	2	Terms of Reference Issued
Financial Reconciliations (shared services plan)						12	BDO	0.5	In Planning
Fixed Asset Register (shared services plan)						10		0	
NDR (shared services plan)						10	SIAS	2	Terms of Reference Issued
Payroll (shared services plan)						12		0	
Sundry Debtors (shared services plan)						10	BDO	2	Terms of Reference Issued
Treasury (shared services plan)						8		0	
Operational Audits									
Climate Emergency Follow Up						3		0	In Planning
Asset Management System Data						10		0	
Museum						10	Yes	9.5	Draft Report Issued
FOI						8		0	
Trees						8		0	
Website Redesign						8	BDO	0.5	In Planning
Project Management						12		0	
Green Homes Grant	Unqualified	-	-	-	-	3	SIAS	3	Final Report Issued

APPENDIX A - PROGRESS AGAINST THE 2022/23 AUDIT PLAN AT 2 SEPTEMBER 2022

AUDITABLE AREA	LEVEL OF ASSURANCE	RECS				AUDIT PLAN DAYS	LEAD AUDITOR ASSIGNED	BILLABLE DAYS COMPLETED	STATUS/COMMENT
		C	H	M	L				
COMF Grant Certification	Unqualified	-	-	-	-	0.5	SIAS	0.5	Final Report Issued
Contract Management, Project Management & Procurement									
Contract Management						12	BDO	0.5	In Planning
Governance									
Corporate Governance						12	BDO	10	In Fieldwork
IT Audits									
Cyber Security (shared services plan)						15		0	
Shared Learning / Joint Reviews									
Shared Learning / Joint Reviews						4		2	Through Year
Follow Ups									
Follow up of Audit Recommendations						8		4	Through Year
To Be Allocated									
Unused Contingency (shared services plan)						4		0	To Be Allocated
Strategic Support									
2023/24 Audit Planning						6		0	Due quarter 4
Annual Governance Statement						3		3	Complete

APPENDIX A - PROGRESS AGAINST THE 2022/23 AUDIT PLAN AT 2 SEPTEMBER 2022

AUDITABLE AREA	LEVEL OF ASSURANCE	RECS				AUDIT PLAN DAYS	LEAD AUDITOR ASSIGNED	BILLABLE DAYS COMPLETED	STATUS/COMMENT
		C	H	M	L				
Audit Committee						10		4	Through Year
Head of Internal Audit Opinion 2021/22						3		3	Complete
Monitoring & Client Meetings						7		3	Through Year
SIAS Development						3		3	Complete
Completion of 2021/22 audits									
Time required to complete work commenced in 2021/22 (7 days shared plan; 3 days WBC)						10	N/A	10	Complete
WBC TOTAL						**133.5**		**49**	
SHARED SERVICES TOTAL						**98**		**13.5**	
COMBINED TOTAL						**231.5**		**62.5**	

Key to recommendation priority levels: C = Critical; H = High; M = Medium; L = Low / Advisory.

APPENDIX B – AUDIT START DATES 2022/23

Apr	May	June	July	August	September
	Museum **Draft Report Issued**	Corporate Governance **In Fieldwork**	Website Redesign **In Planning**	Contract Management **In Planning**	Sundry Debtors (Shared services plan) **Terms of Reference Issued**
		Green Homes Grant **Final Report Issued**	COMF Grant Certification **Final Report Issued**		

October	November	December	January	February	March
Project Management	Asset Management System Data	FOI	Trees	Cyber Security (Shared services plan)	
Climate Emergency Follow Up	Payroll (Shared services plan)	Financial reconciliations (Shared services plan)	Treasury (Shared services plan)		
NDR (Shared services plan) **Terms of Reference Issued**	Council Tax (Shared services plan) **Terms of Reference Issued**	Fixed Asset Register (Shared services plan)			

Audit Plan 2018/19

Benefits 2018/19 **Final report issued April 2019**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
02	We recommend that testing of the module is carried out to reinstate the ability to delete obsolete data.	Medium	Position – 21 August 2019 The system is designed to destroy all documents that are older than 6 years plus current. We discovered that the system was not working properly and has destroyed some documents that are still required to support live Benefit claims and therefore we need to retain. Clearly, we could not allow that to continue so the system has been suspended. We have sought advice on how to fix this issue from the system provider and are awaiting their response. I have chased this today and have also now asked if it's possible to use the system in part so that we can carry on destroying old documents that we no longer require for Council Tax and Business Rates and unsuspend the Benefits part of the system once we have fixed the problem. I will escalate this issue in a week if I have not had a response. Position – September 2019 Issue has now been escalated with Northgate. Position – February 2020 The Northgate system is currently being upgraded. The upgrade is now available in test and the live upgrade is due to take place 1st and 2nd May 2020. We will test this module of the system as part of the overall testing. If this module works, we will be able to run scripts which will 'back archive' documents that would have been due to be archived since it was discovered the system was not working properly. Position – July 2020	Benefits Manager	31 May 2019	✖	~~31 October 2019~~ ~~30 June 2020~~ ~~30 Sept 2020~~ ~~31 March 2021~~ ~~30 Sept 2021~~ ~~30 November 2021~~ ~~31 January 2022~~ ~~15 March 2022~~ 31 August 2022

Benefits 2018/19 **Final report issued April 2019**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
			The required Northgate system upgrade was due to be live now but has been delayed as a result of COVID-19. Northgate have currently rescheduled the upgrade for 8-9 September 2020 and when this takes place, we will test the module and if this is working as expected, run the necessary scripts to archive the data that should have been deleted. Position – November 2020 The required system upgrade was planned for the end of October but did not go live due to system performance issues. This is now expected in March 2021. Discussions are however, taking place with Northgate to see if an interim measure is available so that obsolete data can be removed from the system. Position – February 2021 We are on schedule to upgrade the information@work system 19/20 March 2021. Once it's upgraded, we can re-test the retention and destruction module. Position – July 2021 The system upgrade planned for March 2021 did not go-ahead as we had limited time to carry out testing and were not in a position to be able to sign off the product. A new go-live date has been set for 7/8 September 2021 and testing has commenced. Position – September 2021 We currently are unable to upgrade due to not having a fully operational Test system. All parties are in communication and are trying to identify the issue so that we can progress with testing.				

Benefits 2018/19 **Final report issued April 2019**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
			Position – November 2021 The upgrade to our Document Processing System is now scheduled to take place on 20 & 21 January 2022. Revs and Bens have been working with our IT department and our supplier to overcome the problems we had with the test system. Testing is scheduled to start this month (November 2021). Position – February 2022 The long-awaited upgrade took place on 04.02.22. We are now amending the scripts that will destroy the old documents. The scripts are being amended to do two things that they did not do before: 1. To look for claims that have an outstanding housing benefit overpayment but a non-live housing benefit claim, and 2. Live housing benefit claims. Where the script identifies claims under 1 & 2 no documents will be destroyed regardless of their age as they may be required for audit, for fraudulent investigations and for recovery of overpayments. Position – July 2022 Consultancy is being arranged to assist with a complete re-write of the scripts to destroy unwanted documents. Whilst the writing and testing of a new script is in progress which will automate the whole process, we will manually start identifying old documents and destroy them. **Position – August 2022** **No update received – deadline has been reached and no revised target dare requested.**				

Audit Plan 2020/21

Cyber Security 2020/21 **Final report issued March 2021**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
01	Management should ensure that physical network ports are configured to the appropriate authentication control (802.1X). Furthermore, management should establish a network access control to block unknown or unauthorised devices from connecting to the Councils' IT network. This should include restricting the ability to physically connect to the Council's IT network.	Medium	We have an intrusion detection system in place, which would identify any devices connecting to the network. This is a project we will review and look to implement, assuming budget is available to do so. Position – July 2021 Resources are focussed on the Littlefish transition and implementation. This implementation is not yet due until March 2022. Position – September 2021 Resources are focussed on the Littlefish transition and implementation. This implementation is not yet due until March 2022. Position – November 2021 As above. Position – February 2022 Market assessed as to the product options and costs. Products assessed: CISCO and Forescout. Additional budget required in order to go ahead. IT steering group decision. Paper with options and risks for assessment and decision by that board in March 2022. Position – July 2022 ITSG board meeting delayed. This paper is scheduled for decision at the 19 July board. The recommendation from Head of ICT, given the additional budget required is to not proceed with the recommendation at this time and instead consider a solution in line with the refresh of the Councils corporate WIFI	Head of ICT	31 March 2022	✓ **No longer relevant**	31 July 2022

Cyber Security 2020/21 **Final report issued March 2021**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
			technology solution in 23/34. **Position – August 2022** **Recommendation no longer relevant following approval from ITSG on revised solution.**				

Communications 2020/21 **Final report issued May 2021**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
01	We recommend that the service updates all its policies to ensure that they reflect the current process followed. Going forward, the service should ensure that the policies are updated at regular intervals, and proper version control introduced.	Low	These policies were due to be updated in 2020 but due to the impact of Covid-19 this has been delayed. Position – July 2021 No update received. Position – September 2021 The service has had a very busy summer leading on the communications and engagement for a range of priority council initiatives and projects (e.g. mass vaccination clinics, Sustainable Transport Strategy). An additional resource provided by a Kickstart appointment will be supporting this work. Position – November 2021 Overall guidance on publicity and communications has been updated. The team is still working through additional policies. Position – February 2022 Main policies updated. Position – July 2022 Review of all policies underway for 2022/23.	Communications and Engagement Lead	31 October 2021	×	~~28 February 2022~~ 31 March 2023

APPENDIX C – AUDIT RECOMMENDATIONS FOLLOW UPS – AUGUST 2022

Communications 2020/21

Final report issued May 2021

Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
			Position – August 2022 **Main policies updated – additional ones under review.**				

Debtors 2020/21

Final report issued June 2021

Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
03	Consideration should be given to an annual review of debtor accounts to identify duplicate or dormant for deletion or deactivation.	Low	Position – July 2021 We will speak to Finance about the best way of doing this. Position – September 2021 A complete review of the entire Sundry Debtor service has recently been commenced and this will be included as part of the review. Position – November 2021 No update received. Position – February 2022 No update received. Position – July 2022 To date we have not been able to resource this review as we have had to prioritise Grant work and more recently the Council Tax Energy Rebates. We will pick up this project towards the end of the calendar year once the Energy rebate work is completed. **Position – August 2022** **No update received – target date not yet reached.**	Recovery Team Leader, Revenues Manager and Finance.	31 August 2021	×	~~31 October 2021~~ 31 December 2022

Audit Plan 2021/22

NDR 2021/22

Final report issued March 2022

Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
01	We recommend that: • A review of existing NDR cases pending write-off is conducted and decisions taken regarding whether or not cases should proceed to write-off. Write-offs are conducted at regular intervals going forward (e.g. quarterly).	Medium	In 2022/23 write-offs will be done on a monthly basis. Position – July 2022 No update received. **Position – August 2022** **No update received – target date has been reached.**	Revenues Manager	31 March 2022	×	

Safeguarding 2021/22

Final report issued April 2022

Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
01	When temporary staff members are being appointed, the Council should ensure that necessary safeguarding checks have been completed prior to the employee starting work, and that appropriate records are maintained. If there is an expected delay to such checks being performed, a decision should be recorded to delay the start date until completed	High	HR Management will remind Comensura of the pre-employment checks required by Watford prior to someone starting. HR will carry out spot checks of temporary staff and ask Comensura [or any other provider] to provide evidence of the checks undertaken at least annually. HR will ensure the specification for a future agency partner includes all requirements for pre-employment checks to be undertaken and the checking process to be in place to ensure compliance. Recruiting Managers across the council will be reminded of the need to ensure all compliance	Head of HR (Operations)	1 June 2022 1 April 2023 When required. 1 June 2022	✓ × ✓ ✓	

Safeguarding 2021/22 **Final report issued April 2022**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
			documentation is received prior to commencement of staff in post and the different requirements if agency staff come through Comensura or direct through agency to the council. Position – July 2022 Comensura have been reminded of the pre-employment checks required. Their booking system has the requirement for a DBS check as a pre-requisite. The tender specification for the current tender process for future agency partner has included the requirement for DBS checks to be carried out. HRBPs have reminded managers of the compliance documentation required and this will be raised as new bookings are made. **Position – August 2022** **All recommendations are complete except the one action in progress (spot checks) This has a due date of 1 April 2023.**				

Main Accounting 2021/22 **Final report issued April 2022**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
03	We recommend that procedure notes are produced for feeder system reconciliations to enable them to be carried out correctly and checked in a timely manner. We also recommend that Benefits system reconciliations are signed and dated by another person in Finance.	Low	Procedure documents will be reviewed and updated/created as required. Timeliness of reconciliation will be monitored and managed as part of the tracking processes referenced in the response recommendation 2, above. Position – July 2022	Finance Section Head / Finance Systems Manager	31 October 2022	×	

APPENDIX C – AUDIT RECOMMENDATIONS FOLLOW UPS – AUGUST 2022

Main Accounting 2021/22 **Final report issued April 2022**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
			On target. **Position – August 2022** **In progress and on target - target date is 31 October 2022.**				

Procurement Cards 2021/22 **Final report issued April 2022**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
01	All transaction logs should be signed off by the card holder and a member of management to ensure that transactions are accurate and that there is a reviewer who can confirm that the transactions are appropriate and in line with Council needs. Receipts for all transactions should be retained to ensure VAT is being accounted for appropriately and there is evidence for the purchases made. VAT should be appropriately accounted for on transaction logs as this can affect the amount of recoverable VAT the Council can claim back, therefore creating unnecessary losses.	Medium	Existing guidance covers the requirement to retain receipts, and to document net/vat split on their transaction logs. Guidance will be re-circulated with a reminder of the importance of observing these requirements. In mitigation we can suspend the use of cards where holders do not comply with the requirements. Transaction logs and receipts are reviewed by Finance Officers do not post VAT element if a receipt is not provided. Position - July 2022 New guidance has been written and will be sent out by the end of July. **Position – August 2022** **Procedure adjusted to reflect all recommendations.** **TRDC email sent 30/08/22** **WBC email written and to be sent 26/09/22**	Finance Manager – Systems Shared Services	20 May 2022	× - resolved when WBC e-mail sent.	~~1 August 2022~~ 26 September 2022

APPENDIX C – AUDIT RECOMMENDATIONS FOLLOW UPS – AUGUST 2022

Procurement Cards 2021/22 **Final report issued April 2022**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
02	Controls should be implemented to mitigate the risk of potential fraud and overspend on budget from multiple people using the same procurement card. This could be in the form of acquiring a finance system to support the use of procurement cards, by providing other card users with their own card or through creating a system with the banks to provide single use e-cards for one-off transactions.	Medium	A reminder of existing rules against the sharing of cards will be circulated. Position – July 2022 New guidance has been written and will be sent out by the end of July. **Position – August 2022** **Procedure adjusted to reflect all recommendations.** **TRDC email sent 30/08/22** **WBC email written and to be sent 26/09/22** A review of card holders will be undertaken to ensure cards are held at the appropriate level. This will follow the evaluation of potential system solutions for the management of purchasing cards. If a system solution is pursued, it may result in the ability to use an e-card and/or single-use card technologies which will further mitigate the risk of cards being shared. Position – July 2022 We will be sending communications which will cover sharing of cards and the correct people to have cards by the original target date. **Position – August 2022** **Procedure adjusted to reflect all recommendations** **TRDC email sent 30/08/22** **WBC email written and to be sent 26/09/22**	Finance Manager – Systems Shared Services	20 May 2022 31 October 2022	× - resolved when WBC e-mail sent.	~~1 August 2022~~ 26 September 2022

Cyber Security 2021/22 **Final report issued April 2022**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
01	1.1 Management should ensure that appropriate monitoring controls are in place for the password monitoring and management activities. These should include but not be limited to the following: • brute-forcing of account passwords including password spraying, • login attempts from unexpected geographic areas, • unexpected account lockouts • password database for the deny list hashes, • other unusual behaviour from users. 1.2 The above proposed controls, once in place, should be actively reported upon, through the periodic cyber security reports, to the senior management.	Medium	01 Mar 2022 the Azure AD Password Protection was implemented. Users will not be able to **change** passwords to weak passwords nor known passwords nor passwords from our Ban List of passwords. 1.1 – requires a third-party tool and associated funding would be required. The implementation of the password protection for Azure AD lowers the risk. 1.2 - this would be dependent on the ability to fund with a third-party tool – 1.1. Position – July 2022 Third party tools currently being reviewed and costed. Item not yet due. **Position – August 2022** **1.1 - Third party tools have been evaluated and Netwrix has been selected as the preferred tool.** **1.2 – Netwrix had demonstrated the tool in detail and a 30-day trial to test the system further is available.** **1.3 – Quotation for 1- and 3-year option has been provided.** • **1-year option - £7,806** • **3-year option - £16,483** **1.4 – Implementation of the tool will be dependent on the ability to fund the third-party tool, this will require an approval by ITSG for an additional spend. A paper to review this recommendation and request any growth in budget 2022.**	Head of ICT	31 March 2023	×	

APPENDIX C – AUDIT RECOMMENDATIONS FOLLOW UPS – AUGUST 2022

Cyber Security 2021/22 **Final report issued April 2022**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
03	Management should conduct regular monthly vulnerability scans across the entire IT estate including endpoint, to identify and mitigate vulnerabilities including software flaws, missing patches, misconfigurations and malwares.	Low	This would require additional budget and would need a growth item approved, as there are licence implications for the Qualys scanner. Position – July 2022 Extension of current third-party tools currently being reviewed and costed. Item not yet due. **Position – August 2022** **1.1- Third party Qualys had introduced a new module which will enable the management of remote devices through the cloud.** **1.2 – Both options are currently being evaluated and costed. Decision made will be based on cost, functionality, and management.**	Head of ICT	31 March 2023	×	

Contract Waivers 2021/22 **Final report issued June 2022**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
01	We recommend Procurement and Legal advice is sought (and recorded on the corporate form) before waivers are raised and sent to management for approval.	Medium	This will need discussion with Leadership Board (WBC) / Corporate Management Team (TRDC) and if agreed amendment to the existing firmstep forms. Position – July 2022 Not yet due. **Position – August 2022** **Not yet due**	End of September discussion with Leadership Board / Corporate Management Team	30 September 2022	×	

APPENDIX C – AUDIT RECOMMENDATIONS FOLLOW UPS – AUGUST 2022

Contract Waivers 2021/22

Final report issued June 2022

Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
02	A tracker should be established to record the waiver process and waivers should remain "open" until all relevant evidence is received from services to demonstrate compliance with the Contract Procedure Rules. An annual waivers report should be produced for senior management and members at both authorities to ensure there is accurate and transparent reporting of waiver activity.	Low	The shared service procurement manager should now receive copies of all exemptions. Agree to prepare an annual waivers report for both authorities. Position – July 2022 Not yet due. **Position – August 2022** **Not yet due.**	Procurement Manager	31 March 2023	×	

Creditors 2021/22

Final report issued July 2022

Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
01	We recommend the Council completes a review of all supplier's setup on the eFinancials system to identify if any other employees have been setup as a supplier. Any supplier accounts which are found to be employees should be removed from the eFinancials system and the Council must prohibit the use of payment vouchers to make payments to employees.	Medium	Agreed that a review of supplier accounts will take place. Any staff will be removed. Staff identified will be contacted to advise them of correct procurement routes and processes for claiming expenses. Position - July 2022 Not yet due. **Position – August 2022** **Reviewed the suppliers and identified staff set up as suppliers and all staff removed 30/08/22. Communications to be sent to advice on correct way to make office spend.**	Finance Manager (Systems)	31 July 2022	✓	
02	We recommend: 1. The Council creates a policy/procedure covering the use of CHAPS and Faster Payments. This	Medium	A process note for CHAPS and Faster Payments will be written along with a scheme of delegation, agreed by S151 Officer and published on the intranet.	Finance Manager (Systems)	26 August 2022	× - part 1 and 2 resolved. Revised deadline	31 October 2022

Creditors 2021/22 **Final report issued July 2022**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
	will include: • The criteria which must be met to use CHAPS and Faster payments, • The process for requesting and approving these payments, • Which officers can request and approve these payments and how delegated limits will be set. 2. The Council updates the Payment Voucher request procedure to outline the types of payments which are eligible and ineligible to be made using this method. 3. The policy and procedures for CHAPS, Faster Payments and Payment Vouchers are communicated/re-communicated to all relevant staff across the Council (e.g., in a corporate communication) and placed on key staff systems such as the Intranet for reference		Agreed and will be published as per the above. Agreed they will be published on the intranets and a communication to all staff. Position - July 2022 Not yet due. **Position – August 2022** **1 is resolved ✓ process note created.** **2 is resolved ✓ process updated.** **3 We will publish revised note and new note on the intranet along with Delegated authority listings.** **New deadline: 31 October 2022**			for part 3.	
03	We recommend a reminder notification (e.g., email) is issued to all officers involved in approving new suppliers. This is to re-iterate that complete backing evidence must be obtained through the paperclip attachment and cross checked	Low	Agreed we will remind the evidence required to raise a supplier and what the correct checks are. Position - July 2022 Not yet due.	Finance Manager (Systems)	31 July 2022	✓	

Creditors 2021/22

Final report issued July 2022

Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
	against the details in the new supplier request form, prior to approving the supplier. Should any details entered in the new supplier request form not be supported by backing evidence, the request must be rejected, and the approving officer should contact the requestor to ask for full documentation to be provided in a new request.		**Position – August 2022** **Reminder sent to all staff involved.**				

Benefits 2021/22

Final report issued July 2022

Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
01	We recommend that: • A review of existing housing benefit overpayment cases pending write-off is conducted and decisions taken regarding whether or not cases should proceed to write-off. • Write-offs should be conducted at regular intervals going forward (e.g. quarterly).	Medium	Agreed. Position - July 2022 Not yet due. **Position – August 2022** **No update received – deadline has been reached.**	Recovery Team Leader	31 July 2022	×	
02	We recommend that the number of officers with administrator privileges on the Academy system should be restricted to a minimum number of individuals to preserve the integrity and security of the system.	Low	Agreed. Position - July 2022 Not yet due. **Position – August 2022** **No update received – deadline has been reached.**	Data & Performance Manager	31 July 2022	×	

Council Tax 2021/22

Final report issued July 2022

Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
01	We recommend that: • A review of existing Council Tax cases pending write-off is conducted and decisions taken regarding whether or not cases should proceed to write-off. • Write-offs are conducted at regular intervals going forward (e.g. monthly).	Medium	Agreed. Position - July 2022 Not yet due. **Position – August 2022** **No update received – deadline has been reached.**	Revenues Team Leader	31 August 2022 for the review of write-off's pending. Ongoing write off's to be processed monthly starting from July 2022.	×	

Operational Buildings Compliance 2021/22

Final report issued July 2022

Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
01	The CAM Team should complete all outstanding remedial actions which have been recommended by contractors with immediate effect and retain evidence of their completion. Evidence of timely completion of recommended actions should be retained alongside the remedial log. The CAM Team should develop a remedial log which lists the recommended remedial actions from risk assessments undertaken. The remedial log should include the action, responsible officer, deadline, and completion date for monitoring purposes. These actions should be RAG rated to ensure that immediate remedial	High	Completed - remedial log has been created that is RAG rated with responsible officer, deadline, and completion date. **Position – August 2022** **Completed - Remedial logs for each building now being utilised.**	Compliance & Maintenance Officer	Already Completed	✓	

Operational Buildings Compliance 2021/22 **Final report issued July 2022**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
	actions are prioritised for completion. The log should be monitored and updated by the Compliance & Maintenance Officer monthly to provide clarity on the actions completed.						
02	Electrical installation inspections should be conducted for the five properties identified with outstanding EICs. Once conducted, these inspections should be reviewed within five years to comply with the Electrical Safety Standards in the Private Rented Sector (England) Regulations 2020. All certificates and reports in relation to risk assessments should be uploaded on the Council's local drive to ensure that all documents are retained.	High	EICs on remaining buildings to be commissioned. **Position – August 2022** **All buildings have condition reports. At the time of the audit, FM did not have the electronic record from previous outsourced contractor who undertook this work. Also, 2 buildings now taken out of service. This action has been completed.**	Facilities Manager	31 July 2022	✓	
03	The Compliance & Maintenance Officer should generate monthly reports for the Facilities Manager and the Leadership Board to review on the compliance rates in relation to the following health and safety areas: • Gas Safety • Electrical Safety • Fire Safety • Legionella Safety • Lift Safety The reports should outline the risk assessments undertaken, progress, outcomes, remedial actions completed, due and those delayed for	High	FM to provide programme on a monthly basis to Leadership Board. This will include information on risk assessments and progress with remedial actions. **Position – August 2022** **Compliance report to be provided to senior management on a monthly basis. New asset management system (concerto) will be able to generate regular management reports. FM produce a spreadsheet on current status of compliance that can be provided in the meantime.**	Head of Corporate Asset Management / Facilities Manager	31 July 2022	×	30 September 2022

Operational Buildings Compliance 2021/22 **Final report issued July 2022**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
	greater oversight. The remedial actions should have an assigned action owner and due date for completion.						
04	The Facilities Manager should assign a responsible officer as well as a suitable/achievable deadline for all outstanding recommended actions. The deadlines set should align with the HCC guidance, which is immediate, 1 week, 2 weeks, 1 month and three months for high and medium actions.	High	Monthly review and sign off by senior management on actions and recommendations to be reviewed and signed off by H & S. **Position – August 2022** **All actions now completed but requires sign off by H&S Adviser (meeting on 30/8/22). Target date not yet reached.**	Facilities Manager	15 September 2022	×	7 October 2022
05	All sections of the compliance schedule should be completed to achieve effective monitoring of risk assessments and to ensure that all assessments are completed when they are due. The Council should implement a process to identify which compliance checks they are responsible for completing for all their operational buildings. This will provide a clear direction on who is responsible for completing the assessments / inspections.	Medium	We accept this finding and have already updated the programme which now clearly indicates the status of risk assessments. The programme will also include exception information on any overdue risk assessment. This will be provided in a summary as required. The schedule will set out who is responsible for completing the inspections. The programme is continually monitored and updated as required. **Position – August 2022** **All spaces now clearly state status of inspection/ assessment. This programme to be replaced by new Asset Management system that will generate automatic reports.**	Compliance & Maintenance Officer	31 July 2022	✓	
06	The Facilities Manager should merge all policies in relation to health and safety in buildings to create an overarching Monitoring Compliance section in the Council Buildings Policy. The Policy should provide	Medium	To be updated for ratification at the next H & S Committee meeting. **Position – August 2022** **To update procedures for ratification at next H&S Committee (date to be confirmed**	Facilities Manager	31 July 2022	×	7 October 2022

Operational Buildings Compliance 2021/22 **Final report issued July 2022**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
	detailed guidance on fire safety, electrical safety, water safety, legionella and general health and safety (including Gas, Asbestos and Lift safety). The policy should outline responsibilities and the frequency of the risk assessments (for gas safety, legionella, fire safety and lift safety) to ensure that the Inspectors are aware of the expected frequency of the inspections. In addition, the author, approval, and the proposed review date should be clearly outlined within the policy to ensure that it is updated regularly to align with government guidance.		**by Head of HR). Target date reached.**				
07	An automated process should be implemented for the compliance checks completed by the tenants. This will ensure that all checks are recorded, reported, and escalated where necessary and decrease the risk of manual error. The CAM Team should arrange training sessions with Site Managers to provide guidance on how compliance checks should be completed and recorded.	Medium	A document for building managers / tenants has been produced and a programme of visits explaining responsibilities of building managers/tenants relating to compliance is already underway. We will also share logs of all compliance checks with building managers/tenants. **Position – August 2022** **FM have produced a document on responsibility of senior manager for buildings and started to roll out programme e.g. Museum already addressed.**	Compliance & Maintenance Officer	31 July 2022	×	30 September 2022

APPENDIX D – ASSURANCE AND PRIORITY LEVELS

Audit Opinions		
Assurance Level		**Definition**
Assurance Reviews		
Substantial		A sound system of governance, risk management and control exist, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable		There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited		Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No		Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.
Not Assessed		This opinion is used in relation to consultancy or embedded assurance activities, where the nature of the work is to provide support and advice to management and is not of a sufficient depth to provide an opinion on the adequacy of governance or internal control arrangements. Recommendations will however be made where required to support system or process improvements.
Grant / Funding Certification Reviews		
Unqualified		No material matters have been identified in relation the eligibility, accounting and expenditure associated with the funding received that would cause SIAS to believe that the related funding conditions have not been met.
Qualified		Except for the matters identified within the audit report, the eligibility, accounting and expenditure associated with the funding received meets the requirements of the funding conditions.
Disclaimer Opinion		Based on the limitations indicated within the report, SIAS are unable to provide an opinion in relation to the Council's compliance with the eligibility, accounting and expenditure requirements contained within the funding conditions.
Adverse Opinion		Based on the significance of the matters included within the report, the Council have not complied with the funding conditions associated with the funding received.
Recommendation Priority Levels		
Priority Level		**Definition**
Corporate	**Critical**	Audit findings which, in the present state, represent a serious risk to the organisation as a whole, i.e. reputation, financial resources and / or compliance with regulations. Management action to implement the appropriate controls is required immediately.
Service	**High**	Audit findings indicate a serious weakness or breakdown in control environment, which, if untreated by management intervention, is highly likely to put achievement of core service objectives at risk. Remedial action is required urgently.
	Medium	Audit findings which, if not treated by appropriate management action, are likely to put achievement of some of the core service objectives at risk. Remedial action is required in a timely manner.
	Low	Audit findings indicate opportunities to implement good or best practice, which, if adopted, will enhance the control environment. The appropriate solution should be implemented as soon as is practically possible.