Directorate for Internal Audit and Assurance – Information Handling Policy

27 September 2018

1. Background

1.1. The Scottish Government (SG) has a generic data handling policy, which provides an overview on how SG staff should handle the information resources in their areas. However, the nature of the work undertaken by the Internal Audit function and the standards to which it must adhere require more detailed policies than those provided generically.

1.2. The Public Sector Internal Audit Standards (PSIAS) state that "the chief audit executive 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."

1.3. The PSIAS also state that the HIA must develop:

i. 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;

ii. Defined retention periods, archival and disposal procedures for the various types of information kept;

iii. 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.

1.4. A further consideration is that the Code of Ethics states under the Confidentiality Principle 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".

2. Retention Requirements

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

i. aid planning, performance and review of engagements;

ii. document the extent to which engagement objectives were achieved;

iii. facilitate third party reviews;

iv. provide a basis for assuring the quality of audits; and

v. demonstrate compliance with standards for the professional practice of internal auditing and with relevant legislation and regulations.

2.2. 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.

2.3. 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.

2.4. Information is an asset and needs to be suitably managed and protected. The Internal Audit Directorate must ensure that:

i. Records are relevant, complete and accurate and the information they contain is reliable and authentic;
ii. Information is secure from unauthorised and accidental alteration or erasure, that access and disclosure is properly controlled and audit trails track usage and changes;
iii. 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;
iv. Staff are made aware of their information handling and keeping responsibilities through learning or awareness programmes and guidance.

3. Retention Periods

3.1. 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. the PSIAS). 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:

i. Complying with legislation or organisational policies.

ii. Meeting the needs of Audit Committees. 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 and accounts have been laid.

iii. 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.

iv. Providing information for quality reviewers. When quality reviews have been completed, there is no need to retain records unless there is a good reason for doing so. 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.

v. 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.

3.2. 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 e-mail. 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.

3.3. 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 relevant SIAM 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.

3.4. The retention schedule defines the minimum period for keeping a record, after which the record should be reviewed to determine if kept longer, if it can be destroyed or whether it needs to be kept permanently. The IAD's retention schedule can be found at Annex A.

3.5. 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.

3.6. 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.

4. General Data Protection Regulations (GDPR)

4.1. Under the GDPR, you must have a valid lawful basis in order to process personal data. The full list of lawful bases and the requirements to utilise them can be found here. It is likely that in the vast majority of cases, the IAD will be processing information on the basis of carrying out a public task, which can be used to process personal data:

i. In the exercise of official authority; or
ii. To perform a specific task in the public interest that is set out in law

4.2. The justification for using public task can be made stronger by linking activity to legal gateways. For instance IAD uses public task to process audit information on Revenue Scotland which is in turn operating under the Revenue Scotland Tax Powers Act.

4.3. Personal information should only be held for as long as is required to support the carrying out of the public task. Once the task has been competed then any data that is required to be held for a longer period of time should be anonymised, unless there is a justifiable reason for not doing so as determined by the lead auditor and relevant Senior Internal Audit Manager (SIAM) for the activity. This includes all data held electronically, whether on eRDM, Galileo or another system.

Annex A: Data Retention and Disposal Schedule

1. 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. The lead auditor is responsible for determining and recording the retention period for a specific activity as disposal schedule, agreeing it with the relevant SIAM and informing the Business Support Hub for inclusion in the central disposal register.

2. The disposal schedule should include a description of any sensitive information held (including personal information), the reason for holding the information, the date at which the information can be disposed and any other relevant details.

3. The following table gives an indication of minimum 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. The retention period starts after audits are completed (i.e. when all accepted recommendations have been implemented by management).

Item	Description	Minimum Retention period	Maximum Retention period
1	Audit Reports which include the examination of long term contracts	1 year	6 years
2	Report papers used in the course of a fraud investigation	1 year after legal proceedings have completed	6 years after legal proceeding have completed
3	Annual Reports and information supporting governance statement	1 year	3 years
4	Audit Reports in relation to EU funding		
5	Other Audit Reports	1 year	3 years
6	Terms of Reference	On completion of reviews (i.e. when all agreed actions have been implemented by management	3 years
7	Programme/plans/strategies	As soon as they've been replaced by a new programme/plan/strategy	1 year after last date of the plan
8	Correspondence	Correspondence relating to reviews should be reviewed at the same time as other working	3 years

		papers (see below). Other correspondence should be reviewed after 6 months	
9	Minutes of meetings and related periods	1 year	3 years
10	Working Papers	On completion of reviews (i.e. when all agreed action have been implemented by management).	3 years
11	Internal Audit guides	When superseded	When superseded
12	Manuals and guides relating to departmental procedures	When superseded	When superseded
13	Local auditing standards	When superseded	When superseded