KAAP AGULHAS MUNISIPALITEIT
CAPE AGULHAS MUNICIPALITY
U MASIPALA WASECAPE AGULHAS

Internal Audit Information and Retention Policy

Approved by the Audit Committee on16 October 2020and tabled in Council on 8 December 2020

Contents

1. Introduction:

1.1 This policy has been produced to comply with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditors (ISPPIA) and covers information collected as part of the internal auditing process in all media. It provides general advice about the management, control and disposal of internal audit information and should be read in conjunction with the relevant legislation.

1.2 The Code of Ethics, under the Confidentiality Principle, states that "internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so". In addition, the Internal Audit Standards(ISPPIA) state that the Chief Audit Executive(CAE) "must develop retention requirements consistent with the organisation's guidelines and any pertinent regulatory or other requirements" (2330.A2).

1.3 A record is information created, received and maintained as evidence by an organisation or person in the transaction of business, or in the maintenance of legal obligations, regardless of the medium. Records are gathered and created as part of individual audit engagements and in the planning, direction and control of internal audit work at all levels. Information is a most important internal audit resource, and any internal audit service is unlikely to function effectively without good records. Equally, poor records management by internal audit can render the wider organisation vulnerable to breaching the appropriate regulations. Internal audit services themselves are auditable and good record management demonstrates compliance with the relevant standards.

1.4 Internal auditors record relevant information to support conclusions and engagement results in order to:

- Aid planning, performance and review of engagements.
- document the extent to which engagement objectives were achieved.
- facilitate third party reviews.
- provide a basis for assuring the quality of audits.
- demonstrate compliance with standards for the professional practice of internal auditing and with relevant legislation and regulations.

1.5 This policy is intended to cover general information management for internal audit and does not cover detailed procedures for recording evidence required for legal proceedings.

2. Management of IAA Information

2.1 The CAE hereby establishes and communicate procedures for the management of information to all internal audit staff. The procedures will be consistent with the BVM's records management policy and should:

- Define the information that needs to be kept in order to be able to account for audit work and decisions.
- Set out the aims and objectives for the management of internal audit information (Section 3).
- Establish responsibilities for the maintenance of information (Section 4).
- Provide a filing structure that will allow information to be efficiently retrieved by those with a right to do so for as long as the records need to be kept (Section 5).
- Provide guidelines about securing information (Section 6).
- Define retention periods, archival and disposal procedures for the various types of information kept (Section 7).
- State how requests for information will be dealt with, ensuring that disclosure is properly controlled (Section 8).

2.2 The principles underlying records management (i.e. creation, retention, disposal) apply equally to information in any media (e.g. paper, electronic, voice, video, digital, photographic etc.). This means that procedures for e-mail, information held on shared and personal hard drives, information held on other recording devices (e.g. palmtops, laptops, data sticks) need to be clearly set in the context of managing records.

3. Aims and Objectives:

Aim:

3.1 The aim for an internal audit records management system might be:

- To ensure that relevant, reliable, authentic, complete and usable records are maintained, managed and controlled effectively at best value to meet appropriate legal, operational and information needs.

Objectives:

3.2 Typical objectives for an internal audit information management policy are that:

- Adequate records of information are maintained to account fully and transparently for all actions and decisions and demonstrate due professional care.
- The legal and other rights of staff or those affected by internal audit actions are protected.
- Records are relevant, complete and accurate and the information they contain is reliable and authentic.
- Information can be efficiently retrieved by those with a legitimate right of access, for as long as the information to support audit decisions and conclusions needs to be held.
- Information is secure from unauthorised and accidental alteration or erasure, that access and disclosure is properly controlled, and audit trails track usage and changes.
- Information is held in a robust format which remains readable for as long as it is required.
- There are consistent and documented retention and disposal procedures to include provision for permanent preservation of archival material and secure disposal of information at the end of its life.
- Staff are made aware of their information handling and keeping responsibilities through learning or awareness programmes and guidance.

4. Responsibilities for Managing Information:

4.1 The CAE has overall responsibility for ensuring that information is managed responsibly by the internal audit activity (see IIA Standards 2330 on documenting information). Everybody in the audit activity has a role to play in ensuring that information is complete, up to date and protected against loss and unauthorised access. The CAE might typically provide regular assurance to the organization over the security and use of internal audit information in line with the organisation's information assurance policies.

4.2 Depending on the size and structure of the audit activity, named individuals may be designated Information Asset Owners in line with information assurance procedures and be responsible for the day-to-day management of the records under their control. Their role is to know: what information is held; what is added; what is removed; how information is moved; who has access and why. As a result, they are able to understand and address the risks to the information and ensure that it is used within the law for the public good and provide written input to the CAE on the security and use of their

asset. This would, for example, include appropriate control and treatment of any data downloaded from corporate systems.

4.3 Audit managers/ senior auditors are responsible for ensuring that the internal audit unit's Records Management Policy is implemented through the oversight of their programme of work.

4.4 Individual auditors are responsible for ensuring that they keep appropriate records of their work and manage those records effectively. Records compiled in the course of business are municipal property. Records management responsibilities should be written into job descriptions.

4.5 Staff who work at home or who work away from the office are responsible for ensuring that:

- Information generated by them is relevant, complete, accurate, up to date and filed in the central record repository as soon as possible.
- Information used by audit managers or senior auditors to monitor progress on audits is updated regularly.
- Changes made to information are reflected in all copies.
- Any hardware (e.g. laptops, printers, palmtops, memory devices) and the information they hold are protected in line with the organisation's security/policy arrangements.
- That vital information is frequently backed up so that it is not all lost in the event of hardware failure or theft.
- Disaster recovery arrangements are in line with the organisation's policies.

5. Information Security:

IIA Standards:

5.1 The IIA Standards state that the CAE must control access to engagement records. The CAE must obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate (2330.A1).

Securing Information:

5.2 Information is an asset and needs to be suitably protected. Information security involves:

- Protecting information from unauthorised access or disclosure (confidentiality);
- Ensuring that systems and information are complete and free from unauthorised change or modification (integrity); and

- Ensuring that information and associated services are available to authorised users when and where required (availability).

5.3 Internal Audit is responsible for ensuring that its information risks are properly managed. This is particularly important given that sensitive information about the organisation, including personal information, can sometimes be held on internal audit information systems.

5.4 During the course of an audit, original paper records owned by the area under review are sometimes needed as evidence to support findings. Ideally, copies should be made but on the rare occasion when original evidence is required, a copy of the record or a marker should be placed in the organisation's file and the original returned as soon as possible. In order to maintain audit trails the original records may have to remain within the internal audit records system until the audit is completed (e.g. when all actions have been agreed and completed by management). These documents need to be held securely when in the custody of internal audit. Where digital material is concerned, access to content can be given without custody and relevant metadata examined and, if necessary, the record extracted. The integrity of information and records being used by internal audit must be maintained and a clear distinction made between the records used and those created by the audit service.

5.5 Any records separately created by internal audit must be managed in a manner that adheres to the IIA Standards and does not place the organisation in potential breach of relevant regulations.

6. Record Organisation:

6.1 Whatever system is maintained, internal audit information and records should be appropriately organised.

6.2 A file structure should be designed to ensure that every piece of information has a logical home and can be located quickly and easily. Internal audit file structures will typically be a reflection of audit programmes with files for individual reviews and other more general documents such as those generated by the CAE or admin support functions. Filing systems can be paper-based, electronic or a mixture of both.

6.3 There is now a multiplicity of arrangements for storing audit records ranging from paper to automated tools. There are also many mechanisms for capturing data including scanning and downloading. Irrespective of the means and mechanisms used to capture and store data, there will need to be robust, consistent procedures adopted to handle the records in line with set policies.

6.4 Internal Audit information and records should be organised to ensure that:

- Staff can work effectively and efficiently without having to waste time hunting for information.
- Internal auditors can find what they need quickly and easily or determine who has the data.
- New staff can learn to use the system quickly.
- Any risks that information can be accidentally amended, deleted or that confidential information can be accidentally disseminated are minimised.
- Internal audit work is conducted in an orderly, efficient and accountable manner.
- Audit findings, conclusions and recommendations are fully documented and supported.
- Continuity is provided in the event of a disaster.
- Legislative and regulatory requirements are met.
- Records are relevant, reliable, authentic, complete and usable.
- Records are retained only for as long as they are needed and disposed of in accordance with the organisation's information disposal rules, relevant regulations and legislation.
- There is an "audit trail" which enables any record entry to be traced to a named individual at a given date/time with the secure knowledge that all alterations can be traced and deletions identified.
- New staff can see what has been done, or not done, and why.
- Any decisions made can be justified or recognised at a later date.

6.5 Good naming conventions and filing structures can help to support eficient retrieval.

7. Retention and Disposal

7.1 The IIA Standards state that the CAE must develop:

- Retention requirements for engagement records, regardless of the medium in which each record is stored. These retention requirements must be consistent with the organisation's guidelines and any pertinent regulatory or other requirements (2330.A2);
- Policies governing the custody and retention of consulting engagement records, as well as their release to internal and external parties. These must be consistent with the organisation's guidelines and any pertinent regulatory or other requirements (2330.C1).

7.2 Internal audit information will largely consist of documents (e.g. work in progress such as draft working papers or draft reports). It is not always necessary to retain all versions of working papers and reports,

but it might be useful to retain at least those versions where significant changes were made in order to be able to demonstrate how final versions were reached and to support the decision making process that resulted in final versions of audit reports, findings and recommendations.

7.3 The retention of internal audit information should be considered in the light of both business (e.g. internal audit quality review purposes) and legislative requirements taking into account the cost of retention and the use to which the records might be put in the future.

IAA information retention and disposal is consistent with the municipality's guidelines and any relevant regulations or legislation. The retention periods for internal audit records after which they should be reviewed to determine whether they should be kept for longer, destroyed or sent to an archive for permanent preservation will be defined by relevant policy and legislation. The retention period starts after audits are completed (i.e. when all accepted recommendations have been implemented by management).

7.4 Whenever an e-mail message is sent or received, a decision should be made about whether it needs to be kept. If an e-mail is to be kept it should be moved to the relevant folder in the filing system and given meaningful titles that accurately reflect content. Important e-mails are those that support audit recommendations and conclusions and actions discussed and agreed with management.

7.5 Folders and files should not remain 'live' indefinitely. They should be closed at an appropriate time. The decision factor or 'trigger' that determines closure will vary according to the nature and function of the records, the extent to which they reflect ongoing business and the technology used to store them. For example, this could be when all agreed actions on an audit report have been implemented by management. The CAE should decide an appropriate 'trigger' and put arrangements in place to apply it. New continuation files should be opened if necessary but it should be clear to anyone looking at a record where one part ends and another starts.

7.6 Records should not be kept after they have ceased to be of use unless they are known to be the subject of litigation or a request for information. If so, destruction should be delayed until the litigation is complete or, in the case of an information request, all relevant complaint and appeal provisions have been exhausted. In such cases, a disposal 'hold' should be applied to the records which must only be placed or removed by authorised users. By placing a 'hold' on a folder, any disposal actions are paused and cannot be executed until the hold is removed. The records management system must suspend the execution of any disposal action while the disposal hold is in place.

7.7 It is very important to keep a record of information sent for destruction (the disposal schedule). This record acts as proof that disposal of information is taking place in a controlled manner. It is advisable

that whoever is designated to control the disposal process signs off and dates the disposal schedule as proof that the information has been archived or destroyed. Disposal of records must comply with the relevant regulatory requirements.

7.8 The main reasons information is kept are to provide evidence supporting audit findings and recommendations and to demonstrate that the work was carried out to acceptable standards (i.e. IIA Internal Audit Standards). Those working papers that support audit findings should be kept at least until all accepted recommendations have been implemented. There are, however, reasons for keeping working papers for longer including:

- Complying with legislation or organisational policies.
- Meeting the needs of the Audit Committee. The main Audit Committee meeting in a year is where the Audit opinion for the financial year just ended is considered. Sufficient Internal Audit records to support the audits contributing to the Audit Opinion should be kept at least until after this meeting has taken place.
- Providing external auditors with information to support their work. There is no need to keep everything for this purpose. One way to reduce the number of records kept is to let the external auditors see the annual audit programme and only keep records relating to the reviews that they are interested in seeing and disposing of them after they have seen them.
- Providing information for quality reviewers. IIA Internal Audit Standard number 1310 on external assessments states that "the chief audit executive must develop and maintain a quality assurance and improvement programme that covers all aspects of internal audit activity". When quality reviews have been completed, there is no need to retain records unless there is a good reason for doing so (e.g. they are of historic value). There is no need to retain all evidence supporting all audits until a quality review is completed. The evidence supporting audits that are underway at the time of the quality review should be sufficient for this purpose.

7.9 When information has completed its retention period a decision has to be taken as to whether to keep, move or destroy it. Disposal should be carried out in a secure and timely manner in accordance with policies for data handling, taking account of constraints imposed as a result of any protective markings.

7.10 The retention period for an e-mail is determined by the piece of business to which it relates. Retention decisions therefore have to be taken at the time of receiving or sending email. If arrangements are made to save important e-mails, other e-mails can be destroyed after a very short period. Most e-mails do not need to be kept beyond the timeframe of the task to which they refer. Retention should be consistent with Municipal policy & relevant legislation.

External Service Providers/Shared Services/Third Party Assurance:

7.11 Where internal audit services, or part thereof, are supplied by external parties, contracts with those parties should make clear that any information they collect or generate as part of any review undertaken is the property of the municipality that appointed them and must be accessible as required and handed over at an appropriately agreed point and retained in accordance with the policy for the management of information. Similarly, any papers generated by the audit process must be made available for quality review purposes.

7.12 Where internal audit services are supplied by shared service arrangements, the CAE must ensure that the obligations and guidelines for each of the organisations involved are met.

7.13 Where CAE seek assurance from other assurance providers in municipality (e.g. Health and Safety experts, anti-fraud experts etc.) then they will have to ensure that all information created by these other bodies that support any assurance given by the internal audit service are clearly identifiable, can be located easily and quickly and are kept for whatever period that the internal audit activity requires.

8. Handling Requests for Information:

Introduction:

8.1 Requests for information should be dealt with in accordance with relevant laws, and regulations and the municipality's information sharing policies.

Assignment Information:

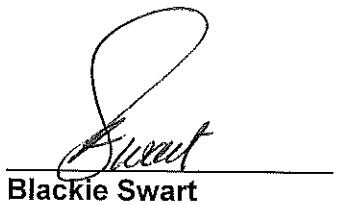
8.2 There is no blanket approach to dealing with requests for internal audit information. Requests for information must be approached on a case-by-case basis. Individual departments may have uniquely sensitive information to which different exemptions apply. When a request for an internal audit report is received, the CAE must consider two questions:

- Is it appropriate to disclose the report or would disclosure undermine or otherwise prejudice the internal audit process?
- What exemptions might apply to the detailed information contained within an internal audit report?

8.3 CAE need to consider whether disclosure would prejudice the internal audit process, following which, the public interest for and against disclosure must be considered.

8.4 The premature release of information (i.e. before an audit is completed) could have an inhibiting effect on the internal audit process (e.g. those involved in the process might not engage or contribute fully).

8.5 The passage of time will have an impact on the level of prejudice caused to the internal audit process by disclosure of internal audit reports. In order to minimise any prejudice to the internal audit process it would be reasonable to ensure that sufficient time has elapsed to allow internal audit report recommendations to be implemented and their effects to be measured prior to disclosure.



Blackie Swart
Chief Audit Executive
9 November 2019

Pieter Strauss
Audit Committee Chairperson
9 November 2019